Acronis

Acronis Cyber Protect 15

UŽIVATELSKÁ PŘÍRUČKA

Obsah

1 Verze a licencování aplikace Acronis Cyber Protect 15

Aplikace Acronis Cyber Protect 15 je k dispozici v pěti verzích:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

Podrobné informace o funkcích zahrnutých v jednotlivých verzích naleznete v tématu Porovnání verzí Acronis Cyber Protect 15 včetně cloudového nasazení.

Všechny verze Acronis Cyber Protect 15 jsou licencované podle počtu chráněného zatížení a jejich typu (pracovní stanice, server a virtuální hostitel). Verze Cyber Protect jsou k dispozici pouze s licencemi na základě předplatného. Verze Cyber Backup jsou k dispozici s licencemi na základě předplatného i s trvalými licencemi. Další informace o dostupných možnostech licencování naleznete v tématu https://www.acronis.com/company/licensing.html.

Správu licencí ve svém prostředí můžete provádět ve webové konzoli Cyber Protect v nabídce **Nastavení** > **Licence**.

Licence můžete také spravovat pro jednotlivé počítače. Ve webové konzoli Cyber Protect vyberte požadovaný počítač a přejděte do nabídky **Zařízení** > **Podrobnosti** > **Licence**.

Klíče trvalé licence pro verzi 15 nelze použít s agenty pro zálohování z verze Acronis Cyber Backup 12.5. Agenti budou nadále fungovat se starými licenčními klíči, i po upgradu serveru pro správu na verzi 15.

Licence na základě předplatného pro zálohování lze použít s agenty verze 12.5 i po upgradu agentů na verzi 15. Licence na základě předplatného aplikace Cyber Protect mohou být používány pouze agenty verze 15.

Poznámka *Funkce jednotlivých verzí se liší. Některé z funkcí popsané v této dokumentaci nemusí být pro vaši licenci k dispozici.*

1.1 Podporované funkce aplikace Cyber Protect podle operačních systémů

Funkce aplikace Cyber Protect jsou podporovány v následujících operačních systémech:

- Windows: Windows 7 a novější verze, Windows Server 2008 R2 a novější verze.

  Správa antivirové ochrany v programu Windows Defender je podporována v systému Windows 8.1 a novějším.
- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.

  Funkce služby Cyber Protect mohou podporovat také další distribuce a verze Linuxu, nebyly ale provedeny žádné testy.
- macOS: 10.13.x a novější (podporována je pouze antivirová ochrana a ochrana proti malwaru).

Důležité *Funkce Cyber Protect jsou podporovány pouze na počítačích, na kterých je nainstalován agent pro ochranu. U virtuálních počítačů, které jsou chráněny v režimu bez agenta, například Agentem pro Hyper-V, Agentem pro VMware nebo Agentem pro Scale Computing, je podporována pouze záloha.*

Funkce služby Cyber Protect	Windows	Linux	macOS
Forenzní záloha	Ano	Ne	Ne
Souvislá ochrana dat (CDP)			
CDP pro soubory a složky	Ano	Ne	Ne
CDP pro změněné soubory prostřednictvím sledování aplikace	Ano	Ne	Ne
Automatické zjišťování a vzdálená instalace			
Zjišťování s využitím sítě	Ano	Ne	Ne
Zjišťování s využitím Active Directory	Ano	Ne	Ne
Zjišťování podle šablony (import počítačů ze souboru)	Ano	Ne	Ne
Ruční přidání zařízení	Ano	Ne	Ne
Ochrana proti malwaru Acronis			
Detekce ransomwaru na základě chování procesu (s využitím umělé inteligence)	Ano	Ne	Ne
Detekce procesů těžby kryptoměn	Ano	Ne	Ne
Ochrana proti malwaru v reálném čase	Ano	Ne	Ano
Automatické obnovení zasažených souborů z místní mezipaměti	Ano	Ne	Ne
Vlastní ochrana pro soubory zálohy Acronis	Ano	Ne	Ne
Vlastní ochrana pro software Acronis	Ano	Ne	Ne
Statická analýza pro přenosné spustitelné soubory	Ano	Ne	Ano*
Ochrana externích jednotek (pevné disky, jednotky flash, SD karty)	Ano	Ne	Ne
Ochrana síťové složky	Ano	Ne	Ne
Ochrana na straně serveru	Ano	Ne	Ne
Ochrana pro Zoom, WebEx, Microsoft Teams a další ochrana pro práci vzdáleně	Ano	Ne	Ne
Ochrana proti malwaru na vyžádání	Ano	Ne	Ano
Kontrolovat archivní soubory	Ano	Ne	Ano
Vyloučení souborů/složek	Ano	Ne	Ano**
Vyloučení procesů	Ano	Ne	Ne
Seznam povolených položek pro celou společnost	Ano	Ne	Ano
Detekce chování	Ano	Ne	Ne
Karanténa	Ano	Ne	Ano
Filtrování adres URL (http/https)	Ano	Ne	Ne

Správa antivirové ochrany v programu Windows Defender	Ano	Ne	Ne
Správa služby Microsoft Security Essentials	Ano	Ne	Ne
Posouzení ohrožení zabezpečení	Ano	Ne	Ne
Správa oprav			
Automatické schvalování oprav	Ano	Ne	Ne
Ruční instalace oprav	Ano	Ne	Ne
Automatické plánování instalace oprav	Ano	Ne	Ne
Opravy odolné proti selhání: před instalací oprav v rámci plánu ochrany zálohujte počítač	Ano	Ne	Ne
Zrušení restartu počítače, pokud běží záloha	Ano	Ne	Ne
Mapa ochrany dat			
Vyhledávání nechráněných souborů v počítačích	Ano	Ne	Ne
Přehled nechráněných umístění	Ano	Ne	Ne
Ochranná akce na mapě ochrany dat	Ano	Ne	Ne
Stav disku			
Kontrola stavu pevného disku a disku SSD s využitím umělé inteligence	Ano	Ne	Ne
Plány chytré ochrany využívající výstrahy z Centra operací kybernetické ochrany Acronis			
Kanál hrozeb	Ano	Ne	Ne
Ovládací prvek pro nápravné akce	Ano	Ne	Ne
Kontrola záloh			
Kontrola šifrovaných záloh	Ano	Ne	Ne
Kontrola záloh disku v místním úložišti, síťových složkách a úložišti Acronis Cloud Storage	Ano	Ne	Ne
Bezpečné obnovení			
Antimalwarová kontrola pomocí antivirové ochrany a ochrany proti malwaru Acronis během procesu obnovení	Ano	Ne	Ne
Vzdálená plocha			
Připojení pomocí klienta HTML5	Ano	Ne	Ne
Připojení pomocí nativního klienta RDP systému Windows	Ano	Ne	Ne
Vzdálené vymazání	Ano***	Ne	Ne
Cyber Protect Monitor	Ano	Ne	Ano

* Statická analýza pro přenosné spustitelné soubory je v systému macOS podporována pouze pro naplánované kontroly.

** V systému macOS můžete pomocí výjimek určit pouze soubory a složky, které nebudou kontrolovány ochranou v reálném čase ani naplánovanými kontrolami.

*** Vzdálené vymazání je k dispozici pouze pro počítače se systémem Windows 10.

2 Instalace

2.1 Přehled instalace

Acronis Cyber Protect podporuje dvě metody nasazování: místní a cloudové. Liší se hlavně umístěním Serveru pro správu Acronis Cyber Protect.

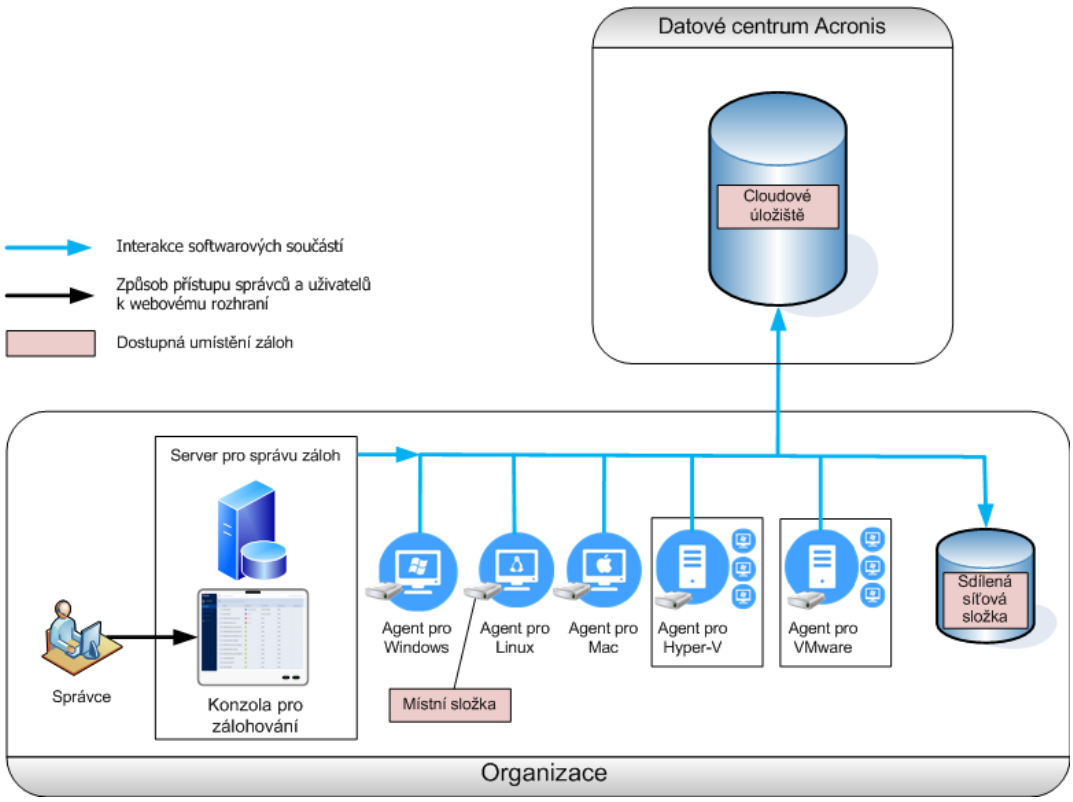
Server pro správu Acronis Cyber Protect je ústřední místo pro správu všech vašich záloh. Při místním nasazení je produkt nainstalován do vaší místní sítě, při cloudovém nasazení je umístěn v jednom z datových center Acronis. Webové rozhraní tohoto serveru se nazývá webová konzole Cyber Protect.

Server pro správu Acronis Cyber Protect zodpovídá za komunikaci s agenty Cyber Protect a provádí obecné funkce správy plánu. Před každou aktivitou ochrany agenti na serveru pro správu ověření předpoklady. Někdy může dojít ke ztrátě připojení k serveru pro správu, což zabrání nasazení nových plánů ochrany. Pokud byl však na počítači již nasazen plán ochrany, bude agent pokračovat v operacích ochrany po dobu 30 dní od přerušení komunikace se serverem pro správu.

Oba typy nasazení vyžadují, aby byl ve všech počítačích, které chcete zálohovat, nainstalován agent pro ochranu. Stejné jsou i podporované typy úložišť. Prostor v cloudovém úložišti se prodává samostatně z licencí produktu Acronis Cyber Protect.

Místní nasazení

Místní nasazení znamená, že všechny součásti produktu jsou nainstalovány ve vaší místní síti. Toto je jediná dostupná metoda nasazení s trvalou licencí. Tuto metodu také musíte použít, pokud vaše počítače nejsou připojené k internetu.



Umístění serveru pro správu

Server pro správu můžete nainstalovat do počítače se systémem Windows nebo Linux.

Doporučený přístup je instalace do systému Windows, protože budete moci ze serveru pro správu nasazovat agenty do ostatních počítačů. S licencí Advanced je možné vytvářet organizační jednotky a přidávat do nich správce. Tímto způsobem můžete správou ochrany pověřit další uživatele, jejichž přístupová oprávnění budou přísně omezená na odpovídající jednotky.

Instalace do systému Linux je doporučována v případě prostředí využívajícího pouze systém Linux. Agenta bude nutné nainstalovat lokálně do počítačů, které chcete zálohovat.

Upgrade z předchozích verzí produktu

Upgrade na verzi Acronis Cyber Protect 15 můžete provést přímo nebo můžete nejdříve odinstalovat předchozí verzi.

Přímý upgrade je k dispozici pouze z verze Acronis Backup 12.5 Update 4 (sestavení 12730 a pozdější). Ostatní verze produktu přímo upgradovat nelze. Další informace o dostupných možnostech upgradu naleznete v tomto článku znalostní báze: https://kb.acronis.com/content/65178.

Poznámka *Důrazně doporučujeme před upgradem zazálohovat systém. V případě selhání upgradu se tak budete moct vrátit k původní konfiguraci.*

Server pro správu aplikace Acronis Cyber Protect 15 je zpětně kompatibilní a podporuje agenty verze 12.5. Tito agenti však nepodporují funkce Cyber Protect (p. 9).

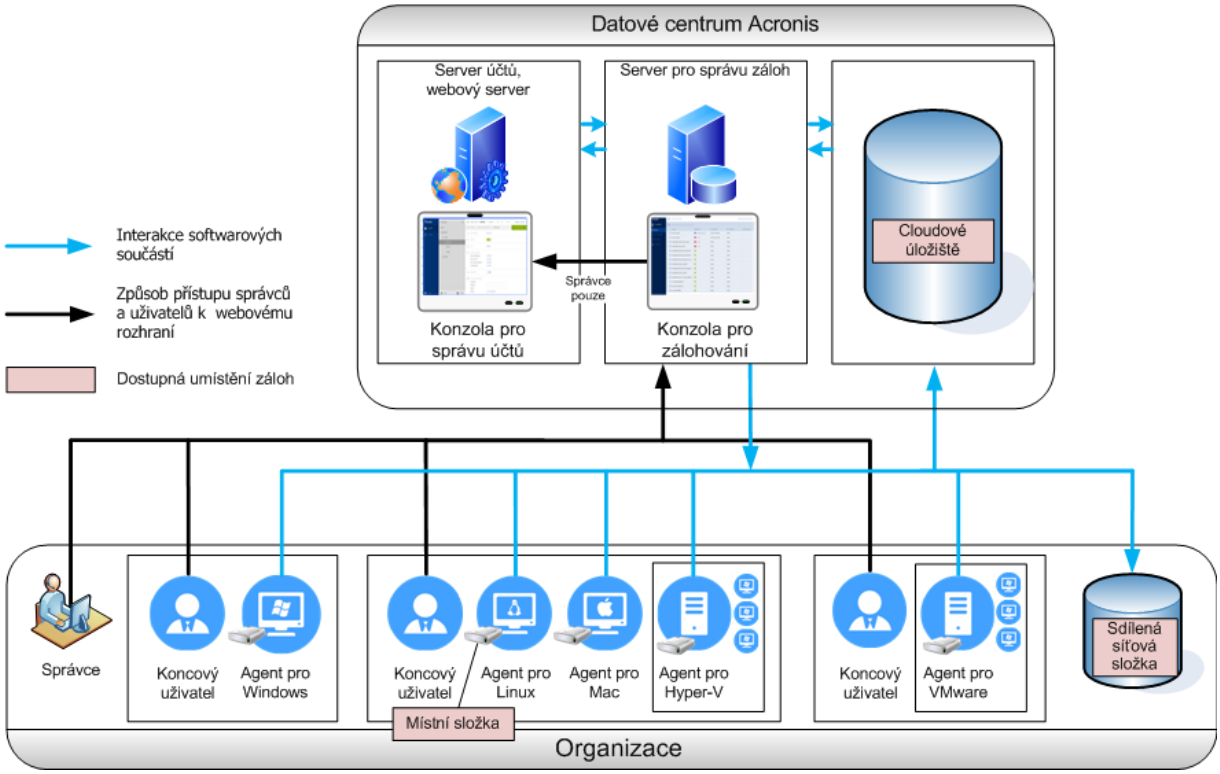
Upgradem agentů nenarušíte existující zálohy a jejich nastavení.

Cloudové nasazení

Cloudové nasazení znamená, že server pro správu je umístěný v jednom z datových center Acronis. Výhodou tohoto přístupu je, že server pro správu nemusíte spravovat ve své místní síti. Acronis Cyber Protect můžete považovat za službu ochrany, kterou vám poskytuje Acronis.

Přístup k serveru účtů umožňuje vytvářet uživatelské účty, nastavovat pro ně kvóty používání služeb a vytvářet skupiny uživatelů (jednotky) odrážející strukturu vaší organizace. K webové konzoli Cyber Protect mají přístup všichni uživatelé, mohou si z ní stáhnout požadovaného agenta a během několika minut ho nainstalovat do svých počítačů.

Účty správce lze vytvářet na úrovni jednotky nebo organizace. Všechny účty mají zobrazení zahrnující oblast, kterou mohou ovládat. Uživatelé mají přístup pouze ke svým zálohám.



Následující tabulka obsahuje přehled rozdílů mezi místním a cloudovým nasazením. Každý sloupec obsahuje funkce, které jsou k dispozici pouze v odpovídajícím typu nasazení.

Místní nasazení	Cloudové nasazení
▪ Lze používat trvalé licence. ▪ Místní server pro správu ▪ Tvůrce spouštěcích médií ▪ Zálohování a správa disků ve spouštěcím médiu ▪ Server SFTP jako umístění zálohy ▪ Acronis Cyber Infrastructure jako umístění zálohy ▪ Pásková zařízení a uzly úložiště Acronis jako umístění zálohy* ▪ Zpracovávání dat mimo hostitele* ▪ Převod zálohy do virtuálního počítače ▪ Upgrade z předchozích verzí produktu Acronis Cyber Protect, včetně produktu Acronis Backup pro VMware ▪ Účast v Programu zkušeností uživatelů Acronis	▪ Zálohování dat Office 365 z cloudu do cloudu, včetně ochrany skupin, veřejných složek a dat služeb OneDrive a SharePoint Online. ▪ Zálohování dat v G Suite z cloudu do cloudu ▪ Agent pro Virtuozzo (záloha virtuálních počítačů Virtuozzo na úrovni hypervizor) ▪ Obnovení po havárii jako cloudová služba**

* Tato funkce není dostupná ve verzi Standard.

** Tato funkce je dostupná pouze ve verzi Disaster Recovery.

2.2 Součásti

Agenti

Agenti jsou aplikace, které provádí zálohování a obnovování dat a další operace v počítačích spravovaných aplikací Acronis Cyber Protect.

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

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

Co chcete zálohovat?	Jakého agenta nainstalovat?	Kam se má nainstalovat?	Dostupnost agenta	
			Interně	Cloud
Fyzické počítače				
Disky, svazky a soubory na fyzických počítačích se systémem Windows	Agent pro Windows	Do počítače, který se bude zálohovat	+	+
Disky, svazky a soubory na fyzických počítačích se systémem Linux	Agent pro Linux		+	+
Disky, svazky a soubory na fyzických počítačích se systémem macOS	Agent pro Mac		+	+
Aplikace				
Databáze SQL	Agent pro SQL	Do počítače, kde běží Microsoft SQL Server	+	+
Databáze a poštovní schránky Exchange	Agent pro Exchange	Do počítače, kde běží Microsoft Exchange Server s rolí poštovní schránky.* Pokud je vyžadována pouze záloha poštovní schránky, může být agent nainstalován na libovolném počítači s Windows, který má síťový přístup k počítači s rolí Klientský přístup Microsoft Exchange Serveru.	+	+ Žádná záloha poštovní schránky
Poštovní schránky Microsoft Office 365	Agent pro Office 365	Do počítače se systémem Windows, který je připojen k internetu	+	+
Počítače, na kterých běží doménové služby Active Directory	Agent pro Active Directory	Do řadiče domény	+	+
Počítače, na nichž běží databáze Oracle	Agent pro Oracle	Do počítače, na němž běží databáze Oracle.	+	–
Virtuální počítače				
Virtuální počítače VMware ESXi	Agent pro VMware (Windows)	Do počítače se systémem Windows, který má síťový přístup k serveru vCenter a k úložišti virtuálních počítačů.**	+	+

Co chcete zálohovat?	Jakého agenta nainstalovat?	Kam se má nainstalovat?	Dostupnost agenta	
			Interně	Cloud
	Agent pro VMware (Virtual Appliance)	Do hostitele ESXi	+	+
Virtuální počítače Hyper-V	Agent pro Hyper-V	Do hostitele Hyper-V	+	+
Virtuální počítače Scale Computing HC3	Agent pro Scale Computing HC3	Na hostiteli Scale Computing HC3.	+	–
Virtuální počítače hostované v systému Windows Azure	Stejného jako u fyzických počítačů.***	Do počítače, který se bude zálohovat.	+	+
Virtuální počítače hostované v systému Amazon EC2			+	+
Virtuální počítače Citrix XenServer			+****	+
Virtuální počítače Red Hat Virtualization (RHV/RHEV)				
Virtuální počítače založené na jádře (KVM)				
Virtuální počítače Oracle				
Virtuální počítače Nutanix AHV				
Mobilní zařízení				
Mobilní zařízení se systémem Android	Mobilní aplikace pro Android	Do mobilního zařízení, které se bude zálohovat.	–	+
Mobilní zařízení se systémem iOS	Mobilní aplikace pro iOS		–	+

*Během instalace Agent pro Exchange ověří, zda je na počítači, kde bude spuštěn, dostatek volného místa. Během částečného obnovení je dočasně potřeba volné místo odpovídající 15 procentům největší databáze Exchange.

**Pokud ESXi používá úložiště připojené pomocí sítě SAN, nainstalujte agenta do počítače připojeného ke stejné síti SAN. Agent bude zálohovat virtuální počítače přímo z úložiště a ne pomocí hostitele ESXi a LAN. Podrobné informace naleznete v části Zálohování nezávislé na síti LAN (str. 335).

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

****S licencí Acronis Cyber Protect Advanced Virtual Host jsou tyto virtuální počítače považované za virtuální (je použito licencování vázané na hostitele). S licencí Acronis Cyber Protect Virtual Host jsou tyto počítače považované za fyzické (je použito licencování vázané na počítače).

Další součásti

Součást	Funkce	Kam se má nainstalovat?	Dostupnost	
			Interně	Cloud
Server pro správu	Spravuje agenty. Zajišťuje webové rozhraní pro uživatele.	Do počítače se systémem Windows nebo Linux.	+	–
Components for Remote Installation	Uloží instalační balíčky agenta do místní složky.	Do počítače se systémem Windows se serverem pro správu.	+	–

Součást	Funkce	Kam se má nainstalovat?	Dostupnost	
			Interně	Cloud
Služba vyhledávání	Provede antimalwarovou kontrolu záloh v cloudovém úložišti, místní nebo sdílené složce. Služba vyhledávání vyžaduje databázi serveru Microsoft SQL Server nebo PostgreSQL Server. Služba vyhledávání není kompatibilní s výchozí vestavěnou databází SQLite. Pokud vyberete databázi SQLite, budou ve webové konzoli skryty následující funkce: ▪ Plány kontroly záloh ▪ Ovládací prvek s podrobnostmi kontroly zálohy ▪ Seznam povolených podnikových aplikací ▪ Bezpečné obnovení ▪ Sloupec **Status** v seznamu záloh Pokud tedy funkce uvedené výše potřebujete, přizpůsobte instalační nastavení a definujte databáze serveru Microsoft SQL Server nebo PostgreSQL pro server pro správu.	Na počítači se systémem Windows nebo Linux, kde běží server pro správu.	+	–
Tvůrce spouštěcích médií	Vytváří spouštěcí média.	Do počítače se systémem Windows nebo Linux.	+	–
Nástroj příkazového řádku	Zajišťuje rozhraní příkazového řádku.	Do počítače se systémem Windows nebo Linux.	+	+
Cyber Protect Monitor	Umožňuje uživatelům sledování záloh mimo webové rozhraní.	Do počítače se systémem Windows nebo mac OS.	+	+
Uzel úložišť	Ukládá zálohy. Je vyžadován pro katalogizaci a deduplikaci.	Na počítači se systémem Windows.	+	–
Katalogová služba	Provádí katalogizaci záloh na uzlech úložišť.	Na počítači se systémem Windows.	+	–

Součást	Funkce	Kam se má nainstalovat?	Dostupnost	
			Interně	Cloud
PXE Server	Povoluje spouštění počítačů ze spouštěcích médií přes síť.	Na počítači se systémem Windows.	+	–

2.3 Softwarové požadavky

2.3.1 Podporované prohlížeče

Webové rozhraní podporuje následující prohlížeče:

- Google Chrome 29 nebo novější,
- Mozilla Firefox 23 nebo novější,
- Opera 16 nebo novější,
- Windows Internet Explorer 10 nebo novější,

  V cloudových nasazeních portál pro správu (str. 447) podporuje Internet Explorer 11 nebo novější.
- Microsoft Edge 25 nebo novější,
- Safari 8 nebo novější v operačních systémech macOS a iOS.

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

2.3.2 Podporované operační systémy a prostředí

2.3.2.1 Agenti

Agent pro Windows

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

Windows XP Professional SP2 (x86) – podporováno prostřednictvím speciální verze Agenta pro Windows Další informace o této podpoře a jejím omezení naleznete v tématu Agent pro Windows XP SP2 (str. 23).

Windows XP Embedded SP3

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

Windows Small Business Server 2003/2003 R2

Windows Vista – všechny verze

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

Windows Small Business Server 2008

Windows 7 – všechny verze

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

Windows Home Server 2011

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – všechny verze

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

Windows Server 2012/2012 R2 – všechny verze

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

Windows 10 – verze Home, Pro, Education, Enterprise, IoT Enterprise a LTSC (dříve LTSB)

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

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

Agent pro SQL, Agent pro Exchange (pro zálohu databáze a zálohu s podporou aplikací) a Agent pro Active Directory

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

- Není podporováno interní nasazení Agenta pro SQL v systému Windows 7, verze Starter a Home (x86, x64)

Agent pro Exchange (pro zálohu poštovní schránky)

Tento agent může být nainstalován do počítače se serverem Microsoft Exchange Server i bez něj.

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

Windows Small Business Server 2008

Windows 7 – všechny verze

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

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – všechny verze

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

Windows Server 2012/2012 R2 – všechny verze

Windows Storage Server 2008/2008 R2/2012/2012 R2

Windows 10 – verze Home, Pro, Education a Enterprise

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

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

Agent pro Office 365

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

Windows Small Business Server 2008

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

Windows Home Server 2011

Windows Small Business Server 2011 – všechny verze

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

Windows Server 2012/2012 R2 – všechny verze

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

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

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

Windows Server 2019 – všechny možnosti instalace (pouze x64) s výjimkou Nano Serveru

Agent pro Oracle

Windows Server 2008R2 – verze Standard, Enterprise, Datacenter a Web (x86, x64)

Windows Server 2012R2 – verze Standard, Enterprise, Datacenter a Web (x86, x64)

Linux – jakékoli jádro a distribuce podporovaná Agentem pro Linux (uvedeno níže)

Agent pro Linux

Linux s jádrem verze 2.6.9 až 5.1 a knihovnou glibc verze 2.3.4 nebo novější, včetně následujících distribucí v systémech x86 a x86_64:

Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0*, 8.1*

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31

SUSE Linux Enterprise Server 10 a 11

SUSE Linux Enterprise Server 12 – podporováno v systémech souborů kromě Btrfs

Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1 – jádra Unbreakable Enterprise Kernel a Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7

ClearOS 5.x, 6.x, 7, 7.1, 7.4, 7.5, 7.6

ALT Linux 7.0

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

* Konfigurace se Stratis nejsou podporovány.

Agent pro Mac

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12

macOS High Sierra 10.13

macOS Mojave 10.14

macOS Catalina 10.15

Agent pro VMware (Virtual Appliance)

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

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

Agent pro VMware (Windows)

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

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

Agent pro Hyper-V

Windows Server 2008 (pouze x64) s rolí Hyper-V, včetně instalačního režimu jádra serveru

Windows Server 2008 R2 s rolí Hyper-V, včetně instalačního režimu jádra serveru

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 s rolí Hyper-V, včetně instalačního režimu jádra serveru

Microsoft Hyper-V Server 2012/2012 R2

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

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

Windows Server 2016 s rolí Hyper V – všechny možnosti instalace, s výjimkou Nano serveru

Microsoft Hyper-V Server 2016

Windows Server 2019 s rolí Hyper V – všechny možnosti instalace, s výjimkou Nano serveru

Microsoft Hyper-V Server 2019

Agent pro Scale Computing HC3 (virtuální zařízení)

Tento agent je dodáván jako virtuální zařízení, které je nasazeno v clusteru Scale Computing HC3 prostřednictvím webové konzole Cyber Protect. Pro tohoto agenta není k dispozici samostatný instalační program.

Scale Computing Hypercore 8.8, 8.9

2.3.2.2 Server pro správu (pouze pro místní nasazení)

V systému Windows

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

Windows Small Business Server 2008*

Windows 7 – všechny verze (x86, x64)

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

Windows Home Server 2011

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – všechny verze

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

Windows Server 2012/2012 R2 – všechny verze

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

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

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

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

* Službu vyhledávání nelze nainstalovat v systému Windows Server 2008 (všechny verze), Windows Small Business Server 2008 a Windows Storage Server 2008.

V systému Linux

Linux s jádrem verze 2.6.23 až 5.1 a knihovnou glibc verze 2.3.4 nebo novější, včetně následujících distribucí v systémech x86 a x86_64:

Red Hat Enterprise Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, .8.0*, 8.1*

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31

SUSE Linux Enterprise Server 11, 12

Debian 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10

CentOS 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1

Oracle Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1 – Unbreakable Enterprise Kernel i Red Hat Compatible Kernel

CloudLinux 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7

ALT Linux 7.0

* Konfigurace se Stratis nejsou podporovány.

2.3.2.3 Uzel úložišť (pouze pro místní nasazení)

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

Windows Small Business Server 2008

Windows 7 – všechny verze (pouze x64)

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

Windows Home Server 2011

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 – všechny verze

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

Windows Server 2012/2012 R2 – všechny verze

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

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

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

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

2.3.2.4 Agent pro Windows XP SP2

Agent pro Windows XP SP2 podporuje pouze 32bitovou verzi systému Windows XP SP2

Chcete-li chránit počítače se systémem Windows XP SP1 (x64), Windows XP SP2 (x64) nebo Windows XP SP3 (x86), použijte běžného Agenta pro Windows.

Instalace

Agent pro Windows XP SP2 vyžaduje minimálně 550 MB místa na disku a 150 MB paměti RAM. Agent při zálohování obvykle spotřebuje 350 MB paměti. Maximální spotřeba paměti může dosáhnout 2 GB (podle množství zpracovávaných dat).

Agenta pro Windows XP SP2 lze instalovat pouze místně do počítače, který chcete zálohovat. Chcete-li stáhnout instalační program agenta, klikněte na ikonu účtu v pravém horním rohu stránky a potom klikněte na **Stažené soubory** > **Agent pro Windows XP SP2**.

Nástroje a Tvůrce spouštěcích médií nelze nainstalovat. Chcete-li stáhnout soubor ISO spouštěcího média, klikněte na ikonu účtu v pravém horním rohu stránky > **Stažené soubory Spouštěcí médium**.

Aktualizace

Agent pro Windows XP SP2 nepodporuje funkci vzdálené aktualizace. Chcete-li agenta aktualizovat, stáhněte novou verzi instalačního programu a proveďte znovu instalaci.

Pokud jste systém Windows XP aktualizovali z SP2 na aktualizaci SP3, odinstalujte Agenta pro Windows XP SP2 a nainstalujte běžného Agenta pro systém Windows.

Omezení

- Dostupné je pouze zálohování na úrovni disku. Jednotlivé soubory lze obnovit ze zálohy disku nebo svazku.
- Plánování podle událostí (str. 145) není podporováno.
- Podmínky k provedení plánu ochrany (str. 147) nejsou podporovány.
- Jsou podporována pouze následující cílová umístění záloh:
  - Cloudové úložiště
  - Místní složka
  - Síťová složka
  - Secure Zone
- Formát zálohy **Verze 12** a funkce, které tento formát vyžadují, nejsou podporovány. Odesílání fyzických dat (str. 185) není podporováno. Pokud je povolena možnost **Výkon a okno pro zálohování** (str. 182), je použito pouze nastavení zelené úrovně.
- Výběr jednotlivých disků/svazků pro obnovu a ruční mapování disků během obnovy není ve webovém rozhraní podporován. Tato funkce je k dispozici pro spouštěcí média.
- Zpracovávání dat mimo hostitele (str. 224) není podporováno.
- Agent pro Windows XP SP2 nemůže provést následující operace se zálohami:
  - Převádění záloh na virtuální počítač (str. 157)
  - Připojování svazků ze zálohy (str. 220)
  - Extrahování souborů ze záloh (str. 211)
  - Export (str. 222) a ruční ověřování zálohy.

  Tyto operace můžete provést jiným agentem.
- Zálohy vytvořené Agentem pro Windows XP SP2 nelze spouštět jako virtuální počítač (str. 326).

2.3.3 Podporované verze serveru Microsoft SQL Server

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.3.4 Podporované verze Microsoft Exchange Server

- **Microsoft Exchange Server 2019** – všechny verze.
- **Microsoft Exchange Server 2016** – všechny verze.
- **Microsoft Exchange Server 2013** – všechny verze, kumulativní aktualizace 1 (CU1) a novější.
- **Microsoft Exchange Server 2010** – všechny verze, všechny aktualizace Service Pack. Zálohování poštovních schránek a granulární obnova ze záloh databáze jsou podporovány počínaje aktualizací Service Pack 1 (SP1).
- **Microsoft Exchange Server 2007** – všechny verze, všechny aktualizace Service Pack. Zálohování poštovních schránek a granulární obnova ze záloh databáze nejsou podporovány.

2.3.5 Podporované verze služby Microsoft SharePoint

Acronis Cyber Protect 15 podporuje následující verze služby SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

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

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

2.3.6 Podporované verze databáze Oracle

- Oracle Database verze 11g, všechna vydání
- Oracle Database verze 12c, všechna vydání

Jsou podporované pouze konfigurace s jednou instancí.

2.3.7 Podporované verze SAP HANA

Platforma HANA 2.0 SPS 03 nainstalovaná v systému RHEL 7.6, který běží na fyzickém počítači nebo na virtuálním počítači VMware ESXi.

Protože platforma SAP HANA nepodporuje obnovení databázových kontejnerů s více tenanty pomocí snímků úložiště, podporuje toto řešení kontejnery SAP HANA pouze s databází jednoho tenanta.

2.3.8 Podporované virtualizační platformy

Následující tabulka shrnuje podporu různých virtualizačních platforem.

Platforma	Zálohování na úrovni hypervizoru (zálohování bez agenta)	Zálohování zevnitř hostujícího operačního systému
VMware		
Verze VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 **Verze VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Bezplatné ESXi)**		+

Platforma	Zálohování na úrovni hypervizoru (zálohování bez agenta)	Zálohování zevnitř hostujícího operačního systému
VMware Server (Virtuální server VMware) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2008 64bitová verze s Hyper-V Windows Server 2008 R2 s Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 s Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8 a 8.1 (x64) s technologií Hyper-V Windows 10 s Hyper-V Windows Server 2016 s Hyper V – všechny možnosti instalace (s výjimkou Nano Serveru) Microsoft Hyper-V Server 2016 Windows Server 2019 s Hyper-V – všechny možnosti instalace (s výjimkou Nano Serveru) Microsoft Hyper-V Server 2019	+	+
Microsoft Virtual PC 2004 a 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Pouze plně virtualizovaní (neboli HVM) hosté Paravirtualizovaní (neboli PV) hosté nejsou podporováni.
Red Hat a Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Virtuální počítače založené na jádře (KVM)		+
Parallels		
Parallels Workstation		+

Platforma	Zálohování na úrovni hypervizoru (zálohování bez agenta)	Zálohování zevnitř hostujícího operačního systému
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Pouze plně virtualizovaní (neboli HVM) hosté Paravirtualizovaní (neboli PV) hosté nejsou podporováni.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x až 20180425.x		+
Amazon		
Instance Amazon EC2		+
Microsoft Azure		
Virtuální počítače Azure		+

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

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

Omezení

- **Počítače odolné vůči chybám**

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

- **Nezávislé disky a disky RDM**

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

- **Průchozí disky**

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

- **Clustering hosta Hyper-V**

  Agent pro Hyper-V nepodporuje zálohování virtuálních počítačů Hyper-V, které jsou uzly clusteru Windows Server Failover Cluster. Snímek VSS na úrovni hostitele může dokonce dočasně odpojit

disk externího kvora z clusteru. Pokud si tyto počítače přejete zálohovat, nainstalujte agenta do hostujícího operačního systému.

- **Připojení iSCSI v rámci hostovaného systému**

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

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

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

  - Migrace P2V a V2P. Použití Agenta pro Linux nebo spouštěcího média k vytvoření zálohy a spouštěcího média pro obnovení.
  - Spuštění virtuálního počítače ze zálohy vytvořené Agentem pro Linux nebo spouštěcím médiem.
  - Převod zálohy vytvořené Agentem pro Linux nebo spouštěcím médiem do virtuálního počítače.

- **Šifrované virtuální počítače** (zavedeno ve verzi VMware vSphere 6.5)
  - Šifrované virtuální počítač jsou zálohovány v nešifrovaném stavu. Pokud je pro vás šifrování důležité, povolte při vytváření plánu ochrany (str. 153) šifrování záloh.
  - Obnovené virtuální počítače jsou vždy nešifrované. Po dokončení obnovení můžete šifrování ručně povolit.
  - Jestliže zálohujete šifrované virtuální počítače, doporučujeme zašifrovat také virtuální počítač, na kterém je spuštěn Agent pro VMware. V opačném případě mohou být operace se šifrovanými počítači pomalejší, než je očekáváno. Pro počítač s agentem použijte **zásady šifrování virtuálního počítače** ve webovém klientu vSphere.
  - Šifrované virtuální počítače budou zálohovány prostřednictvím sítě LAN, a to i v případě, že pro agenta nakonfigurujete transportní režim SAN. Agent se vrátí do transportního režimu NBD, protože VMware nepodporuje transportní režim SAN k zálohování šifrovaných virtuálních disků.

- **Secure Boot** (zavedeno ve verzi VMware vSphere 6.5)

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

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

2.3.9 Linuxové balíky

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

- Balíček se soubory hlaviček jádra nebo zdrojovými soubory jádra Verze balíčku musí odpovídat verzi jádra.
- Kompilační systém GNU Compiler Collection (GCC). Verze GCC musí být ta, ve které bylo jádro zkompilováno.
- Nástroj pro tvorbu.
- Překladač jazyka Perl

- Knihovny **`libelf-dev`**, **`libelf-devel`** nebo **`elfutils-libelf-devel`**, které od verze 4.15 slouží k vytváření jader a jsou nakonfigurované pomocí CONFIG_UNWINDER_ORC=y. V některých distribucích, jako je Fedora 28, je potřeba je nainstalovat odděleně od hlaviček jádra.

Názvy těchto balíčků se budou lišit podle distribuce systému Linux.

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

Jsou vyžadované balíčky již nainstalovány?

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

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

   ```
   cat /proc/version
   ```

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

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

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

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

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

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

   ```
   perl --version
   ```

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

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

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

Instalace balíčků z úložiště

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

Distribuce systému Linux	Názvy balíčků	Postup instalace
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Instalační program stáhne a nainstaluje balíčky automaticky v rámci předplatného Red Hat.

	perl	Spusťte následující příkaz: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Instalační program stáhne a nainstaluje balíčky automaticky.
	perl	Spusťte následující příkaz: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		Spusťte následující příkazy:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

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

Balíčky budou staženy z úložiště distribuce a nainstalovány.

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

Ruční instalace balíčků

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

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

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

- V systémech Red Hat Enterprise Linux, CentOS nebo Fedora spusťte následující příkaz jako uživatel root:
  `rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3`
- V systému Ubuntu spusťte následující příkaz:
  `sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3`

Příklad: Ruční instalace balíčků v systému Fedora 14

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

1. Spuštěním následujícího příkazu zjistěte verzi jádra a požadovanou verzi GCC:
   `cat /proc/version`

Výstup tohoto příkazu zahrnuje následující:

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

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

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

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

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

4. Nainstalujte balíčky spuštěním následujících příkazů jako uživatel root:

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

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

2.3.10 Kompatibilita se šifrovacím softwarem

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

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

Zálohovat lze data šifrovaná pomocí následujících programů pro šifrování disků:

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

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

Běžné pravidlo instalace

Před instalací agentů ochrany se důrazně doporučuje instalovat šifrovací software.

Způsob používání Secure Zone

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

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

Běžné pravidla zálohování

V operačním systému můžete provádět zálohování na úrovni disku. Nezkoušejte provádět zálohu pomocí spouštěcího média.

Postupy obnovení pro konkrétní software

Microsoft BitLocker Drive Encryption

Jak provést obnovu systému, který byl zašifrován programem BitLocker:

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

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

McAfee Endpoint Encryption a PGP Whole Disk Encryption

Šifrovaný systémový diskový oddíl můžete obnovit pouze pomocí spouštěcích médií.

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

2.4 Systémové požadavky

V následující tabulce je souhrn požadavků na místo na disku a paměť pro typické případy instalace. Instalace je prováděna s výchozími nastaveními.

Součásti k instalaci	Místo na disku vyžadované k instalaci	Minimální spotřeba paměti
Agent pro Windows	850 MB	150 MB
Agent pro Windows a jeden z následujících agentů: ▪ Agent pro SQL ▪ Agent pro Exchange	950 MB	170 MB
Agent pro Windows a jeden z následujících agentů: ▪ Agent pro VMware (Windows) ▪ Agent pro Hyper-V	1170 MB	180 MB
Agent pro Office 365	500 MB	170 MB
Agent pro Linux	2,0 GB	130 MB
Agent pro Mac	500 MB	150 MB
Pouze pro místní nasazení		
Server pro server pro správu v systému Windows	1,7 GB	200 MB
Server pro server pro správu v systému Linux	1,5 GB	200 MB
Server pro správu a Agent pro Windows	2,4 GB	360 MB
Server pro správu a agenti v počítači se systémem Windows, Microsoft SQL Serverem, Microsoft Exchange Serverem a doménovými službami Active Directory	3,35 GB	400 MB
Server pro správu a Agent pro Linux	4,0 GB	340 MB

Uzel úložišť a Agent pro Windows ▪ Pouze 64bitová platforma ▪ K používání deduplikace je vyžadováno minimálně 8 GB paměti RAM. Další informace naleznete v části Osvědčené postupy při deduplikaci (str. 436).	1,1 GB	330 MB

Agent při zálohování obvykle spotřebuje 350 MB paměti (měřeno při zálohování 500GB svazku). Maximální spotřeba paměti může dosáhnout 2 GB (podle množství a typu zpracovávaných dat).

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

Server pro správu s jedním registrovaným počítačem spotřebuje 200 MB paměti. Každý z nově registrovaných počítačů přidá přibližně 2 MB. Z toho vyplývá, že server se 100 registrovanými počítači spotřebuje přibližně 400 MB paměti nad požadavky operačního systému a spuštěných aplikací. Maximální počet registrovaných počítačů je 900–1000. Důvodem tohoto omezení je databáze SQLite integrovaná v serveru pro správu.

Toto omezení můžete obejít zadáním instance externího Microsoft SQL Serveru při instalaci serveru pro správu. S externí SQL databází lze registrovat až 8 000 počítačů bez výrazného snížení výkonu. Server SQL poté spotřebuje přibližně 8 GB paměti RAM. Pro lepší výkon zálohování doporučujeme spravovat počítače podle skupin, přičemž každá skupina by měla obsahovat maximálně 500 počítačů.

2.5 Podporované systémy souborů

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

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

Systém souborů	Podporováno				Omezení
	Agenti	Spouštěcí médium pro prostředí WinPE	Spouštěcí média pro systém Linux	Spouštěcí médium pro systém Mac	
FAT16/32	Všichni agenti	+	+	+	Bez omezení
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	Agent pro Mac	-	-	+	

Systém souborů	Podporováno				Omezení
	Agenti	Spouštěcí médium pro prostředí WinPE	Spouštěcí média pro systém Linux	Spouštěcí médium pro systém Mac	
APFS		-	-	+	▪ Podporováno od systému macOS High Sierra 10.13 ▪ Pokud obnovu provádíte na jiný než původní počítač nebo na počítač bez operačního systému, měli byste znovu ručně vytvořit konfiguraci disků.
JFS	Agent pro Linux	-	+	-	▪ Ze zálohy disku nelze vyloučit soubory ▪ Nelze povolit rychlou přírůstkovou/rozdílovou zálohu.
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	▪ Ze zálohy disku nelze vyloučit soubory ▪ Nelze povolit rychlou přírůstkovou/rozdílovou zálohu. ▪ Během obnovení nelze změnit velikost svazků.
ReFS	Všichni agenti	+	+	+	
XFS		+	+	+	
Linux swap	Agent pro Linux	-	+	-	Bez omezení
exFAT	Všichni agenti	+	+ Spouštěcí médium nelze použít k obnovení, pokud *je záloha uložena v systému* exFAT	+	▪ Jsou podporovány pouze zálohy disků/svazků. ▪ Ze zálohy nelze vyloučit soubory. ▪ Ze zálohy nelze obnovit jednotlivé soubory.

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

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

Jestliže systém neodpovídá těmto požadavkům, zálohování se nezdaří.

Deduplikace dat

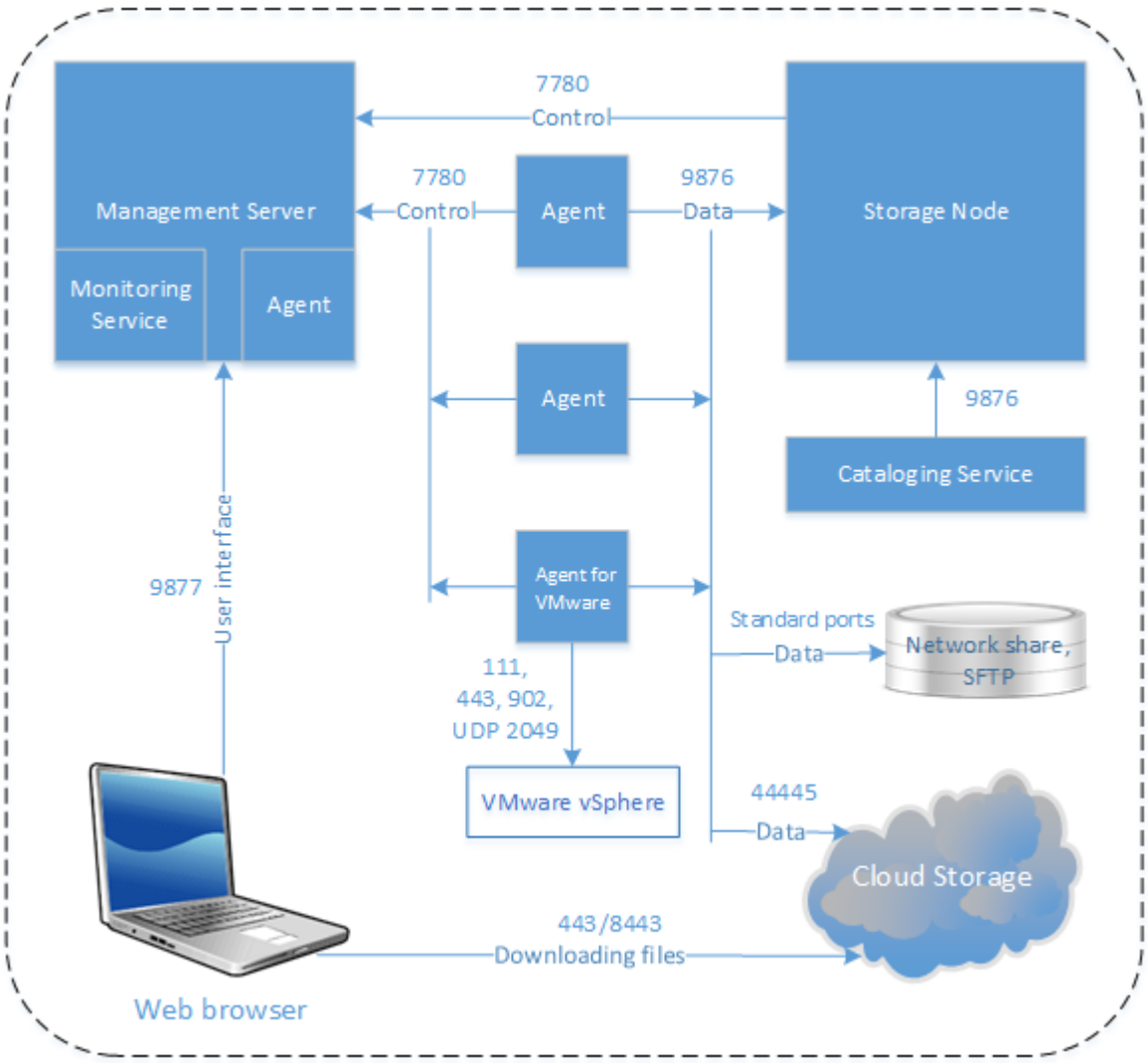
V systému Windows Server 2012 a novější verzi můžete pro svazek NTFS zapnout funkci deduplikace dat. Deduplikace dat snižuje velikost použitého místa ve svazku tak, že ukládá duplicitní části souborů svazku pouze jednou.

Svazek se zapnutou deduplikací dat můžete zálohovat a obnovit na úrovni disku bez omezení. Je podporováno zálohování na úrovni souborů, s výjimkou případů, kdy je používán zprostředkovatel Acronis VSS Provider. Pokud chcete obnovit soubory ze zálohy disku, buď spusťte virtuální počítač, nebo připojte zálohu (str. 220) v počítači se systémem Windows Server 2012 nebo novější verzí a pak zkopírujte soubory z připojeného svazku.

Funkce deduplikace dat serveru Windows Server nesouvisí s funkcí deduplikace aplikace Acronis Backup.

2.6 Místní nasazení

Místní nasazení zahrnuje řadu softwarových součástí popsaných v části Součásti (str. 15). Níže uvedený diagram znázorňuje interakci součástí a porty potřebné pro tuto interakci. Směr šipky ukazuje, která součást iniciuje spojení.

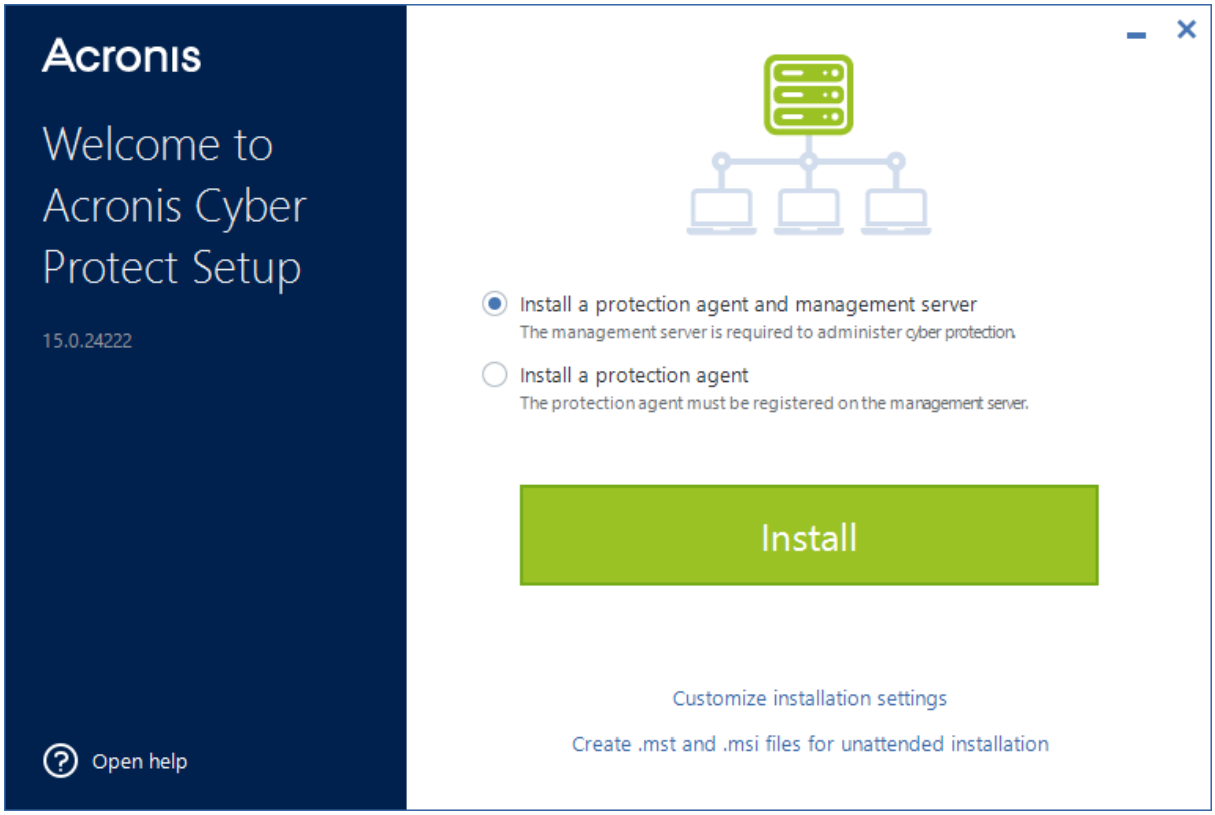


2.6.1 Instalace serveru pro správu

2.6.1.1 Instalace ve Windows

Postup instalace serveru pro správu

1. Přihlaste se jako správce a spusťte instalační program aplikace Acronis Cyber Protect.
2. [Volitelné] Pokud chcete změnit jazyk instalačního programu, klikněte na **Jazyk instalace**.
3. Vyjádřete souhlas s licenčními podmínkami a vyberte, jestli se počítač bude účastnit Programu zkušeností uživatelů Acronis (ACEP).
4. Ponechte výchozí nastavení **Nainstalovat agenta pro ochranu a server pro správu**.



5. Proveďte jeden z následujících úkonů:
   - Klikněte na **Instalovat**.

     Toto je nejsnazší způsob instalace produktu. Většina instalačních parametrů bude nastavena na výchozí hodnoty.

     Nainstalují se následující součásti:
     - Server pro správu
     - Components for Remote Installation
     - Agent pro Windows
     - Ostatní agenti (Agent pro Hyper-V, Agent pro Exchange, Agent pro SQL a Agent pro Active Directory), pokud je v počítači detekován odpovídající hypervizor nebo aplikace.
     - Tvůrce spouštěcích médií
     - Nástroj příkazového řádku
     - Sledování Cyber Protect
   - Klikněte na **Přizpůsobit nastavení instalace** a nakonfigurujte instalaci.

Budete moct vybrat součásti, které chcete nainstalovat, a zadat další parametry. Další informace naleznete v části Přizpůsobení nastavení instalace (str. 37).

- Klikněte na možnost **Vytvořit soubory MST a MSI pro bezobslužnou instalaci** a extrahujte instalační balíčky. Zkontrolujte nebo upravte instalační nastavení, která se přidají do souboru .mst, a potom klikněte na **Generovat**. Další kroky tohoto postupu nejsou nutné.

  Pokud chcete agenty nasadit pomocí zásad skupiny, postupujte podle pokynů v části Instalace agentů pomocí zásad skupiny (str. 101).

6. Pokračujte v instalaci.
7. Po dokončení instalace klikněte na **Zavřít**.

Přizpůsobení nastavení instalace

V této části je popsáno nastavení, které lze změnit během instalace.

Obecná nastavení

- Součásti, které se mají nainstalovat.

Součást	Popis
Server pro správu	Server pro správu je ústřední místo pro správu všech vašich záloh. Při místním nasazení je nainstalován ve vaší místní síti.
Agent pro Windows	Tento agent zálohuje disky, svazky a soubory a bude nainstalován v počítačích se systémem Windows. Vždy bude nainstalován, není možné ho vybrat.
Agent pro Hyper-V	Tento agent zálohuje virtuální počítače Hyper-V a bude nainstalován na hostitelích Hyper-V. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna role Hyper-V.
Agent pro SQL	Tento agent zálohuje databáze serveru SQL Server a bude nainstalován v počítačích, kde běží Microsoft SQL Server. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.
Agent pro Exchange	Tento agent zálohuje databáze a poštovní schránky Exchange a bude nainstalován v počítačích, kde běží Microsoft Exchange Server s rolí poštovní schránky. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.
Agent pro Active Directory	Tento agent zálohuje data doménových služeb Active Directory a bude nainstalován na řadičích domény. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.
Agent pro VMware (Windows)	Tento agent zálohuje virtuální počítače VMware a bude nainstalován na počítačích se systémem Windows, které mají síťový přístup k serveru vCenter. Bude nainstalován, pokud je vybrán.
Agent pro Office 365	Tento agent zálohuje poštovní schránky Microsoft Office 365 do místního umístění a bude nainstalován na počítačích se systémem Windows. Bude nainstalován, pokud je vybrán.
Agent pro Oracle	Tento agent zálohuje databáze Oracle a bude nainstalován v počítačích, kde běží databáze Oracle. Bude nainstalován, pokud je vybrán.
Cyber Protect Monitor	Tato komponenta umožňuje uživateli sledovat provádění běžících úloh v oznamovací oblasti a bude nainstalována na počítačích se systémem Windows. Bude nainstalován, pokud je vybrán.

Nástroj příkazového řádku	Cyber Protect podporuje rozhraní příkazového řádku s nástrojem acrocmd. acrocmd neobsahuje žádné nástroje, které fyzicky spouštějí příkazy. Pouze poskytuje rozhraní příkazového řádku pro součásti Cyber Protect – agenty a server pro správu. Bude nainstalován, pokud je vybrán.

- Složku, kam se produkt nainstaluje.
- Účty, pod kterými tyto služby poběží.

  Můžete si vybrat jeden z úkonů níže:

  - **Použití uživatelských účtů služby** (výchozí pro službu agenta)

    Uživatelské účty služby jsou systémové účty Windows sloužící k provozu služeb. Výhodou tohoto nastavení je, že zásady zabezpečení domény nemají vliv na uživatelská práva těchto účtů. Ve výchozím nastavení běží agent pod účtem **Místní systém**.
  - **Vytvoření nového účtu** (výchozí pro službu serveru pro správu a službu uzlu úložišť)

    Názvy účtů pro službu agenta, serveru pro správu a službu uzlu úložišť budou v tomto pořadí **Agent User**, **AMS User** a **ASN User**.
  - **Použití následujícího účtu**

    V případě instalace produktu do řadiče domény vás instalační program vyzve k zadání existujících účtů (nebo stejného účtu) pro každé zařízení. Z bezpečnostních důvodů instalační program automaticky nevytváří nové účty na řadiči domény.

    Toto nastavení také zvolte, pokud chcete, aby server pro správu používal existující server Microsoft SQL nainstalovaný v jiném počítači a ověření systému Windows pro tento SQL Server.

  Při volbě možnosti **Vytvořit nový účet** nebo **Použít následující účet** zajistěte, aby zásady zabezpečení domény neměly vliv na práva příslušných účtů. Je-li účet zbaven uživatelských práv přidělených během instalace, nemusí daná součást správně fungovat nebo nebude fungovat vůbec.

Oprávnění vyžadovaná pro přihlašovací účet

Agent pro ochranu je spuštěn jako služba Managed Machine Service (MMS) na počítači se systémem Windows. Účet, v rámci kterého bude agent spuštěn, musí mít specifická práva, aby agent pracoval správně. Uživatel služby MMS by měl mít proto přidělena následující práva:

1. Měl by být členem skupin **Backup Operators** a **Administrators**. V řadiči domény musí být uživatel zařazen ve skupině **Správci domény**.
2. Uživatel musí mít oprávnění **Úplné řízení** pro složku **`%PROGRAMDATA%\Acronis`** (v systému Windows XP a Server 2003, **`%ALLUSERSPROFILE%\Application Data\Acronis`**) a její podsložky.
3. Musí mít oprávnění **Úplné řízení** pro určité klíče registru v následujícím klíči: **`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`**.
4. Musí mít následující uživatelská oprávnění:
   - Přihlášení jako služba
   - Nastavení paměťových kvót pro proces
   - Nahrazení tokenu úrovně procesu
   - Úprava hodnot prostředí firmwaru

Uživatel ASN User musí mít na počítači, kde je nainstalován produkt Acronis Storage Node, místní oprávnění správce.

Postup přidělení uživatelských oprávnění

Podle pokynů níže přidělte uživatelská oprávnění (v tomto příkladu se používá uživatelské oprávnění **Přihlášení jako služba**, kroky jsou stejné i pro jiná uživatelská oprávnění):

1. Přihlaste se k počítači pomocí účtu s oprávněními správce.
2. Na **ovládacím panelu** otevřete nabídku **Nástroje pro správu** (nebo klikněte na možnost Win+R, zadejte **control admintools** a stiskněte Enter) a otevřete nabídku **Místní zásady zabezpečení**.
3. Rozbalte položku **Místní zásady** a klikněte na položku **Přiřazení uživatelských práv.**
4. V pravém podokně klikněte pravým tlačítkem myši na položku **Přihlášení jako služba** a vyberte **Vlastnosti**.
5. Chcete-li přidat nového uživatele, klikněte na položku **Přidat uživatele nebo skupinu…**.
6. V okně pro **výběr uživatelů, počítačů, účtů služby nebo skupin** vyhledejte uživatele, kterého chcete zadat, a klikněte na tlačítko **OK**.
7. Kliknutím na tlačítko **OK** v nabídce **vlastností možnosti Přihlášení jako služba** uložte změny.

Důležité *Uživatel, kterého přidáváte k uživatelskému oprávnění* ***Přihlášení jako služba****, nesmí být uveden v zásadě* ***Zamítnout přihlášení jako služba*** *v části* ***Místní zásady zabezpečení****.*

Upozorňujeme, že po dokončení instalace se nedoporučuje ručně měnit přihlašovací účty.

Instalace serveru pro správu

- Databáze, která bude používána serverem pro správu. Ve výchozím nastavení je používána vestavěná databáze SQLite.

  Můžete zvolit libovolnou edici z následujících verzí Microsoft SQL Serveru:

  - Microsoft SQL Server 2012
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2017 (spuštěný v systému Windows)
  - Microsoft SQL Server 2019 (spuštěný v systému Windows)

  Vybranou instanci mohou používat i jiné programy.

  Pokud je název instance výchozí (**MSSQLSERVER**), je třeba zadat jen název počítače, kde se tato instance nachází. Pokud je název instance vlastní, je třeba zadat název počítače i název instance.

  Před výběrem instance nainstalované v jiném počítači zkontrolujte, zda je v tomto počítači povolená služba SQL Server Browser Service a protokol TCP/IP. Pokyny ke spuštění služby SQL Server Browser Service naleznete na adrese http://msdn.microsoft.com/en-us/library/ms189093.aspx. Protokol TCP/IP je možné povolit pomocí podobného postupu.
- Databáze, která bude používána službou vyhledávání. Služba vyhledávání může používat stejnou databázi serveru Microsoft SQL Server, která je zadaná pro server pro správu, nebo oddělenou databázi serveru PostrgeSQL Server. Služba vyhledávání nemůže používat vestavěnou databázi SQLite.
- Port, který bude používán webovým prohlížečem pro přístup k serveru pro správu (výchozí je port 9877), a port, který bude používán pro komunikaci mezi součástmi produktu (výchozí je port 7780). Změna druhého portu po instalaci bude vyžadovat opětovnou registraci všech součástí.

  Brána firewall systému Windows se během instalace nakonfiguruje automaticky. Pokud používáte jinou bránu firewall, zajistěte, aby byly porty otevřené pro příchozí i odchozí požadavky, které přes ni prochází.

Instalace agenta

- Tato možnost určuje, zda se při zálohování nebo obnovování z cloudového úložiště bude agent připojovat k internetu pomocí proxy serveru HTTP.

  Pokud je požadován proxy server, zadejte jeho název hostitele nebo IP adresu a číslo portu. Pokud proxy server vyžaduje ověřování, zadejte pověření serveru proxy.

Poznámka *Aktualizace definic ochrany (p. 105) (antivirové a antimalwarové definice, definice rozšířené detekce, definice posouzení ohrožení zabezpečení a správy oprav) není možné, pokud používáte proxy server.*

2.6.1.2 Instalace v systému Linux

Příprava

1. Před instalací produktu v distribuci systému Linux, která nepoužívá RPM (jako je například Ubuntu), musíte nainstalovat RPM ručně, například spuštěním následujícího příkazu jako uživatel s oprávněním root: **`apt-get install rpm`**.
2. Pokud chcete Agenta pro Linux nainstalovat společně se serverem pro správu, přesvědčte se, jestli jsou v počítači nainstalovány nezbytné balíčky systému Linux (str. 28).
3. Zvolte databázi, která bude používána serverem pro správu.

   Ve výchozím nastavení je používána vestavěná databáze SQLite. Případně můžete použít službu PostgreSQL. Více informací o konfiguraci serveru pro správu pomocí služby PostgreSQL najdete v článku http://kb.acronis.com/content/60395.

   Poznámka: *Pokud přepnete na službu PostgreSQL poté, co už server pro správu určitou dobu fungoval, budete muset přidat zařízení, konfigurovat plány ochrany a provést další nastavení od začátku.*

Instalace

K instalaci serveru pro správu potřebujete alespoň 4 GB volného místa na disku.

Postup instalace serveru pro správu

1. Jako uživatel root spusťte instalační soubor.
2. Potvrďte podmínky licenčního ujednání.
3. [Volitelné] Vyberte součásti, které chcete nainstalovat.

   Ve výchozím nastavení se nainstalují následující součásti:

   - Server pro správu
   - Agent pro Linux
   - Tvůrce spouštěcích médií
4. Zadejte port, který bude používán webovým prohlížečem pro přístup k serveru pro správu. Výchozí hodnota je 9877.
5. Zadejte port, který bude použit pro komunikaci mezi součástmi produktu. Výchozí hodnota je 7780.
6. Kliknutím na tlačítko **Další** zahajte instalaci.
7. Do dokončení instalace klikněte na možnost **Otevřít webovou konzolu** a potom klikněte na tlačítko **Konec**. Webová konzole Cyber Protect se zobrazí ve vašem výchozím internetovém prohlížeči.

2.6.1.3 Zařízení Acronis Cyber Protect

Pomocí zařízení Acronis Cyber Protect můžete snadno získat virtuální počítač s následujícím softwarem:

- CentOS
- Součásti Acronis Cyber Protect:
  - Server pro správu
  - Agent pro Linux
  - Agent pro VMware (Linux)

Zařízení se dodává jako archiv ZIP. Archiv obsahuje soubory OVF a ISO. Můžete nasadit soubor OVF do hostitele ESXi nebo pomocí souboru ISO spustit existující virtuální počítač. Archiv také obsahuje soubor VMDK, který je třeba vložit do stejného adresáře jako soubor OVF.

Poznámka *VMware Host Client (webový klient sloužící ke správě samostatného hostitele ESXi 6.0+) nedovoluje nasazovat šablony OVF obsahující diskový obraz ISO. Pokud je toto váš případ, vytvořte virtuální počítač splňující požadavky níže a potom nainstalujte software pomocí souboru ISO.*

Požadavky na virtuální zařízení jsou následující:

- Minimální systémové požadavky:
  - 2 procesory
  - 6 GB RAM
  - jeden virtuální disk 10 GB (doporučeno 40 GB).
- V nastaveních virtuálního počítače VMware klikněte na kartu **Možnosti** > **Obecné** > **Parametry konfigurace** a potom se přesvědčte, zda má parametr **`disk.EnableUUID`** hodnotu **`true`**.

Instalace softwaru

1. Proveďte jeden z následujících úkonů:
   - Nasaďte zařízení ze souboru OVF. Po dokončení nasazení zapněte výsledný počítač.
   - Spusťte existující virtuální počítač ze souboru ISO.
2. Vyberte možnost **Instalovat nebo aktualizovat Acronis Cyber Protect** a poté stiskněte klávesu **Enter**. Počkejte, až se zobrazí úvodní okno instalace.
3. [Volitelné] Nastavení instalace změníte vybráním možnosti **Změnit nastavení** a stisknutím klávesy **Enter**. Můžete určit následující nastavení:
   - Název hostitele zařízení (ve výchozím nastavení **`AcronisAppliance-`**`<libovolná součást>`).
   - Heslo k účtu root, který se použije pro přihlášení k webové konzoli Cyber Protect (ve výchozím nastavení **není zadáno**).

     Ponecháte-li výchozí hodnotu, zobrazí se po instalaci Acronis Cyber Protect výzva k zadání hesla. Bez tohoto hesla se nebudete moct přihlásit do webové konzole Cyber Protect ani do webové konzole řídicího panelu.
   - Nastavení sítě karty síťového rozhraní
     - **Používat DHCP** (výchozí nastavení)
     - **Nastavit statickou IP adresu**

     Pokud je v počítači více síťových karet, vybere software náhodně jednu z nich a použije v ní tato nastavení.
4. Vyberte možnost **Nainstalovat s aktuálním nastavením**.

Ve výsledku se do počítače nainstaluje CentOS a Acronis Cyber Protect.

Další akce

Po dokončení instalace zobrazí software odkazy do webové konzole Cyber Protect a do webové konzole řídicího panelu. Připojte se k webové konzoli Cyber Protect a začněte používat Acronis Cyber Protect: Přidejte další zařízení, vytvořte plány zálohování atd.

Virtuální počítače ESXi přidáte kliknutím na **Přidat** > **VMware ESXi** a potom zadáním adresy a pověření pro server vCenter nebo samostatného hostitele ESXi.

Neexistují žádná nastavení Acronis Cyber Protect, která se konfigurují ve webové konzole řídicího panelu. Konzola se poskytuje pro vyšší pohodlí a k řešení potíží.

Aktualizace softwaru

1. Stáhněte a rozbalte archiv ZIP s novou verzí zařízení.
2. Spusťte počítač z obrazu ISO rozbaleného v předchozím kroku.
   a. Uložte obraz ISO do datového úložiště vSphere.
   b. Připojte obraz ISO k jednotce CD/DVD počítače.
   c. Restartujte počítač.
   d. [Pouze při první aktualizaci] Stiskněte klávesu **F2** a potom změňte pořadí spouštění tak, aby se jako první použila jednotka CD/DVD.
3. Vyberte možnost **Instalovat nebo aktualizovat Acronis Cyber Protect** a poté stiskněte klávesu **Enter**.
4. Vyberte možnost **Aktualizovat** a poté stiskněte klávesu **Enter**.
5. Po dokončení aktualizace odpojte obraz ISO od jednotky CD/DVD počítače.

Ve výsledku se Acronis Cyber Protect aktualizuje. Je-li verze systému CentOS v souboru ISO novější než verze na disku, bude se před aktualizací Acronis Cyber Protect aktualizovat operační systém.

2.6.2 Přidávání počítačů prostřednictvím webového rozhraní

Přidávání počítače do serveru pro správu zahájíte kliknutím na **Všechna zařízení** > **Přidat**.

Pokud je server pro správu nainstalovaný v systému Linux, budete požádáni o výběr instalačního programu na základě typu počítače, který chcete přidat. Po stažení instalačního programu ho v daném počítači spusťte ručně.

Operace popisované dále v této části jsou možné, pokud je server pro správu nainstalovaný v systému Windows. Agent bude ve většině případů do vybraného počítače nasazen na pozadí.

2.6.2.1 Přidání počítače se systémem Windows

Příprava

1. Pro úspěšnou instalaci na vzdáleném počítači se systémem Windows Vista a novějším musí být na daném počítači *vypnutá* volba **Ovládací panel > Možnosti složky > Zobrazení > Používat průvodce sdílením**.

2. Chcete-li docílit úspěšné instalace na vzdálený počítač, který *není* členem domény služby Active Directory, je nutné, aby byla funkce Řízení uživatelských účtů (UAC) a její vzdálená omezení *zakázána* (str. 44).
3. Sdílení souborů a tiskáren musí být na vzdáleném počítači *zapnuto*. Tato možnost je dostupná následujícím způsobem:

- V počítači se systémem Windows 2003 Server: přejděte do nabídky **Ovládací panely > Brána Windows Firewall > Výjimky > Sdílení souborů a tiskáren**.
- V počítači se systémem Windows Vista, Windows Server 2008, Windows 7 nebo novější: přejděte na **Ovládací panely > Brána Windows Firewall > Centrum síťových připojení a sdílení > Změnit pokročilé nastavení sdílení**.

4. Acronis Cyber Protect pro vzdálenou instalaci používá TCP porty **445**, **25001** a **43234**.

   Port **445** je automaticky otevřen, jestliže je povolené sdílení souborů a tiskáren. Porty 43234 a 25001 jsou automaticky otevřeny pomocí brány firewall systému Windows. V případě, že používáte jinou bránu firewall, ujistěte se, že tyto tři porty jsou otevřeny (přidány k výjimkám) příchozím i odchozím žádostem.

   Po dokončení vzdálené instalace je port **25001** automaticky zavřen pomocí brány firewall systému Windows. Porty **445** a **43234** musí zůstat otevřené, pokud agenta chcete v budoucnu vzdáleně aktualizovat. Port **25001** bude při každé aktualizaci automaticky otevřen a zavřen pomocí brány firewall systému Windows. Pokud používáte jiný firewall, nechte všechny tři porty otevřené.

Poznámka *Agenta pro Windows nelze nainstalovat na vzdáleném počítači se systémem Windows XP.*

Instalační balíčky

Agent se instalují z instalačních balíčků. Server pro správu načte balíčky z místní složky zadané v následujícím klíči registru:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles<číslo sestavení produktu>. Výchozí umístění je **%ProgramFiles%\Acronis\RemoteInstallationFiles**<číslo sestavení produktu>.

Je možné, že instalační balíčky budete muset stáhnout ručně, a to v následujících případech:

- Součásti pro vzdálenou instalaci nebyly nainstalovány během instalace serveru pro správu.
- Instalační balíčky byly ručně odebrány z umístění zadaného v klíči registru.
- Potřebujete přidat 32bitový počítač na 64bitový server pro správu nebo naopak.
- Potřebujete aktualizovat agenty na 32bitovém počítači z 64bitového serveru pro správu nebo naopak pomocí karty **Agenti**.

Získání instalačních balíčků

1. Ve webové konzoli Cyber Protect klikněte na ikonu účtu v pravém horním rohu stránky > **Stažené soubory**.
2. Vyberte **Offline instalační program pro Windows**. Dávejte pozor na požadovanou bitovou architekturu – 32bitová nebo 64bitová.
3. Uložte instalační program do umístění balíčků.

Přidání počítače

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **Windows** nebo na tlačítko odpovídající aplikaci, kterou chcete chránit. V závislosti na tlačítku, na které kliknete, se vybere jedna za následujících možností:
   - Agent pro Windows
   - Agent pro Hyper-V
   - Agent pro SQL + Agent pro Windows
   - Agent pro Exchange + Agent pro Windows

     Pokud jste klikli na **Microsoft Exchange Server** > **Poštovní schránky Exchange** a alespoň jeden Agent pro Exchange již byl zaregistrován, přejdete přímo ke kroku 6.

- Agent pro Active Directory + Agent pro Windows
- Agent pro Office 365

3. Vyberte agenta pro nasazení.
4. Zadejte název hostitele nebo IP adresu cílového počítače a přihlašovací údaje účtu s oprávněními správce na daném počítači.

   Uživatel, kterého použijete pro vzdálenou instalaci, by měl být vestavěným uživatelem s oprávněními správce. Pokud chcete použít jiný uživatelský účet, měl by daný uživatel náležet do skupiny Administrators a podle popisu v následujícím článku byste měli změnit registr v počítači, který chcete přidat: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
5. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

   Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.
6. Klikněte na **Instalovat**.
7. Jestliže jste v kroku 2 klikli na **Microsoft Exchange Server** > **Poštovní schránky Exchange**, zadejte počítač, ve kterém je povolena role **klientského přístupu** (CAS) serveru Microsoft Exchange Server. Další informace najdete v tématu Zálohování poštovní schránky (str. 309).

Požadavky na službu Řízení uživatelských účtů (UAC)

V počítači se systémem Windows Vista nebo novějším, který není členem domény Active Directory, vyžadují operace centralizované správy (včetně vzdálené instalace) zakázanou službu UAC a její vzdálená omezení.

Jak vypnout službu UAC

Proveďte jeden z následujících postupů podle verze operačního systému:

- **V operačním systému Windows verze starší než Windows 8:**

  Přejděte do nabídky **Ovládací panely > Zobrazit podle: Malé ikony > Uživatelské účty > Změnit nastavení nástroje Řízení uživatelských účtů** a poté přesuňte posuvný ovladač na možnost **Nikdy neupozorňovat**. Poté počítač restartujte.
- **V libovolném operačním systému Windows**:
  1. Otevřete Editor registru.
  2. Vyhledejte následující klíč registru: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Hodnotu **EnableLUA** změňte na **0**.
  4. Restartujte počítač.

Zakázání vzdálených omezení UAC

1. Otevřete Editor registru.
2. Vyhledejte následující klíč registru: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Hodnotu **LocalAccountTokenFilterPolicy** změňte na **1**.

   Pokud hodnota **LocalAccountTokenFilterPolicy** neexistuje, vytvořte ji jako DWORD (32 bitů). Další informace o této hodnotě naleznete v dokumentaci společnosti Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Poznámka** Z důvodu zabezpečení doporučujeme po dokončení operace správy (například vzdálené instalace) vrátit obě nastavení na původní hodnotu: **EnableLUA**=**1** a **LocalAccountTokenFilterPolicy** = **0

2.6.2.2 Přidání počítače se systémem Linux

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **Linux**. Tím se stáhne instalační soubor.
3. Spusťte instalační program lokálně (str. 50) v počítači, který chcete chránit.

2.6.2.3 Přidání počítače se systémem OS X

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **Mac**. Tím se stáhne instalační soubor.
3. Spusťte instalační program lokálně (str. 51) v počítači, který chcete chránit.

2.6.2.4 Přidání serveru vCenter nebo hostitele ESXi

Přidání serveru vCenter nebo samostatného hostitele ESXi na server pro správu lze provést čtyřmi způsoby:

- Nasazení Agenta pro VMware (Virtual Appliance) (str. 45)

  Tato metoda se doporučuje pro většinu případů. Virtuální zařízení bude automaticky nasazeno do všech hostitelů spravovaných vámi zadaným serverem vCenter. Můžete vybrat hostitele a přizpůsobit nastavení virtuálního zařízení.
- Instalace Agenta pro VMware (Windows) (str. 46)

  Pro účely zálohování bez zátěže nebo zálohování nezávislého na síti LAN je vhodné používat Agenta pro VMware nainstalovaného na fyzickém počítači se systémem Windows.
  - **Zálohování bez zátěže**

    Tuto možnost použijte, pokud jsou produkční hostitelé ESXi tak silně zatíženi, že není vhodné spouštět virtuální zařízení.
  - **Zálohování nezávislé na LAN**

    Pokud ESXi používá úložiště připojené pomocí sítě SAN, nainstalujte agenta do počítače připojeného ke stejné síti SAN. Agent bude zálohovat virtuální počítače přímo z úložiště a ne pomocí hostitele ESXi a LAN. Podrobné informace naleznete v části Zálohování nezávislé na síti LAN (str. 335).

  Pokud server pro správu běží v systému Windows, bude agent automaticky nasazen do vámi zadaného počítače. Jinak je nutné nainstalovat agenta ručně.
- Registrace už nainstalovaného Agenta pro VMware (str. 46)

  Toto je nezbytný krok po reinstalaci serveru pro správu. Můžete také zaregistrovat a nakonfigurovat agenta pro VMware (Virtual Appliance) nasazeného z šablony OVF.
- Konfigurace již zaregistrovaného Agenta pro VMware (str. 47)

  Toto je nezbytný krok po ruční instalaci Agenta pro VMware (Windows) nebo nasazení zařízení Acronis Cyber Protect (str. 40). Můžete také přiřadit již nakonfigurovaného Agenta pro VMware k jinému serveru vCenter Server nebo samostatnému hostiteli ESXi.

Nasazení Agenta pro VMware (Virtual Appliance) prostřednictvím webového rozhraní

1. Klikněte na **Všechna zařízení** > **Přidat**.

2. Klikněte na **VMware ESXi**.
3. Vyberte možnost **Nasadit jako virtuální zařízení do všech hostitelů serveru vCenter**.
4. Zadejte adresu a pověření k přístupu pro server vCenter nebo samostatného hostitele ESXi. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.
5. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

   Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.
6. [Volitelné] Kliknutím na **Nastavení** přizpůsobte nastavení nasazení:
   - Hostitelé ESXi, do kterých chcete nasadit agenta (pouze pokud byl v předchozím kroku zadán server vCenter).
   - Název virtuálního zařízení.
   - Datové úložiště, kde bude zařízení umístěno.
   - Fond zdrojů/prostředků nebo virtuální zařízení vApp, které budou obsahovat zařízení.
   - Síť, ke které bude připojený síťový adaptér virtuálního zařízení.
   - Nastavení sítě virtuálního zařízení. Můžete zvolit automatickou konfiguraci DHCP, nebo můžete hodnoty zadat ručně – včetně statické IP adresy.
7. Klikněte na **Nasadit**.

Instalace Agenta pro VMware (Windows)

Příprava

Proveďte přípravné kroky popisované v části Přidání počítače se systémem Windows (str. 42).

Instalace

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **VMware ESXi**.
3. Vyberte možnost **Vzdáleně instalovat do počítače se systémem Windows**.
4. Vyberte agenta pro nasazení.
5. Zadejte název hostitele nebo IP adresu cílového počítače a přihlašovací údaje účtu s oprávněními správce na daném počítači.
6. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

   Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.
7. Klikněte na **Připojit**.
8. Zadejte adresu a pověření pro server vCenter nebo samostatného hostitele ESXi a poté klikněte na **Připojit**. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.
9. Chcete-li nainstalovat agenta, klikněte na **Instalovat**.

Registrace už nainstalovaného Agenta pro VMware

Tato část popisuje registraci Agenta pro VMware prostřednictvím webového rozhraní.

Náhradní metody registrace:

- Agenta pro VMware (Virtual Appliance) můžete registrovat zadáním serveru pro správu v uživatelském rozhraní virtuálního zařízení. Viz krok 3 v kapitole „Konfigurace virtuálního zařízení“ v části „Nasazení Agenta pro VMware (Virtual Appliance) z šablony OVF“.
- Agent pro VMware (Windows) se registruje při jeho místní instalaci (str. 48).

Postup registrace Agenta pro VMware

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **VMware ESXi**.
3. Vyberte možnost **Registrovat již nainstalovaného agenta**.
4. Vyberte agenta pro nasazení.
5. Při registraci *Agenta pro VMware (Windows)* zadejte název hostitele nebo IP adresu počítače, kde je agent nainstalovaný, a pověření účtu s oprávněními správce na tomto počítači.

   Při registraci *Agenta pro VMware (Virtual Appliance)* zadejte název hostitele nebo IP adresu virtuálního zařízení a pověření pro server vCenter nebo samostatného hostitele ESXi, kde je zařízení spuštěno.
6. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

   Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.
7. Klikněte na **Připojit**.
8. Zadejte název hostitele nebo IP adresu serveru vCenter nebo hostitele ESXi a pověření pro přístup k němu a poté klikněte na **Připojit**. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.
9. Kliknutím na **Registrovat** agenta zaregistrujte.

Konfigurace již zaregistrovaného Agenta pro VMware

Tato část popisuje postup přidružení Agenta pro VMware k serveru vCenter Server nebo hostiteli ESXi ve webovém rozhraní. Tuto akci můžete případně provést v konzole Agenta pro VMware (Virtual Appliance).

Tímto postupem můžete také změnit existující přidružení agenta k serveru vCenter Server nebo hostiteli ESXi. Případně to můžete udělat v konzole Agenta pro VMware (Virtual Appliance) nebo kliknutím na možnost **Nastavení** > **Agenti** > agent > **Podrobnosti** > **vCenter/ESXi**.

Jak nakonfigurovat Agenta pro VMware

1. Klikněte na **Všechna zařízení** > **Přidat**.
2. Klikněte na **VMware ESXi**.
3. V softwaru se zobrazuje nenakonfigurovaný Agent pro VMware uvedený jako první v abecedním pořadí.

   Jsou-li všichni agenti registrovaní na serveru pro správu nakonfigurovaní, zobrazí se kliknutím na možnost **Konfigurovat již zaregistrovaného agenta** v softwaru agent uvedený jako první v abecedním pořadí.
4. V případě potřeby klikněte na možnost **Počítač s agentem** a vyberte agenta ke konfiguraci.
5. Zadejte nebo změňte název hostitele nebo IP adresu serveru vCenter nebo hostitele ESXi a pověření pro přístup k němu. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.
6. Kliknutím na **Konfigurovat** uložte změny.

2.6.2.5 Přidání clusteru Scale Computing HC3

Přidání clusteru Scale Computing HC3 na server pro správu Cyber Protect

1. Nasazení Agenta pro Scale Computing HC3 (virtuální zařízení) (p. 97) v clusteru.
2. Nakonfigurujte (p. 97) připojení k tomuto clusteru a také k serveru pro správu Cyber Protect.

2.6.3 Lokální instalace agentů

2.6.3.1 Instalace ve Windows

Postup instalace Agenta pro Windows, Agenta pro Hyper-V, Agenta pro Exchange, Agenta pro SQL nebo Agenta pro Active Directory

1. Přihlaste se jako správce a spusťte instalační program aplikace Acronis Cyber Protect.
2. [Volitelné] Pokud chcete změnit jazyk instalačního programu, klikněte na **Jazyk instalace**.
3. Vyjádřete souhlas s licenčními podmínkami a vyberte, jestli se počítač bude účastnit Programu zkušeností uživatelů Acronis (ACEP).
4. Vyberte možnost **Instalovat agenta pro ochranu**.
5. Proveďte jeden z následujících úkonů:
   - Klikněte na **Instalovat**.

     Toto je nejsnazší způsob instalace produktu. Většina instalačních parametrů bude nastavena na výchozí hodnoty.

     Nainstalují se následující součásti:
     - Agent pro Windows
     - Ostatní agenti (Agent pro Hyper-V, Agent pro Exchange, Agent pro SQL a Agent pro Active Directory), pokud je v počítači detekován odpovídající hypervizor nebo aplikace.
     - Tvůrce spouštěcích médií
     - Nástroj příkazového řádku
     - Cyber Protect Monitor
   - Klikněte na **Přizpůsobit nastavení instalace** a nakonfigurujte instalaci.

     Budete moct vybrat součásti, které chcete nainstalovat, a zadat další parametry. Další informace naleznete v části Přizpůsobení nastavení instalace (str. 37).
   - Klikněte na možnost **Vytvořit soubory MST a MSI pro bezobslužnou instalaci** a extrahujte instalační balíčky. Zkontrolujte nebo upravte instalační nastavení, která se přidají do souboru .mst, a potom klikněte na **Generovat**. Další kroky tohoto postupu nejsou nutné.

     Pokud chcete agenty nasadit pomocí zásad skupiny, postupujte podle pokynů v části Instalace agentů pomocí zásad skupiny (str. 101).
6. Zadejte server pro správu, kde bude počítač s agentem zaregistrovaný:
   a. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
   b. Zadejte pověření správce serveru pro správu nebo registrační token.

      Další informace o vygenerování registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny (str. 101).

      Pokud nejste správce serveru pro správu, můžete počítač zaregistrovat výběrem možnosti **Připojit bez ověřování**. To je možné v případě, že server pro správu umožňuje anonymní registraci, což může být zakázáno (str. 443).
   c. Klikněte na tlačítko **Hotovo**.
7. Při zobrazení výzvy vyberte, zda se má počítač přidat do organizace nebo do některé jednotky.

Tato výzva se zobrazí, pokud spravujete více jednotek nebo organizaci s alespoň jednou jednotkou. Jinak se počítač bez výzev přidá do jednotky nebo organizace, kterou spravujete. Další informace najdete v části Správci a jednotky (str. 444).

8. Pokračujte v instalaci.
9. Po dokončení instalace klikněte na **Zavřít**.
10. Pokud jste nainstalovali Agent pro Exchange, budete moci zálohovat databáze Exchange. Pokud chcete zálohovat poštovní schránky Exchange, otevřete webovou konzoli Cyber Protect, klikněte na **Přidat** > **Microsoft Exchange Server** > **Poštovní schránky Exchange** a zadejte počítač, ve kterém je povolena role **klientského přístupu** (CAS) serveru Microsoft Exchange Server. Další informace najdete v tématu Zálohování poštovní schránky (str. 309).

Instalace Agenta pro VMware (Windows), Agenta pro Office 365, Agenta pro Oracle nebo Agenta pro Exchange do počítače bez serveru Microsoft Exchange Server

1. Přihlaste se jako správce a spusťte instalační program aplikace Acronis Cyber Protect.
2. [Volitelné] Pokud chcete změnit jazyk instalačního programu, klikněte na **Jazyk instalace**.
3. Vyjádřete souhlas s licenčními podmínkami a vyberte, jestli se počítač bude účastnit Programu zkušeností uživatelů Acronis (ACEP).
4. Vyberte možnost **Instalovat agenta pro ochranu** a klikněte na **Přizpůsobit nastavení instalace**.
5. Vedle možnosti **Co je nutno nainstalovat** klikněte na **Změnit**.
6. Zaškrtněte odpovídající políčka pro agenty, které chcete nainstalovat. Zrušte zaškrtnutí políček u součástí, které instalovat nechcete. Pokračujte kliknutím na **Hotovo**.
7. Zadejte server pro správu, kde bude počítač s agentem zaregistrovaný:
   a. Vedle možnosti **Server pro správu Acronis Cyber Protect** klikněte na **Zadat**.
   b. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
   c. Zadejte pověření správce serveru pro správu nebo registrační token.

      Další informace o vygenerování registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny (str. 101).

      Pokud nejste správce serveru pro správu, můžete počítač zaregistrovat výběrem možnosti **Připojit bez ověřování**. To je možné v případě, že server pro správu umožňuje anonymní registraci, což může být zakázáno (str. 443).
   d. Klikněte na tlačítko **Hotovo**.
8. Při zobrazení výzvy vyberte, zda se má počítač přidat do organizace nebo do některé jednotky.

   Tato výzva se zobrazí, pokud spravujete více jednotek nebo organizaci s alespoň jednou jednotkou. Jinak se počítač bez výzev přidá do jednotky nebo organizace, kterou spravujete. Další informace najdete v části Správci a jednotky (str. 444).
9. [Volitelné] Změňte další nastavení instalace způsobem popsaným v části Přizpůsobit nastavení instalace (str. 37).
10. Kliknutím na **Instalovat** zahajte instalaci.
11. Po dokončení instalace klikněte na **Zavřít**.
12. [Pouze při instalaci Agenta pro VMware (Windows)] Proveďte postup popsaný v části Konfigurace už zaregistrovaného Agenta pro VMware (str. 47).
13. [Pouze při instalaci Agenta pro Exchange] Otevřete webovou konzoli Cyber Protect, klikněte na **Přidat** > **Microsoft Exchange Server** > **Poštovní schránky Exchange** a zadejte počítač, ve kterém je povolena role **klientského přístupu** (CAS) serveru Microsoft Exchange Server. Další informace najdete v tématu Zálohování poštovní schránky (str. 309).

2.6.3.2 Instalace v systému Linux

Příprava

1. Před instalací produktu v distribuci systému Linux, která nepoužívá RPM (jako je například Ubuntu), musíte nainstalovat RPM ručně, například spuštěním následujícího příkazu jako uživatel s oprávněním root: **`apt-get install rpm`**.
2. Přesvědčte se, že v počítači jsou nainstalovány nezbytné balíčky systému Linux (str. 28).

Instalace

K instalaci Agenta pro Linux potřebujete alespoň 2,0 GB volného místa na disku.

Postup instalace Agenta pro Linux:

1. Spusťte příslušný instalační soubor (.i686 nebo .x86_64) jako uživatel root.
2. Potvrďte podmínky licenčního ujednání.
3. Určete součásti, které chcete nainstalovat:
   a. Zrušte zaškrtnutí políčka **Server pro správu Acronis Cyber Protect**.
   b. Zaškrtněte políčka pro agenty, které chcete nainstalovat. Dostupní jsou následující agenti:
      - **Agent pro Linux**
      - **Agent pro Oracle**

      Agent pro Oracle vyžaduje zároveň instalaci Agenta pro Linux.
   c. Klikněte na tlačítko **Další**.
4. Zadejte server pro správu, kde bude počítač s agentem zaregistrovaný:
   a. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
   b. Zadejte uživatelské jméno a heslo správce serveru pro správu nebo zvolte anonymní registraci.

      Zadání pověření je vhodné, pokud vaše organizace má jednotky, aby bylo možné počítač přidat do jednotky spravované zadaným správcem. Při anonymní registraci je počítač vždy přidán k organizaci. Další informace najdete v části Správci a jednotky (str. 444).

      Zadání pověření je nezbytné, pokud je anonymní registrace na serveru pro správu zakázána (str. 443).
   c. Klikněte na tlačítko **Další**.
5. Při zobrazení výzvy vyberte, zda se má počítač s agentem přidat do organizace nebo do některé jednotky a potom stiskněte **Enter**.

   Tato výzva se zobrazí, pokud účet zadaný v předchozím kroku spravuje více jednotek nebo organizaci s alespoň jednou jednotkou.
6. Je-li v počítači povoleno zabezpečené spouštění UEFI, budete informováni, že po instalaci je třeba restartovat systém. Zapamatujte si, které heslo (pro kořenového uživatele nebo uživatele acronis) se má použít.

   Poznámka *Během instalace se vygeneruje klíč Acronis sloužící k podepsání modulu* ***`snapapi`****, který je zaregistrovaný jako klíč vlastníka počítače (MOK). Restartování je povinné z důvodu zapsání tohoto klíče. Bez zapsání tohoto klíče nebude agent fungovat. Pokud po instalaci agenta povolíte zabezpečené spouštění UEFI, opakujte instalaci včetně kroku 6.*
7. Po dokončení instalace proveďte jeden z následujících úkonů:
   - Pokud jste byli v předchozím kroku vyzváni k restartování systému, klikněte na **Restartovat**.

     Během restartování systému si zvolte správu MOK, vyberte možnost **Zapsat MOK** a potom klíč zapište pomocí hesla doporučeného v předchozím kroku.

- Jinak klikněte na **Konec**.

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

2.6.3.3 Instalace v macOS

Postup instalace Agenta pro Mac

1. Klikněte dvakrát na instalační soubor (.dmg).
2. Počkejte, až operační systém připojí obraz instalačního disku.
3. Dvakrát klikněte na tlačítko **Instalovat** a potom klikněte na tlačítko **Pokračovat**.
4. [Volitelné] Kliknutím na **Změnit umístění instalace** změňte disk, kam bude software nainstalován. Ve výchozím nastavení je vybrán systémový spouštěcí disk.
5. Klikněte na **Instalovat**. Pokud se zobrazí výzva, zadejte uživatelské jméno a heslo správce.
6. Zadejte server pro správu, kde bude počítač s agentem zaregistrovaný:
   a. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
   b. Zadejte uživatelské jméno a heslo správce serveru pro správu nebo zvolte anonymní registraci.

      Zadání pověření je vhodné, pokud vaše organizace má jednotky, aby bylo možné počítač přidat do jednotky spravované zadaným správcem. Při anonymní registraci je počítač vždy přidán k organizaci. Další informace najdete v části Správci a jednotky (str. 444).

      Zadání pověření je nezbytné, pokud anonymní registrace na serveru pro správu je zakázána (str. 443).
   c. Klikněte na **Registrovat**.
7. Při zobrazení výzvy vyberte, zda se má počítač s agentem přidat do organizace nebo do některé jednotky a potom klikněte na **Hotovo**.

   Tato výzva se zobrazí, pokud účet zadaný v předchozím kroku spravuje více jednotek nebo organizaci s alespoň jednou jednotkou.
8. Po dokončení instalace klikněte na **Zavřít**.

2.6.4 Bezobslužná instalace nebo odinstalace

2.6.4.1 Bezobslužná instalace nebo odinstalace v systému Windows

Toto téma popisuje instalaci nebo odinstalaci Acronis Cyber Protect v bezobslužném režimu v počítači se systémem Windows pomocí instalační služby systému Windows (program **`msiexec`**). V doméně Active Directory je dalším způsobem provedení bezobslužné instalace použití zásad skupiny, viz Instalace agentů pomocí zásad skupiny (str. 101).

Během instalace můžete použít soubor označovaný jako **transformace** (soubor MST). Transformace je soubor s parametry instalace. Případně můžete parametry instalace zadat přímo v příkazovém řádku.

Vytvoření souboru transformace MST a extrahování instalačních balíčků

1. Přihlaste se jako správce a spusťte instalační program.
2. Klikněte na možnost **Vytvořit soubory MST a MSI pro bezobslužnou instalaci**.
3. V části **Bytová verze součásti** vyberte možnost **32bitová**, nebo **64bitová**.
4. V části **Co je nutno nainstalovat** vyberte požadované součásti. Instalační balíčky těchto součástí se extrahují z instalačního programu.

5. Zkontrolujte nebo upravte další nastavení instalace, která se přidají do souboru MST.
6. Klikněte na možnost **Generovat**.

Vygeneruje se soubor transformace MST a instalační balíčky MSI a CAB se extrahují do vybrané složky.

Instalace produktu pomocí transformace MST

Spusťte následující příkaz:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Vysvětlení:

- `<název balíčku>` je název souboru MSI. Tento název je **AB.msi** nebo **AB64.msi** podle bitové architektury operačního systému.
- `<název transformace>` je název transformace. Tento název je **AB.msi.mst** nebo **AB64.msi.mst** podle bitové architektury operačního systému.

Příklad: **`msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`**

Instalace nebo odinstalace produktu ručním zadáním parametrů

Spusťte následující příkaz:

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

V této části je `<název balíčku>` název souboru MSI. Tento název je **AB.msi** nebo **AB64.msi** podle bitové architektury operačního systému.

Dostupné parametry a jejich hodnoty jsou popsány v tématu Parametry bezobslužné instalace nebo odinstalace (str. 52).

Příklady

- Instalace serveru pro správu a součástí pro vzdálenou instalaci.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
ACEP_AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
```

- Instalace agenta pro Windows, nástroje příkazového řádku a nástroje Cyber Protect Monitor. Registrace počítače s agentem na dříve nainstalovaný server pro správu.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonito
r TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
ACEP_AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

Parametry bezobslužné instalace nebo odinstalace

Tato část popisuje parametry použité během bezobslužné instalace nebo odinstalace v systému Windows.

Kromě těchto parametrů můžete využít další parametry procesu **`msiexec`**, jak je uvedeno v části https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parametry instalace

Společné parametry

ADDLOCAL=<seznam součástí>

Součásti určené k instalaci jsou oddělené čárkami bez mezer. Všechny určené součásti se musí před instalací extrahovat z instalačního programu.

Následuje úplný seznam součástí.

Součást	Nutno instalovat společně s	Bitová architektura	Název součásti a popis
AcronisCentralizedManagementServer	WebConsole	32bitová nebo 64bitová	Server pro správu
WebConsole	AcronisCentralizedManagementServer	32bitová nebo 64bitová	Webová konzola
ComponentRegisterFeature	AcronisCentralizedManagementServer	32bitová nebo 64bitová	Components for Remote Installation
AtpScanService	AcronisCentralizedManagementServer	32bitová nebo 64bitová	Služba vyhledávání
AgentsCoreComponents		32bitová nebo 64bitová	Klíčové součásti pro agenty
BackupAndRecoveryAgent	AgentsCoreComponents	32bitová nebo 64bitová	Agent pro Windows
ArxAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro SQL
ARADAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32bitová nebo 64bitová	Agent pro Office 365
AcronisESXSupport	AgentsCoreComponents	32bitová nebo 64bitová	Agent pro VMware (Windows)
HyperVAgent	AgentsCoreComponents	32bitová nebo 64bitová	Agent pro Hyper-V

Součást	Nutno instalovat společně s	Bitová architektura	Název součásti a popis
ESXVirtualAppliance		32bitová nebo 64bitová	Agent pro VMware (Virtual Appliance)
ScaleVirtualAppliance		32bitová nebo 64bitová	Agent pro Scale Computing HC3 (virtuální zařízení)
CommandLineTool		32bitová nebo 64bitová	Nástroj příkazového řádku
TrayMonitor	BackupAndRecoveryAgent	32bitová nebo 64bitová	Cyber Protect Monitor
BackupAndRecoveryBootableComponents		32bitová nebo 64bitová	Tvůrce spouštěcích médií
PXEServer		32bitová nebo 64bitová	PXE Server
StorageServer	BackupAndRecoveryAgent	64bitový	Uzel úložišť
CatalogBrowser	JRE 8 Update 111 nebo novější	64bitový	Katalogová služba

TARGETDIR=<cesta>

Složku, kam se produkt nainstaluje.

REBOOT=ReallySuppress

Pokud je zadaný tento parametr, je zakázané restartování počítače.

CURRENT_LANGUAGE=<ID jazyka>

Jazyk produktu. Dostupné hodnoty jsou následující: **en**, **en_GB**, **cs**, **da**, **de**, **es_ES**, **fr**, **ko**, **it**, **hu**, **nl**, **ja**, **pl**, **pt**, **pt_BR**, **ru**, **tr**, **zh**, **zh_TW**.

ACEP_AGREEMENT={0,1}

Je-li hodnota **1**, zapojí se počítač do Programu zkušeností uživatelů Acronis (ACEP).

REGISTRATION_ADDRESS=<název hostitele nebo IP adresa>:<port>

Název hostitele nebo IP adresa počítače, ve kterém je server pro správu nainstalovaný. Agenti, uzel úložišť a služba katalogu zadané v parametru **ADDLOCAL** se zaregistrují do tohoto serveru pro správu. Číslo portu je povinné, pokud se liší od výchozí hodnoty (9877).

Pokud je anonymní registrace na serveru pro správu zakázána (str. 443), musíte zadat buď parametr **REGISTRATION_TOKEN**, nebo parametry **REGISTRATION_LOGIN** a **REGISTRATION_PASSWORD**.

REGISTRATION_TOKEN=<token>

Registrační token, který byl generován ve webové konzoli Cyber Protect, jak je popsáno v části Instalace agentů pomocí zásad skupiny (str. 101).

REGISTRATION_LOGIN=<uživatelské jméno>, **REGISTRATION_PASSWORD=**<heslo>

Uživatelské jméno a heslo správce serveru pro správu.

REGISTRATION_TENANT=<ID jednotky>

Jednotka v rámci organizace. Agenti, uzel úložišť a služba katalogu zadané v parametru **ADDLOCAL** se přidají do této jednotky.

Chcete-li získat ID jednotky, ve webové konzoli Cyber Protect klikněte na možnost **Nastavení** > **Účty**, vyberte jednotku a klikněte na **Podrobnosti**.

Tento parametr příkazového řádku nefunguje bez parametru **REGISTRATION_TOKEN**, nebo **REGISTRATION_LOGIN** a **REGISTRATION_PASSWORD**. V takovém případě budou součásti přidány do organizace.

Bez použití tohoto parametru budou součásti přidány do organizace.

REGISTRATION_REQUIRED={0,1}

Výsledek instalace v případě selhání registrace. Pokud je hodnota **1**, instalace se nezdaří. Pokud je hodnota **0**, instalace je dokončena úspěšně i v případě, že součást nebyla zaregistrována.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<hodnota veřejného klíče>

Tyto vzájemně se vylučující parametry definují metodu kontroly certifikátu serveru pro správu během registrace. Certifikát zkontrolujte, chcete-li ověřit autentičnost serveru pro správu, abyste zabránili útokům MITM.

Pokud je hodnota **1**, ověření využívá systémovou certifikační autoritu nebo certifikační autoritu dodávanou spolu s produktem. Je-li zadán připnutý veřejný klíč, ověření tento klíč použije. Pokud je hodnota **0** nebo nejsou parametry zadány, ověření certifikátu se neprovádí, ale registrační provoz zůstane šifrován.

/l*v <soubor protokolu>

Pokud je zadán parametr, uloží se do daného souboru protokol instalace v podrobném režimu. Soubor protokolu lze použít k analýze potíží s instalací.

Parametry instalace serveru pro správu

WEB_SERVER_PORT=<číslo portu>

Port, který webový prohlížeč použije pro přístup k serveru pro správu. Ve výchozím nastavení 9877.

AMS_ZMQ_PORT=<číslo portu>

Port, který se použije ke komunikaci mezi součástmi produktu. Ve výchozím nastavení 7780.

SQL_INSTANCE=<instance>

Databáze, která bude používána serverem pro správu. Můžete zvolit libovolnou verzi Microsoft SQL Serveru 2012, Microsoft SQL Serveru 2014 nebo Microsoft SQL Serveru 2016. Vybranou instanci mohou používat i jiné aplikace.

Bez použití tohoto parametru se použije integrovaná databáze SQLite.

SQL_USER_NAME=<uživatelské jméno> a **SQL_PASSWORD=**<heslo>

Pověření přihlašovacího účtu k serveru Microsoft SQL Server. Server pro správu použije tato pověření pro připojení k vybrané instanci serveru SQL Server. Pokud tyto parametry nejsou k dispozici, použije server pro správu pověření účtu služby serveru pro správu (**AMS User**).

Účet, pod kterým poběží služba serveru pro správu

Zadejte jeden z následujících parametrů:

- **AMS_USE_SYSTEM_ACCOUNT={0,1}**

  Pokud je hodnota **1**, použije se systémový účet.

- **AMS_CREATE_NEW_ACCOUNT={0,1}**
  Pokud je hodnota **1**, vytvoří se nový účet.
- **AMS_SERVICE_USERNAME=**<uživatelské jméno> a **AMS_SERVICE_PASSWORD=**<heslo>
  Použije se zadaný účet.

Parametry instalace agenta

HTTP_PROXY_ADDRESS=<IP adresa> a **HTTP_PROXY_PORT=**<port>

Proxy server HTTP, který použije agent. Bez těchto parametrů se nepoužije žádný proxy server.

HTTP_PROXY_LOGIN=<přihlašovací jméno> a **HTTP_PROXY_PASSWORD=**<heslo>

Přihlašovací údaje k proxy serveru HTTP. Tyto parametry použijte, pokud server vyžaduje ověřování.

HTTP_PROXY_ONLINE_BACKUP={0,1}

Pokud je hodnota **0** nebo pokud parametr není zadán, agent použije proxy server pouze pro zálohování a obnovení pomocí cloudu. Pokud je hodnota **1**, agent se prostřednictvím proxy serveru připojí také k serveru pro správu.

SET_ESX_SERVER={0,1}

Je-li hodnota **0**, nepřipojí se instalovaný Agent pro VMware k serveru vCenter ani k hostiteli ESXi. Po instalaci postupujte podle pokynů v části Konfigurace již zaregistrovaného Agenta pro VMware (str. 47).

Pokud je hodnota **1**, zadejte následující parametry:

ESX_HOST=<název hostitele nebo IP adresa>

Název hostitele nebo IP adresa serveru vCenter nebo hostitele ESXi.

ESX_USER=<uživatelské jméno> a **ESX_PASSWORD=**<heslo>

Pověření pro přístup k serveru vCenter Server nebo hostiteli ESXi.

Účet, pod kterým bude spuštěna služba agenta

Zadejte jeden z následujících parametrů:

- **MMS_USE_SYSTEM_ACCOUNT={0,1}**
  Pokud je hodnota **1**, použije se systémový účet.
- **MMS_CREATE_NEW_ACCOUNT={0,1}**
  Pokud je hodnota **1**, vytvoří se nový účet.
- **MMS_SERVICE_USERNAME=**<uživatelské jméno> a **MMS_SERVICE_PASSWORD=**<heslo>
  Použije se zadaný účet.

Parametry instalace uzlu úložišť

Účet, pod kterým bude spuštěna služba uzlu úložišť

Zadejte jeden z následujících parametrů:

- **ASN_USE_SYSTEM_ACCOUNT={0,1}**
  Pokud je hodnota **1**, použije se systémový účet.
- **ASN_CREATE_NEW_ACCOUNT={0,1}**
  Pokud je hodnota **1**, vytvoří se nový účet.
- **ASN_SERVICE_USERNAME=**<uživatelské jméno> a **ASN_SERVICE_PASSWORD=**<heslo>
  Použije se zadaný účet.

Parametry odinstalace

REMOVE={<seznam součástí>**|ALL}**

Součásti určené k odebrání jsou oddělené čárkami bez mezer.

Dostupné součásti jsou popsány výše v tomto oddílu.

Pokud je hodnota **ALL**, odinstalují se všechny součásti produktu. Dále můžete zadat následující parametr:

DELETE_ALL_SETTINGS={0, 1}

Pokud je hodnota **1**, budou odebrány všechny protokoly, úlohy a nastavení konfigurace daného produktu.

2.6.4.2 Bezobslužná instalace nebo odinstalace v systému Linux

Toto téma popisuje instalaci nebo odinstalaci Acronis Cyber Protect v bezobslužném režimu v počítači se systémem Linux pomocí příkazového řádku.

Jak nainstalovat nebo odinstalovat produkt

1. Otevřete Terminál.
2. Spusťte následující příkaz:

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   V tomto příkazu je <název balíčku> název instalačního balíčku (soubor I686 nebo X86_64).
3. [Pouze v případě instalace Agenta pro Linux] Je-li v počítači povoleno zabezpečené spouštění UEFI, budete informováni, že po instalaci je třeba restartovat systém. Zapamatujte si, které heslo (pro kořenového uživatele nebo uživatele acronis) se má použít. Během restartování systému si zvolte správu MOK, vyberte možnost **Zapsat MOK** a potom klíč zapište pomocí doporučeného hesla.

Pokud po instalaci agenta povolíte zabezpečené spouštění UEFI, opakujte instalaci včetně kroku 3. V opačném případě se zálohování nezdaří.

Parametry instalace

Společné parametry

{-i |--id=}<seznam součástí>

Součásti určené k instalaci jsou oddělené čárkami bez mezer.

Pro instalaci jsou dostupné následující součásti:

Součást	Popis součásti
AcronisCentralizedManagementServer	Server pro správu
BackupAndRecoveryAgent	Agent pro Linux
BackupAndRecoveryBootableComponents	Tvůrce spouštěcích médií

Bez použití tohoto parametru se nainstalují všechny součásti výše.

--language=<ID jazyka>

Jazyk produktu. Dostupné hodnoty jsou následující: **en**, **en_GB**, **cs**, **da**, **de**, **es_ES**, **fr**, **ko**, **it**, **hu**, **nl**, **ja**, **pl**, **pt**, **pt_BR**, **ru**, **tr**, **zh**, **zh_TW**.

{-d|--debug}

Pokud je zadán tento parametr, zapíše se protokol instalace v podrobném režimu. Protokol se nachází v souboru **/var/log/trueimage-setup.log**.

{-t|--strict}

Pokud je zadán tento parametr, způsobí jakékoli upozornění zobrazené v průběhu instalace selhání instalace. Bez použití tohoto parametru se instalace úspěšně dokončí i přes zobrazená upozornění.

{-n|--nodeps}

Pokud je zadán tento parametr, budou v průběhu instalace ignorovány chybějící požadované Linuxové balíky.

Parametry instalace serveru pro správu

{-W |--web-server-port=}<číslo portu>

Port, který webový prohlížeč použije pro přístup k serveru pro správu. Ve výchozím nastavení 9877.

--ams-tcp-port=<číslo portu>

Port, který se použije ke komunikaci mezi součástmi produktu. Ve výchozím nastavení 7780.

Parametry instalace agenta

Zadejte jeden z následujících parametrů:

- **--skip-registration**

  Nezaregistruje agenta na serveru pro správu.

- **{-C |--ams=}**<název hostitele nebo IP adresa>

  Název hostitele nebo IP adresa počítače, ve kterém je server pro správu nainstalovaný. Agent se zaregistruje na tomto serveru pro správu.

  Nainstalujete-li agenta a server pro správu v rámci jednoho příkazu, zaregistruje se agent na tomto serveru pro správu bez ohledu na parametr **-C**.

  Pokud je anonymní registrace na serveru pro správu zakázána (str. 443), musíte zadat buď parametr **token**, nebo parametry **login** a **password**.

  --token=<token>

  Registrační token, který byl generován ve webové konzoli Cyber Protect, jak je popsáno v části Instalace agentů pomocí zásad skupiny (str. 101).

  {-g |--login=}<uživatelské jméno> a **{-w |--password=}**<heslo>

  Pověření správce serveru pro správu.

  --unit=<ID jednotky>

  Jednotka v rámci organizace. Agent bude přidán do této jednotky.

  Chcete-li získat ID jednotky, ve webové konzoli Cyber Protect klikněte na možnost **Nastavení** > **Účty**, vyberte jednotku a klikněte na **Podrobnosti**.

  Bez použití tohoto parametru bude agent přidán do organizace.

  --reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}

  Metoda kontroly certifikátu serveru pro správu během registrace. Certifikát zkontrolujte, chcete-li ověřit autentičnost serveru pro správu, abyste zabránili útokům MITM.

  Pokud je hodnota **https** nebo parametr není zadán, ověření certifikátu se neprovádí, ale registrační provoz zůstane šifrován. Pokud hodnota *není* **https**, ověření využívá systémovou certifikační autoritu nebo certifikační autoritu dodávanou spolu s produktem nebo připnutý veřejný klíč.

  --reg-transport-pinned-public-key=<hodnota veřejného klíče>

Hodnota připíchnutého veřejného klíče. Tento parametr by měl být zadán společně s parametrem **--reg-transport=https-pinned-public-key** nebo místo něj.

- **--http-proxy-host=**<IP adresa> a **--http-proxy-port=**<port>

  Proxy server HTTP, který agent použije pro zálohování a obnovení pomocí cloudu a pro připojení k serveru pro správu. Bez těchto parametrů se nepoužije žádný proxy server.

- **--http-proxy-login=**<přihlašovací jméno> a **--http-proxy-password=**<heslo>

  Přihlašovací údaje k proxy serveru HTTP. Tyto parametry použijte, pokud server vyžaduje ověřování.

Parametry odinstalace

{-u|--uninstall}

Odinstaluje produkt.

--purge

Odebere protokoly, úlohy a nastavení konfigurace daného produktu.

Informační parametry

{-?|--help}

Zobrazí popis parametrů.

--usage

Zobrazí krátký popis použití příkazu.

{-v|--version}

Zobrazí verzi instalačního balíčku.

--product-info

Zobrazí název produktu a verzi instalačního balíčku.

Příklady

- Instalace serveru pro správu.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Instalace serveru pro správu, zadání vlastních portů.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
--web-server-port 6543 --ams-tcp-port 8123
```

- Instalace agenta pro Linux a jeho registrace na určeném serveru pro správu.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams
10.10.1.1 --login root --password 123456
```

- Instalace agenta pro Linux a jeho registrace v dané jednotce na určeném serveru pro správu.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams
10.10.1.1 --login root --password 123456 –unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

2.6.4.3 Bezobslužná instalace nebo odinstalace v systému macOS

Toto téma popisuje instalaci, registraci a odinstalaci agenta Acronis Cyber Protect v bezobslužném režimu v počítači se systémem macOS pomocí příkazového řádku. Informace ohledně stažení instalačního souboru (.dmg) naleznete v tématu Přidání počítače se systémem macOS (p. 45).

Postup instalace Agenta pro Mac

1. Vytvořte dočasný adresář, kam vložíte instalační soubor (.dmg).

   ```
   mkdir <dmg_kořen>
   ```

   <dmg_kořen> je libovolný název.

2. Vložte soubor .dmg.

   ```
   hdiutil attach <dmg_soubor> -mountpoint <dmg_root>
   ```

   <dmg_soubor> je název instalačního souboru. Například **AcronisCyberProtect_15_MAC.dmg**.

3. Spusťte instalační program.

   ```
   sudo installer -pkg <dmg_kořen>/Install.pkg -target LocalSystem
   ```

4. Odpojte instalační soubor (.dmg).

   ```
   hdiutil detach <dmg_kořen>
   ```

Příklady

```
mkdir mydirectory

hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint
mydirectory

sudo installer -pkg mydirectory/Install.pkg -target LocalSystem

hdiutil detach mydirectory
```

Postup registrace Agenta pro Mac

Proveďte jeden z následujících úkonů:

- Zaregistrujte agenta anonymně.

  ```
  sudo
  /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
  ent -o register -a <adresa serveru pro správu:port>
  ```

  Vysvětlení:

  <adresa serveru pro správu:port> je název hostitele nebo IP adresa počítače, kde je server pro správu aplikace Acronis Cyber Protect nainstalován. Číslo portu je povinné, pokud se liší od výchozí hodnoty (9877).

  Tato možnost je k dispozici, pouze pokud je na serveru pro správu povolena anonymní registrace. Pokud je povolena, musíte počítač zaregistrovat v rámci konkrétního účtu správce nebo pomocí registračního tokenu. Další informace o anonymní registraci naleznete v tématu Konfigurace anonymní registrace (p. 443).

- Zaregistrujte agenta v rámci konkrétního účtu správce.

  ```
  sudo
  /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
  ent -o register -a <adresa serveru pro správu:port> -u <uživatelské jméno> -p <heslo>
  ```

  Vysvětlení:

  <uživatelské jméno> a <heslo> jsou pověření pro účet správce, v rámci kterého bude agent zaregistrován.

- Zaregistrujte agenta v konkrétní jednotce.

  ```
  sudo
  /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
  ent -o register -a <adresa serveru pro správu:port> --tenant <ID jednotky>
  ```

  Pokud je anonymní registrace na serveru pro správu zakázána, je třeba přidat pověření pro účet správce:

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -a <adresa serveru pro správu:port> -u <uživatelské jméno> -p <heslo>
--tenant <ID jednotky>
```

Chcete-li získat ID jednotky, ve webové konzoli Cyber Protect klikněte na možnost **Nastavení** > **Účty**, vyberte požadovanou jednotku a klikněte na **Podrobnosti**.

Důležité *Správci můžou zaregistrovat agenty zadáním ID jednotky pouze na své úrovni hierarchie organizace. Správci jednotky můžou zaregistrovat počítače ve svých vlastních jednotkách a podjednotkách. Správci organizace můžou zaregistrovat počítače ve všech jednotkách. Další informace o různých účtech správců naleznete v tématu Správa uživatelských účtů a organizačních jednotek (p. 444).*

- Zaregistrujte agenta pomocí registračního tokenu.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -a <adresa serveru pro správu:port> --token <token>
```

Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Registrační token můžete vygenerovat ve webové konzoli služby Cyber Protect podle popisu v části Nasazení agentů pomocí zásad skupiny (str. 101).

Důležité *V systému macOS 10.14 a novější verzi je třeba agentovi pro ochranu udělit úplný přístup k disku. Přejděte do nabídky* ***Aplikace*** *>****Nástroje*** *a spusťte* ***průvodce agentem Cyber Protect****. Postupujte podle pokynů v okně aplikace.*

Příklady

Registrace pomocí uživatelského jména a hesla.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

Registrace zadáním ID jednotky a pověření správce.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant
4dd941c1-c03f-11ea-86d8-005056bdd3a0
```

Registrace pomocí tokenu.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -a https://10.250.144.179:9877 --token D91D-DC46-4F0B
```

Postup odinstalace Agenta pro Mac

Spusťte následující příkaz:

```
sudo
/Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Unins
tall.app/Contents/MacOS/AgentUninstall /confirm
```

Chcete-li odinstalovat Agenta pro Mac a odebrat všechny protokoly, úlohy a konfigurační nastavení, spusťte následující příkaz:

```
sudo
/Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Unins
tall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

2.6.5 Registrace počítačů ručně

Mimo registrace počítače na serveru pro správu Cyber Protect během instalace agenta můžete počítač zaregistrovat také pomocí rozhraní příkazového řádku. Tento postup může být potřeba, pokud jste nainstalovali agenta, ale automatická registrace například selhala, nebo pokud chcete zaregistrovat existující počítač v rámci nového účtu.

Registrace počítače

Na příkazovém řádku počítače, kde je agent nainstalován, spusťte jeden z následujících příkazů:

- Anonymní registrace počítače:

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
```

  `<cesta k registračnímu nástroji>` je:
  - Windows: **%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe**
  - Linux: **/usr/lib/Acronis/RegisterAgentTool/RegisterAgent**
  - macOS: **/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent**

  `<adresa serveru pro správu:port>` je název hostitele nebo IP adresa počítače, kde je server pro správu aplikace Acronis Cyber Protect nainstalován. Pokud používáte výchozí port 9877, nemusíte ho zadávat explicitně.

  Tato možnost je k dispozici, pouze pokud je na serveru pro správu povolena anonymní registrace. Pokud je povolena, musíte počítač zaregistrovat v rámci konkrétního účtu správce nebo pomocí registračního tokenu. Další informace o anonymní registraci naleznete v tématu Konfigurace anonymní registrace (p. 443).

- Registrace agenta v rámci konkrétního účtu správce:

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
-u <uživatelské jméno> -p <heslo>
```

  `<uživatelské jméno>` a `<heslo>` jsou pověření pro účet správce, v rámci kterého bude agent zaregistrován.

- Chcete-li počítač zaregistrovat v konkrétní jednotce, zadejte ID jednotky:

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
--tenant <ID jednotky>
```

  Chcete-li získat ID jednotky, ve webové konzoli Cyber Protect klikněte na možnost **Nastavení** > **Účty**, vyberte požadovanou jednotku a klikněte na **Podrobnosti**.

  Pokud je anonymní registrace na serveru pro správu zakázána, je třeba přidat pověření pro účet správce:

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
-u <uživatelské jméno> -p <heslo> --tenant <ID jednotky>
```

  Důležité *Správci můžou agenty zaregistrovat pouze na své úrovni hierarchie organizace. Správci jednotky můžou agenty zaregistrovat ve svých vlastních jednotkách a podjednotkách. Správci organizace můžou agenty zaregistrovat ve všech jednotkách. Další informace o různých účtech správců naleznete v tématu Správa uživatelských účtů a organizačních jednotek (p. 444).*

- Registrace agenta pomocí registračního tokenu:

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
--token <token>
```

Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Další informace o vygenerování nového registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny.

Zrušení registrace počítače

Na příkazovém řádku počítače, kde je agent nainstalován, spusťte příkaz:

```
<path to the registration tool> -o unregister
```

Příklady

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877

"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877 -u johndoe -p johnspassword

"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf

"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant
590b1dd7-8adb-11ea-bf44-0050569deecf

"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD

"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877 -u johndoe -p johnspassword

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant
590b1dd7-8adb-11ea-bf44-0050569deecf

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant
590b1dd7-8adb-11ea-bf44-0050569deecf

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Hesla se speciálními znaky nebo mezerami

Pokud vaše heslo obsahuje zvláštní znaky nebo mezery, při zadávání na příkazovém řádku ho napište s uvozovkami.

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

Příklad (Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Pokud se stále zobrazuje chyba:

1. Zakódujte heslo ve formátu base64 na adrese https://www.base64encode.org/ (https://www.base64encode.org - https://www.base64encode.org).
2. Na příkazovém řádku zadejte zakódované heslo pomocí parametru -b nebo --base64.

```
<cesta k registračnímu nástroji> -o register –a <adresa serveru pro správu:port>
-u <uživatelské jméno> -b -p <šifrované heslo>
```

Příklad (Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register –a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

2.6.6 Kontrola dostupných aktualizací

Tyto funkce jsou k dispozici pouze správcům organizace (str. 444).

Po každém přihlášení k webové konzoli Cyber Protect zkontroluje Acronis Cyber Protect na webových stránkách společnosti Acronis, zda je k dispozici nová verze. Pokud je, zobrazí se ve webové konzoli Cyber Protect odkaz ke stažení nové verze v dolní části každé stránky na kartách **Zařízení**, **Plány** a **Úložiště záloh**. Odkaz je také k dispozici na stránce **Nastavení** > **Agenti**.

Chcete-li zapnout nebo vypnout automatickou kontrolu aktualizací, změňte systémové nastavení **Aktualizace** (str. 442).

Chcete-li zkontrolovat aktualizace ručně, klikněte na tlačítko s ikonou otazníku v pravém horním rohu > **O aplikaci** > **Zkontrolovat aktualizace** nebo na ikonu s otazníkem > **Zkontrolovat aktualizace**.

2.6.7 Správa licencí

Licencování produktu Acronis Cyber Protect je založeno na počtu zálohovaných fyzických počítačů a virtualizačních hostitelů. Lze používat předplatné i trvalé licence. Platnost předplatného začíná ve chvíli jeho registrace na webu Acronis.

Abyste mohli začít používat Acronis Cyber Protect, musíte na server pro správu přidat alespoň jeden licenční klíč. Licence je počítači automaticky přiřazena po použití plánu ochrany.

Licenci lze také přiřadit a odejmout ručně. Ruční správa licencí je k dispozici pouze pro správce organizace (str. 444).

Přístup na stránku Licence

1. Proveďte jeden z následujících úkonů:
   - Klikněte na **Nastavení**.
   - V pravém horním rohu klikněte na ikonu účtu.
2. Klikněte na **Licence**.

Postup přidání licenčního klíče

1. Klikněte na **Přidat klíče**.
2. Zadejte licenční klíče.
3. Klikněte na tlačítko **Přidat**.
4. Abyste mohli aktivovat předplatné, musíte být přihlášeni. Pokud jste zadali alespoň jeden klíč předplatného, zadejte e-mailovou adresu a heslo vašeho účtu Acronis a klikněte na **Přihlásit**. Pokud jste zadali jenom trvalé klíče, tento krok přeskočte.
5. Klikněte na tlačítko **Hotovo**.

Tip *Pokud jste už klíče předplatného zaregistrovali, server pro správu je může naimportovat z vašeho účtu Acronis. Chcete-li klíče předplatného synchronizovat, klikněte na* ***Synchronizovat*** *a přihlaste se.*

Správa trvalých licencí

Postup přiřazení trvalé licence počítači

1. Vyberte trvalou licenci.

   Software zobrazí licenční klíče, které odpovídají vybrané licenci.
2. Vyberte klíč k přiřazení.
3. Klikněte na **Přiřadit**.

   Software zobrazí počítače, kterým lze přiřadit vybraný klíč.
4. Vyberte počítač a klikněte na **Hotovo**.

Postup odejmutí trvalé licence z počítače

1. Vyberte trvalou licenci.

   Software zobrazí licenční klíče, které odpovídají vybrané licenci. Počítač, kterému je klíč přiřazen, se zobrazuje ve sloupci **Přiřazeno**.
2. Vyberte licenční klíč k odejmutí.
3. Klikněte na **Odejmout**.
4. Potvrďte své rozhodnutí.

   Odejmutý klíč zůstane v seznamu licenčních klíčů. Je možné ho přiřadit k jinému počítači.

Správa licencí předplatného

Postup přiřazení licence předplatného počítači

1. Vyberte licenci předplatného.
   Software zobrazí počítače, které už mají přiřazenou vybranou licenci.
2. Klikněte na **Přiřadit**.
   Software zobrazí počítače, kterým lze přiřadit vybranou licenci.
3. Vyberte počítač a klikněte na **Hotovo**.

Postup odejmutí licence předplatného z počítače

1. Vyberte licenci předplatného.
   Software zobrazí počítače, které už mají přiřazenou vybranou licenci.
2. Vyberte počítač, kterému chcete licenci odejmout.
3. Klikněte na **Odejmout licenci**.
4. Potvrďte své rozhodnutí.

2.7 Cloudové nasazení

2.7.1 Aktivace účtu

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

- **Odkaz pro aktivaci účtu.** Klikněte na odkaz a nastavte si heslo účtu. Zapamatujte si vaše přihlašovací jméno, který se zobrazuje na stránce aktivace účtu.
- **Odkaz na stránku pro přihlášení k webové konzoli Cyber Protect.** Tento odkaz v budoucnu použijete pro přístup ke konzoli. Přihlašovací jméno a heslo jsou stejné jako v předchozím kroku.

2.7.2 Příprava

Krok 1

Vyberte agenta (podle toho, co se chystáte zálohovat). Informace o agentech najdete v části Součásti (str. 15).

Krok 2

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

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

Pokud chcete instalační programy ukládat lokálně, stáhněte si balíček obsahující všechny agenty pro instalaci ve Windows pomocí odkazu na konci stránky **Přidat zařízení**. Dostupné jsou 32bitové i 64bitové balíčky. Tyto balíčky umožňují přizpůsobení seznamu instalovaných komponent. Je pomocí nich možné také provést bezobslužnou instalaci, například prostřednictvím zásad skupiny. Tento pokročilý scénář je popsán v části Instalace agentů pomocí zásad skupiny (str. 101).

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

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

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

Krok 3

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

- **443** a **8443**: Tyto porty se používají k přístupu k webové konzoli Cyber Protect, k registraci agentů, stahování certifikátů, autorizaci uživatelů a stahování souborů z cloudového úložiště.
- **7770...7800**: Pomocí těchto portů agenti komunikují se serverem pro správu.
- **44445**: Agenti používají tento port pro přenos dat při zálohování a obnově.

Pokud vaše síť používá proxy server, přečtěte si část Nastavení proxy serveru (str. 67), kde zjistíte, zda je nutné tato nastavení konfigurovat v každém počítači, kde je spuštěn agent ochrany.

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

2.7.3 Nastavení proxy serveru

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

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

Poznámka *Aktualizace definic ochrany (p. 105) (antivirové a antimalwarové definice, definice rozšířené detekce, definice posouzení ohrožení zabezpečení a správy oprav) není možné, pokud používáte proxy server.*

V systému Windows

Pokud je proxy server nakonfigurován v systému Windows (**Ovládací panely** > **Možnosti Internetu** > **Připojení**), instalační program přečte nastavení proxy serveru z registru a automaticky je použije. Nastavení proxy serveru můžete také provést během instalace (str. 69) nebo před ní pomocí níže popsaného postupu. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte stejný postup.

Nastavení proxy v systému Windows

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

```
Windows Registry Editor Version 5.00

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

3. Výraz `proxy.company.com` nahraďte názvem hostitele nebo IP adresou vašeho proxy serveru a výraz `000001bb` nahraďte hexadecimální hodnotou čísla portu. Například `000001bb` je port 443.
4. Pokud proxy server vyžaduje ověřování, nahraďte hodnoty `proxy_jméno` a `proxy_heslo` přihlašovacími údaji proxy serveru. Jinak tyto řádky ze souboru odstraňte.

5. Uložte soubor pod názvem **proxy.reg**.
6. Spusťte soubor jako správce.
7. Potvrďte, že chcete upravit registr systému Windows.
8. Pokud agent pro ochranu ještě není nainstalován, je možné ho nainstalovat teď. Jinak proveďte následující úkony k restartu agenta:
   a. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
   b. Klikněte na tlačítko **OK**.
   c. Spusťte následující příkazy:

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

V systému Linux

Spusťte instalační soubor s parametry **--http-proxy-host=**ADRESA **--http-proxy-port=**PORT**--http-proxy-login=**PŘIHLAŠOVACÍ JMÉNO **--http-proxy-password=**HESLO. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte postup popsaný níže.

Nastavení proxy v systému Linux

1. Otevřete soubor **/etc/Acronis/Global.config** v textovém editoru.
2. Proveďte jeden z následujících úkonů:
   - Pokud bylo nastavení serveru proxy zadáno při instalaci agenta, najděte následující část:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADRESA"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"PŘIHLAŠOVACÍ JMÉNO"</value>
    <value name="Password" type="TString">"HESLO"</value>
</key>
```

   - V opačném případě zkopírujte výše uvedené řádky a vložte je do souboru mezi značky **<registry name="Global">...</registry>**.
3. Výraz v části ADRESA nahraďte novým názvem hostitele nebo IP adresou vašeho proxy serveru a výraz PORT nahraďte desítkovou hodnotou čísla portu.
4. Pokud proxy server vyžaduje ověřování, nahraďte PŘIHLAŠOVACÍ JMÉNO a HESLO přihlašovacími údaji serveru proxy. Jinak tyto řádky ze souboru odstraňte.
5. Uložte soubor.
6. Restartujte agenta provedením následujícího příkazu v libovolném adresáři:

```
sudo service acronis_mms restart
```

V systému macOS

Nastavení proxy serveru můžete provést během instalace (str. 69) nebo před ní pomocí níže popsaného postupu. Pokud byste chtěli nastavení proxy serveru změnit po instalaci, použijte stejný postup.

Nastavení proxy v systému macOS

1. Vytvořte soubor **/Library/Application Support/Acronis/Registry/Global.config** a otevřete jej v textovém editoru, například Text Edit.
2. Zkopírujte a vložte do souboru následující řádky:
   <?xml version="1.0" ?>
   <registry name="Global">

```
    <key name="HttpProxy">
      <value name="Enabled" type="Tdword">"1"</value>
      <value name="Host" type="TString">"proxy.firma.com"</value>
      <value name="Port" type="Tdword">"443"</value>
      <value name="Login" type="TString">"proxy_jméno"</value>
      <value name="Password" type="TString">"proxy_heslo"</value>
    </key>
  </registry>
```

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

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

Ve spouštěcím médiu

Při práci ve spouštěcím médiu bude pravděpodobně nutné získat přístup ke cloudovému úložišti přes proxy server. Nastavení proxy serveru zadáte kliknutím na **Nástroje** > **Proxy server** a zadáním názvu hostitele nebo IP adresy, portu a přihlašovacích údajů proxy serveru.

2.7.4 Instalace agentů

Ve Windows

1. Zkontrolujte, že je počítač připojen k internetu.
2. Přihlaste se jako správce a spusťte instalační program.
3. [Volitelné] Klikněte na možnost **Přizpůsobit nastavení instalace** a proveďte příslušné změny, pokud chcete:
   - Změnit součásti k instalaci (zejména vypnutí instalace nástroje Cyber Protect Monitor a nástroje příkazového řádku).
   - Změnit metodu registrace počítače ve službě kybernetické ochrany. Můžete přepnout možnost **Použít konzoli Cyber Protect** (výchozí) na **Použít pověření** nebo **Použít registrační token**.
   - Změnit instalační cestu.
   - Změnit účet pro službu agenta.
   - Ověřit nebo změnit název hostitele nebo IP adresu, port a přihlašovací údaje proxy serveru. Pokud je proxy server povolen ve Windows, automaticky se detekuje a použije.
4. Klikněte na **Instalovat**.
5. [Pouze při instalaci Agenta pro VMware] Zadejte adresu a pověření k přístupu pro server vCenter nebo samostatného hostitele ESXi, jehož virtuální počítače bude agent zálohovat, a potom klikněte na tlačítko **Hotovo**. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.

6. [Pouze při instalaci na řadiči domény] Zadejte uživatelský účet, ve kterém bude služba agenta spuštěna, a potom klikněte na tlačítko **Hotovo**. Z bezpečnostních důvodů instalační program automaticky nevytváří nové účty na řadiči domény.
7. Pokud jste v kroku 3 ponechali výchozí metodu registrace **Použít konzoli Cyber Protect**, počkejte, až se zobrazí registrační obrazovka, a potom přejděte k dalšímu kroku. Jinak nejsou potřeba žádné další akce.
8. Proveďte jeden z následujících úkonů:
   - Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do webové konzole Cyber Protect, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
   - Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

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

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

   Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení k webové konzoli Cyber Protect.

V systému Linux

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

   Pokud je při spuštění souboru v síti zapnutý proxy server, zadejte název hostitele / IP adresu a port serveru v následujícím formátu: **`--http-proxy-host`**=ADRESA **`--http-proxy-port`**=PORT **`--http-proxy-login`**=PŘIHLAŠOVACÍ JMÉNO **`--http-proxy-password`**=HESLO.

   Chcete-li změnit výchozí metodu registrace počítače ve službě kybernetické ochrany, spusťte instalační soubor s jedním z následujících parametrů:
   - **`--register-with-credentials`** – požádá během instalace o uživatelské jméno a heslo
   - **`--token=STRING`** – použije registrační token
   - **`--skip-registration`** – přeskočí registraci
3. Zaškrtněte políčka pro agenty, které chcete nainstalovat. Dostupní jsou následující agenti:
   - **Agent pro Linux**
   - **Agent pro Virtuozzo**

   Agenta pro Virtuozzo nelze instalovat bez Agenta pro Linux.
4. Pokud jste v kroku 2 ponechali výchozí metodu registrace, přejděte k dalšímu kroku. Jinak zadejte uživatelské jméno a heslo pro službu kybernetické ochrany nebo počkejte, až bude počítač zaregistrován pomocí tokenu.
5. Proveďte jeden z následujících úkonů:
   - Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do webové konzole Cyber Protect, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
   - Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V

takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

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

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

Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení k webové konzoli Cyber Protect.

6. Je-li v počítači povoleno zabezpečené spouštění UEFI, budete informováni, že po instalaci je třeba restartovat systém. Zapamatujte si, které heslo (pro kořenového uživatele nebo uživatele acronis) se má použít.

   Poznámka *Během instalace se vygeneruje nový klíč sloužící k podepsání modulu* ***snapapi****, který je zaregistrovaný jako klíč vlastníka počítače (MOK). Restartování je povinné z důvodu zapsání tohoto klíče. Bez zapsání tohoto klíče nebude agent fungovat. Pokud po instalaci agenta povolíte zabezpečené spouštění UEFI, opakujte instalaci včetně kroku 6.*

7. Po dokončení instalace proveďte jeden z následujících úkonů:
   - Pokud jste byli v předchozím kroku vyzváni k restartování systému, klikněte na **Restartovat**.

     Během restartování systému si zvolte správu MOK, vyberte možnost **Zapsat MOK** a potom klíč zapište pomocí hesla doporučeného v předchozím kroku.
   - Jinak klikněte na **Konec**.

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

V systému macOS

1. Zkontrolujte, že je počítač připojen k internetu.
2. Klikněte dvakrát na instalační soubor (.dmg).
3. Počkejte, až operační systém připojí obraz instalačního disku.
4. Klikněte dvakrát na tlačítko **Instalovat**.
5. Pokud je v síti zapnutý proxy server, klikněte na řádku nabídek na položku **Agent pro ochranu**, klikněte na **Nastavení proxy serveru** a zadejte název hostitele / IP adresu, port a přihlašovací údaje proxy serveru.
6. Pokud se zobrazí výzva, zadejte pověření správce.
7. Klikněte na možnost **Pokračovat**.
8. Počkejte, až se zobrazí registrační obrazovka.
9. Proveďte jeden z následujících úkonů:
   - Klikněte na **Zaregistrovat počítač**. V otevřeném okně prohlížeče se přihlaste do webové konzole Cyber Protect, zkontrolujte registrační údaje a potom klikněte na možnost **Potvrdit registraci**.
   - Klikněte na možnost **Zobrazit informace o registraci**. Instalační program zobrazí registrační odkaz a registrační kód. Můžete je zkopírovat a provést registrační kroky na jiném počítači. V takovém případě budete muset zadat registrační kód do registračního formuláře. Registrační kód je platný jednu hodinu.

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

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

Počítač poté bude přiřazen k účtu, který byl použit pro přihlášení k webové konzoli Cyber Protect.

2.7.4.1 Změna přihlašovacího účtu na počítačích se systémem Windows

Na obrazovce **Vybrat komponenty** definujte účet, v rámci kterého budou služby spuštěny, určením možnosti **Účet pro přihlášení ke službě agenta**. Je možné vybrat jednu z následujících možností:

- **Použití uživatelských účtů služby** (výchozí pro službu agenta)

  Uživatelské účty služby jsou systémové účty Windows sloužící k provozu služeb. Výhodou tohoto nastavení je, že zásady zabezpečení domény nemají vliv na uživatelská práva těchto účtů. Ve výchozím nastavení běží agent pod účtem **Místní systém**.
- **Vytvoření nového účtu**

  Název účtu pro agenta bude Agent User.
- **Použití následujícího účtu**

  V případě instalace agenta do řadiče domény vás systém vyzve k zadání existujících účtů (nebo stejného účtu) pro agenta. Z bezpečnostních důvodů systém automaticky nevytváří nové účty na řadiči domény.

Při volbě možnosti **Vytvořit nový účet** nebo **Použít následující účet** zajistěte, aby zásady zabezpečení domény neměly vliv na práva příslušných účtů. Je-li účet zbaven uživatelských práv přidělených během instalace, nemusí daná součást správně fungovat nebo nebude fungovat vůbec.

Oprávnění vyžadovaná pro přihlašovací účet

Agent pro ochranu je spuštěn jako služba Managed Machine Service (MMS) na počítači se systémem Windows. Účet, v rámci kterého bude agent spuštěn, musí mít specifická práva, aby agent pracoval správně. Uživatel služby MMS by měl mít proto přidělena následující práva:

1. Měl by být členem skupin **Backup Operators** a **Administrators**. V řadiči domény musí být uživatel zařazen ve skupině **Správci domény**.
2. Uživatel musí mít oprávnění **Úplné řízení** pro složku **`%PROGRAMDATA%\Acronis`** (v systému Windows XP a Server 2003, **`%ALLUSERSPROFILE%\Application Data\Acronis`**) a její podsložky.
3. Musí mít oprávnění **Úplné řízení** pro určité klíče registru v následujícím klíči: **`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`**.
4. Musí mít následující uživatelská oprávnění:
   - Přihlášení jako služba
   - Nastavení paměťových kvót pro proces
   - Nahrazení tokenu úrovně procesu
   - Úprava hodnot prostředí firmwaru

Postup přidělení uživatelských oprávnění

Podle pokynů níže přidělte uživatelská oprávnění (v tomto příkladu se používá uživatelské oprávnění **Přihlášení jako služba**, kroky jsou stejné i pro jiná uživatelská oprávnění):

1. Přihlaste se k počítači pomocí účtu s oprávněními správce.
2. Na **ovládacím panelu** otevřete nabídku **Nástroje pro správu** (nebo klikněte na možnost Win+R, zadejte **control admintools** a stiskněte Enter) a otevřete nabídku **Místní zásady zabezpečení**.
3. Rozbalte položku **Místní zásady** a klikněte na položku **Přiřazení uživatelských práv.**
4. V pravém podokně klikněte pravým tlačítkem myši na položku **Přihlášení jako služba** a vyberte **Vlastnosti**.

5. Chcete-li přidat nového uživatele, klikněte na položku **Přidat uživatele nebo skupinu…**.
6. V okně pro **výběr uživatelů, počítačů, účtů služby nebo skupin** vyhledejte uživatele, kterého chcete zadat, a klikněte na tlačítko **OK**.
7. Kliknutím na tlačítko **OK** v nabídce **vlastností možnosti Přihlášení jako služba** uložte změny.

***Důležité** Uživatel, kterého přidáváte k uživatelskému oprávnění **Přihlášení jako služba**, nesmí být uveden v zásadě **Zamítnout přihlášení jako služba** v části **Místní zásady zabezpečení**.*

Upozorňujeme, že po dokončení instalace se nedoporučuje ručně měnit přihlašovací účty.

2.7.5 Bezobslužná instalace nebo odinstalace

2.7.5.1 Bezobslužná instalace nebo odinstalace v systému Windows

Toto téma popisuje instalaci nebo odinstalaci agentů pro ochranu v bezobslužném režimu v počítači se systémem Windows pomocí instalační služby systému Windows (program **`msiexec`**). V doméně Active Directory je dalším způsobem provedení bezobslužné instalace použití zásad skupiny, viz Instalace agentů pomocí zásad skupiny (str. 101).

Během instalace můžete použít soubor označovaný jako **transformace** (soubor MST). Transformace je soubor s parametry instalace. Případně můžete parametry instalace zadat přímo na příkazovém řádku.

Vytvoření souboru transformace MST a extrahování instalačních balíčků

1. Přihlaste se jako správce a spusťte instalační program.
2. Klikněte na možnost **Vytvořit soubory MST a MSI pro bezobslužnou instalaci**.
3. V části **Co je nutno nainstalovat** vyberte požadované součásti. Instalační balíčky těchto součástí se extrahují z instalačního programu.
4. V nabídce **Nastavení registrace** vyberte položku **Použít pověření** nebo **Použít registrační token**. Další informace o vygenerování registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny.
5. Zkontrolujte nebo upravte další nastavení instalace, která se přidají do souboru MST.
6. Klikněte na tlačítko **Pokračovat** a vyberte složku, kde bude vygenerován soubor transformace .mst a budou extrahovány instalační balíčky .msi a .cab.
7. Klikněte na možnost **Generovat**.

Instalace produktu pomocí transformace MST

Na příkazovém řádku spusťte následující příkaz.

Šablona příkazu:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Vysvětlení:

- `<název balíčku>` je název souboru MSI.
- `<název transformace>` je název transformace.

Příklad příkazu:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

Instalace nebo odinstalace produktu ručním zadáním parametrů

Na příkazovém řádku spusťte následující příkaz.

Šablona příkazu (instalace):

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

V této části je `<název balíčku>` název souboru MSI. Všechny dostupné parametry a jejich hodnoty jsou popsány v tématu Parametry bezobslužné instalace nebo odinstalace (p. 74).

Šablona příkazu (odinstalace):

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Balíček .msi musí mít stejnou verzi jako produkt, který chcete nainstalovat.

Parametry bezobslužné instalace nebo odinstalace

Tato část popisuje parametry použité během bezobslužné instalace nebo odinstalace v systému Windows. Kromě těchto parametrů můžete využít další parametry procesu **`msiexec`**, jak je uvedeno v části https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parametry instalace

Základní parametry

`ADDLOCAL=``<seznam součástí>`

Součásti určené k instalaci jsou oddělené čárkami bez mezer. Všechny určené součásti se musí před instalací extrahovat z instalačního programu.

Následuje úplný seznam součástí:

Součást	Nutno instalovat společně s	Bitová architektura	Název součásti a popis
MmsMspComponents		32bitová nebo 64bitová	Klíčové součásti pro agenty
BackupAndRecoveryAgent	MmsMspComponents	32bitová nebo 64bitová	Agent pro Windows
ArxAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro SQL
ARADAgentFeature	BackupAndRecoveryAgent	32bitová nebo 64bitová	Agent pro Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32bitová nebo 64bitová	Agent pro Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32bitová nebo	Agent pro Oracle

Součást	Nutno instalovat společně s	Bitová architektura	Název součásti a popis
		64bitová	
AcronisESXSupport	MmsMspComponents	64bitový	Agent pro VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32bitová nebo 64bitová	Agent pro Hyper-V
CommandLineTool		32bitová nebo 64bitová	Nástroj příkazového řádku
TrayMonitor	BackupAndRecoveryAgent	32bitová nebo 64bitová	Sledování kybernetické ochrany

TARGETDIR=`<cesta>`

Složku, kam se produkt nainstaluje. Ve výchozím nastavení se jedná o následující složku: `C:\Program Files\BackupClient`.

REBOOT=ReallySuppress

Pokud je zadaný tento parametr, je zakázané restartování počítače.

/l*v `<soubor protokolu>`

Pokud je zadán parametr, uloží se do daného souboru protokol instalace v podrobném režimu. Soubor protokolu lze použít k analýze potíží s instalací.

CURRENT_LANGUAGE=`<ID jazyka>`

Jazyk produktu. Dostupné hodnoty jsou následující: **en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.** Pokud tento parametr není zadán, bude jazyk produktu definován na základě vašeho systémového jazyka, pokud se nachází v seznamu výše. V opačném případě bude jazyk produktu nastaven na angličtinu (**en**).

Parametry registrace

REGISTRATION_ADDRESS

Toto je adresa URL pro službu Cyber Protect. Tento parametr můžete použít buď s parametry **REGISTRATION_LOGIN** a **REGISTRATION_PASSWORD** , nebo s parametrem **REGISTRATION_TOKEN** .

- Pokud **REGISTRATION_ADDRESS** použijete s parametry **REGISTRATION_LOGIN** a **REGISTRATION_PASSWORD** , zadejte adresu, kterou používáte **pro přihlášení** ke službě Cyber Protect. Například `https://cloud.company.com`:

- Pokud **REGISTRATION_ADDRESS** použijete s parametrem **REGISTRATION_TOKEN** , zadejte přesnou adresu datového centra. Toto je adresa URL, která se zobrazí **po přihlášení ke službě** Cyber Protect. Například `https://eu2-cloud.company.com`.

V tomto případě nepoužívejte `https://cloud.company.com`.

REGISTRATION_LOGIN a **REGISTRATION_PASSWORD**

Pověření pro účet, v rámci kterého bude zaregistrován agent ve službě Cyber Protect. Nesmí se jednat o partnerský účet správce.

REGISTRATION_PASSWORD_ENCODED

Heslo pro účet, v rámci kterého bude zaregistrován agent ve službě Cyber Protect, kódovaný ve formátu base64. Další informace k šifrování hesla naleznete v tématu Ruční registrace počítačů (p. 84).

REGISTRATION_TOKEN

Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Registrační token můžete vygenerovat ve webové konzoli podle popisu v části Nasazení agentů pomocí zásad skupiny (str. 101).

REGISTRATION_REQUIRED={0,1}

Definuje, jak bude instalace dokončena, pokud se registrace nezdaří. Pokud je hodnota **1**, , instalace se také nezdaří. Výchozí hodnota je **0**, takže pokud tento parametr nezadáte, instalace se dokončí úspěšně, i když agent není zaregistrován.

Další parametry

K definování přihlašovacího účtu pro službu agenta v systému Windows použijte jeden z následujících parametrů:

- **MMS_USE_SYSTEM_ACCOUNT={0,1}**

  Pokud je hodnota **1**, bude agent běžet v rámci účtu **Local System**.
- **MMS_CREATE_NEW_ACCOUNT={0,1}**

  Pokud je hodnota **1**, bude agent běžet v rámci nově vytvořeného účtu pojmenovaného **Acronis Agent User**.
- **MMS_SERVICE_USERNAME=**<uživatelské jméno> a **MMS_SERVICE_PASSWORD=**<heslo>

  Pomocí těchto parametrů zadejte existující účet, v rámci kterého bude agent běžet.

Další informace o přihlašovacích účtech naleznete v tématu Změna přihlašovacího účtu na počítačích se systémem Windows.

SET_ESX_SERVER={0,1}

Je-li hodnota **0**, nepřipojí se instalovaný Agent pro VMware k serveru vCenter ani k hostiteli ESXi. Pokud je hodnota **1**, zadejte následující parametry:

- **ESX_HOST=**<název hostitele>

  Název hostitele nebo IP adresa serveru vCenter nebo hostitele ESXi.
- **ESX_USER=**<uživatelské jméno> a **ESX_PASSWORD=**<heslo>

  Pověření pro přístup k serveru vCenter Server nebo hostiteli ESXi.

HTTP_PROXY_ADDRESS=<IP adresa> a **HTTP_PROXY_PORT=**<port>

Proxy server HTTP, který použije agent. Bez těchto parametrů se nepoužije žádný proxy server.

HTTP_PROXY_LOGIN=<přihlašovací jméno> a **HTTP_PROXY_PASSWORD=**<heslo>

Přihlašovací údaje k proxy serveru HTTP. Tyto parametry použijte, pokud server vyžaduje ověřování.

HTTP_PROXY_ONLINE_BACKUP={0,1}

Pokud je hodnota **0** nebo pokud parametr není zadán, agent použije proxy server pouze pro zálohování a obnovení pomocí cloudu. Pokud je hodnota **1**, agent se prostřednictvím proxy serveru připojí také k serveru pro správu.

Parametry odinstalace

REMOVE={<seznam součástí>**|ALL}**

Součásti určené k odebrání jsou oddělené čárkami bez mezer. Pokud je hodnota **ALL**, odinstalují se všechny součásti produktu.

Dále můžete zadat následující parametr:

DELETE_ALL_SETTINGS={0, 1}

Pokud je hodnota **1**, budou odebrány všechny protokoly, úlohy a nastavení konfigurace daného produktu.

Příklady

- Instalace Agenta pro Windows, nástroje příkazového řádku a nástroje Sledování kybernetické ochrany. Registrace zařízení do služby Cyber Protect zadáním uživatelského jména a hesla.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Instalace Agenta pro Windows, nástroje příkazového řádku a nástroje Sledování kybernetické ochrany. Vytvoření nového přihlašovacího účtu pro službu agenta v systému Windows. Registrace počítače do služby Cyber Protect pomocí tokenu.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress
MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C
```

- Instalace Agenta pro Windows, nástroje příkazového řádku, Agenta pro Oracle a nástroje Sledování kybernetické ochrany. Registrace počítače do služby Cyber Protect zadáním uživatelského jména a hesla kódovaného ve formátu base64.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFea
ture,TrayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress
CURRENT_LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1
REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Instalace Agenta pro Windows, nástroje příkazového řádku a nástroje Sledování kybernetické ochrany. Registrace počítače do služby Cyber Protect pomocí tokenu. Nastavení proxy serveru HTTP.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress
CURRENT_LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1
REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C
HTTP_PROXY_ADDRESS=https://my-proxy.company.com HTTP_PROXY_PORT=80
HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- Odinstalace všech agentů a odstranění jejich protokolů, úloh a konfiguračních nastavení.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL
DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress
```

2.7.5.2 Bezobslužná instalace nebo odinstalace v systému Linux

Toto téma popisuje instalaci nebo odinstalaci agentů pro ochranu v bezobslužném režimu v počítači se systémem Linux pomocí příkazového řádku.

Jak nainstalovat nebo odinstalovat agenta pro ochranu

1. Otevřete Terminál.

2. Proveďte jeden z následujících úkonů:

- Chcete-li zahájit instalaci zadáním parametrů na příkazovém řádku, spusťte následující příkaz:

```
<package name> -a <parameter 1> ... <parameter N>
```

  V tomto příkazu je `<název balíčku>` název instalačního balíčku (soubor I686 nebo X86_64). Všechny dostupné parametry a jejich hodnoty jsou popsány v tématu Parametry bezobslužné instalace nebo odinstalace (p. 79).

- Chcete-li zahájit instalaci s parametry zadanými v odděleném textovém souboru, spusťte následující příkaz:

```
<package name> -a --options-file=<path to the file>
```

  Tento přístup může být užitečný v případě, že na příkazovém řádku nechcete zadávat citlivé informace. V takovém případě můžete zadat konfigurační nastavení do odděleného textového souboru a zajistit, že k němu budete mít přístup pouze vy. Každý parametr zadejte na nový řádek a za ním zadejte požadovanou hodnotu, například:

```
--rain=https://cloud.company.com
--login=johndoe
--password=johnspassword
--auto
```

  nebo

```
-C
https://cloud.company.com
-g
johndoe
-w
johnspassword
-a
--language
en
```

  Pokud je stejný parametr zadán na příkazovém řádku i v textovém souboru, má přednost hodnota na příkazovém řádku.

3. Je-li v počítači povoleno zabezpečené spouštění UEFI, budete informováni, že po instalaci je třeba restartovat systém. Zapamatujte si, které heslo (pro kořenového uživatele nebo uživatele acronis) se

má použít. Během restartování systému si zvolte správu MOK, vyberte možnost **Zapsat MOK** a potom klíč zapište pomocí doporučeného hesla.

Pokud po instalaci agenta povolíte zabezpečené spouštění UEFI, opakujte instalaci včetně kroku 3. V opačném případě se zálohování nezdaří.

Parametry bezobslužné instalace nebo odinstalace

Tato část popisuje parametry použité během bezobslužné instalace nebo odinstalace v systému Linux.

Minimální konfigurace pro bezobslužnou instalaci zahrnuje **-a** a registrační parametry (například parametry **--login** a **--password** a parametry **--rain** a **--token**). Instalaci můžete přizpůsobit zadáním více parametrů.

Parametry instalace

Základní parametry

{-i |--id=}<seznam součástí>

Součásti určené k instalaci jsou oddělené čárkami bez mezer. V instalačním balíčku .x86_64 jsou k dispozici následující součásti:

Součást	Popis součásti
BackupAndRecoveryAgent	Agent pro Linux
AgentForPCS	Agent pro Virtuozzo
OracleAgentFeature	Agent pro Oracle

Bez použití tohoto parametru se nainstalují všechny součásti výše.

Agent pro Virtuozzo i Agent pro Oracle vyžadují, aby byl zároveň nainstalován Agent pro Linux.

Instalační balíček .i686 zahrnuje pouze BackupAndRecoveryAgent.

{-a|--auto}

Instalace a registrace se dokončí bez dalšího zásahu uživatele. Pokud používáte tento parametr, musíte zadat účet, v rámci kterého bude agent registrován ve službě Cyber Protect, a to buď pomocí parametru **--token**, nebo parametrů **--login** a **--password**.

{-t|--strict}

Je-li parametr zadán, způsobí každé varování vygenerované během instalace selhání instalace. Bez použití tohoto parametru se instalace úspěšně dokončí i přes zobrazená upozornění.

{-n|--nodeps}

V průběhu instalace budou ignorovány chybějící požadované linuxové balíky.

{-d|--debug}

Zapíše protokol instalace v podrobném režimu.

--options-file=<umístění>

Instalační parametry budou přečteny z textového souboru namísto z příkazového řádku.

--language=<ID jazyka>

Jazyk produktu. Dostupné hodnoty jsou následující: **en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW**.

Pokud tento parametr není zadán, bude jazyk produktu definován na základě vašeho systémového jazyka, pokud se nachází v seznamu výše. V opačném případě bude jazyk produktu nastaven na angličtinu (**en**).

Parametry registrace

Zadejte jeden z následujících parametrů:

- **{-g|--login=}**<uživatelské jméno> a **{-w|--password=}**<heslo>

  Pověření pro účet, v rámci kterého bude zaregistrován agent ve službě Cyber Protect. Nesmí se jednat o partnerský účet správce.

- **--token=**<token>

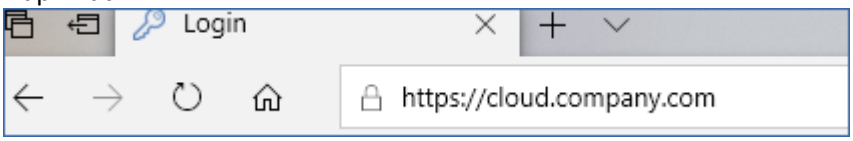
  Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Registrační token můžete vygenerovat ve webové konzoli podle popisu v části Nasazení agentů pomocí zásad skupiny (str. 101).

  Parametr **--token** nelze použít společně s parametry **--login**, **--password** a **--register-with-credentials**.

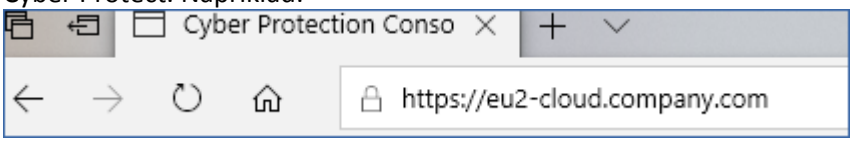
  - **{-C|--rain=}**<adresa služby>

    Adresa URL služby Cyber Protect.

    Pokud k registraci používáte parametry **--login** a **--password**, nemusíte explicitně zadávat tento parametr, protože instalační program využívá ve výchozím nastavení správnou adresu – jedná se o adresu, kterou používáte pro **přihlášení** ke službě Cyber Protect. Například:

    Pokud však parametr **{-C|--rain=}** použijete s parametrem **--token**, musíte zadat přesnou adresu datového centra. Toto je adresa URL, která se zobrazí **po přihlášení ke službě** Cyber Protect. Například:

- **--register-with-credentials**

  Pokud je parametr zadán, spustí se grafické rozhraní instalačního programu. K dokončení registrace zadejte uživatelské jméno a heslo pro účet, v rámci kterého bude agent zaregistrován ve službě Cyber Protect. Nesmí se jednat o partnerský účet správce.

- **--skip-registration**

  Tento parametr použijte, pokud potřebujete nainstalovat agenta, ale chcete ho ve službě Cyber Protect zaregistrovat později. Pokyny k provedení tohoto postupu naleznete v tématu Ruční registrace počítačů (p. 84).

Další parametry

--http-proxy-host=<IP adresa> a **--http-proxy-port=**<port>

Proxy server HTTP, který agent použije pro zálohování a obnovení pomocí cloudu a pro připojení k serveru pro správu. Bez těchto parametrů se nepoužije žádný proxy server.

--http-proxy-login=<přihlašovací jméno> a **--http-proxy-password=**<heslo>

Přihlašovací údaje k proxy serveru HTTP. Tyto parametry použijte, pokud server vyžaduje ověřování.

--tmp-dir=<umístění>

Určuje složku, do které jsou během instalace uloženy dočasné soubory. Výchozí složka je **/var/tmp**.

{-s|--disable-native-shared}

Během instalace budou použity knihovny pro opětovnou distribuci, i když ve vašem systému už mohou být obsaženy.

--skip-prereq-check

Nebude provedena kontrola, zda jsou již nainstalovány balíčky vyžadované pro kompilaci modulu snapapi.

--force-weak-snapapi

Instalační program neprovede kompilaci modulu snapapi. Namísto toho použije připravený modul, který nemusí přesně odpovídat linuxovému jádru. Použití této možnosti nedoporučujeme.

--skip-svc-start

Služby nebudou po instalaci automaticky spuštěny. Tento parametr se nejčastěji používá s parametrem **--skip-registration**.

Informační parametry

{-?|--help}

Zobrazí popis parametrů.

--usage

Zobrazí krátký popis použití příkazu.

{-v|--version}

Zobrazí verzi instalačního balíčku.

--product-info

Zobrazí název produktu a verzi instalačního balíčku.

--snapapi-list

Zobrazí dostupné připravené moduly snapapi.

--components-list

Zobrazí nainstalované součásti.

Parametry pro starší funkce

Tyto parametry se týkají starší součásti agent.exe.

{-e|--ssl=}<cesta>

Udává cestu k vlastnímu certifikačnímu souboru pro komunikaci s využitím SSL.

{-p|--port=}<port>

Udává port, na kterém soubor agent.exe naslouchá pro připojení. Výchozí port je 9876.

Parametry odinstalace

{-u|--uninstall}

Odinstaluje produkt.

--purge

Odinstaluje produkt a odstraní jeho protokoly, úlohy a konfigurační nastavení. Pokud použijete parametr **--purge**, nemusíte explicitně zadávat parametr **--uninstall**.

Příklady

- Instalace Agenta pro Linux bez registrace.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a
--skip-registration
```

- Instalace Agenta pro Linux, Agenta pro Virtuozzo a Agenta pro Oracle a jejich registrace pomocí pověření.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe
--password=johnspassword
```

- Instalace Agenta pro Oracle a Agenta pro Linux a jejich registrace pomocí registračního tokenu.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i
BackupAndRecoveryAgent,OracleAgentFeature -a
--rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- Instalace Agenta pro Linux, Agenta pro Virtuozzo a Agenta pro Oracle s konfiguračním nastavením v samostatném textovém souboru.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a
--options-file=/home/mydirectory/configuration_file
```

- Odinstalace Agenta pro Linux, Agenta pro Virtuozzo a Agenta pro Oracle a odstranění všech jejich protokolů, úloh a konfiguračních nastavení.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

2.7.5.3 Bezobslužná instalace a odinstalace v macOS

Toto téma popisuje instalaci, registraci a odinstalaci agenta Acronis Cyber Protect v bezobslužném režimu v počítači se systémem macOS pomocí příkazového řádku. Informace ohledně stažení instalačního souboru (.dmg) naleznete v tématu Přidání počítače se systémem macOS (p. 45).

Postup instalace Agenta pro Mac

1. Vytvořte dočasný adresář, kam vložíte instalační soubor (.dmg).

```
mkdir <dmg_kořen>
```

<dmg_kořen> je libovolný název.

2. Vložte soubor .dmg.

```
hdiutil attach <dmg_soubor> -mountpoint <dmg_root>
```

<dmg_soubor> je název instalačního souboru. Například **AcronisAgentMspMacOSX64.dmg**.

3. Spusťte instalační program.

```
sudo installer -pkg <dmg_kořen>/Install.pkg -target LocalSystem
```

4. Odpojte instalační soubor (.dmg).

```
hdiutil detach <dmg_kořen>
```

Příklady

```
mkdir mydirectory
hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
hdiutil detach mydirectory
```

Postup registrace Agenta pro Mac

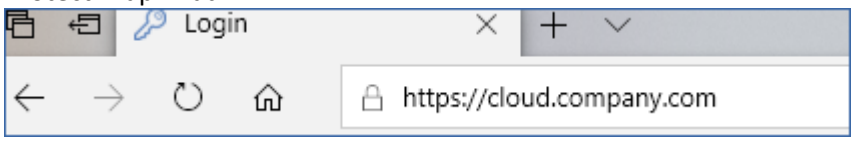
Proveďte jeden z následujících úkonů:

- Registrace agenta v rámci konkrétního účtu zadáním uživatelského jména a hesla.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -t cloud -a <adresa služby> -u <uživatelské jméno> -p <heslo>
```

  Vysvětlení:

  `<adresa služby Cyber Protect>` je adresa, kterou používáte **pro přihlášení** ke službě Cyber Protect. Například:



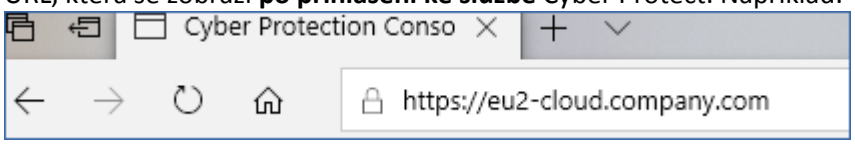
  `<uživatelské jméno>` a `<heslo>` jsou pověření pro účet, v rámci kterého bude agent zaregistrován. Nesmí se jednat o partnerský účet správce.

- Zaregistrujte agenta pomocí registračního tokenu.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -t cloud -a <adresa služby> --token <token>
```

  Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Registrační token můžete vygenerovat ve webové konzoli služby Cyber Protect podle popisu v části Nasazení agentů pomocí zásad skupiny (str. 101).

  Při použití registračního tokenu musíte zadat přesnou adresu datového centra. Toto je adresa URL, která se zobrazí **po přihlášení ke službě** Cyber Protect. Například:



Důležité *Pokud používáte macOS 10.14 nebo novější verzi, udělte agentovi pro ochranu úplný přístup k disku. Přejděte do nabídky* ***Aplikace*** *>****Nástroje*** *a spusťte* ***průvodce agentem Cyber Protect****. Postupujte podle pokynů v okně aplikace.*

Příklady

Registrace pomocí uživatelského jména a hesla.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Registrace pomocí tokenu.

```
sudo
/Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAg
ent -o register -t cloud -a https://eu2-cloud company.com --token D91D-DC46-4F0B
```

Postup odinstalace Agenta pro Mac

Spusťte následující příkaz:

```
sudo
/Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Unins
tall.app/Contents/MacOS/AgentUninstall /confirm
```

Chcete-li během odinstalace odebrat všechny protokoly, úlohy a konfigurační nastavení, spusťte následující příkaz:

```
sudo
/Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Unins
tall.app/Contents/MacOS/AgentUninstall /confirm /purge
```

2.7.6 Registrace počítačů ručně

Mimo registrace počítače ve službě Cyber Protect během instalace agenta můžete počítač zaregistrovat také pomocí rozhraní příkazového řádku. Tento postup může být potřeba, pokud jste nainstalovali agenta, ale automatická registrace například selhala, nebo pokud chcete zaregistrovat existující počítač v rámci nového účtu.

Registrace počítače

Na příkazovém řádku počítače, kde je agent nainstalován, spusťte jeden z následujících příkazů:

- Registrace počítače v rámci aktuálního účtu:

  ```
  <cesta k registračnímu nástroji> -o register -s mms -t cloud --update
  ```

  `<cesta k registračnímu nástroji>` je:

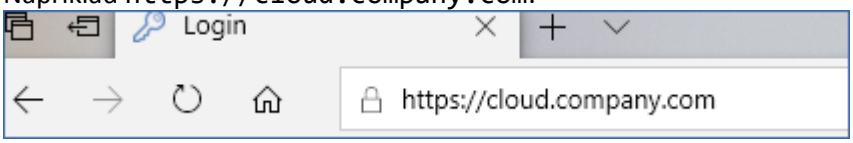
  - Windows: **%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe**
  - Linux: **/usr/lib/Acronis/RegisterAgentTool/RegisterAgent**
  - macOS: **/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent**

- Registrace počítače v rámci jiného účtu:

  ```
  <cesta k registračnímu nástroji> -o register -t cloud –a <adresa služby> -u
  <uživatelské jméno> -p <heslo>
  ```

  `<uživatelské jméno>` a `<heslo>` jsou pověření pro konkrétní účet, v rámci kterého bude agent zaregistrován. Nesmí se jednat o partnerský účet správce.

  `<adresa služby>` je adresa URL, kterou používáte **pro přihlášení** ke službě Cyber Protect. Například `https://cloud.company.com`.

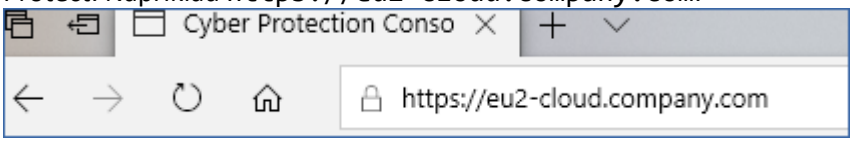
- Registrace počítače pomocí registračního tokenu:

  ```
  <cesta k registračnímu nástroji> -o register -t cloud -a <adresa služby> --token
  <token>
  ```

  Registrační token je řada 12 znaků oddělených spojovníky ve třech segmentech. Další informace o vygenerování nového registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny (str. 101).

  Při použití registračního tokenu musíte jako hodnotu `<adresa služby>` zadat přesnou adresu datového centra. Toto je adresa URL, která se zobrazí **po přihlášení ke službě** Cyber

Protect. Například `https://eu2-cloud.company.com`.



V tomto případě nepoužívejte `https://cloud.company.com`.

Zrušení registrace počítače

Na příkazovém řádku počítače, kde je agent nainstalován, spusťte příkaz:

```
<path to the registration tool> -o unregister
```

Příklady

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms
-t cloud --update

"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud –a https://cloud.company.com -u johndoe -p johnspassword

"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://au1-cloud.company.com --token 3B4C-E967-4FBD

"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud
--update

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register –t cloud –a
https://cloud.company.com -u johndoe -p johnspassword

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C

sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t
cloud --update

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud –a
https://cloud.company.com -u johndoe -p johnspassword

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://us5-cloud.company.com --token 9DBF-3DA9-4DAB

sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

Hesla se speciálními znaky nebo mezerami

Pokud vaše heslo obsahuje zvláštní znaky nebo mezery, při zadávání na příkazovém řádku ho napište s uvozovkami.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

Příklad (Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud –a https://cloud.company.com -u johndoe -p "johns password"
```

Pokud se stále zobrazuje chyba:

- Zakódujte heslo ve formátu base64 na adrese https://www.base64encode.org/ (https://www.base64encode.org - https://www.base64encode.org).
- Na příkazovém řádku zadejte zakódované heslo pomocí parametru -b nebo --base64.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

Příklad (Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud –a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

2.8 Automatické zjišťování počítačů

Funkce zjišťování počítačů umožňuje provádět následující operace:

- Automatizace procesu instalace agenta pro ochranu a registrace počítače automatickým zjištěním počítačů ve vaší doméně Active Directory (AD) nebo místní síti.
- Instalace a aktualizace agenta pro ochranu na skupině počítačů.
- Použití synchronizace se službou Active Directory k omezení úsilí a administrativních nákladů na zajišťování zdrojů a správu počítačů ve velkém prostředí AD.

Důležité *Zjišťování počítačů lze provádět pouze s použitím agentů nainstalovaných na počítačích se systémem Windows. Momentálně dokáže agent pro zjišťování detekovat i počítače s jiným systémem, než je Windows, ale vzdálená instalace softwaru je možná pouze na počítačích se systémem Windows.*
Pokud ve vašem prostředí neexistuje žádný počítač s nainstalovaným agentem, bude funkce automatického zjišťování skrytá – část ***Více zařízení*** *bude v průvodci* ***Přidat nové zařízení*** *skrytá.*

Po přidání do webové konzole jsou počítače kategorizovány následovně:

- **Zjištěno** – počítače, které byly zjištěny, ale není na nich nainstalován agent pro ochranu.
- **Spravováno** – počítače, na kterých je nainstalován agent pro ochranu.
- **Nechráněno** – počítače, na které není plán ochrany použit. Nechráněné počítače zahrnují zjištěné i spravované počítače bez použitého plánu ochrany.
- **Chráněno** – počítače, na které je plán ochrany použit.

Jak to funguje

Během kontroly místní sítě používá agent pro zjišťování následující technologie: Zjišťování NetBIOS, Web Service Discovery (WSD) a tabulku Address Resolution Protocol (ARP). Agent se pro každý počítač pokusí získat následující parametry:

- Název (krátký / název hostitele NetBIOS)
- FQDN
- Doména / pracovní skupina
- Adresy IPv4/IPv6

- Adresy MAC
- Operační systém (název/verze/skupina)
- Kategorie počítače (pracovní stanice / server / řadič domény)

Při kontrole Active Directory agent načte také parametr organizační jednotky (OU) a podrobnější informace o názvu a operačním systému. Nenačte IP adresu a informace o adrese MAC.

Předpoklady

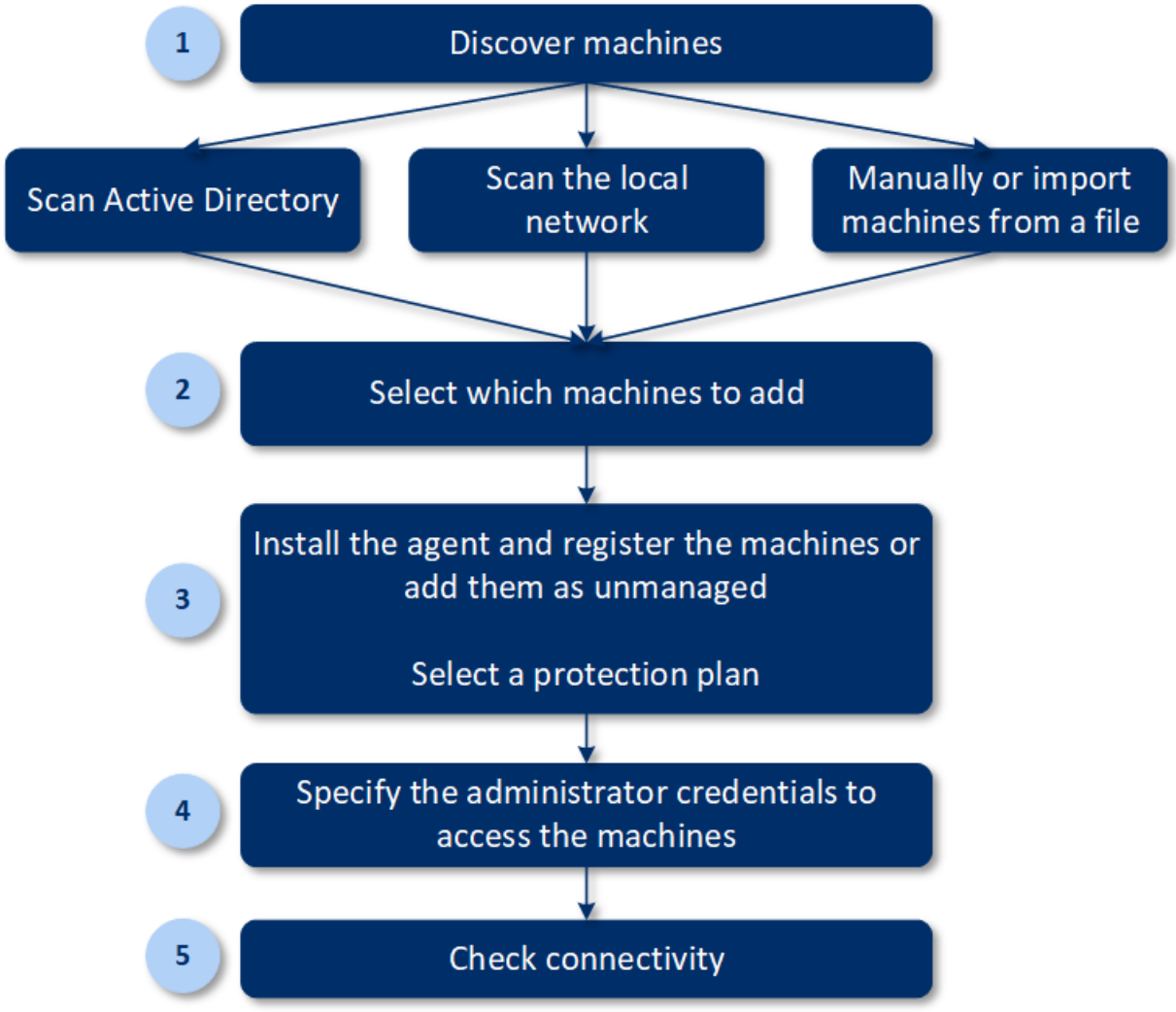
Před zjištěním počítačů musíte alespoň na jednom počítači v místní síti nainstalovat agenta pro ochranu (str. 69), aby ho bylo možné použít jako agenta pro zjišťování.

Pokud plánujete zjišťovat počítače v doméně Active Directory, musíte agenta nainstalovat alespoň na jednom počítači v této doméně. Tento agent bude během kontroly služby Active Directory použit jako agent pro zjišťování.

Počítač se serverem Windows Server 2012 R2 vyžaduje pro úspěšnou vzdálenou instalaci agenta pro ochranu instalaci aktualizace KB2999226.

Proces zjišťování počítače

Na následujícím schématu vidíte hlavní kroky procesu zjišťování počítače:



Celý proces automatického zjišťování obecně zahrnuje následující kroky:

1. Vyberte metodu zjištění počítačů:
   - Kontrola služby Active Directory
   - Kontrola místní sítě
   - Ruční – přidání počítače podle IP adresy nebo názvu hostitele nebo import seznamu počítačů ze souboru.
2. Počítače, které chcete přidat, vyberte ze seznamu získaného v rámci předchozího kroku.
3. Vyberte způsob přidání počítačů:
   - Na počítačích bude nainstalován agent pro ochranu a další komponenty a budou také zaregistrovány ve webové konzoli.
   - Počítače budou zaregistrovány ve webové konzoli (pokud již mají nainstalovaného agenta).
   - Počítače budou do webové konzole přidány jako **Nespravované počítače** bez instalace agenta a komponent.

   Pokud jste vybrali jeden z prvních dvou způsobů, můžete také vybrat plán ochrany z existujících plánů a použít ho na počítače.
4. Na vybraných počítačích zadejte pověření uživatele s právy správce.
5. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

   Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.
6. Zkontrolujte, zda se s pomocí zadaných přihlašovacích údajů můžete k počítačům připojit.

V následujících tématech naleznete podrobnější informace o postupu zjišťování.

2.8.1 Automatické zjišťování a ruční zjišťování

Před zahájením zjišťování ověřte, zda jsou splněny předpoklady (str. 86).

Zjišťování počítačů

1. Ve webové konzoli přejděte do nabídky **Zařízení** > **Všechna zařízení**.
2. Klikněte na tlačítko **Přidat**.
3. V nabídce **Více zařízení** klikněte na tlačítko **Pouze Windows**. Otevře se průvodce zjišťováním.
4. [Pokud vaše organizace zahrnuje jednotky] Vyberte jednotku. V nabídce **Agent pro zjišťování** pak budete moct vybrat agenty spojené s vybranou jednotkou a jejími podřízenými jednotkami.
5. Vyberte agenta pro zjišťování, který provede kontrolu za účelem zjištění počítačů.
6. Vyberte metodu zjišťování:
   - **Hledat ve službě Active Directory**. Ověřte, zda je počítač s agentem pro zjišťování členem domény Active Directory.
   - **Kontrola místní sítě**. Pokud vybraný agent pro zjišťování nenalezl žádné počítače, vyberte jiného agenta pro zjišťování.
   - **Zadat ručně nebo importovat ze souboru**. Ručně definujte počítače, které budou přidány, nebo je importujte z textového souboru.
7. [Pokud je vybrána metoda zjišťování Active Directory] Vyberte způsob vyhledání počítačů:
   - **V seznamu organizačních jednotek**. Vyberte skupinu počítačů, kterou chcete přidat.
   - **Podle dotazu dialektu LDAP**. K výběru počítačů vyberte dotaz Dialekt LDAP. **Výchozí bod hledání** definuje, kde se má hledat, zatímco možnost **Filtr** umožňuje zadat kritéria výběru počítače.

8. [Pokud je vybrána metoda zjišťování Active Directory nebo metoda místní sítě] Pomocí seznamu vyberte počítače, které chcete přidat.

   [Pokud je vybrána ruční metoda zjišťování] Zadejte IP adresy nebo názvy hostitele počítače či importujte seznam počítačů z textového souboru. Soubor musí obsahovat IP adresy / názvy hostitele uvedené po jednom na řádku. Zde je příklad souboru:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   Po ručním přidání adres počítačů nebo po importu ze souboru se agent pokusí odeslat příkaz ping na přidané počítače a definovat jejich dostupnost.

9. Vyberte, co se má provést po zjišťování:

   - **Instalovat agenty a registrovat počítače**. Kliknutím na položku **Vybrat komponenty** můžete vybrat, které komponenty se na počítačích nainstalují. Další informace naleznete v tématu Výběr komponent k instalaci (str. 90). Zároveň můžete nainstalovat až 100 agentů.

     Na obrazovce **Vybrat komponenty** definujte účet, v rámci kterého budou služby spuštěny, určením možnosti **Účet pro přihlášení ke službě agenta**. Je možné vybrat jednu z následujících možností:

     - **Použití uživatelských účtů služby** (výchozí pro službu agenta)

       Uživatelské účty služby jsou systémové účty Windows sloužící k provozu služeb. Výhodou tohoto nastavení je, že zásady zabezpečení domény nemají vliv na uživatelská práva těchto účtů. Ve výchozím nastavení běží agent pod účtem **Místní systém**.

     - **Vytvoření nového účtu**

       Název účtu pro agenta bude Agent User.

     - **Použití následujícího účtu**

       V případě instalace agenta do řadiče domény vás systém vyzve k zadání existujících účtů (nebo stejného účtu) pro agenta. Z bezpečnostních důvodů systém automaticky nevytváří nové účty na řadiči domény.

     Při volbě možnosti **Vytvořit nový účet** nebo **Použít následující účet** zajistěte, aby zásady zabezpečení domény neměly vliv na práva příslušných účtů. Je-li účet zbaven uživatelských práv přidělených během instalace, nemusí daná součást správně fungovat nebo nebude fungovat vůbec.

   - **Zaregistrovat počítače s nainstalovanými agenty**. Tato možnost se použije, pokud je agent na počítačích již nainstalován a je třeba je jen zaregistrovat ve službě Cyber Protect. Pokud na počítačích není žádný agent nalezen, budou počítače přidány jako **nespravované**.
   - **Přidat jako nespravované počítače**. Agent se na počítačích nenainstaluje. Budete si je moct zobrazit ve webové konzoli a agenta nainstalovat nebo zaregistrovat později.

   [Pokud je vybrána akce po zjištění **Instalovat agenty a registrovat počítače**] **Je-li to vyžadováno, restartovat počítač** – je-li tato možnost povolena, počítač bude restartován tolikrát, kolikrát je to vyžadováno k dokončení instalace.

   Restart počítače může být vyžadován v jednom z následujících případů:

   - Požadované součásti jsou nainstalovány a k dokončení instalace je nutný restart počítače.
   - Instalace je dokončena, ale restart je vyžadován, protože některé soubory byly během instalace uzamčeny.
   - Instalace je dokončena, ale restart je vyžadován pro další dříve nainstalovaný software.

[Pokud je vybrána možnost **Je-li to vyžadováno, restartovat počítač**] **Nerestartovat, pokud je uživatel přihlášen** – je-li tato možnost povolena, počítač nebude automaticky restartován, pokud je uživatel přihlášen k systému. Pokud uživatel například pracuje a instalace vyžaduje restart, systém restartován nebude.

Pokud byly nainstalovány požadované komponenty a restart nebyl proveden, protože byl přihlášený uživatel, budete muset k dokončení instalace agenta počítač restartovat a instalaci znovu spustit.

Pokud byl agent nainstalován, ale nebyl proveden restart, je nutné počítač restartovat.

[Pokud vaše organizace zahrnuje jednotky] **Jednotka, kde se mají počítače zaregistrovat** – vyberte jednotku, kde budou počítače zaregistrovány.

Pokud jste vybrali jednu z prvních dvou akcí po zjištění, můžete také na počítače použít plán ochrany. Pokud máte několik plánů ochrany, můžete vybrat, který se má použít.

10. Zadejte přihlašovací údaje uživatele, který má pro všechny počítače oprávnění správce.

Důležité *Upozorňujeme, že ke vzdálené instalaci agenta není vyžadována příprava, pouze pokud zadáte pověření integrovaného účtu správce (první účet vytvořený při instalaci operačního systému). Pokud chcete definovat vlastní pověření správce, musíte provést doplňující ruční přípravné kroky popsané v části Přidání počítače se systémem Windows > Příprava.*

11. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.

    Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.

12. Systém zkontroluje připojení ke všem počítačům. Pokud připojení k některým počítačům selže, můžete pro tyto počítače změnit pověření.

Po zahájení zjišťování počítačů naleznete odpovídající úlohu v aktivitě **Kontrolní panel** > **Aktivity** > **Zjišťování počítačů**.

2.8.1.1 Výběr komponent k instalaci

Popis povinných a doplňujících komponent naleznete v následující tabulce:

Součást	Popis
Povinná komponenta	
Agent pro Windows	Tento agent zálohuje disky, svazky a soubory a bude nainstalován v počítačích se systémem Windows. Vždy bude nainstalován, není možné ho vybrat.
Další komponenty	
Agent pro Hyper-V	Tento agent zálohuje virtuální počítače Hyper-V a bude nainstalován na hostitelích Hyper-V. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna role Hyper-V.
Agent pro SQL	Tento agent zálohuje databáze serveru SQL Server a bude nainstalován v počítačích, kde běží Microsoft SQL Server. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.
Agent pro Exchange	Tento agent zálohuje databáze a poštovní schránky Exchange a bude nainstalován v počítačích, kde běží Microsoft Exchange Server s rolí poštovní schránky. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.

Agent pro Active Directory	Tento agent zálohuje data doménových služeb Active Directory a bude nainstalován na řadičích domény. Bude nainstalován, pokud je vybrán a pokud je na počítači zjištěna aplikace.
Agent pro VMware (Windows)	Tento agent zálohuje virtuální počítače VMware a bude nainstalován na počítačích se systémem Windows, které mají síťový přístup k serveru vCenter. Bude nainstalován, pokud je vybrán.
Agent pro Office 365	Tento agent zálohuje poštovní schránky Microsoft Office 365 do místního umístění a bude nainstalován na počítačích se systémem Windows. Bude nainstalován, pokud je vybrán.
Agent pro Oracle	Tento agent zálohuje databáze Oracle a bude nainstalován v počítačích, kde běží databáze Oracle. Bude nainstalován, pokud je vybrán.
Cyber Protect Monitor	Tato komponenta umožňuje uživateli sledovat provádění běžících úloh v oznamovací oblasti a bude nainstalována na počítačích se systémem Windows. Bude nainstalován, pokud je vybrán.
Nástroj příkazového řádku	Cyber Protect podporuje rozhraní příkazového řádku s nástrojem acrocmd. acrocmd neobsahuje žádné nástroje, které fyzicky spouštějí příkazy. Pouze poskytuje rozhraní příkazového řádku pro součásti Cyber Protect – agenty a server pro správu. Bude nainstalován, pokud je vybrán.
Tvůrce spouštěcích médií	Tato součást umožňuje uživatelům vytvářet spouštěcí média, a pokud ji vyberete, bude nainstalována na počítačích se systémem Windows.

2.8.2 Správa zjištěných počítačů

Po provedení procesu zjišťování naleznete všechny zjištěné počítače v nabídce **Zařízení** > **Nespravované počítače**.

Tento oddíl je rozdělen do pododdílů podle použité metody zjišťování. Kompletní seznam parametrů počítačů je uveden níže (může se lišit v závislosti na metodě zjišťování):

Název	Popis
Název	Název počítače. IP adresa se zobrazí, pokud se nepodařilo zjistit název počítače.
IP adresa	IP adresa počítače.
Typ zjištění	Metoda zjišťování, která byla použita ke zjištění počítače.
Organizační jednotka	Organizační jednotka ve službě Active Directory, do které počítač spadá. Tento sloupec se zobrazí, když zobrazíte seznam počítačů v nabídce **Nespravované počítače** > **Active Directory**.
Operační systém	Operační systém nainstalovaný v počítači.

V části **Výjimky** můžete přidat počítače, které je třeba během procesu zjišťování přeskočit. Pokud například nepotřebujete zjištění konkrétních počítačů, můžete je přidat na seznam.

Chcete-li přidat počítač na seznam **Výjimky**, vyberte ho v seznamu a klikněte na položku **Přidat do výjimek**. Chcete-li odebrat počítač ze seznamu **Výjimky**, přejděte do nabídky **Nespravované počítače** > **Výjimky**, vyberte počítač a klikněte na položku **Odebrat z výjimek**.

Pokud chcete nainstalovat agenta pro ochranu a zaregistrovat skupinu zjištěných počítačů ve službě Cyber Protect, vyberte je v seznamu a klikněte na položku **Instalovat a zaregistrovat**. V otevřeném průvodci také můžete přiřadit plán ochrany skupině počítačů.

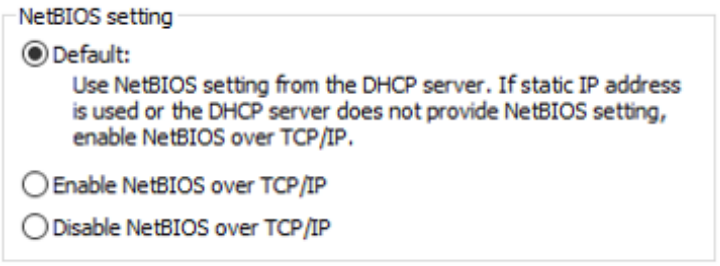
Po nainstalování agenta ochrany na počítačích se tyto počítače zobrazí v části **Zařízení** > **Počítače s agenty**.

Chcete-li zkontrolovat stav ochrany, přejděte do nabídky **Kontrolní panel** > **Přehled** a přidejte ovládací prvek **Stav ochrany** (p. 406) nebo ovládací prvek **Zjištěný počítač** (p. 406).

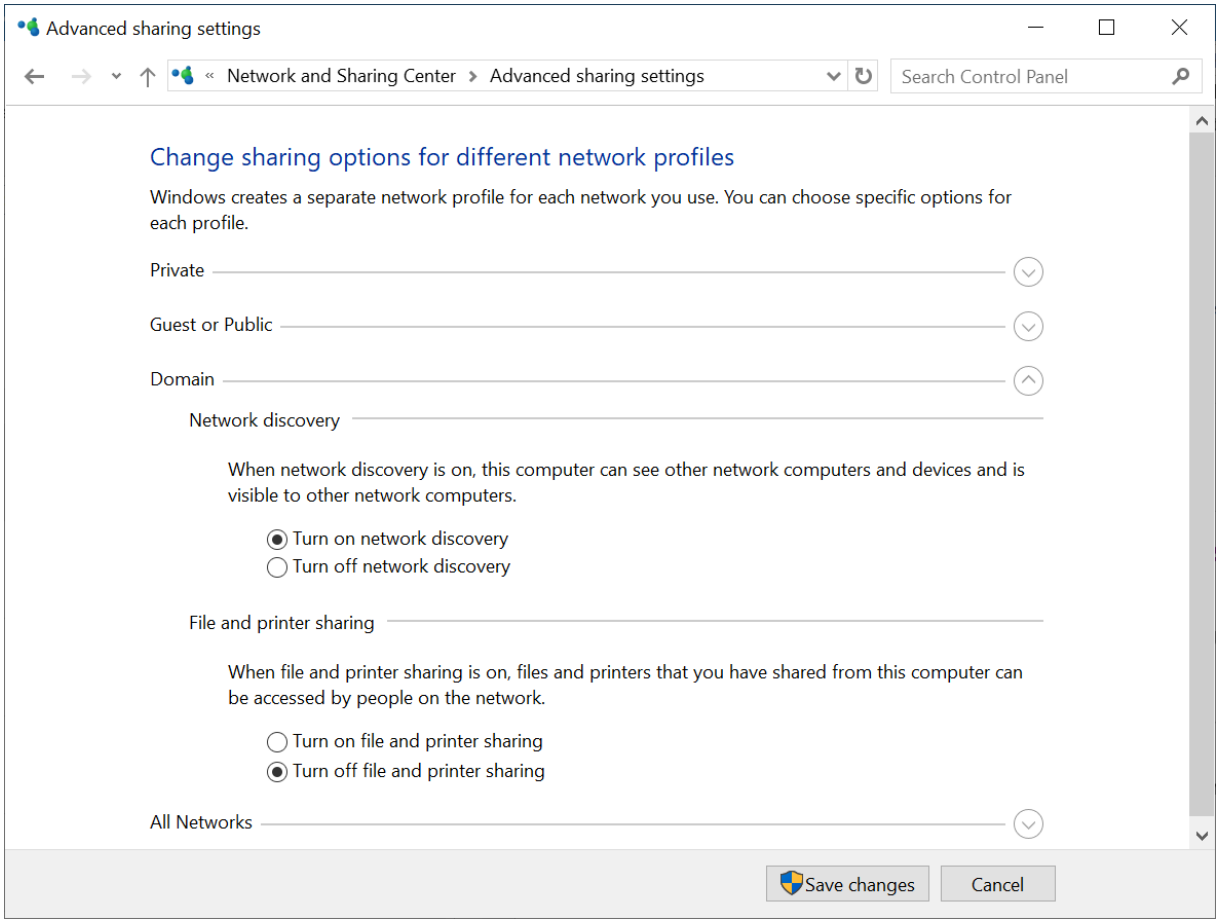
2.8.3 Odstraňování problémů

Pokud máte s funkcí automatického zjišťování problémy, vyzkoušejte následující kroky:

- Zkontrolujte, zda je povolena možnost NetBIOS přes TCP/IP nebo zda je nastavena na výchozí hodnotu.



- V nabídce **Ovládací panely** > **Centrum síťových připojení a sdílení** > **Pokročilé nastavení sdílení** zapněte zjišťování sítě.



- Zkontrolujte, zda **služba Function Discovery Provider Host** běží na počítači, který zjišťování provádí, a na počítačích, které mají být zjištěny.

- Zkontrolujte, zda **služba Function Discovery Resource Publication** běží na počítačích, které mají být zjištěny.

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

2.9.1 Než začnete

Systémové požadavky agenta

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

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

Kolik agentů potřebuji?

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

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

Pokud máte více agentů, nedoporučujeme používat místně připojené úložiště (tzn. ukládat zálohy na virtuální disky přidané do virtuálního zařízení). Další informace najdete v článku Použití místně připojeného úložiště (str. 342).

Vypnutí automatického nástroje DRS u agenta

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

2.9.2 Nasazení šablony OVF

Umístění šablony OVF

Šablona OVF obsahuje jeden soubor OVF a dva soubory VMDK.

V místních nasazeních

Po dokončení instalace serveru pro správu bude balíček OVF virtuálního zařízení umístěný ve složce **%ProgramFiles%\Acronis\ESXAppliance** (systém Windows) nebo **/usr/lib/Acronis/ESXAppliance** (systém Linux).

V cloudových nasazeních

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

Do vašeho počítače se stáhne archiv .zip.

2. Rozbalte archiv .zip.

Nasazení šablony OVF

1. Zajistěte, aby byl k souborům šablony OVF přístup z počítače s klientem vSphere.
2. Spusťte klienta vSphere a přihlaste se na server vCenter.
3. Nasaďte šablonu OVF.
   - Při konfiguraci úložiště vyberte sdílené datové úložiště, pokud existuje. Tlustý nebo tenký formát disku není důležitý, protože neovlivňuje výkon zařízení.
   - Při konfiguraci síťových připojení v cloudových nasazeních nezapomeňte vybrat síť, která umožňuje internetové připojení, aby se agent mohl řádně zaregistrovat v cloudu. Při konfiguraci síťových připojení v místních nasazeních vyberte síť, která obsahuje server pro správu.

2.9.3 Konfigurace virtuálního zařízení

1. **Spuštění virtuálního zařízení**

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

2. **Proxy server**

   Pokud máte v síti zapnutý proxy server:

   a. Pokud chcete spustit příkazové prostředí, stiskněte v uživatelském rozhraní virtuálního zařízení klávesy CTRL+SHIFT+F2.

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

   c. Najděte následující oddíl:

   ```
   <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"0"</value>
       <value name="Host" type="TString">"ADRESA"</value>
       <value name="Port" type="Tdword">"PORT"</value>
       <value name="Login" type="TString">"PŘIHLAŠOVACÍ JMÉNO"</value>
       <value name="Password" type="TString">"HESLO"</value>
   </key>
   ```

   d. Nahraďte **0** hodnotou **1**.

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

   f. Pokud proxy server vyžaduje ověřování, nahraďte PŘIHLAŠOVACÍ JMÉNO a HESLO přihlašovacími údaji serveru proxy. Jinak tyto řádky ze souboru odstraňte.

   g. Uložte soubor.

   h. Spusťte příkaz **reboot**.

   Jinak tento krok přeskočte.

3. **Nastavení sítě**

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

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

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

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

Zadejte pověření, která budou agenti používat pro připojení k serveru vCenter nebo hostiteli ESXi. Doporučujeme používat účet, který má přiřazenou roli **Správce**. V opačném případě použijte účet, který má potřebná oprávnění (str. 346) na vCenter Serveru nebo v ESXi.

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

5. **Server pro správu**
   a. V části **Možnosti agenta** u položky **Server pro správu** klikněte na **Změnit**.
   b. V poli **Název/IP serveru** proveďte jeden z následujících úkonů:
      - Pro místní nasazení vyberte **Místní**. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
      - Pro cloudové nasazení vyberte **Cloud**. Software zobrazí adresu služby kybernetické ochrany. Tuto adresu neměňte, pokud jste nedostali jiný pokyn.
   c. V polích **Uživatelské jméno** a **Heslo** proveďte jeden z následujících úkonů::
      - Pro místní nasazení zadejte uživatelské jméno a heslo správce serveru pro správu.
      - Pro cloudové nasazení zadejte uživatelské jméno a heslo služby kybernetické ochrany. Pod tímto účtem se zaregistruje agent i jím spravované virtuální počítače.
6. **Časové pásmo**

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

   K virtuálnímu zařízení můžete připojit další disk, aby Agent pro VMware mohl zálohovat do tohoto místně připojeného umístění (str. 342).

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

2.9.4 Aktualizace Agenta pro VMware (Virtual Appliance)

V místních nasazeních použijte stejný postup aktualizace jako pro ostatní agenty (str. 103).

V cloudových nasazeních lze agenty s verzí 12.5.23094 a pozdější aktualizovat pomocí webové konzole Cyber Protect.

Aktualizace Agenta pro VMware (virtuální zařízení) pomocí webové konzole Cyber Protect

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

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

Poznámka *Během aktualizace všechny probíhající zálohy selžou.*

Aktualizace Agenta pro VMware (virtuální zařízení), který má starší verzi než 12.5.23094

1. Odeberte Agenta pro VMware (Virtual Appliance) způsobem popsaným v části Odinstalace produktu (str. 104). V kroku 5 odstraňte agenta z **Nastavení** > **Agenti**, a to i tehdy, pokud agenta plánujete znovu nainstalovat.
2. Nasaďte Agenta pro VMware (Virtual Appliance), jak je popsáno v části Nasazení šablony OVF (str. 93).

3. Konfigurujte Agenta pro VMware (Virtual Appliance) způsobem popsaným v části Konfigurace virtuálního zařízení (str. 94).

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

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

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

2.10 Nasazování Agenta pro Scale Computing HC3 (virtuální zařízení)

2.10.1 Než začnete

Toto zařízení je předkonfigurovaný virtuální počítač, který nasadíte v clusteru Scale Computing HC3. Obsahuje agenta pro ochranu, který umožňuje spravovat kybernetickou ochranu pro všechny virtuální počítače v clusteru.

Systémové požadavky agenta

Při nasazování virtuálního zařízení si můžete vybrat mezi různými kombinacemi procesorů vCPU a paměti RAM. Pro většinu operací je optimální a dostatečný počet 2 procesory vCPU a 4 GB paměti RAM. Pokud předpokládáte, že šířka pásma při zatížení zálohováním překročí 100 MB za sekundu (například u 10gigabitových sítí), a chcete při zálohování zlepšit výkon, doporučujeme použít 4 procesory vCPU a 8 GB paměti RAM.

Vlastní virtuální disky zařízení nezabírají více než 6 GB.

Kolik agentů potřebuji?

Jeden agent dokáže ochránit celý cluster. Pokud však potřebujete distribuovat šířku pásma při zatížení zálohováním, můžete mít v clusteru více agentů.

Pokud máte v clusteru více agentů, jsou virtuální počítače automaticky rovnoměrně distribuovány mezi agenty tak, aby každý agent spravovat stejný počet počítačů.

Automatická redistribuce proběhne, když nerovnováha zatížení mezi agenty dosáhne 20 procent. K tomu může dojít například při přidání nebo odebrání počítače nebo agenta. Například zjistíte, že potřebujete více agentů za účelem zlepšení propustnosti, a umístíte do clusteru další virtuální počítač. Server pro správu přiřadí novému agentovi nejvhodnější počítače. Zatížení předchozích agentů se sníží. Pokud agenta ze serveru pro správu odeberete, počítače přiřazené tomuto agentovi budou rozmístěny mezi zbývající agenty. To se však nestane, pokud se agent poškodí nebo je z clusteru Scale Computing HC3 odstraněn ručně. Redistribuce se spustí pouze poté, co takového agenta odstraníte z webového rozhraní Cyber Protect.

Výsledek automatického rozdělení je možné zobrazit:

- Ve sloupci **Agent**, který je dostupný pro každý virtuální počítač v části **Všechna zařízení**
- V části **Přiřazené virtuální počítače** na panelu **Podrobnosti** po výběru agenta v nabídce **Nastavení** > **Agenti**

2.10.2 Nasazení virtuálního zařízení

1. Přihlaste se k účtu Cyber Protect.
2. Klikněte na **Zařízení** > **Všechna zařízení** > **Přidat** > **Scale Computing HC3**.
3. Vyberte počet virtuálních počítačů, které chcete nasadit.
4. Zadejte IP adresu nebo název hostitele clusteru Scale Computing HC3.
5. Zadejte přihlašovací údaje k účtu, který má v tomto clusteru přiřazenu roli **Vytvoření/úprava virtuálního počítače**.
6. Zadejte síťovou složku, která se použije jako dočasné úložiště souboru obrazu pro virtuální zařízení. Budete potřebovat minimálně 2 GB volného místa.
7. Zadejte přihlašovací údaje k účtu, který má k této síťové složce přístup pro čtení a zápis.
8. Klikněte na **Nasadit**.

Po dokončení nasazení nakonfigurujte virtuální zařízení.

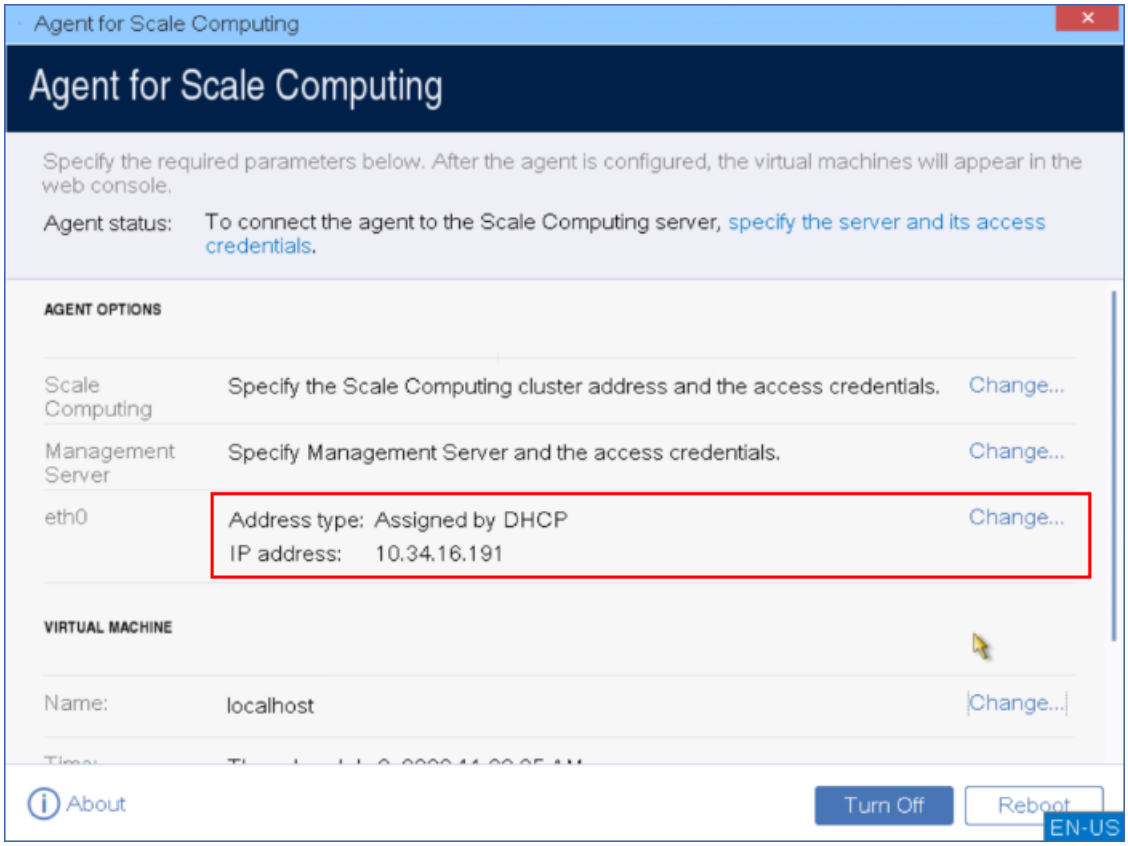
2.10.3 Konfigurace virtuálního zařízení

Po nasazení musíte virtuální zařízení nakonfigurovat, aby se dokázalo připojit ke clusteru Scale Computing HC3, který bude chránit, i k serveru pro správu Cyber Protect.

Konfigurace virtuálního zařízení

1. Přihlaste se k účtu Scale Computing HC3.
2. Vyberte virtuální počítač s agentem, který chcete nakonfigurovat, a klikněte na položku **Konzole**.

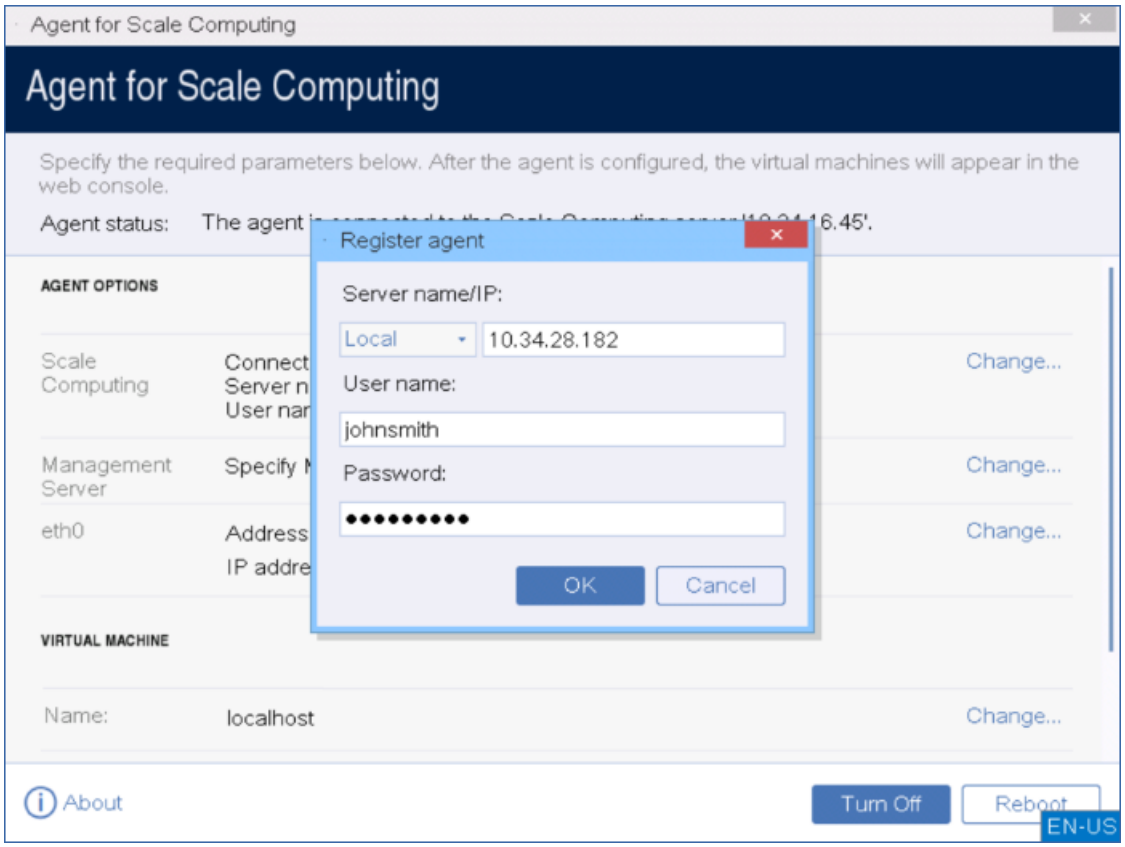
3. Nakonfigurujte síťová rozhraní zařízení Konfigurovat může být potřeba jedno a více rozhraní – závisí to na počtu sítí, které zařízení používá. Zkontrolujte, zda v sítích, které váš virtuální počítač používá, jsou platné automaticky přiřazené adresy DHCP (jsou-li nějaké) nebo je přiřaďte ručně.



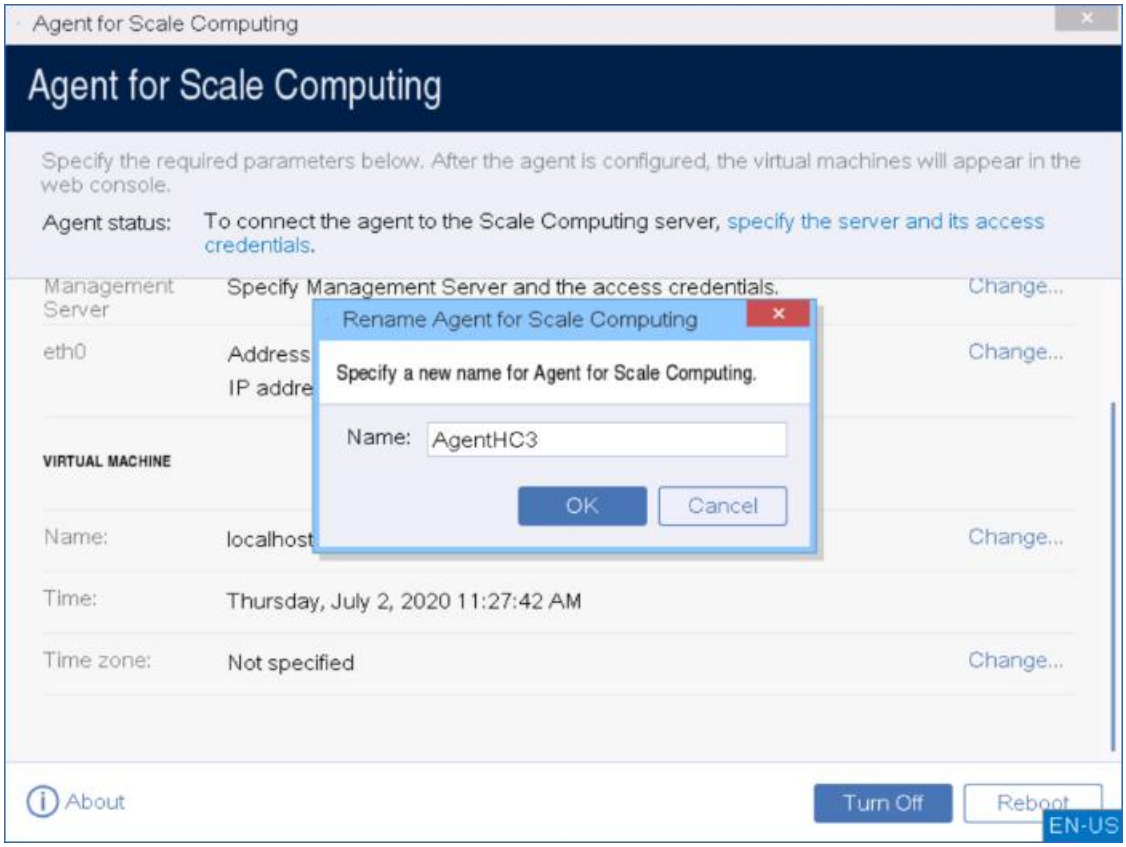
4. Zadejte adresu clusteru Scale Computing HC3 a přihlašovací údaje:
   - Název DNS nebo IP adresu clusteru.
   - Do polí **Uživatelské jméno** a **Heslo** zadejte přihlašovací údaje účtu Scale Computing HC3, který má přiřazeny příslušné role.

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

5. Zadejte adresu serveru pro správu Cyber Protect a přihlašovací údaje pro přístup k serveru.



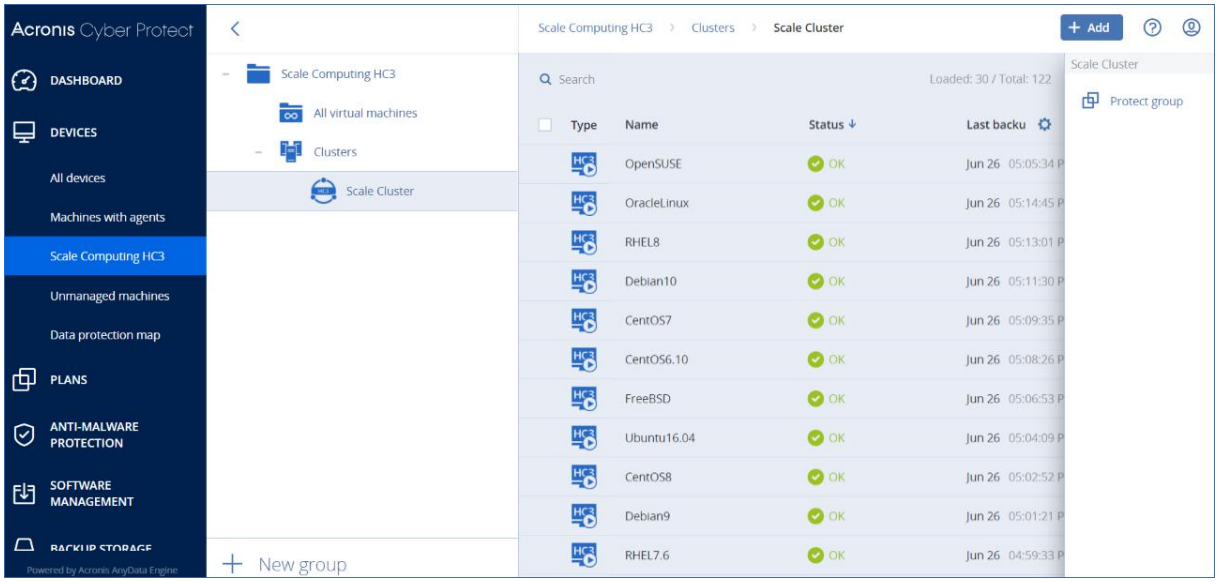
6. [Volitelné] Zadejte název agenta. Tento název se zobrazí ve webové konzoli Cyber Protect.



7. [Volitelné] Vyberte časové pásmo vašeho umístění, aby se naplánované operace spouštěly ve správný čas.

Ochrana virtuálních počítačů v clusteru Scale Computing HC3

1. Přihlaste se k účtu Cyber Protect.
2. Přejděte do nabídky **Zařízení** > **Scale Computing HC3**> <váš cluster> nebo vyhledejte své počítače v nabídce **Zařízení** > **Všechna zařízení**.
3. Vyberte požadované počítače a použijte pro ně plán ochrany.



2.10.4 Agent pro Scale Computing HC3 – požadované role

Tato část popisuje oprávnění vyžadovaná k operacím s virtuálními počítači Scale Computing HC3 a k nasazování virtuálních zařízení.

Operace	Role
Zálohování virtuálního počítače	Zálohování Vytvoření/úprava virtuálního počítače
Obnovení do existujícího virtuálního počítače	Zálohování Vytvoření/úprava virtuálního počítače Správa napájení virtuálního počítače Odstranění virtuálního počítače Nastavení clusteru
Obnovení do nového virtuálního počítače	Zálohování Vytvoření/úprava virtuálního počítače Správa napájení virtuálního počítače Odstranění virtuálního počítače Nastavení clusteru
Nasazení virtuální zařízení	Vytvoření/úprava virtuálního počítače

2.11 Instalace agentů pomocí zásad skupiny

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

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

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

Předpoklady

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

- Máte doménu Active Directory s doménovým řadičem na němž běží Microsoft Windows Server 2003 nebo vyšší.

- Jste v doméně členem skupiny **Domain Admins**.
- Stáhli jste si instalační program **Všichni agenti pro instalaci v systému Windows**. Odkaz ke stažení je dostupný na stránce **Přidat zařízení** ve webové konzoli Cyber Protect.

Krok 1: Vygenerování registračního tokenu

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

Jak vygenerovat registrační token

1. Přihlaste se k webové konzoli Cyber Protect zadáním přihlašovacích údajů k účtu, ke kterému mají být počítače přiřazeny.
2. Klikněte na **Všechna zařízení** > **Přidat**.
3. Posuňte se dolů na možnost **Registrační token** a potom klikněte na možnost **Generovat**.
4. Zadejte dobu platnosti tokenu a poté klikněte na možnost **Generovat token**.
5. Zkopírujte token nebo si jej zapište. Uložte si token, pokud jej budete potřebovat pro další použití.

   Kliknutím na možnost **Spravovat aktivní tokeny** můžete zobrazit a spravovat již vygenerované tokeny. Nezapomeňte, že z bezpečnostních důvodů tato tabulka nezobrazuje plné hodnoty tokenů.

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

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

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

Krok 3: Nastavení objektů zásad skupiny

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

- Klikněte pravým tlačítkem myši na název domény nebo organizační jednotky a potom klikněte na příkaz **Vlastnosti**. V dialogovém okně klikněte na kartu **Zásady skupiny** a klikněte na tlačítko **Nový**.

V systému Windows Server 2008 a novějším:

- Klikněte pravým tlačítkem myši na název domény nebo organizační jednotky a potom klikněte na příkaz **Zde vytvořit a propojit objekt zásad skupiny**.

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

   V systému Windows Server 2012 a novějším:
   - Rozbalte položku **Zásady** > **Nastavení softwaru**.
9. Pravým tlačítkem klikněte na položku **Instalace softwaru**, vyberte nabídku **Nový** a klikněte na položku **Balíček**.
10. Vyberte instalační balíček MSI agenta ve sdílené složce, kterou jste vytvořili, a klikněte na možnost **Otevřít**.
11. V dialogovém okně **Nasazení softwaru** klikněte na tlačítko **Pokročilé** a potom na tlačítko **OK**.
12. Na kartě **Úpravy** klikněte na možnost **Přidat** a vyberte soubor transformace MST, který jste vytvořili.
13. Kliknutím na tlačítko **OK** zavřete dialogové okno **Nasazení softwaru**.

2.12 Aktualizace agentů

Předpoklady

Na počítačích se systémem Windows vyžadují funkce Cyber Protect balíček Microsoft Visual C++ 2017 k opětovné distribuci. Před aktualizací agenta zkontrolujte, zda je na počítači již nainstalován, nebo ho nainstalujte. Po instalaci může být vyžadován restart. Balíček Microsoft Visual C++ 2017 k opětovné distribuci naleznete zde https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

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

Agenty lze aktualizovat pomocí webové konzole Cyber Protect nebo opakováním instalace libovolným dostupným způsobem. Chcete-li současně aktualizovat více agentů, postupujte následujícím způsobem.

Aktualizace agentů pomocí webové konzole Cyber Protect

1. [Pouze pro místní nasazení] Aktualizujte server pro správu.
2. [Pouze pro místní nasazení] Ověřte, zda jsou na počítači se serverem pro správu k dispozici instalační balíčky. Přesný popis kroků naleznete v části Přidání počítače se systémem Windows (str. 42) > Instalační balíčky.
3. Ve webové konzoli Cyber Protect klikněte na položky **Nastavení** > **Agenti**.

Software zobrazí seznam počítačů. Počítače s neaktuálními verzemi agentů jsou označeny oranžovým vykřičníkem.

4. Vyberte počítače, ve kterých chcete agenty aktualizovat. Počítače musí být online.
5. Klikněte na možnost **Aktualizovat agenta**.
6. Vyberte agenta pro nasazení.
7. Zadejte přihlašovací údaje účtu s oprávněním správce v cílovém počítači.
8. Vyberte název nebo IP adresu, které agent použije pro přístup k serveru pro správu.
9. Výchozí výběr je název serveru. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání registrace agenta.

   [Pouze pro místní nasazení] Průběh aktualizace se zobrazuje na kartě **Aktivity**.

Poznámka *Během aktualizace všechny probíhající zálohy selžou.*

Aktualizace definic Cyber Protect na počítači

1. Klikněte na možnost **Nastavení** > **Agenti**.
2. Vyberte počítač, ve kterém chcete aktualizovat definice Cyber Protect, a klikněte na tlačítko **Aktualizovat definice**. Počítač musí být online.

Přiřazení role aktualizátora agentovi

1. Klikněte na možnost **Nastavení** > **Agenti**.
2. Vyberte počítač, kterému chcete přiřadit roli aktualizátora (p. 105), klikněte na **Podrobnosti** a v části **Definice Cyber Protect** povolte možnost **Pomocí tohoto agenta stáhnout a distribuovat opravy a aktualizace**.

Vymazání dat uložených v mezipaměti na agentovi

1. Klikněte na možnost **Nastavení** > **Agenti**.
2. Vyberte počítač, ve kterém chcete vymazat data uložená v mezipaměti (zastaralé soubory aktualizací a data správy oprav), a klikněte na tlačítko **Vymazat mezipaměť**.

2.13 Odinstalace produktu

Pokud z počítače chcete odebrat jednotlivé součásti produktu, spusťte instalační program, zvolte možnost úpravy produktu a zrušte výběr součástí, které chcete odebrat. Odkazy na instalační programy se nachází na stránce **Stažené soubory** (klikněte na ikonu účtu v pravém horním rohu stránky > **Stažené soubory**).

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

Upozornění *V případě místních nasazení dejte pozor, abyste omylem neodinstalovali server pro správu. Webová konzole Cyber Protect pak nebude k dispozici. a nemohli byste nadále zálohovat a obnovovat žádné počítače registrované na serveru pro správu.*

V systému Windows

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

   Pokud odinstalováváte agenta a plánujete ho znovu nainstalovat, nechte toto políčko nezaškrtnuté. Pokud toto políčko zaškrtnete, počítač může být ve webové konzoli Cyber Protect duplikován a zálohy starého počítače nemusí být spojeny s novým počítačem.
4. Potvrďte své rozhodnutí.

5. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě ve webové konzoli Cyber Protect klikněte na položky **Nastavení** > **Agenti**, vyberte počítač, na který byl agent nainstalován, a klikněte na **Odstranit**.

V systému Linux

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

   Pokud odinstalováváte agenta a plánujete ho znovu nainstalovat, nechte toto políčko nezaškrtnuté. Pokud toto políčko zaškrtnete, počítač může být ve webové konzoli Cyber Protect duplikován a zálohy starého počítače nemusí být spojeny s novým počítačem.
3. Potvrďte své rozhodnutí.
4. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě ve webové konzoli Cyber Protect klikněte na položky **Nastavení** > **Agenti**, vyberte počítač, na který byl agent nainstalován, a klikněte na **Odstranit**.

V systému macOS

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

Odebrání Agenta pro VMware (Virtual Appliance)

1. Spusťte klienta vSphere a přihlaste se na server vCenter.
2. Po zapnutí virtuálního zařízení na něj klikněte pravým tlačítkem a pak klikněte na položky **Napájení** > **Vypnout**. Potvrďte své rozhodnutí.
3. Pokud virtuální zařízení používá místně připojené úložiště na virtuálním disku a chcete na tomto disku zachovat data, postupujte následovně:
   a. Pravým tlačítkem klikněte na VA a potom na položku **Upravit nastavení**.
   b. Vyberte disk s úložištěm a potom klikněte na příkaz **Odstranit**. Pod položkou **Možnosti odstranění** klikněte na příkaz **Odstranit z virtuálního počítače**.
   c. Klikněte na tlačítko **OK**.

   Výsledkem je, že disk zůstane v úložišti dat. Disk můžete připojit k jinému VA.
4. Pravým tlačítkem klikněte na VA a potom na položku **Odstranit z disku**. Potvrďte své rozhodnutí.
5. Pokud agenta plánujete znovu nainstalovat, tento krok přeskočte. V opačném případě ve webové konzoli Cyber Protect klikněte na položky **Nastavení** > **Agenti**, vyberte virtuální zařízení a klikněte na **Odstranit**.

2.14 Nastavení ochrany

Obecné nastavení ochrany pro Cyber Protect můžete nakonfigurovat ve webové konzoli Cyber Protect v nabídce **Nastavení** > **Ochrana**.

Automatické aktualizace komponent

Služba Cyber Protect používá k aktualizacím komponent peer-to-peer technologii, aby minimalizovala provoz v síti. Můžete si vybrat jednoho a více vyhrazených agentů, kteří stáhnou aktualizace z internetu a distribuují je mezi další agenty v síti jako peer-to-peer agenty.

Ve výchozím nastavení je možnost **Pomocí tohoto agenta stáhnout a distribuovat opravy a aktualizace** pro agenty zakázána. To znamená, že všichni zaregistrovaní agenti vyhledávají nejnovější aktualizace a distribuují je. Pokud uživatel možnost **Pomocí tohoto agenta stáhnout a distribuovat opravy a aktualizace** povolí pro určitého agenta, tento agent obdrží roli Aktualizátor a všichni ostatní agenti tohoto agenta využijí k vyhledávání a distribuci aktualizací. Agenti s rolí Aktualizátor musí být dostatečně výkonní s vysokorychlostním stabilním připojením k internetu a musí mít dostatek místa na disku.

Postup aktualizace je následující:

1. Agent s rolí Aktualizátor podle harmonogramu zkontroluje soubor indexů za účelem aktualizace hlavních součástí.
2. Agent s rolí Aktualizátor začne stahovat a distribuovat aktualizace všem agentům.

Přiřazení role Aktualizátor agentovi pro ochranu

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Nastavení** > **Agenti**.
2. Vyberte počítač, kterému chcete roli Aktualizátor přiřadit.
3. Klikněte na položku **Podrobnosti** a zapněte přepínač **Pomocí tohoto agenta stáhnout a distribuovat opravy a aktualizace**.

Konfigurace automatické aktualizace definic ochrany

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Nastavení** > **Ochrana**.
2. Klikněte na možnost **Aktualizace definic ochrany**.
3. Klikněte na možnost **Harmonogram** a nakonfigurujte automatickou aktualizaci následujících součástí:

- Ochrana proti malwaru
- Posouzení ohrožení zabezpečení
- Správa oprav

  Typ harmonogramu:

  - **Denní** – určete, ve které dny v týdnu se mají definice aktualizovat.

    Spustit v – vyberte čas, kdy se mají definice aktualizovat.
  - **Po hodině** – určete podrobnější hodinový harmonogram aktualizací.

    Spustit každých – určete pravidelnost spuštění aktualizace.

    Od ... **Do** – určete konkrétní časový rozsah pro aktualizace.

Aktualizace definic ochrany pro konkrétní počítače ručně

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Nastavení** > **Agenti**.
2. Vyberte počítače, ve kterých chcete aktualizovat definice ochrany, a klikněte na tlačítko **Aktualizovat definice**.

Změna umístění pro stahování definic ochrany

Ve výchozím nastavení se definice ochrany stáhnou do dočasné složky vašeho operačního systému a pak jsou uloženy do programové složky Acronis. Pokud chcete aplikaci Acronis Cyber Protect nakonfigurovat tak, aby stahovala definice do jiné dočasné složky, změňte konfigurační soubor následovně:

- Na počítačích se systémem Windows: **%programdata%\Acronis\AtpDatabaseMirror\config.json**
- Na počítačích se systémem Linux: **/var/lib/Acronis/AtpDatabaseMirror/config.json**

Ve výchozím nastavení je konfigurační soubor prázdný. Do souboru zadejte následující hodnotu:

"mirror_temp_dir": "<path_to_download_cyber_protect_database>"

Například:

```
{
      "mirror_temp_dir": "C:\\temp"
}
```

Zadaná cesta může být absolutní nebo relativní z adresáře dat aplikace.

Pokud složku nelze vytvořit nebo pokud server pro správu nemůže do vybraného adresáře zapisovat, použije se výchozí umístění.

Úložiště mezipaměti

Umístění dat uložených v mezipaměti:

- Na počítačích se systémem Windows: **C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache**
- Na počítačích se systémem Linux: **/opt/acronis/var/atp-downloader/Cache**
- Na počítačích se systémem macOS: **/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache**

V části **Zastaralé soubory aktualizace a data správy oprav** zadejte, po jaké době se mají data v mezipaměti odstranit.

Maximální velikost úložiště mezipaměti (GB) pro agenty:

- **Role Aktualizátor** – definujte velikost úložiště mezipaměti na počítačích s rolí Aktualizátor.
- **Ostatní role** – definujte velikost úložiště mezipaměti na ostatních počítačích.

Výběr zdroje nejnovějších definic ochrany

Nejnovější definice ochrany můžete stáhnout z následujících umístění:

- Cloud

  Agent pro ochranu se připojí k internetu a stáhne nejnovější definice ochrany z cloudu Acronis. Ve výchozím nastavení všichni agenti zaregistrovaní na serveru pro správu vyhledávají a distribuují aktualizace. Další informace o roli Aktualizátor naleznete v části *Automatické aktualizace komponent* výše.

- Server pro správu Cyber Protect

  Je-li tato možnost vybrána, nepotřebují agenti přístup k internetu. Připojují se pouze k serveru pro správu, kde jsou uloženy definice ochrany. Server pro správu však musí být připojený k internetu, aby bylo možné stáhnout nejnovější definice ochrany.

- Vlastní webové servery

  Tato možnost je určena pouze pro účely řešení problémů a testování. Vyberte ji, pouze když vás k tomu vyzve tým podpory Acronis. Tým podpory vám také poskytne adresy URL, které je třeba zadat do následujících polí:

  - Definice antivirové ochrany a ochrany proti malwaru
  - Rozšířené definice detekce

- Definice posouzení ohrožení zabezpečení a správy oprav

Vzdálené připojení

Povolení vzdáleného připojení k počítačům prostřednictvím klienta RDP nebo HTML5

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Nastavení** > **Ochrana**.
2. Klikněte na možnost **Vzdálené připojení** a zapněte přepínač **Připojení ke vzdálené ploše**.

   Pokud je tento přepínač vypnutý, budou možnosti **Připojit pomocí klienta RDP** / **Připojit pomocí klienta HTML5** ve webové konzoli Cyber Protect skryty a uživatelé se nebudou moct vzdáleně připojit k počítačům. Tato možnost ovlivňuje všechny uživatele ve vaší organizaci.

   Chcete-li povolit sdílení vzdáleného připojení s uživateli, zaškrtněte políčko **Sdílet připojení ke vzdálené ploše**. Po výběru zařízení se nová možnost **Sdílet vzdálené připojení** zobrazí v pravé nabídce. Výběrem možnosti můžete vygenerovat odkaz pro přístup ke vzdálenému počítači. Tento odkaz pak můžete sdílet s uživateli, kterým chcete vzdálený přístup udělit.

3 Přístup k webové konzoli Cyber Protect

Chcete-li se připojit k webové konzoli Cyber Protect, zadejte do adresního řádku webového prohlížeče adresu přihlašovací stránky a přihlaste se podle níže uvedeného popisu.

Místní nasazení

Adresa přihlašovací stránky je IP adresa nebo název počítače s nainstalovaným serverem pro správu.

Je podporován protokol HTTP i HTTPS na stejném portu TCP, který lze nakonfigurovat během instalace serveru pro správu (str. 37). Výchozí port je 9877.

Můžete nakonfigurovat server pro správu (str. 114) tak, aby zakázal přístup k webové konzoli Cyber Protect přes HTTP a zajistil použití certifikátu SSL od externích dodavatelů.

V systému Windows

Pokud je server pro správu nainstalovaný ve Windows, lze se k webové konzoli Cyber Protect přihlásit dvěma způsoby:

- Kliknutím na možnost **Přihlásit se** se přihlaste jako aktuální uživatel systému Windows.

  Toto je nejjednodušší způsob přihlášení ze stejného počítače, na kterém je nainstalovaný server pro správu.

  Pokud je server pro správu nainstalovaný na jiném počítači, tato metoda funguje za následujících podmínek:

  - Počítač, ke kterému se přihlašujete, je ve stejné doméně Active Directory jako server pro správu.
  - Jste přihlášeni jako uživatel domény.

  Doporučujeme webový prohlížeč nakonfigurovat na Integrované ověřování systému Windows (str. 109). V opačném případě vás prohlížeč požádá o uživatelské jméno a heslo. Tuto možnost však můžete zakázat.
- Klikněte na **Zadat uživatelské jméno a heslo** a zadejte uživatelské jméno a heslo.

V každém případě váš účet musí být v seznamu správců serveru pro správu. Ve výchozím nastavení tento seznam obsahuje skupinu **Administrators** na počítači s nainstalovaným serverem pro správu. Další informace najdete v části Správci a jednotky (str. 444).

Zakázání možnosti Přihlásit se jako aktuální uživatel systému Windows

1. Na počítači, kde je nainstalovaný server pro správu, přejděte do nabídky **`C:\Program Files\Acronis\AccountServer`**.
2. Otevřete soubor **account_server.json** pro úpravy.
3. Přejděte do části „connectors“ a odstraňte následující řádky:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Přejděte do části „checksum“ a změňte hodnotu „sum“ následovně:

```
"sum": "v/85MOBjfdb8oyPqpmr24U5KHqdbolxDSfW91fuglCI="
```

5. V nabídce Služby systému Windows restartujte službu Acronis Service Manager Service.

V systému Linux

Pokud je server pro správu nainstalován v systému Linux, zadejte uživatelské jméno a heslo účtu, který je v seznamu správců serveru pro správu. Ve výchozím nastavení tento seznam obsahuje pouze skupinu **root** na počítači s nainstalovaným serverem pro správu. Další informace najdete v části Správci a jednotky (str. 444).

Cloudové nasazení

Adresa přihlašovací stránky je https://backup.acronis.com/. Uživatelské jméno a heslo je stejné jako pro váš účet Acronis.

Pokud byl váš účet vytvořen správcem zálohování, musíte ho kliknutím na odkaz v aktivačním e-mailu aktivovat a nastavit jeho heslo.

Změna jazyka

Když jste přihlášení, můžete jazyk webového rozhraní změnit kliknutím na ikonu účtu v pravém horním rohu.

3.1 Nakonfigurování webového prohlížeče na Integrované ověřování systému Windows

Integrované ověřování systému Windows je možné, pokud k webové konzoli Cyber Protect přistupujete z počítače se systémem Windows a jakýmkoli podporovaným prohlížečem (str. 19).

Doporučujeme webový prohlížeč nakonfigurovat na Integrované ověřování systému Windows. V opačném případě vás prohlížeč požádá o uživatelské jméno a heslo.

Konfigurace aplikace Internet Explorer, Microsoft Edge, Opera a Google Chrome

Pokud je počítač, ve kterém běží prohlížeč, ve stejné doméně Active Directory jako počítač, na kterém běží server pro správu, přidejte si přihlašovací stránku konzoly do seznamu webů **Místní intranet**.

V opačném případě přidejte přihlašovací stránku konzoly do seznamu **Důvěryhodné servery** a povolte nastavení **Automatické přihlášení pod aktuálním uživatelským jménem a heslem**.

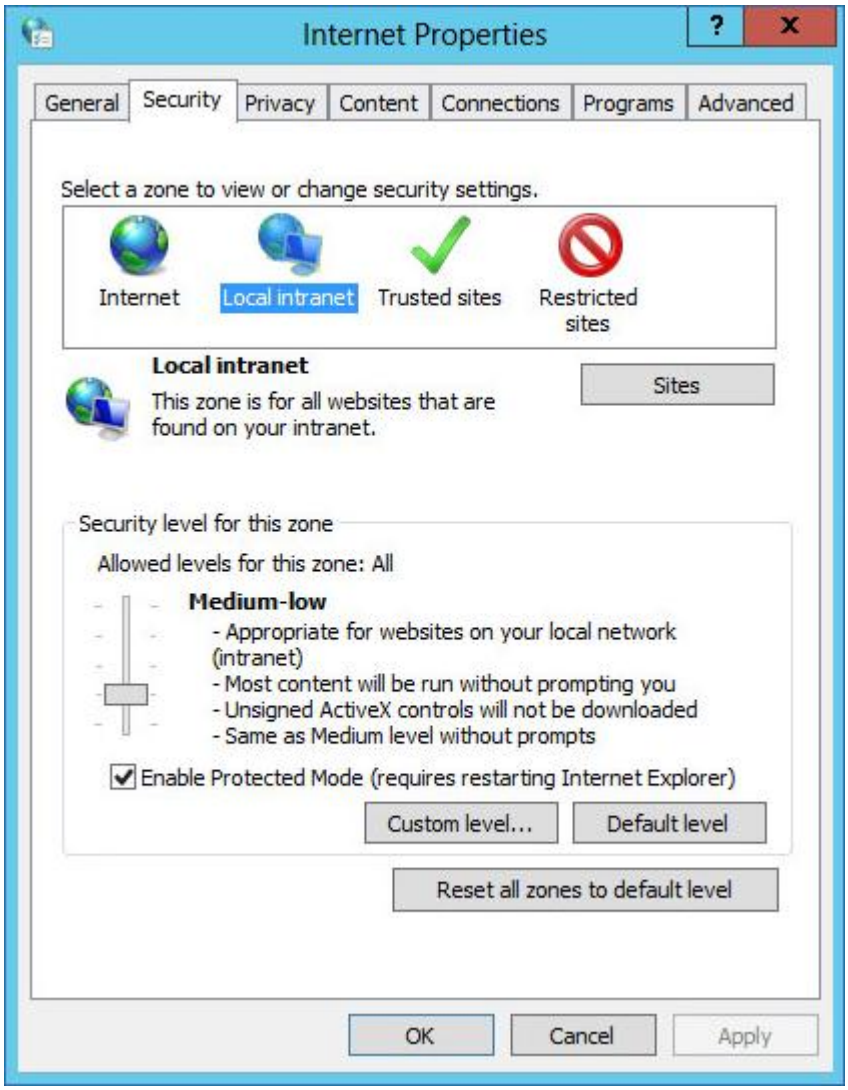
Podrobné pokyny jsou uvedené dále v této části. Vzhledem k tomu, že tyto prohlížeče používají nastavení systému Windows, je také možné je nakonfigurovat pomocí zásad skupiny v doméně Active Directory.

Nakonfigurování prohlížeče Mozilla Firefox

1. V aplikaci Firefox přejděte na adresu URL `about:config` a potom kliknutím na tlačítko vyjádřete, že **souhlasíte s riziky**.
2. Pomocí pole **Hledat** vyhledejte předvolbu `network.negotiate-auth.trusted-uris`.
3. Dvakrát na ni klikněte a potom zadejte adresu stránky pro přihlášení k webové konzoli Cyber Protect.
4. Opakujte kroky 2–3 pro předvolbu `network.automatic-ntlm-auth.trusted-uris`.
5. Zavřete okno `about:config`.

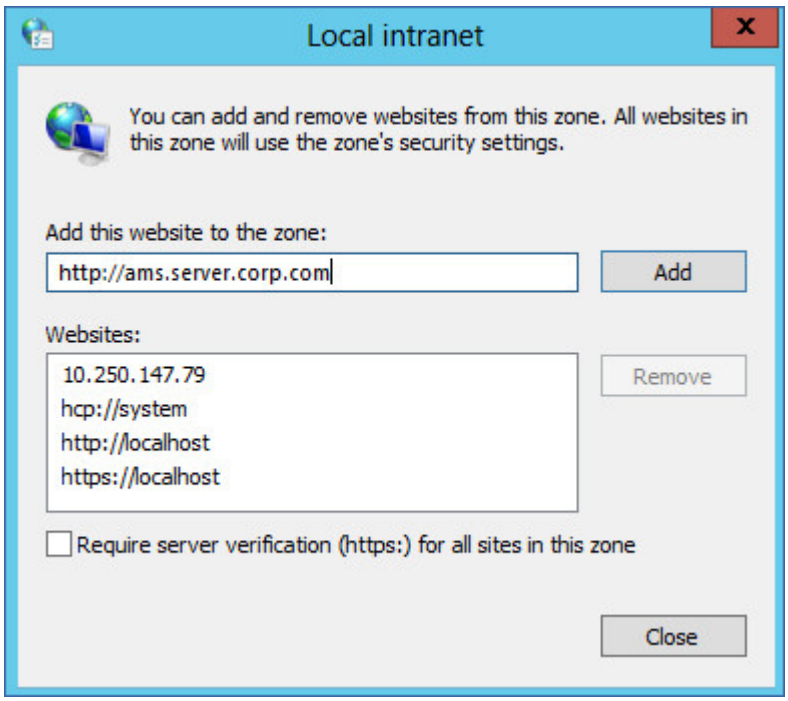
3.1.1 Přidání konzoly do seznamu místních intranetových webů

1. Zvolte **Ovládací panely** > **Možnosti Internetu**.
2. Na kartě **Zabezpečení** vyberte **Místní intranet**.



3. Klikněte na možnost **Weby**.

4. V části **Přidat tento web k zóně** zadejte adresu stránky pro přihlášení k webové konzoli Cyber Protect a klikněte na položku **Přidat**.

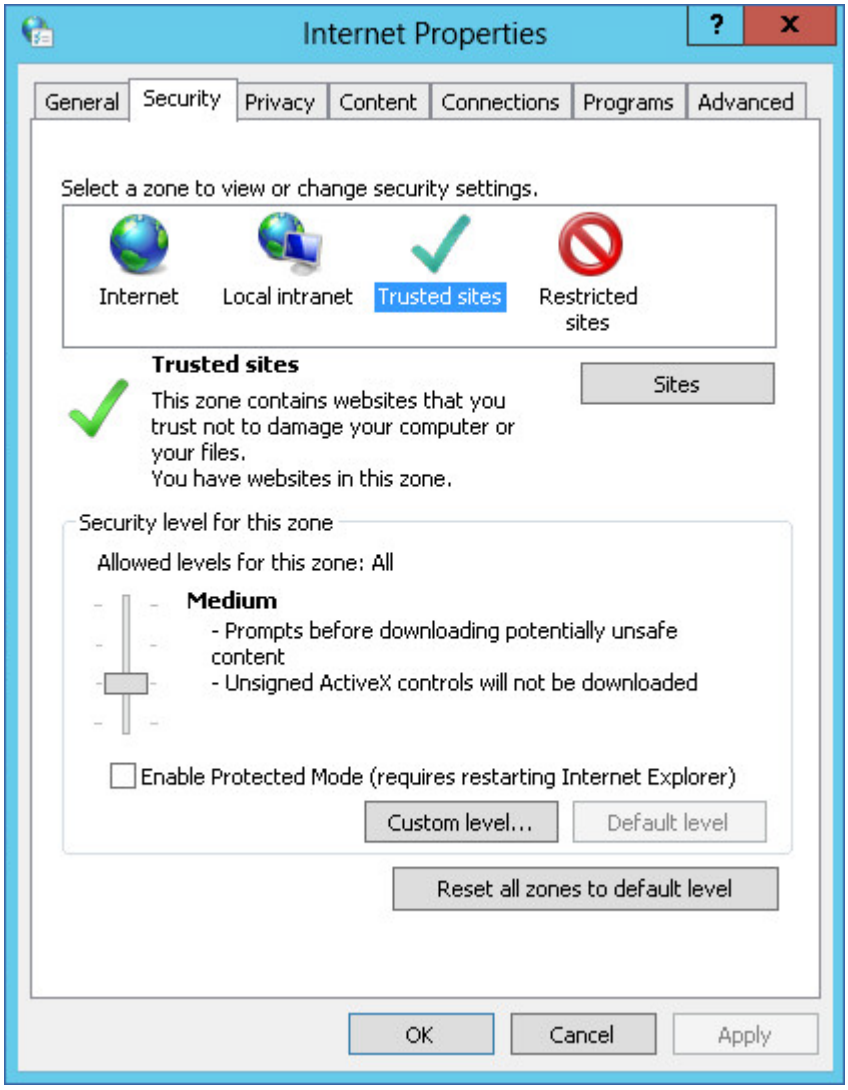


5. Klikněte na tlačítko **Close** (Zavřít).
6. Klikněte na tlačítko **OK**.

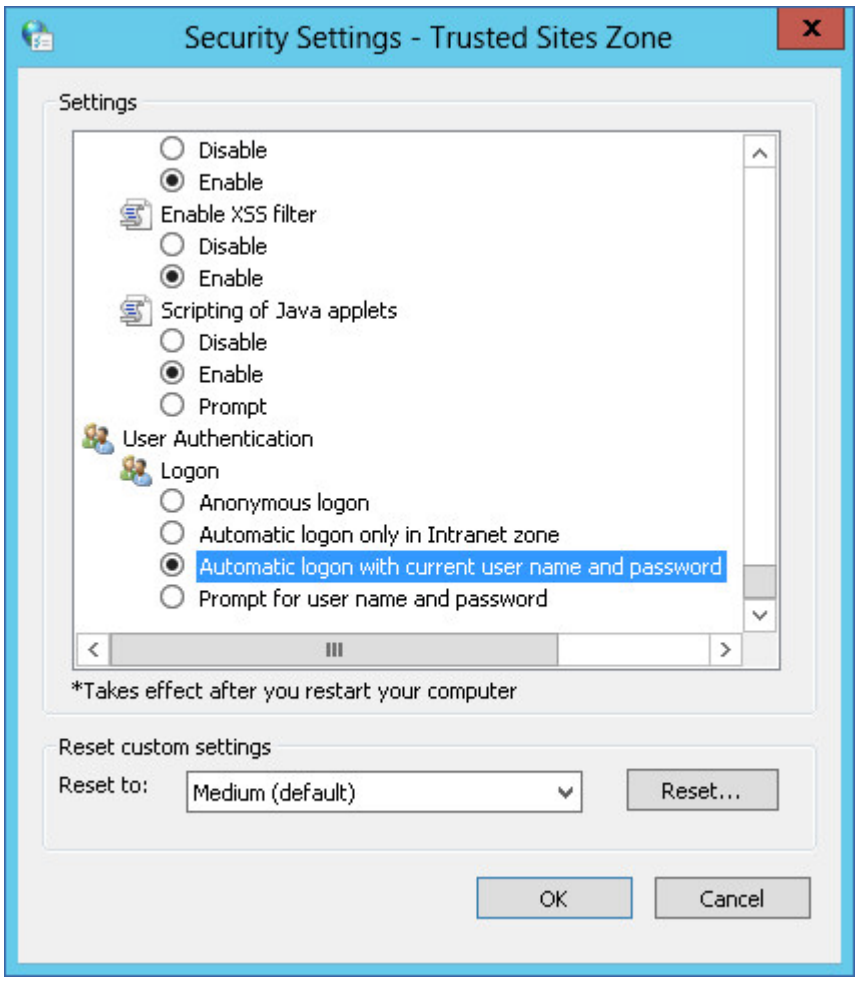
3.1.2 Přidání konzoly do seznamu důvěryhodných serverů

1. Zvolte **Ovládací panely** > **Možnosti Internetu**.

2. Na kartě **Zabezpečení** vyberte **Důvěryhodné servery** a potom klikněte na **Vlastní úroveň**.

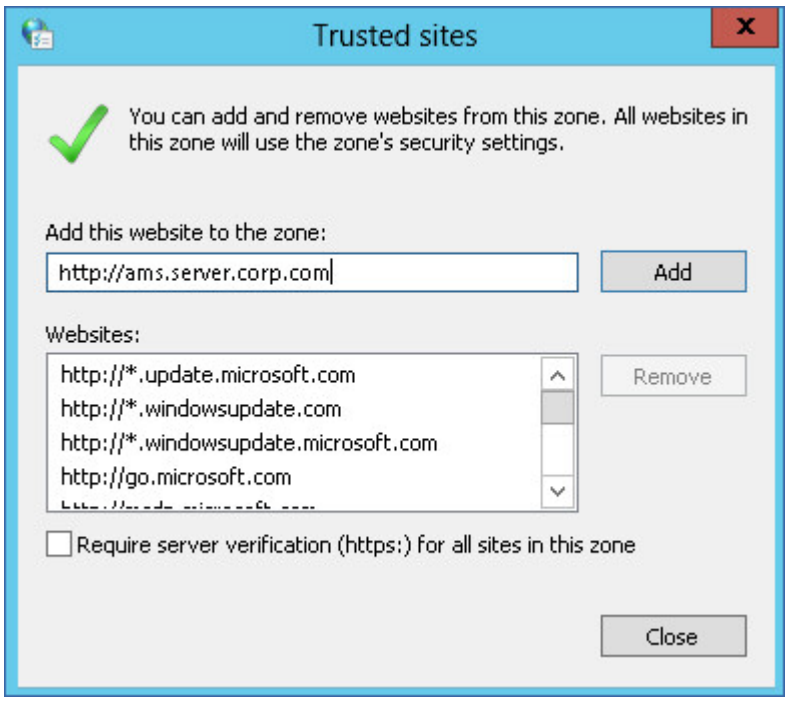


3. V části **Přihlášení** vyberte **Automatické přihlášení pod aktuálním uživatelským jménem a heslem** a potom klikněte na **OK**.



4. Na kartě **Zabezpečení** (stále s vybranou položkou **Důvěryhodné servery**) klikněte na tlačítko **Servery**.

5. V části **Přidat tento web k zóně** zadejte adresu stránky pro přihlášení k webové konzoli Cyber Protect a klikněte na položku **Přidat**.



6. Klikněte na tlačítko **Close** (Zavřít).
7. Klikněte na tlačítko **OK**.

3.2 Nastavení certifikátu SSL

V této části naleznete následující postupy:

- Konfigurace agenta pro ochranu, který používá vámi podepsaný certifikát Secure Socket Layer (SSL) vygenerovaný serverem pro správu.
- Změna certifikátu Secure Socket Layer (SSL) podepsaného svým držitelem a vygenerovaného serverem pro správu na certifikát vydaný důvěryhodnou certifikační autoritou, jako je například GoDaddy, Comodo nebo GlobalSign. Po této změně bude certifikát používaný serverem pro správu důvěryhodný v jakémkoli počítači. Při přihlašování k webové konzoli Cyber Protect pomocí protokolu HTTPS se v prohlížeči neobjeví výstraha zabezpečení.

Volitelně můžete nakonfigurovat server pro správu tak, že zakáže přístup k webové konzoli Cyber Protect přes HTTP přesměrováním všech uživatelů na HTTPS.

3.2.1 Použití certifikátu s vlastní certifikací

Konfigurace agenta ochrany v systému Windows

1. Na počítači s agentem otevřete editor registrů.
2. Vyhledejte následující klíč registru:
   HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.
3. Nastavte hodnotu **VerifyPeer** na **0**.
4. Zkontrolujte, zda je hodnota **VerifyHost** nastavena na **0**.
5. Restartujte službu Managed Machine Service (MMS):
   a. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
   b. Klikněte na tlačítko **OK**.

c. Spusťte následující příkazy:

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

Konfigurace agenta ochrany v systému Linux

1. Na počítači s agentem otevřete soubor **/etc/Acronis/BackupAndRecovery.config** pro úpravy**.**
2. Přejděte ke klíči **CurlOptions** a nastavte hodnotu pro **VerifyPeer** na **0.** Zkontrolujte, zda je hodnota **VerifyHost** také nastavena na **0.**
3. Uložte úpravy.
4. Restartujte službu Managed Machine Service (MMS) provedením následujícího příkazu v libovolném adresáři:

```
sudo service acronis_mms restart
```

Konfigurace agenta ochrany v systému macOS

1. Na počítači s agentem zastavte službu Managed Machine Service (MMS):
   a. Přejděte do umístění **Aplikace** > **Nástroje** > **Terminál**.
   b. Spusťte následující příkaz:

```
sudo launchctl stop acronis_mms
```

2. Otevřete soubor **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** pro úpravy.
3. Přejděte ke klíči **CurlOptions** a nastavte hodnotu pro **VerifyPeer** na **0**. Zkontrolujte, zda je hodnota **VerifyHost** také nastavena na **0**.
4. Uložte úpravy.
5. Spusťte službu Managed Machine Service (MMS) provedením následujícího příkazu v terminálu:

```
sudo launchctl starts acronis_mms
```

3.2.2 Použití certifikátu vydaného důvěryhodnou certifikační autoritou

Konfigurace nastavení certifikátu SSL

1. Musíte mít následující:
   - soubor certifikátu (PEM, CERT, nebo jiný formát),
   - soubor s privátním klíčem pro certifikát (obvykle KEY),
   - heslo k privátnímu klíči, pokud je zašifrovaný.
2. Zkopírujte soubory do počítače se serverem pro správu.
3. Na tomto počítači otevřete v textovém editoru následující konfigurační soubor:
   - Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**
4. Vyhledejte následující oddíl:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
    "auto_redirect": false
}
```

5. Mezi uvozovky na řádku **"cert_file"** zadejte úplnou cestu k souboru certifikátu. Například:

- Windows (pozor na lomítka): **"cert_file": "C:/certificate/local-domain.ams.cert"**
- Linux: **"cert_file": "/home/user/local-domain.ams.cert"**

6. Mezi uvozovky na řádku **"key_file"** zadejte úplnou cestu k souboru privátního klíče. Například:
   - Windows (pozor na lomítka): **"key_file": "C:/certificate/private.key"**
   - Linux: **"key_file": "/home/user/private.key"**
7. Je-li privátní klíč zašifrovaný, zadejte mezi uvozovky na řádku **"passphrase"** heslo k souboru privátního klíče. Například: **"passphrase": "my secret passphrase"**
8. Chcete-li zakázat přístup k webové konzoli Cyber Protectpřes HTTP přesměrováním všech uživatelů na HTTPS, změňte hodnotu **"auto_redirect"** z **false** na **true**. Jinak tento krok přeskočte.
9. Uložte soubor **api_gateway.json**.

Důležité *Buďte opatrní, abyste nedopatřením neodstranili z konfiguračního souboru žádné čárky, závorky ani uvozovky.*

10. Restartujte službu serveru pro správu Acronis podle postupu níže.

Jak restartovat službu serveru pro správu Acronis v systému Windows

1. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
2. Klikněte na tlačítko **OK**.
3. Spusťte následující příkazy:

```
net stop asm
net start asm
```

Jak restartovat službu serveru pro správu Acronis v systému Linux

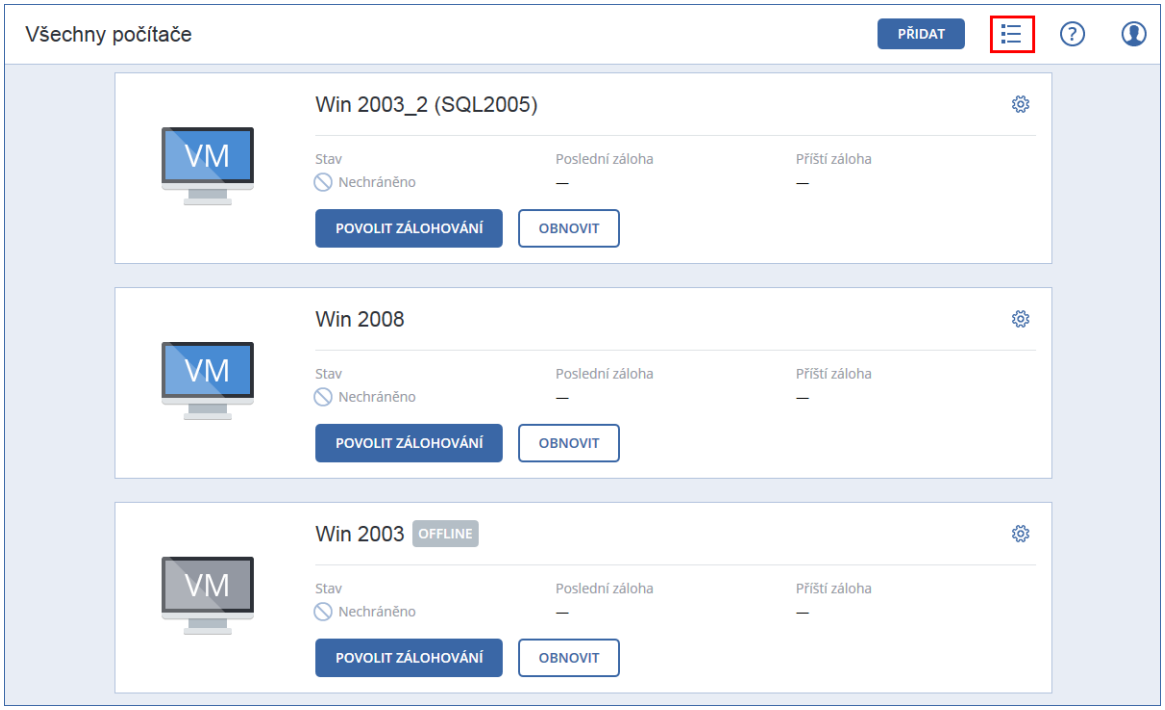
1. Otevřete **Terminál**.
2. V jakémkoli adresáři spusťte následující příkaz:

```
sudo service acronis_asm restart
```

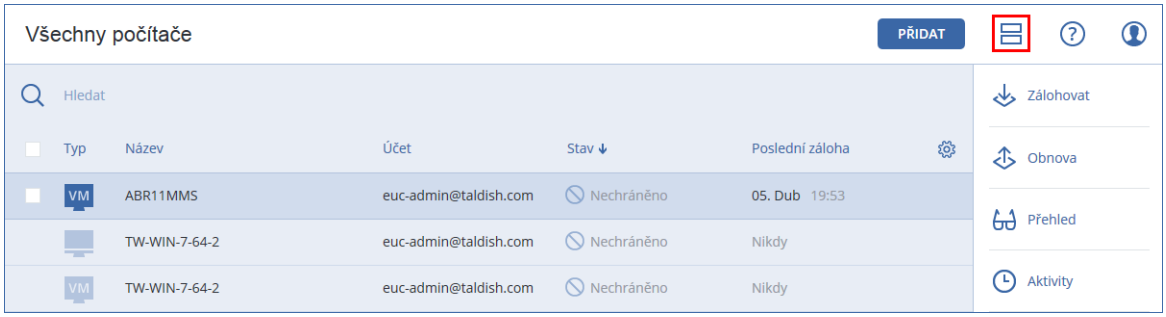
4 Zobrazení webové konzole Cyber Protect

Webová konzole Cyber Protect má dvě zobrazení: jednoduché zobrazení a tabulkové zobrazení. Chcete-li přepnout mezi zobrazeními, klikněte na odpovídající ikonu v pravém horním rohu.

Jednoduché zobrazení podporuje malé množství počítačů.



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



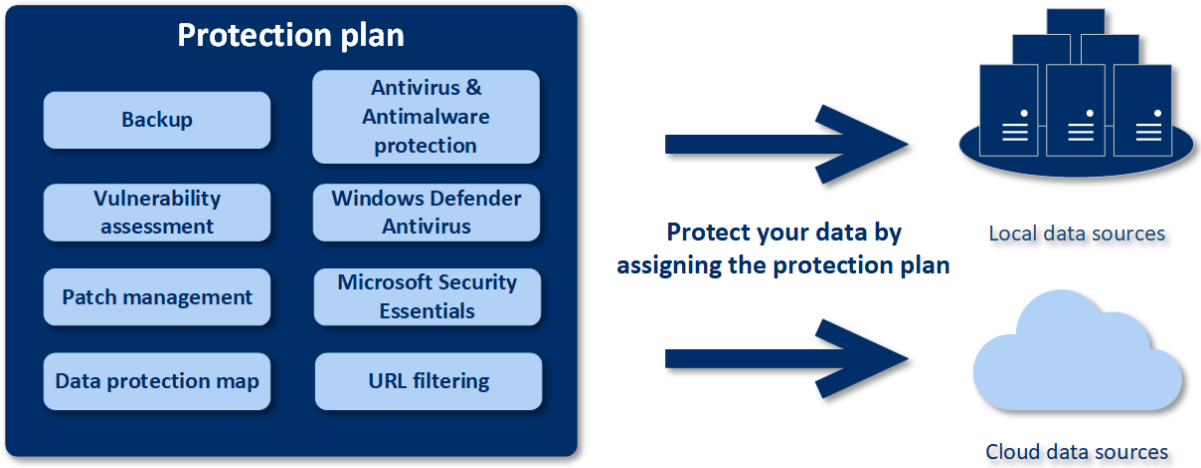
Obě zobrazení zprostředkovávají přístup ke stejným funkcím a operacím. Tento dokument popisuje přístup k operacím z tabulkového zobrazení.

5 Plán ochrany a moduly

Plán ochrany je plán, který kombinuje několik modulů ochrany dat včetně:

- Zálohování (p. 122) – umožňuje zálohovat datové zdroje do místního nebo cloudového úložiště.
- Antivirová ochrana a ochrana proti malwaru (p. 354) – umožňuje kontrolovat počítače pomocí zabudovaného řešení ochrany proti malwaru.
- Filtrování adres URL (p. 364) – umožňuje chránit počítače před hrozbami přicházejícími z internetu zablokováním přístupu ke škodlivým adresám URL a obsahu ke stažení.
- Antivirová ochrana v programu Windows Defender (p. 361) – umožňuje spravovat nastavení antivirové ochrany v programu Windows Defender k ochraně vašeho prostředí.
- Microsoft Security Essentials (p. 363) – umožňuje spravovat nastavení služby Microsoft Security Essentials k ochraně vašeho prostředí.
- Posouzení ohrožení zabezpečení (p. 375) – automaticky zjistí ohrožení zabezpečení v produktech společnosti Microsoft a produktech jiných výrobců nainstalovaných na vašich počítačích a upozorní vás na ně.
- Správa oprav (p. 378) – umožňuje instalovat opravy a aktualizace pro produkty společnosti Microsoft a produkty třetích stran na vaše počítače za účelem vyřešení zjištěných ohrožení zabezpečení.
- Mapa ochrany dat (p. 410) – umožňuje zjišťovat data za účelem monitorování stavu ochrany důležitých souborů.

Pomocí plánu ochrany můžete své datové zdroje kompletně chránit před externími i interními hrozbami. Povolením a zakázáním různých modulů a jejich nastavením můžete vytvořit flexibilní plány, které vyhovují různých obchodním potřebám.



5.1 Vytvoření plánu ochrany

Plán ochrany je možné použít pro několik počítačů hned při jeho vytvoření nebo později. Když vytvoříte plán, systém zkontroluje operační systém a typ zařízení (např. pracovní stanice, virtuální počítač atd.) a zobrazí pouze moduly plánu, které jsou pro vaše zařízení relevantní.

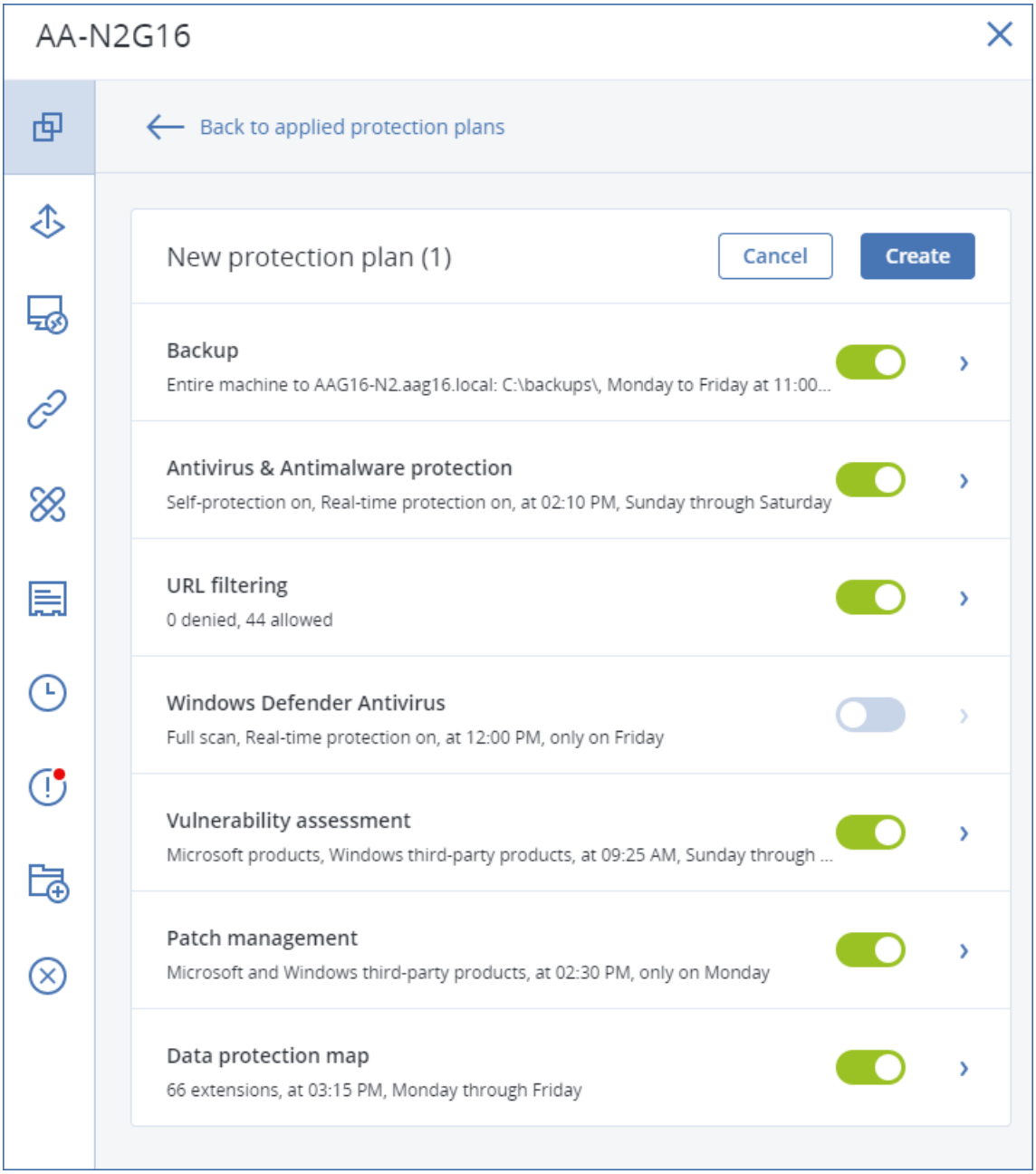
Plán ochrany lze vytvořit dvěma způsoby:

- V části **Zařízení** – vyberte jedno nebo více zařízení, která mají být chráněna, a vytvořte pro ně plán.
- V části **Plán** – vytvořte plán a vyberte počítače, na které ho chcete použít (p. 122).

Nejprve se podíváme na první způsob.

Vytvoření prvního plánu ochrany

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Všechna zařízení**.
2. Vyberte počítače, které chcete ochránit.
3. Klikněte na tlačítko **Chránit** a na položku **Vytvořit plán**. Zobrazí se plán ochrany s výchozím nastavením.



4. [Volitelné] Chcete-li upravit název plánu ochrany, klikněte na ikonu tužky vedle názvu.
5. [Volitelné] Chcete-li povolit nebo zakázat modul plánu ochrany, klikněte na přepínač vedle názvu modulu.

6. [Volitelné] Chcete-li nakonfigurovat parametry modulu, klikněte na odpovídající část plánu ochrany.
7. Jakmile budete hotovi, klikněte na tlačítko **Vytvořit**.

Moduly Zálohování, Antivirová ochrana a ochrana proti malwaru, Posouzení ohrožení zabezpečení, Správa oprav a Mapa ochrany dat lze spustit na vyžádání kliknutím na tlačítko **Spustit nyní**.

5.2 Řešení konfliktů plánů

Plán ochrany může mít následující stavy:

- **Aktivní** – plán, který je přiřazen zařízením a je na nich spuštěn.
- **Neaktivní** – plán, který je přiřazen zařízením, ale je zakázán a není na nich spuštěn.

Použití několika plánů na zařízení

Na jedno zařízení můžete použít několik plánů ochrany. Získáte tak kombinaci různých plánů ochrany přiřazených k jednomu zařízení. Můžete například použít jeden plán, který má povolen pouze modul Antivirová ochrana a ochrana proti malwaru, a jiný plán, který má povolený pouze modul Zálohování. Plány ochrany lze kombinovat, pouze pokud nemají moduly, které se protínají. Pokud jsou stejné moduly povoleny ve více plánech ochrany, musíte vyřešit případné konflikty mezi plány.

Řešení konfliktů plánů

Plán je v konfliktu s již použitými plány

Když vytvoříte nový plán na zařízení nebo na zařízeních s již použitými plány, které jsou v konfliktu s novým plánem, můžete takový konflikt vyřešit jedním z následujících způsobů:

- Vytvořte nový plán, použijte ho a zakažte všechny již použité konfliktní plány.
- Vytvořte nový plán a zakažte ho.

Když upravíte plán na zařízení nebo na zařízeních s již použitými plány, které jsou v konfliktu s provedenými změnami, můžete takový konflikt vyřešit jedním z následujících způsobů:

- Uložte změny plánu a zakažte všechny již použité konfliktní plány.
- Uložte změny plánu a zakažte ho.

Plán zařízení je v konfliktu se skupinovým plánem

Pokud je zařízení zahrnuto do skupiny zařízení s přiřazeným skupinovým plánem a pokusíte se zařízení přiřadit nový plán, systém vás požádá o vyřešení konfliktu jedním z následujících způsobů:

- Odeberte zařízení ze skupiny a použijte na zařízení nový plán.
- Použijte nový plán na celou skupinu nebo upravte aktuální skupinový plán.

Problém s licencí

Přiřazená kvóta na zařízení musí odpovídat plánu ochrany, který chcete spustit, aktualizovat nebo použít. Chcete-li problém s licencí vyřešit, proveďte jeden z následujících úkonů:

- Zakažte moduly, které nejsou přiřazenou kvótou podporovány, a pokračujte v používání plánu.
- Změňte přiřazenou kvótu ručně: Přejděte do nabídky **Zařízení** > **<konkrétní zařízení>** > **Podrobnosti** > **Kvóta služeb**. Zrušte stávající kvótu a přiřaďte novou.

5.3 Operace s plány ochrany

Informace o vytvoření plánu ochrany najdete v tématu Vytvoření plánu ochrany.

Dostupné akce s plánem ochrany

S plánem ochrany můžete provádět následující akce:

- Přejmenovat plán
- Povolit/zakázat moduly a upravit nastavení jednotlivých modulů
- Povolit/zakázat plán
- Přiřadit plán zařízením nebo skupině zařízení
- Odvolat plán ze zařízení
- Importovat/exportovat plán

  Poznámka *Importovat lze pouze plány ochrany vytvořené v produktu Acronis Cyber Protect 15. Plány ochrany vytvořené ve starších verzích nejsou s produktem Acronis Cyber Protect 15 kompatibilní.*

- Odstranit plán

Použití existujícího plánu ochrany

1. Vyberte počítače, které chcete ochránit.
2. Klikněte na tlačítko **Chránit**. Pokud je pro vybrané počítače již použit plán ochrany, klikněte na možnost **Přidat plán**.
3. Software zobrazí dříve vytvořené plány ochrany.
4. Vyberte požadovanou ochranu a klikněte na tlačítko **Použít**.

Úprava plánu ochrany

1. Pokud chcete upravit plán ochrany pro všechny počítače, pro které se používá, vyberte jeden z nich. Jinak vyberte konkrétní počítače, u kterých chcete plán ochrany upravit.
2. Klikněte na tlačítko **Chránit**.
3. Vyberte plán ochrany, který chcete upravit.
4. Klikněte na ikonu tří teček vedle názvu plánu ochrany a na tlačítko **Upravit**.
5. Chcete-li upravit parametry plánu, klikněte na odpovídající část panelu plánu ochrany.
6. Klikněte na **Uložit změny**.
7. Pokud chcete plán ochrany změnit u všech počítačů, kde se používá, klikněte na možnost **Použít změny na tento plán ochrany**. Jinak klikněte na možnost **Vytvořit nový plán ochrany pouze pro zvolená zařízení**.

Odvolání plánu ochrany z počítačů

1. Vyberte počítače, ze kterých chcete plán ochrany odvolat.
2. Klikněte na tlačítko **Chránit**.
3. Pokud počítače používají několik plánů ochrany, vyberte ten, který chcete odvolat.
4. Klikněte na ikonu tří teček vedle názvu plánu ochrany a na tlačítko **Odvolat**.

Odstranění plánu ochrany

1. Vyberte libovolný počítač, pro který platí plán ochrany, který chcete odstranit.
2. Klikněte na tlačítko **Chránit**.
3. Pokud počítač používá několik plánů ochrany, vyberte ten, který chcete odstranit.
4. Klikněte na ikonu tří teček vedle názvu plánu ochrany a na tlačítko **Odstranit**.

   Plán ochrany se odvolá ze všech počítačů a zcela se odstraní z webového rozhraní.

6 Zálohování

Soubor pravidel, který specifikuje, jak jsou na daném počítači chráněna data.

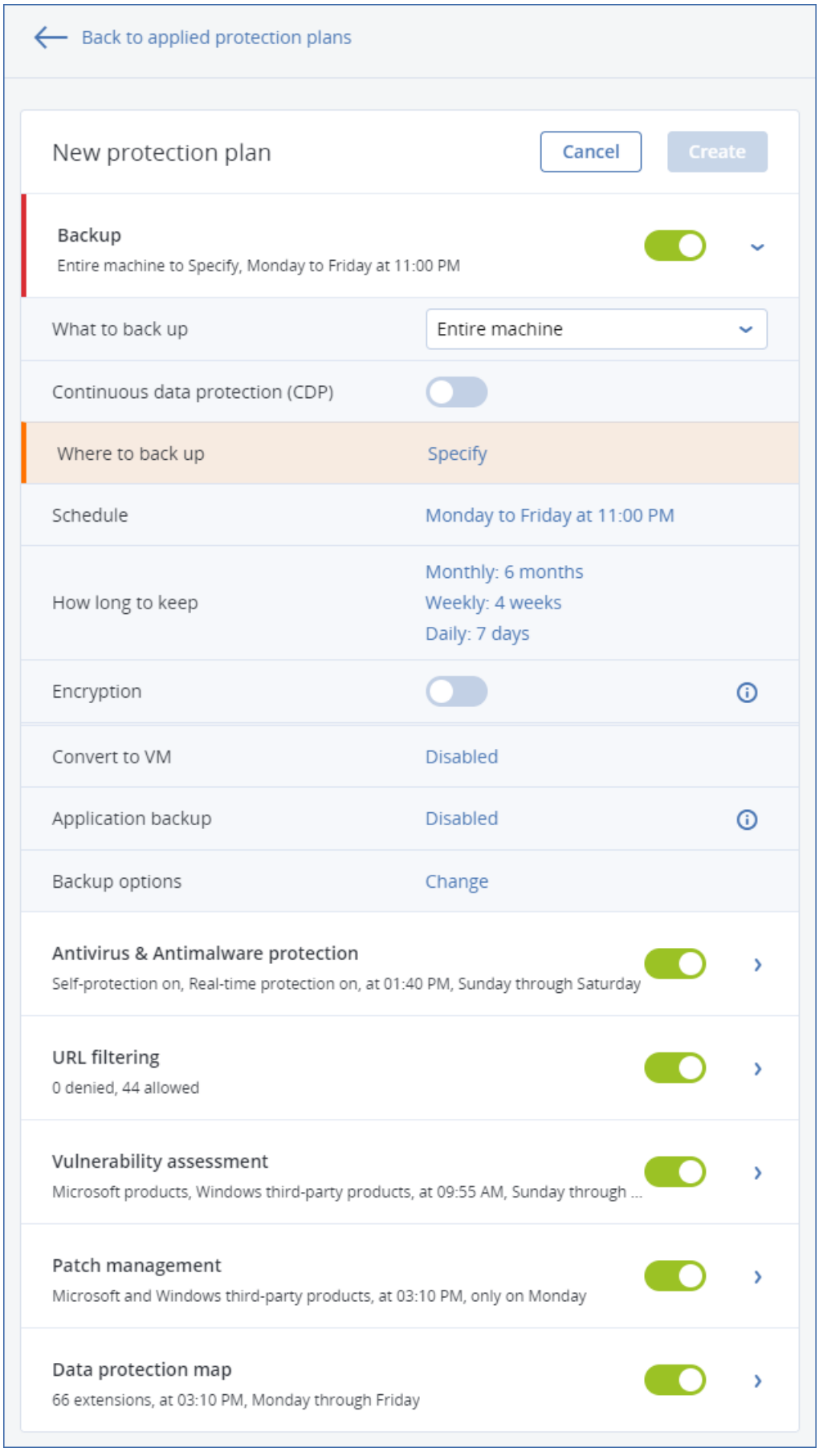
Plán ochrany je možné použít pro několik počítačů hned při jeho vytvoření nebo později.

Poznámka *Pokud se v případě místního nasazení na serveru pro správu nacházejí pouze standardní licence, nelze použít plán ochrany na více fyzických počítačů. Každý fyzický počítač musí mít svůj vlastní plán ochrany.*

Vytvoření prvního plánu ochrany s povoleným modulem zálohování

1. Vyberte počítače, které chcete zálohovat.
2. Klikněte na tlačítko **Chránit**.

Software zobrazí plány ochrany, které jsou na počítači použity. Pokud k počítači zatím žádné plány přiřazeny nejsou, zobrazí se výchozí plán ochrany, který lze použít. Nastavení můžete upravit podle potřeby a použít tento plán nebo vytvořit nový.

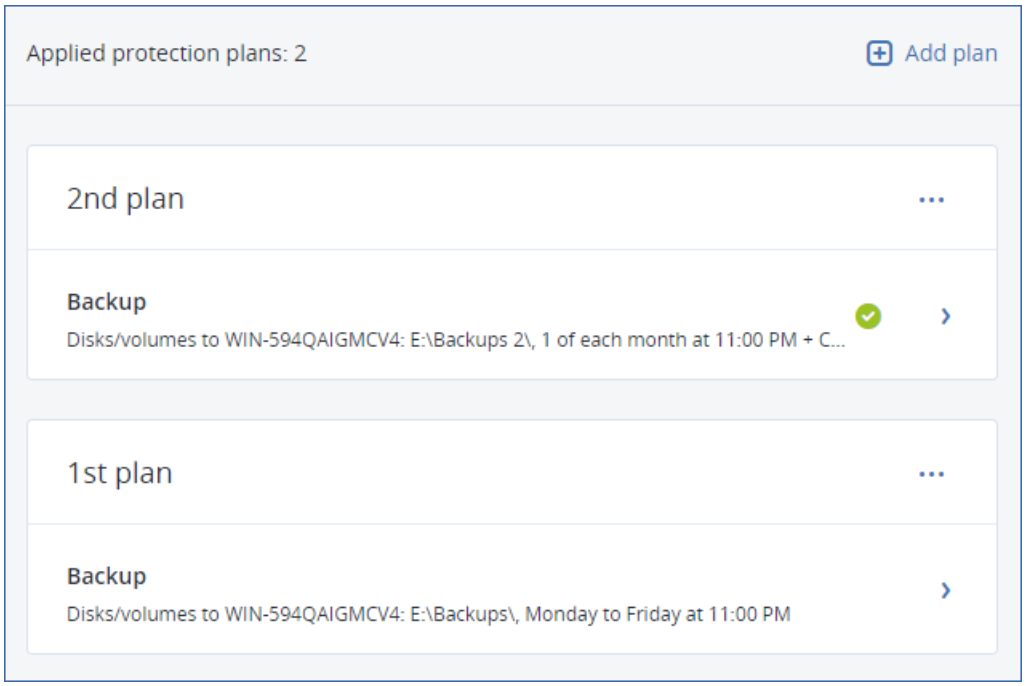

Back to applied protection plans
New protection plan
Cancel
Create
Backup
Entire machine to Specify, Monday to Friday at 11:00 PM
What to back up
Entire machine
Continuous data protection (CDP)
Where to back up
Specify
Schedule
Monday to Friday at 11:00 PM
How long to keep
Monthly: 6 months
Weekly: 4 weeks
Daily: 7 days
Encryption
Convert to VM
Disabled
Application backup
Disabled
Backup options
Change
Antivirus & Antimalware protection
Self-protection on, Real-time protection on, at 01:40 PM, Sunday through Saturday
URL filtering
0 denied, 44 allowed
Vulnerability assessment
Microsoft products, Windows third-party products, at 09:55 AM, Sunday through ...
Patch management
Microsoft and Windows third-party products, at 03:10 PM, only on Monday
Data protection map
66 extensions, at 03:10 PM, Monday through Friday

3. Chcete-li vytvořit nový plán, klikněte na položku **Vytvořit plán**. Povolte modul **Zálohování** a vraťte nastavení.
4. [Volitelné] Chcete-li upravit název plánu ochrany, klikněte na výchozí název.
5. [Volitelné] Chcete-li upravit parametry modulu Zálohování, klikněte na odpovídající část panelu plánu ochrany.
6. [Volitelné] Chcete-li upravit možnosti zálohování, klikněte na tlačítko **Změnit** vedle položky **Možnosti zálohování**.
7. Klikněte na tlačítko **Vytvořit**.

Použití existujícího plánu ochrany

1. Vyberte počítače, které chcete zálohovat.
2. Klikněte na tlačítko **Chránit**. Pokud je pro vybrané počítače již použit společný plán ochrany, klikněte na možnost **Přidat plán**.

   Software zobrazí dříve vytvořené plány ochrany.



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

6.1 Shrnutí modulu Zálohování

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

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

<table>
<tr><th>CO ZÁLOHOVAT</th><th>ZÁLOHOVANÉ POLOŽKY
Metody výběru</th><th>KAM ZÁLOHOVAT</th><th>PLÁN
Schémata zálohování
(neplatí pro cloud)</th><th>JAK DLOUHO UCHOVÁVAT</th></tr>
<tr><td>Disky/svazky (fyzické počítače)</td><td>Přímý výběr (str. 130)
Pravidla zásad (str. 130)
Filtry souborů (str. 172)</td><td>Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)
Server SFTP (str. 137)*
NFS (str. 137)*
Secure Zone (str. 137)*
Spravované umístění (str. 137)*
Páskové zařízení (str. 137)*</td><td rowspan="2">Vždy přírůstkový (jeden soubor) (str. 143)*
Vždy plná (str. 143)
Týdenní plná, denní přírůstková (str. 143)
Měsíčně plná, týdně rozdílová a denně přírůstková (GFS) (str. 143)
Vlastní (F-D-I) (str. 143)</td><td rowspan="4">Podle stáří zálohy (jedno pravidlo/na sadu záloh) (str. 152)
Podle počtu záloh (str. 152)
Podle celkové velikosti záloh (str. 152)*
Zachovat natrvalo (str. 152)</td></tr>
<tr><td>Disky/svazky (virtuální počítače)</td><td>Pravidla zásad (str. 130)
Filtry souborů (str. 172)</td><td>Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)
Server SFTP (str. 137)*
NFS (str. 137)*
Spravované umístění (str. 137)*
Páskové zařízení (str. 137)*</td></tr>
<tr><td>Soubory (pouze fyzické počítače)</td><td>Přímý výběr (str. 128)
Pravidla zásad (str. 128)
Filtry souborů (str. 172)</td><td>Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)
Server SFTP (str. 137)*
NFS (str. 137)*
Secure Zone (str. 137)*
Spravované umístění (str. 137)*
Páskové zařízení (str. 137)</td><td rowspan="2">Vždy plná (str. 143)
Týdenní plná, denní přírůstková (str. 143)
Měsíčně plná, týdně rozdílová a denně přírůstková (GFS) (str. 143)
Vždy přírůstkový (jeden soubor) (str. 143)*
Vlastní (F-D-I) (str. 143)</td></tr>
<tr><td>Konfigurace ESXi</td><td>Přímý výběr (str. 132)</td><td>Místní složka (str. 137)
Síťová složka (str. 137)
Server SFTP (str. 137)
NFS (str. 137)*</td></tr>
</table>

<table>
<tr><th>CO ZÁLOHOVAT</th><th>ZÁLOHOVANÉ POLOŽKY
Metody výběru</th><th>KAM ZÁLOHOVAT</th><th>PLÁN
Schémata zálohování
(neplatí pro cloud)</th><th>JAK DLOUHO UCHOVÁVAT</th></tr>
<tr><td>Stav systému (pouze v cloudových nasazeních)</td><td>Přímý výběr (str. 130)</td><td>Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)</td><td rowspan="3">Vždy plná (str. 143)
Týdenní plná, denní přírůstková (str. 143)
Vlastní (F-I) (str. 143)</td><td rowspan="3"></td></tr>
<tr><td>Databáze SQL</td><td>Přímý výběr (str. 303)</td><td rowspan="2">Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)
Spravované umístění (str. 137)*
Páskové zařízení (str. 137)</td></tr>
<tr><td>Databáze Exchange</td><td>Přímý výběr (str. 304)</td></tr>
<tr><td>Poštovní schránky Exchange</td><td>Přímý výběr (str. 310)</td><td rowspan="2">Cloud (str. 137)
Místní složka (str. 137)
Síťová složka (str. 137)
Spravované umístění (str. 137)*</td><td rowspan="2">Vždy přírůstková (jeden soubor) (str. 143)</td></tr>
<tr><td>Poštovní schránky Office 365</td><td>Přímý výběr (str. 323)</td><td>Podle stáří zálohy (jedno pravidlo/na sadu záloh) (str. 152)
Podle počtu záloh (str. 152)
Zachovat natrvalo (str. 152)</td></tr>
</table>

* Viz omezení níže.

Omezení

Server SFTP and páskové zařízení

- Tato umístění nemohou být cílem záloh počítačů s macOS.
- Tato umístění nemohou být cílem záloh s podporou aplikací.
- Schéma zálohování **Vždy přírůstkový (jeden soubor)** není při zálohování do těchto umístění k dispozici.
- Pravidlo zachování **Podle celkové velikosti záloh** není pro tato umístění k dispozici.

NFS

- Zálohování do sdílených úložišť NFS není v systému Windows dostupné.
- Schéma zálohování **Vždy přírůstkový (jeden soubor)** pro soubory (fyzické počítače) není při zálohování do úložišť NFS k dispozici.

Secure Zone

- Oddíl Secure Zone nelze vytvořit v počítačích Mac.
- Schéma zálohování **Vždy přírůstkový (jeden soubor)** pro soubory (fyzické počítače) není při zálohování do oddílu Secure Zone k dispozici.

Spravované umístění

- Spravované umístění s povolenou deduplikací nebo šifrováním nelze vybrat jako cíl:
  - Když je schéma zálohování nastaveno na možnost **Vždy přírůstkový (jeden soubor)**
  - Když je formát zálohy nastavený na **Verze 12**
  - Pro zálohy na úrovni disků počítačů s macOS
  - Pro zálohy poštovních schránek Exchange a poštovních schránek Office 365
- Pravidlo zachování **Podle celkové velikosti záloh** není pro spravovaná umístění se zapnutou deduplikací k dispozici.

Vždy přírůstková (jeden soubor)

- Schéma zálohování **Vždy přírůstkový (jeden soubor)** není při zálohování na server SFTP nebo páskové zařízení k dispozici.
- Schéma zálohování **Vždy přírůstkový (jeden soubor)** pro soubory (fyzické počítače) je k dispozici, pouze když je primární umístění zálohy Acronis Cloud.

Podle celkové velikosti záloh

- Pravidlo zachování **Podle celkové velikosti záloh** není k dispozici:
  - když je schéma zálohování nastaveno na možnost **Vždy přírůstková (jeden soubor)**,
  - Při zálohování na server SFTP, páskové zařízení nebo spravované umístění se zapnutou deduplikací

6.2 Výběr dat pro zálohování

6.2.1 Výběr souborů a složek

Zálohování na úrovni souborů je dostupné pro fyzické počítače a virtuální počítače zálohované agentem nainstalovaným v hostovaném systému.

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

Soubory lze vybrat dvěma způsoby: přímo na každém počítači nebo pomocí pravidel zásad. Obě metody umožňují další zpřesnění výběru pomocí filtrů souborů (str. 172).

Přímý výběr

1. V části **Co se má zálohovat** vyberte možnost **Soubory/složky**.
2. Klikněte na příkaz **Položky k zálohování**.
3. V části **Vybrat položky pro zálohování** vyberte možnost **Přímo**.
4. U každého počítače zahrnutého do plánu ochrany:
   a. Klikněte na možnost **Vybrat soubory a složky**.
   b. Klikněte na možnost **Místní složka** nebo **Síťová složka**.
      Sdílené umístění musí být na vybraném počítači dostupné.
   c. Vyhledejte požadované soubory a složky nebo cestu zadejte a klikněte na tlačítko s šipkou.
      Při zobrazení žádosti zadejte pro složku uživatelské jméno a heslo.
      Zálohování složky s anonymním přístupem není podporováno.
   d. Vyberte požadované soubory a složky.
   e. Klikněte na tlačítko **Hotovo**.

Použití pravidel zásad

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

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

Výběrová pravidla pro Windows

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

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

Výběrová pravidla pro Linux

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

Výběrová pravidla pro macOS

- Úplná cesta k souboru nebo adresáři.
- Šablony:
  - **`[All Profiles Folder]`** vybere složku **/Users**. Jedná se o složku, kde jsou ve výchozím nastavení umístěny všechny uživatelské profily.

Příklady:

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

- Chcete-li zálohovat adresář, kde jsou nainstalovány aplikace, zadejte **/Applications**.

6.2.2 Výběr stavu systému

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

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

Záloha stavu systému se skládá z následujících souborů:

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

6.2.3 Výběr disků nebo svazků

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

Existují dva způsoby výběru disků nebo svazků: přímo na každém počítači nebo pomocí pravidel zásad. Je možné vyloučit soubory ze zálohy disku nastavením funkce Filtry souborů (str. 172).

Přímý výběr

Přímý výběr je dostupný jen u fyzických počítačů. Chcete-li povolit přímý výběr disků a svazků na virtuálním počítači, musíte nainstalovat agenta pro kybernetickou ochranu v hostovaném operačním systému.

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

Použití pravidel zásad

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

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

Pravidla pro Windows, Linux a macOS

- **[All Volumes]** vybere všechny svazky se systémem Windows a všechny připojené svazky na počítačích se systémem Linux nebo macOS.

Pravidla pro Windows

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

Pravidla pro Linux

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

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

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

Chcete-li vybrat logický svazek, zadejte jeho cestu tak, jak se zobrazuje po spuštění příkazu **ls /dev/mapper** pod kořenovým účtem. Například:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

Tento výstup zobrazuje dva logické svazky, **lv1** a **lv2**, které patří do skupiny svazků **vg_1**. Chcete-li tyto svazky zálohovat, zadejte toto:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Pravidla pro macOS

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

6.2.3.1 Co ukládá záloha disku nebo svazku?

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

Se zapnutou možností zálohování (str. 190) **sektor po sektoru** obsahuje záloha disku všechny sektory disku. Zálohování sektor po sektoru lze použít k zálohování disků s nerozpoznaným nebo nepodporovaným systémem souborů a dalších vlastních datových formátů.

Windows

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

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

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

- Odkládací soubor (pagefile.sys) a soubor hiberfil.sys, který při hibernaci uchovává obsah paměti RAM. Po obnově se na odpovídajícím místě tyto soubory znovu vytvoří s nulovou velikostí.
- Záloha provedená v rámci operačního systému (na rozdíl od spouštěcího média nebo zálohování virtuálních počítačů na úrovni hypervizoru):
  - Stínová kopie svazku systému Windows. Cesta je určená hodnotou registru **VSS Default Provider**, kterou lze nalézt v klíči registru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. To znamená, že v operačních systémech počínaje systémem Windows Vista se body obnovení nezálohují.
  - Je-li možnost zálohování (str. 194) **Služba Stínová kopie svazku (VSS)** zapnutá, soubory a složky uvedené v klíči registru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** se nezálohují.

Linux

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

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

Mac

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

Následující položky jsou vyloučeny:

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

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

6.2.4 Výběr konfigurace ESXi

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

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

Záloha konfigurace hostitele ESXi zahrnuje následující položky:

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

Předpoklady

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

Omezení

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

Jak vybrat konfiguraci ESXi

1. Klikněte na **Zařízení** > **Všechna zařízení** a potom vyberte hostitele ESXi, které chcete zálohovat.
2. Klikněte na možnost **Zálohovat**.
3. V okně **Co se má zálohovat** vyberte možnost **Konfigurace ESXi**.
4. Do pole **Heslo účtu root ESXi** zadejte heslo účtu root každého z vybraných hostitelů nebo použijte stejné heslo u všech hostitelů.

6.3 Souvislá ochrana dat (CDP)

Zálohy se obvykle provádějí s pravidelnými, ale poměrně dlouhými intervaly z důvodů výkonu. Pokud dojde k náhlému poškození systému, změny dat mezi poslední zálohou a selháním systému budou ztraceny.

Funkce **Souvislá ochrana dat** umožňuje průběžné zálohování změn vybraných dat mezi naplánovanými zálohami:

- Sledováním změn v určených souborech/složkách
- Sledováním změn souborů změněných určenými aplikacemi

Z dat vybraných k zálohování můžete pro souvislou ochranu dat vybrat konkrétní soubory. Systém vytvoří zálohu každé změny těchto souborů. Tyto soubory můžete vrátit do okamžiku poslední změny.

Funkce **Souvislá ochrana dat** je momentálně podporována pro následující operační systémy:

- Windows 7 a novější
- Windows Server 2008 R2 a novější

Podporovaný systém souborů: Pouze NTFS, pouze místní složky (sdílené složky podporovány nejsou).

Možnost **Souvislá ochrana dat** není kompatibilní s možností **Zálohování aplikací**.

Jak to funguje

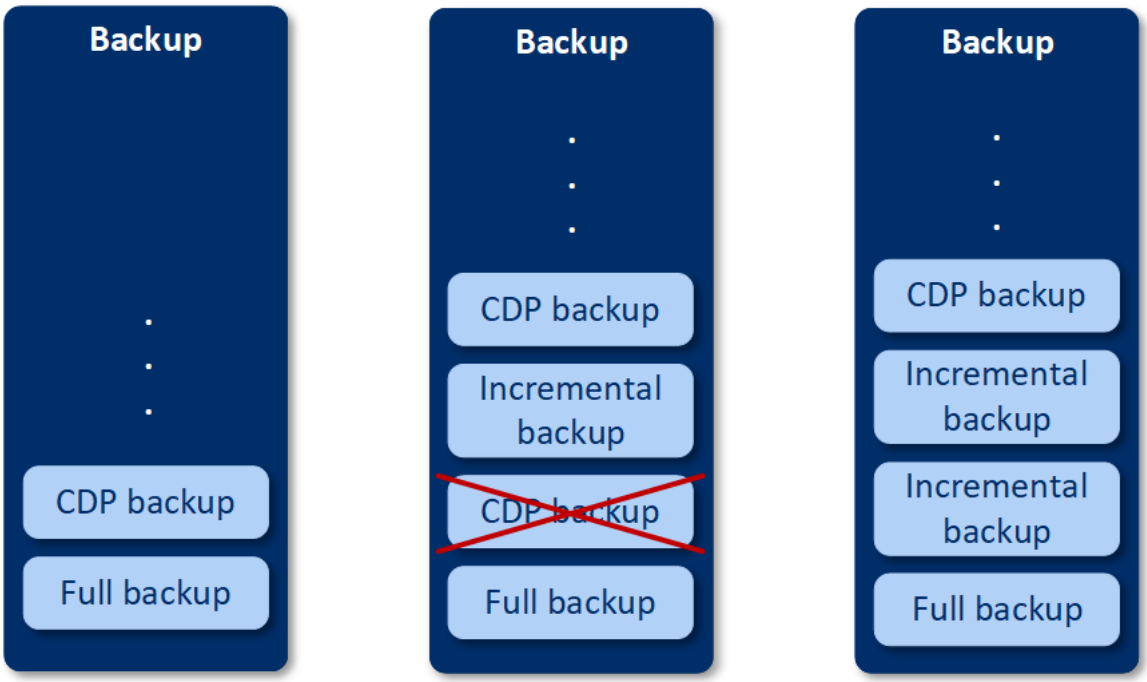
Zálohu, která se vytváří souvisle, nazveme zálohou souvislé ochrany dat. Před vytvořením zálohy souvislé ochrany dat je nejdříve nutné vytvořit plnou nebo přírůstkovou zálohu.

Při prvním spuštění plánu ochrany s povoleným plánem zálohování a **souvislou ochranou dat** se nejdříve vytvoří plná záloha. Následně se vytvoří záloha souvislé ochrany dat pro vybrané nebo změněné soubory a složky. Záloha souvislé ochrany dat vždy obsahuje vybraná data v nejnovějším

stavu. Když provedete změny ve vybraných souborech nebo složkách, nevytvoří se žádná nová záloha souvislé ochrany dat a všechny změny jsou zaznamenány do stejné zálohy souvislé ochrany dat.

Když nastane čas naplánované přírůstkové zálohy, záloha souvislé ochrany dat se zruší a po provedení přírůstkové zálohy se vytvoří nová záloha souvislé ochrany dat.

Záloha souvislé ochrany dat tak vždy zůstává nejnovější zálohou v řetězci záloh, protože má poslední aktuální stav chráněných souborů a složek.



Pokud již máte plán ochrany s povoleným modulem zálohování a rozhodnete se povolit **souvislou ochranu dat**, vytvoří se záloha souvislé ochrany dat hned po povolení možnosti, protože řetězec záloh již má plné zálohy.

Podporované zdroje dat a cílová umístění pro souvislou ochranu dat

Pokud má souvislá ochrana dat správně fungovat, musíte pro následující zdroje dat zadat následující položky:

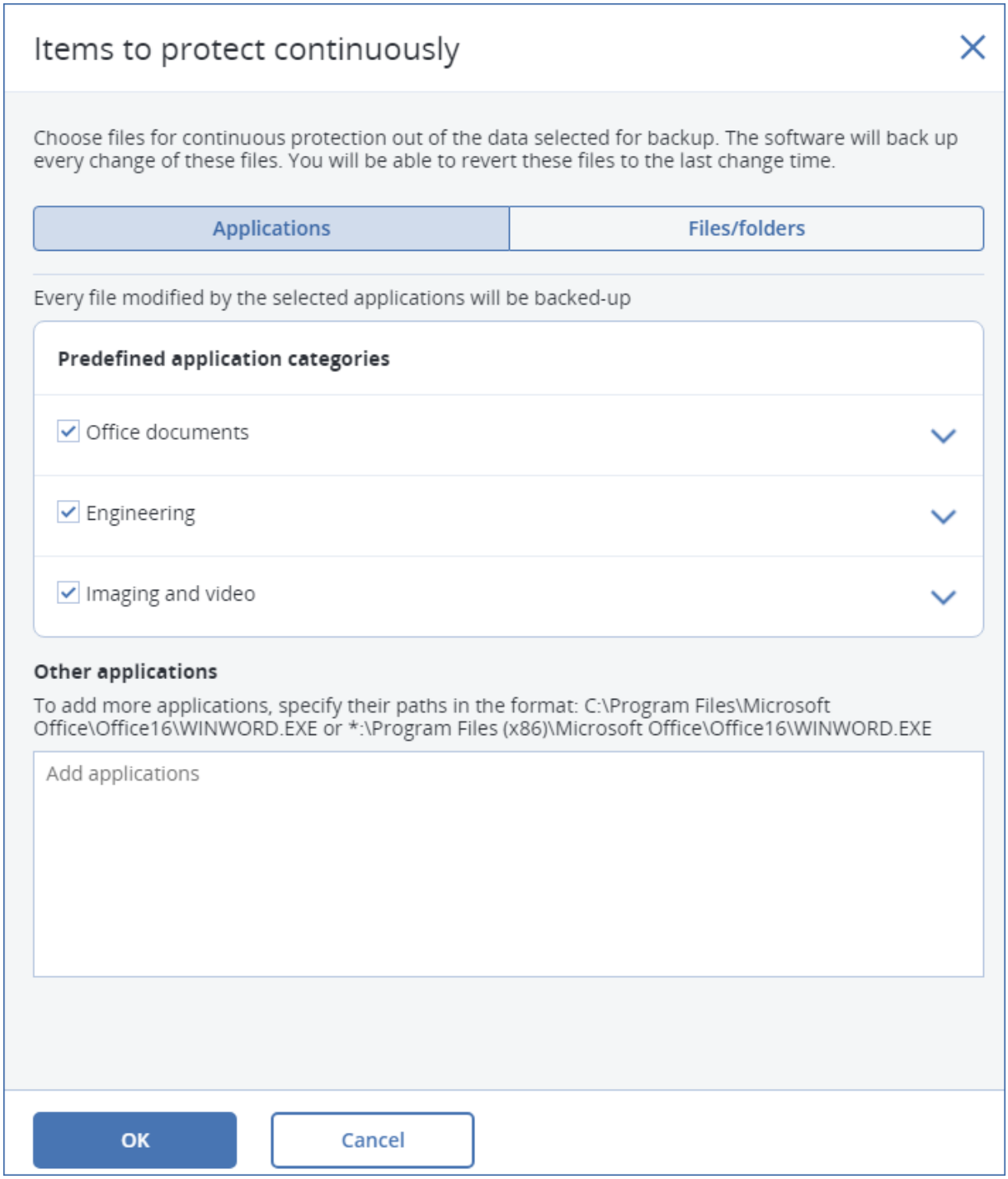
Co zálohovat	Položky k zálohování
Celý počítač	Je nutné zadat soubory/složky, nebo aplikace.
Disky/svazky	Je nutné zadat disky/svazky a soubory/složky, nebo aplikace.
Soubory/složky	Je nutné zadat soubory/složky. Aplikace lze zadat (není povinné).

Pro souvislou ochranu dat jsou podporována následující cílová umístění záloh:

- Místní složka
- Síťová složka
- Umístění definované skriptem
- Cloudové úložiště
- Acronis Cyber Infrastructure

Ochrana zařízení s použitím souvislé ochrany dat

1. Ve webové konzoli Cyber Protect vytvořte plán ochrany s povoleným modulem **zálohování**.
2. Povolte možnost **Souvislá ochrana dat (CDP)**.
3. Zadejte **položky, které mají být chráněny souvisle**:
   - **Aplikace** (každý soubor změněný vybranými aplikacemi bude zálohován). Tuto možnost doporučujeme použít k ochraně dokumentů sady Office s využitím zálohy souvislé ochrany dat.



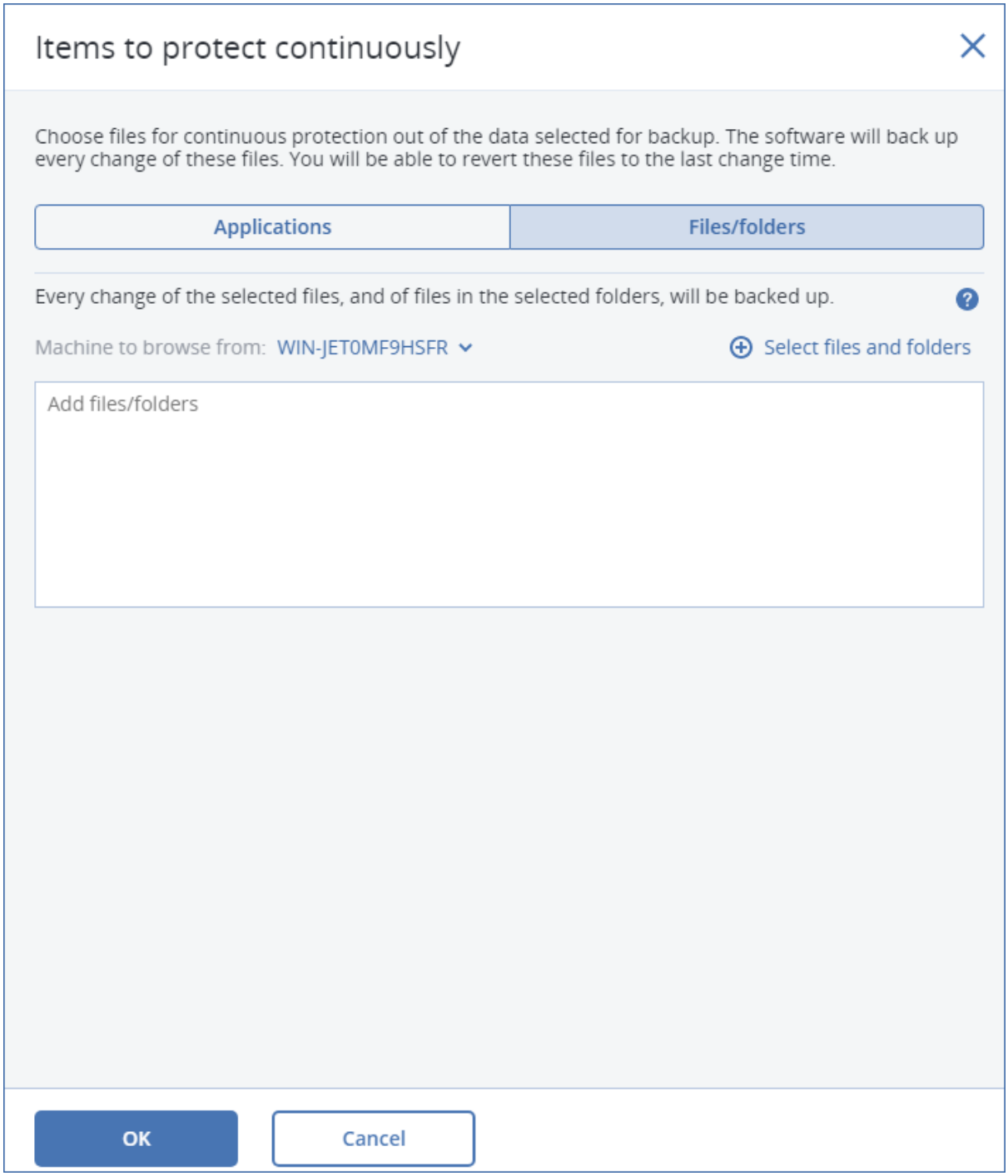
Můžete vybrat aplikace z předem definovaných kategorií nebo zadat jiné aplikace definováním cesty ke spustitelnému souboru aplikace. Použijte jeden z následujících formátů:

`C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

NEBO

***:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE**

- **Soubory/složky** (každý soubor změněný ve vybraném umístění bude zálohován). Tuto možnost doporučujeme použít k ochraně souborů a složek, které se neustále mění.



Počítač k procházení – zadejte počítač, jehož soubory/složky chcete vybrat pro souvislou ochranu dat.

Klikněte na možnost **Vybrat soubory a složky** a vyberte soubory/složky na zadaném počítači.

Důležité *Pokud ručně zadáte celou složku, jejíž soubory budou souvisle zálohovány, použijte masku, například:*
*Správná cesta: D:\Data**
Nesprávná cesta: D:\Data

V textovém poli můžete také zadat pravidla pro výběr souborů/složek, které budou zálohovány. Další podrobnosti o definování pravidel naleznete v tématu „Výběr souborů a složek (str. 128)“. Dokončete nastavení kliknutím na **Hotovo**.

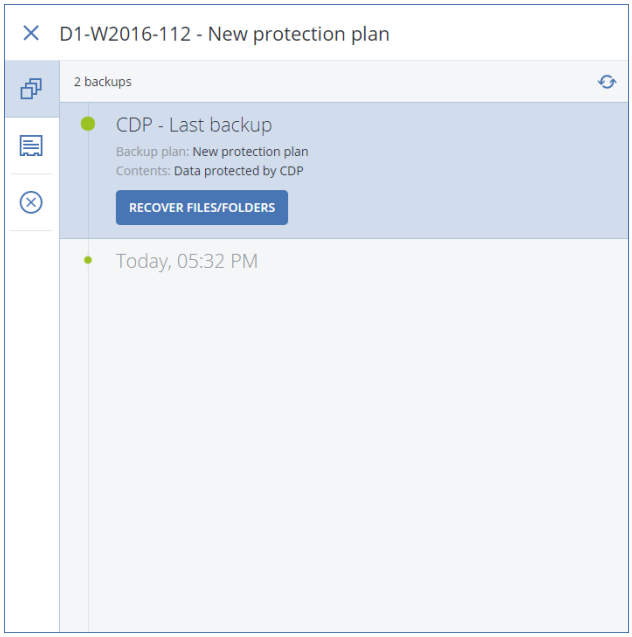
4. Klikněte na tlačítko **Vytvořit**.

Vybranému počítači bude přiřazen plán ochrany s povolenou souvislou ochranou dat. Po první běžné záloze budou souvisle vytvářeny zálohy s nejnovější kopií dat chráněných souvislou ochranou dat. Zálohována budou data definovaná pomocí aplikací i souborů/složek.

Souvisle zálohovaná data budou uchovávána podle zásad uchovávání definovaných pro modul zálohování.

Odlišení záloh, které jsou souvisle chráněny

Zálohy, které jsou souvisle chráněny, mají předponu CDP.



Obnovení celého počítače do posledního stavu

Pokud chcete mít možnost obnovit celý počítač do posledního stavu, můžete použít možnost **Souvislá ochrana dat (CDP)** v modulu zálohování plánu ochrany.

Ze zálohy souvislé ochrany dat můžete obnovit buď celý počítač, nebo soubory a složky. V prvním případě se celý počítač vrátí do posledního stavu, ve druhém se do posledního stavu vrátí soubory a složky.

6.4 Výběr cíle

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

Jak vybrat umístění zálohy

1. Klikněte na možnost **Kam se má zálohovat**.

2. Proveďte jeden z následujících úkonů:
   - Vyberte dříve použité nebo předem definované umístění zálohy.
   - Klikněte na **Přidat umístění** a potom zadejte nové umístění zálohy.

Podporovaná umístění

- **Cloudové úložiště**

  Zálohy se budou ukládat do cloudového datového centra.

- **Místní složka**

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

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

- **Síťová složka**

  Toto je složka sdílená pomocí SMB/CIFS/DFS.

  Vyhledejte požadovanou sdílenou složku nebo zadejte cestu v následujícím formátu:

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

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

  Potom klikněte na tlačítko s šipkou. Při zobrazení žádosti zadejte pro složku uživatelské jméno a heslo. Tato pověření můžete kdykoli změnit kliknutím na ikonu klíče vedle názvu složky.

  Zálohování složky s anonymním přístupem není podporováno.

- **Acronis Cyber Infrastructure**

  Acronis Cyber Infrastructure můžete použít jako vysoce spolehlivé softwarově definované úložiště s redundancí dat a automatickými samoopravnými procesy. Úložiště lze nakonfigurovat jako bránu pro ukládání záloh v Microsoft Azure nebo v různých řešeních pro ukládání dat kompatibilních se službou S3 nebo Swift. Toto úložiště může také fungovat jako NFS back-end. Další informace najdete v tématu O řešení Acronis Cyber Infrastructure (str. 142).

  Důležité *Zálohování do Acronis Cyber Infrastructure není k dispozici pro počítače se systémem macOS.*

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

  Vyhledejte požadovanou složku NFS nebo zadejte cestu v následujícím formátu:

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

  Potom klikněte na tlačítko s šipkou.

  Složky NFS chráněné heslem nelze zálohovat.

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

  Secure Zone je zabezpečený oddíl na disku zálohovaného počítače. Tento oddíl je nutné před konfigurací zálohy ručně vytvořit. Informace o tom, jak oddíl Secure Zone vytvořit a o jeho výhodách a omezeních naleznete v tématu O službě Secure Zone (str. 140).

- **SFTP**

  Zadejte název nebo adresu serveru SFTP. Podporovány jsou následující zápisy:

  `sftp://<server>`
  `sftp://<server>/<složka>`

  Po zadání uživatelského jména a hesla můžete procházet složky na serveru.

  V každém zápisu je také možné zadat port, uživatelské jméno a heslo.

```
sftp://<server>:<port>/<složka>
sftp://<uživatelské jméno>@<server>:<port>/<složka>
sftp://<uživatelské jméno>:<heslo>@<server>:<port>/<složka>
```

Pokud není určeno číslo portu, použije se port 22.

Uživatelé, pro které je nakonfigurován přístup prostřednictvím protokolu SFTP bez hesla, nemohou zálohovat na server SFTP.

Zálohování na servery FTP není podporováno.

Pokročilé možnosti úložiště

- **Definováno skriptem** (k dispozici v počítačích se systémem Windows)

  Zálohy jednotlivých počítačů můžete ukládat do složek definovaných skriptem. Software podporuje skripty napsané v jazyce JScript, VBScript nebo Python 3.5. Při nasazování plánu ochrany spustí software skript v každém počítači. Výstupem skriptu pro jednotlivé počítače by měla být místní nebo síťová cesta ke složce. Pokud složka neexistuje, bude vytvořena (omezení: skripty napsané v jazyce Python nemohou vytvářet složky v síťových úložištích). Na kartě **Úložiště záloh** se každá složka zobrazuje jako samostatné umístění zálohy.

  V části **Typ skriptu** vyberte typ skriptu (**JScript**, **VBScript** nebo **Python**) a potom daný skript naimportujte nebo zkopírujte a vložte. U síťových složek zadejte pověření k přístupu s oprávněními pro čtení a zápis.

  Příklad. Výstupem následujícího skriptu JScript je umístění zálohy počítače ve formátu **\\bkpsrv**<název počítače>:

  ```
  WScript.echo("\\\\bkpsrv\\" +
  WScript.CreateObject("WScript.Network").ComputerName);
  ```

  Zálohy jednotlivých počítačů budou ve výsledku ukládány do složky se stejným názvem na serveru **bkpsrv**.

- **Uzel úložišť**

  Uzel úložišť je server určený k optimalizaci použití různých prostředků (například firemní kapacity úložišť, zatížení sítě a vytížení procesoru produkčních serverů) potřebných k zabezpečení podnikových dat. Tohoto cíle lze dosáhnout uspořádáním a správou umístění, která slouží jako vyhrazená úložiště podnikových záloh (spravovaná umístění).

  Je možné vybrat dříve vytvořené umístění nebo vytvořit nové kliknutím na **Přidat umístění** > **Uzel úložišť**. Informace o nastaveních najdete v části Přidání spravovaného umístění (str. 434).

  Může se zobrazit výzva k zadání uživatelského jména a hesla pro uzel úložišť. Ke všem spravovaným umístěním v uzlu úložišť mají přístup členové následujících skupin Windows v počítači, kde je nainstalován uzel úložišť:

  - **Správci**
  - **Acronis ASN Remote Users**

    Skupina se vytvoří automaticky při instalaci uzlu úložišť. Ve výchozím nastavení je tato skupina prázdná. Můžete do ní ručně přidat uživatele.

- **Páska**

  Je-li páskové zařízení připojeno k zálohovanému počítači nebo k uzlu úložišť, zobrazí se v seznamu umístění výchozí fond pásek. Tento fond se vytvoří automaticky.

  Je možné vybrat výchozí fond nebo vytvořit nový kliknutím na **Přidat umístění** > **Páska**. Informace o nastavení fondů najdete v části Vytvoření fondu (str. 426).

6.4.1 O službě Secure Zone

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

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

Proč použít Secure Zone?

Secure Zone:

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

Omezení

- Oddíl Secure Zone nelze vytvořit na počítači Mac.
- Secure Zone je oddíl na základním disku. Nelze ho vytvořit na dynamickém disku nebo jako logický svazek (spravovaný službou LVM).
- Secure Zone se formátuje se systémem souborů FAT32. Protože FAT32 má pro velikost souborů limit 4 GB, větší zálohy se při uložení do oddílu Secure Zone rozdělují. Na proces a rychlost obnovy to nemá vliv.
- Secure Zone nepodporuje jednosouborový formát záloh (str. 451). Když změníte cíl na Secure Zone v plánu ochrany s metodou **Vždy přírůstková (jeden soubor)**, změní se tato metoda na **Týdenní plná, denní přírůstková**.

Jak tvorba oddílu Secure Zone transformuje disk.

- Oddíl Secure Zone se vytváří vždy na konci pevného disku.
- Pokud není na konci disku dostatek nepřiděleného místa, ale existuje nepřidělené místo mezi svazky, budou svazky přesunuty tak, aby se nepřidělené místo vyskytovalo na konci disku.
- Jestliže již bylo všechno nepřidělené místo shromážděno, ale stále to nestačí, aplikace využije volné místo ve vybraných svazcích a proporcionálně zmenší jejich velikost.
- Ve svazku však musí být volné místo, aby mohl fungovat operační systém a aplikace (například kvůli tvorbě dočasných souborů). Aplikace nebude zmenšovat svazky, kde volné místo tvoří méně než 25 % celkové velikosti svazku. Aplikace bude pokračovat v proporcionálním zmenšování svazků teprve tehdy, když budou všechny svazky na disku mít 25 % volného místa nebo méně.

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

Důležité *Při přesouvání a změně velikosti svazku, ze kterého je systém spuštěn, bude vyžadováno restartování počítače.*

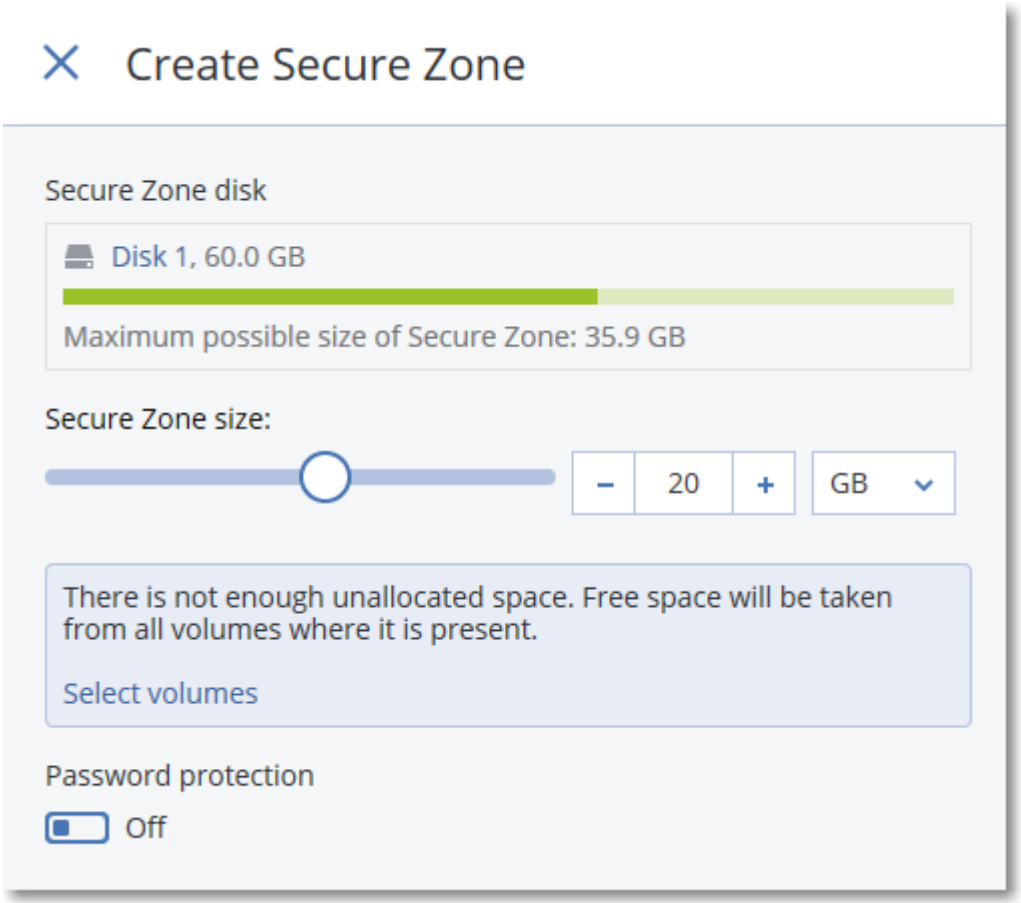
Jak vytvořit oddíl Secure Zone

1. Vyberte počítač, na kterém chcete vytvořit oddíl Secure Zone.

2. Klikněte na **Podrobnosti** > **Vytvořit Secure Zone**.
3. V části **Disk Secure Zone** klikněte na možnost **Vybrat** a potom vyberte pevný disk, na který chcete zónu vytvořit.

   Aplikace vypočítá maximální možnou velikost oddílu Secure Zone.
4. Zadejte velikost oddílu Secure Zone nebo určete velikost přetažením posuvníku mezi minimální a maximální hodnotou.

   Minimální velikost je přibližně 50 MB v závislosti na geometrii pevného disku. Maximální velikost odpovídá součtu nepřiděleného místa na disku a celkovému volnému místu na všech svazcích disku.
5. Jestliže všechno nepřidělené místo nepostačuje pro vámi zadanou velikost oddílu, aplikace využije volné místo na stávajících svazcích. Ve výchozím nastavení jsou vybrány všechny svazky. Chcete-li některé svazky vyloučit, klikněte na možnost **Vyberte svazky**. Jinak tento krok přeskočte.



6. [Volitelné] Povolte přepínač **Ochrana heslem** a zadejte heslo.

   Zadané heslo bude vyžadováno při přístupu k zálohám umístěným v oddílu Secure Zone. Při zálohování do oddílu Secure Zone není heslo vyžadováno, pokud není zálohování prováděno pro spouštěcí médium.
7. Klikněte na tlačítko **Vytvořit**.

   Software zobrazí očekávané rozložení oddílů. Klikněte na tlačítko **OK**.
8. Počkejte, až software vytvoří oddílu Secure Zone.

Nyní můžete při vytváření plánu ochrany vybrat oddíl Secure Zone v nabídce **Kam zálohovat**.

Jak odstranit oddíl Secure Zone

1. Vyberte počítač s oddílem Secure Zone.
2. Klikněte na **Podrobnosti**.
3. Klikněte na ikonu ozubeného kola vedle **Secure Zone** a poté klikněte na tlačítko **Odstranit**.
4. [Volitelné] Zadejte svazky, k nimž chcete přidat místo, které bude odstraněním zóny uvolněno. Ve výchozím nastavení jsou vybrány všechny svazky.

   Místo bude rozděleno rovnoměrně mezi vybrané svazky. Pokud nevyberete žádné svazky, uvolněné místo nebude přiděleno.

   Při změně velikosti svazku, ze kterého je systém spuštěn, bude vyžadováno restartování počítače.
5. Klikněte na možnost **Odstranit**.

Oddíl Secure Zone a všechny v něm uložené zálohy budou odstraněny.

6.4.2 O řešení Acronis Cyber Infrastructure

Acronis Cyber Protect 15 podporuje integraci s Acronis Cyber Infrastructure 3.5 Update 5 a novější verzí.

Zálohování do Acronis Cyber Infrastructure není k dispozici pro počítače se systémem macOS.

Instalace

Chcete-li používat řešení Acronis Cyber Infrastructure, nasaďte ho do hardwarových serverů ve firmě. K plnému využití produktu se doporučuje alespoň pět fyzických serverů. Pokud potřebujete pouze funkce brány, stačí použít jeden fyzický nebo virtuální server nebo nakonfigurovat cluster brány s využitím požadovaného počtu serverů.

Zajistěte synchronizaci času mezi serverem pro správu a řešením Acronis Cyber Infrastructure. Časová nastavení pro Acronis Cyber Infrastructure je možné nakonfigurovat v průběhu nasazování. Synchronizace času přes protokol NTP (Network Time Protocol) je ve výchozím nastavení zapnutá.

Můžete nasadit několik instancí Acronis Cyber Infrastructure a zaregistrovat je na stejném serveru pro správu.

Registrace

Registrace se provádí ve webovém rozhraní řešení Acronis Cyber Infrastructure. Acronis Cyber Infrastructure mohou registrovat pouze správci organizace a pouze v dané organizaci. Po registraci je úložiště dostupné všem organizačním jednotkám. Můžete ho také přidat jako umístění zálohy do libovolné jednotky nebo do organizace.

Reverzní operace (zrušení registrace) se provádí v rozhraní řešení Acronis Cyber Protect. Klikněte na **Nastavení** > **Uzly úložišť**, klikněte na požadovanou instanci Acronis Cyber Infrastructure a potom klikněte na **Odstranit**.

Přidání umístění zálohy

Do jednotky nebo organizace je možné přidat pouze jedno umístění zálohy na každou instanci Acronis Cyber Infrastructure. Umístění přidané na úrovni jednotky je dostupné této jednotce a správcům organizace. Umístění přidané na úrovni organizace je dostupné pouze správcům organizace.

Při přidávání umístění vytvoříte a zadáte jeho název. Jestliže potřebujete přidat existující umístění na nový nebo jiný server pro správu, zaškrtněte políčko **Použít existující umístění**, klikněte na **Procházet** a potom vyberte umístění ze seznamu.

Pokud je na serveru pro správu zaregistrováno několik instancí Acronis Cyber Infrastructure, je možné vybrat instanci Acronis Cyber Infrastructure při přidávání umístění.

Schémata zálohování, operace a omezení

Přímý přístup k Acronis Cyber Infrastructure ze spouštěcího média není k dispozici. Chcete-li pracovat s Acronis Cyber Infrastructure, zaregistrujte médium na serveru pro správu (str. 253) a spravujte ho pomocí webové konzole Cyber Protect.

Přístup k Acronis Cyber Infrastructure přes rozhraní příkazového řádku není k dispozici.

V případě dostupných schémat zálohování a operací se zálohami je řešení Acronis Cyber Infrastructure podobné cloudovému úložišti. Rozdíl je pouze v tom, že v průběhu provádění plánu ochrany je možné replikovat zálohy *z* Acronis Cyber Infrastructure.

Dokumentace

Celá sada dokumentace k řešení Acronis Cyber Infrastructure je k dispozici na webových stránkách společnosti Acronis.

6.5 Plán

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

Plán používá nastavení času (včetně časového pásma) operačního systému, ve kterém je agent nainstalován. Časové pásmo Agenta pro VMware (Virtual Appliance) lze nakonfigurovat v rozhraní agenta (str. 94).

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

Parametry plánu závisí na cíli zálohy.

Při zálohování do cloudového úložiště

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

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

Zálohy lze naplánovat tak, aby se spouštěly na základě událostí a ne na základě času. To provedete výběrem typu události v nástroji pro výběr plánu. Další informace najdete v části Plánování podle událostí (str. 145).

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

Při zálohování do jiných úložišť

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

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

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

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

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

Zálohy používají nový jednosouborový formát (str. 451).

Toto schéma zálohování není při zálohování na páskové zařízení, server SFTP nebo do Secure Zone k dispozici.

- **Vždy plná**

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

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

  Všechny zálohy jsou plné.

- **Týdenní plná, denní přírůstková**

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

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

- **Měsíčně plná, týdně rozdílová a denně přírůstková (GFS)**

  Ve výchozím nastavení se přírůstkové zálohy provádí denně, od pondělí do pátku, rozdílové zálohy každou sobotu a plné zálohy každý první den v měsíci. Tyto plány a čas spuštění zálohy můžete upravovat.

  Toto schéma zálohování se na panelu plánů ochrany zobrazuje jako **Vlastní**.

- **Vlastní**

  Určete plány pro plné, rozdílové a přírůstkové zálohy.

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

U všech schémat zálohování lze naplánovat, aby se zálohy spouštěly na základě událostí a ne na základě času. To provedete výběrem typu události v nástroji pro výběr plánu. Další informace najdete v tématu Plánování podle událostí (str. 145).

Další možnosti plánování

U každého cíle můžete provést toto:

- Zadejte podmínky spuštění zálohy, aby se naplánovaná záloha provedla pouze při splnění těchto podmínek. Další informace najdete v části Podmínky spuštění (str. 147).
- Nastavte období, pro které plán platí. Zaškrtněte políčko **Spustit plán v časovém rozsahu** a zadejte období.
- Vypněte použití plánu. Když je plán vypnutý, pravidla zachování se nepoužijí (pokud nebyla záloha spuštěna ručně).
- Nastavte zpoždění oproti naplánovanému času. Hodnota zpoždění u každého počítače se vybere náhodně a může být v rozsahu od nuly do maximální zadané hodnoty. Toto nastavení možná budete chtít použít při zálohování více počítačů do síťového umístění, abyste se vyhnuli nadměrnému zatížení sítě.

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

Poznámka: *Při cloudovém nasazení je tato možnost ve výchozím nastavení zapnutá a maximální zpoždění je nastaveno na 30 minut. Při místním nasazení jsou ve výchozím nastavení všechny zálohy zahájeny přesně podle plánu.*

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

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

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

6.5.1 Plánování podle událostí

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

Můžete si vybrat některou z následujících událostí:

- **Po uplynutí času od poslední zálohy**

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

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

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

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

  Musíte zadat vlastnosti události (str. 146).

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

CO ZÁLOHOVAT	Po uplynutí času od poslední zálohy	Když se uživatel přihlásí do systému	Když se uživatel odhlásí od systému	Při spuštění systému	Při vypnutí systému	Při události v protokolu událostí systému Windows
Disky/svazky nebo soubory (fyzické počítače)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Disky/svazky (virtuální počítače)	Windows, Linux	–	–	–	–	–

Konfigurace ESXi	Windows, Linux	–	–	–	–	–
Poštovní schránky Office 365	Windows	–	–	–	–	Windows
Databáze a poštovní schránky Exchange	Windows	–	–	–	–	Windows
Databáze SQL	Windows	–	–	–	–	Windows

6.5.1.1 Při události v protokolu událostí systému Windows

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

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

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

Vlastnosti události

Název protokolu

Udává název protokolu. V seznamu vyberte název standardního protokolu (**aplikační**, **zabezpečení** nebo **systémový**) nebo název protokolu zadejte, například: **Relace Microsoft Office**

Zdroj události

Udává zdroj události obvykle označující programovou nebo systémovou komponentu, která událost způsobila, například: **disk**.

Zdroj události, který obsahuje zadaný řetězec, spustí naplánovanou zálohu. Tato možnost nerozlišuje velká a malá písmena. Pokud tedy zadáte řetězec **service**, spustí zálohu zdroje události **Service Control Manager** a **Time-Service**.

Typ události

Uvádí typ události: **Chyba**, **Upozornění**, **Informace**, **Audit byl úspěšný** nebo **Audit se nezdařil**.

ID události

Udává číslo události, které obvykle identifikuje konkrétní druh událostí mezi událostmi stejného zdroje.

Například událost **Chyba** se zdrojem události **disk** a ID události **7** nastane, když systém Windows zjistí vadný blok na disku, zatímco událost **Chyba**se zdrojem události **disk** a ID události **15** nastane, když disk zatím není připraven na přístup.

Příklad: Nouzová záloha při zjištění vadného bloku

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

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

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

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

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

6.5.2 Podmínky spuštění

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

K těmto nastavením se dostanete tak, že při nastavování harmonogramu pro plán ochrany kliknete na možnost **Zobrazit více**.

Chování plánovače v případě, že podmínka (nebo více podmínek) není splněna, určuje možnost zálohy Podmínky spuštění zálohování (str. 194). Pro řešení situace, kdy podmínky nejsou splněny příliš dlouho a další odklad zálohování se stává rizikovým, můžete nastavit časový interval, po jehož uplynutí bude zálohování spuštěno bez ohledu na podmínku.

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

CO ZÁLOHOVAT	Disky/svazky nebo soubory (fyzické počítače)	Disky/svazky (virtuální počítače)	Konfigurace ESXi	Poštovní schránky Office 365	Databáze a poštovní schránky Exchange	Databáze SQL
Uživatel je nečinný (str. 148)	Windows	–	–	–	–	–
Hostitel umístění zálohy je dostupný (str. 148)	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Uživatelé se odhlásili (str. 149)	Windows	–	–	–	–	–
Vyhovuje časovému intervalu (str. 149)	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Šetřit baterii (str. 150)	Windows	–	–	–	–	–
Nespouštět při připojení účtovaném podle objemu dat (str. 150)	Windows	–	–	–	–	–

Nespouštět při připojení k následujícím sítím Wi-Fi (str. 151)	Windows	–	–	–	–	–
Kontrolovat IP adresu zařízení (str. 151)	Windows	–	–	–	–	–

6.5.2.1 Uživatel je nečinný

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

Příklad

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

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

Výsledek

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

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

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

6.5.2.2 Hostitel umístění zálohy je dostupný

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

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

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

Příklad

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

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

Výsledek:

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

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

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

6.5.2.3 Uživatelé se odhlásili

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

Příklad

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

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

Výsledek:

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

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

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

6.5.2.4 Vyhovuje časovému intervalu

Omezí čas spuštění zálohování na zadaný interval.

Příklad

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

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

Výsledek:

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

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

6.5.2.5 Šetřit baterii

Zabrání zálohování, pokud není zařízení (přenosný počítač nebo tablet) připojené k napájecímu zdroji. Podle hodnoty možnosti zálohování Podmínky spuštění zálohování (str. 194) se vynechané zálohování spustí nebo nespustí po připojení zařízení k napájecímu zdroji. Dostupné jsou následující možnosti:

- **Nespouštět při napájení z baterie**

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

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

Příklad

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

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

Výsledek:

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

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

6.5.2.6 Nespouštět při připojení účtovaném podle objemu dat

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

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

Příklad

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

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

Výsledek:

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

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

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

6.5.2.7 Nespouštět při připojení k následujícím sítím Wi-Fi

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

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

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

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

Příklad

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

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

Výsledek:

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

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

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

6.5.2.8 Kontrolovat IP adresu zařízení

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

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

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

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

Příklad

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

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

Výsledek:

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

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

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

6.6 Pravidla zachování

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

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

     Určete, jak dlouho budou zálohy vytvořené plánem ochrany uchovávány. Ve výchozím nastavení jsou pravidla zachování určena pro každou sadu záloh (str. 451) samostatně. Pokud chcete použít pro všechny zálohy jedno pravidlo, klikněte na možnost **Přepnout na jedno pravidlo pro všechny sady záloh**.
   - **Podle počtu záloh**

     Určete maximální počet záloh, které zůstanou zachovány.
   - **Podle celkové velikosti záloh**

     Určete maximální velikost záloh, které zůstanou zachovány.

     Toto nastavení není k dispozici u schématu zálohování **Vždy přírůstkový (jeden soubor)** ani při zálohování na cloudové úložiště, server SFTP nebo páskové zařízení.
   - **Zachovat zálohy na neurčito**
3. Zvolte, kdy se má spustit úloha vyčištění:
   - **Po záloze** (výchozí)

     Po vytvoření nové zálohy se použijí pravidla zachování.
   - **Před zálohou**

     Po vytvoření nové zálohy se použijí pravidla zachování.

     Toto nastavení není k dispozici při zálohování clusterů Microsoft SQL Serveru nebo Microsoft Exchange Serveru.

Co ještě potřebujete vědět

- Poslední záloha vytvořená v plánu ochrany bude vždy zachována, a to i v případě, že je zjištěno porušení pravidel zachovávání. Prosím, nepokoušejte se před zálohováním odstranit jedinou zálohu, kterou máte, aplikováním pravidel zachovávání.

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

  Toto chování je možné změnit pomocí možnosti zálohy Slučování záloh (str. 163).
- Pravidla uchovávání jsou součástí plánu ochrany. Přestanou pro zálohy počítače fungovat, jakmile je plán ochrany odejmut z počítače, nebo je ze serveru pro správu odstraněn samotný počítač. Pokud už nepotřebujete zálohy vytvořené podle plánu, odstraňte je podle pokynů v části Odstranění záloh (str. 223).

6.7 Šifrování

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

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

Šifrování v plánu ochrany

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

Určení nastavení šifrování v plánu ochrany

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

Šifrování jako vlastnost počítače

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

Uložení nastavení šifrování na počítači ovlivní plány ochrany následujícím způsobem:

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

Tuto možnost je možné použít na počítači, na kterém běží agent pro VMware. Postupujte však obezřetně v případě, kdy je ke stejnému serveru vCenter připojených o více agentů pro VMware. Pro

všechny agenty je potřeba použít stejné nastavení šifrování, protože mezi nimi funguje určitý způsob vyrovnávání zatížení.

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

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

Jak uložit nastavení šifrování na počítači

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

     `<instalační_cesta>` je instalační cesta agenta pro ochranu. Ve výchozím nastavení je to **%ProgramFiles%\BackupClient** v případě cloudového nasazení a **%ProgramFiles%\Acronis** v případě místního nasazení.
   - V systému Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<šifrovací_heslo>`

Jak resetovat nastavení šifrování na počítači

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

     `<instalační_cesta>` je instalační cesta agenta pro ochranu. Ve výchozím nastavení je to **%ProgramFiles%\BackupClient** v případě cloudového nasazení a **%ProgramFiles%\Acronis** v případě místního nasazení.
   - V systému Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Změna nastavení šifrování pomocí nástroje Cyber Protect Monitor.

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

Jak funguje šifrování

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

Šifrovací klíč je poté šifrován s algoritmem AES-256 pomocí hodnoty hashovací funkce SHA-256 hesla jako klíče. Samotné heslo není uloženo nikde na disku nebo v zálohách; hash hesla se používá pouze

k ověřovacím účelům. S tímto dvouúrovňovým zabezpečením jsou data chráněna před neautorizovaným přístupem, ale obnovení ztraceného hesla není možné.

6.8 Notarizace

Notarizace umožňuje potvrdit, že soubor je autentický a nebyl od zálohy změněn Notarizaci doporučujeme povolit při zálohování souborů právních dokumentů nebo dalších souborů, které vyžadují potvrzení pravosti.

Notarizace je dostupná pouze pro zálohy na úrovni souborů. Soubory s digitálním podpisem jsou přeskočeny, protože již notarizaci nevyžadují.

Notarizace *není* k dispozici:

- Když je formát zálohy nastavený na **Verze 11**.
- Pokud je cílem zálohy oddíl Secure Zone.
- Když je cílem zálohy spravované umístění s povolenou deduplikací nebo šifrováním.

Použití notarizace

Pokud chcete povolit notarizaci všech souborů zvolených pro zálohování (kromě souborů s digitálním podpisem), aktivujte při vytváření plánu ochrany přepínač **Notarizace**.

Při konfiguraci obnovení budou notarizované soubory označeny zvláštní ikonou a můžete ověřit pravost souborů (str. 209).

Jak to funguje

Během zálohování agent vypočítá kódy hash zálohovaných souborů, vytvoří hashovací strom (založený na struktuře složek), uloží strom do zálohy a poté odešle kořenový hashovací strom notářské službě. Notářská služba uloží kořenový hashovací strom v databázi blockchain Ethereum, čímž se zajistí, že tato hodnota se nezmění.

Při ověřování pravosti souborů agent vypočítá hash souboru a porovná jej s kódem hash, který je uložen v hashovacím stromu uvnitř zálohy. Pokud se kódy hash neshodují, soubor není považován za autentický. V opačném případě je autenticita souboru zaručena hashovacím stromem.

Chcete-li ověřit, že samotný hashovací strom nebyl zfalšován, agent odešle kořenový hashovací strom notářské službě. Notářská služba jej porovná se stromem uloženým v databázi blockchain. Když se kódy hash shodují, je zaručena autenticita souboru. V opačném případě se zobrazí zpráva s upozorněním, že soubor není autentický.

6.9 Převod na virtuální počítač

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

Převod na virtuální počítač je k dispozici pouze pro zálohy na úrovni disku. Pokud zálohy zahrnují systémový svazek a obsahují všechny informace potřebné ke spuštění operačního systému, může se výsledný virtuální počítač spustit samostatně. V opačném případě můžete jeho virtuální disky přidat k jinému virtuálnímu počítači.

Metody převodu

- **Pravidelný převod**

  Existují dva způsoby, jak konfigurovat pravidelný převod:

- **Nastavení převodu na součást plánu ochrany** (str. 157)

  Převod se provede po každém zálohování (pokud je konfigurováno pro primární umístění) nebo po každé replikaci (pokud je konfigurována pro druhé a další umístění).
- **Vytvoření zvláštního plánu převodu.** (str. 228)

  Tato metoda umožňuje specifikovat zvláštní plán převodu.

- **Obnovení do nového virtuálního počítače** (str. 200)

  Tato metoda vám umožní vybrat disky k obnově a upravit nastavení pro jednotlivé virtuální disky. Tuto metodu použijte, pokud chcete převod provést pouze jednou nebo jen příležitostně, například k provedení migrace fyzických počítačů na virtuální (str. 351).

6.9.1 Co potřebujete vědět o převodu

Podporované typy virtuálních počítačů

Převod zálohy na virtuální počítač může provést stejný agent, který vytvořil zálohu, nebo jiný agent.

Chcete-li provést převod na VMware ESXi nebo Hyper-V, potřebujete hostitele ESXi nebo Hyper-V a agenta pro ochranu (Agent pro VMware nebo Agent pro Hyper-V), který spravuje tohoto hostitele.

Převod na soubory VHDX předpokládá, že soubory budou připojeny jako virtuální disky k virtuálnímu počítači Hyper-V.

V následující tabulce je uveden souhrn typů virtuálních počítačů, které mohou agenti vytvořit:

Typ virtuálního počítače	Agent pro VMware	Agent pro Hyper-V	Agent pro Windows	Agent pro Linux	Agent pro Mac
VMware ESXi	+	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–
VMware Workstation	+	+	+	+	–
Soubory VHDX	+	+	+	+	–

Omezení

- Agent pro Windows, Agent pro VMware (Windows) a Agent pro Hyper-V nedokáže převádět zálohy uložené v NFS.
- Zálohy uložené na serveru NFS nebo SFTP nelze převádět ve zvláštním plánu převodu (str. 228).
- Zálohy uložené v oddílu Secure Zone mohou být převedeny pouze agentem spuštěným na stejném počítači.
- Zálohy, které obsahují logické svazky systému Linux (LVM), je možné převádět, pouze pokud byly vytvořeny Agentem pro VMware nebo Agentem pro Hyper-V a jsou-li nasměrované na stejný hypervizor. Převod mezi hypervizory není podporován.
- Když jsou zálohy počítače s Windows převedeny na VMware Workstation nebo soubory VHDX, výsledný virtuální počítač zdědí typ procesoru z počítače, který provádí převod. Výsledkem je, že v hostovaném operačním systému jsou nainstalovány příslušné ovladače procesoru. Pokud je spuštěn na hostiteli s jiným typem procesoru, hostovaný systém zobrazí chybu ovladače. V takovém případě aktualizujte ovladač ručně.

Porovnání pravidelného převodu na ESXi a Hyper-V a spuštění virtuálního počítače ze zálohy

Obě operace vám umožní vytvořit virtuální počítač, který může být spuštěn během několika sekund, pokud původní počítač selže.

Pravidelný převod klade vyšší nároky na výpočetní výkon a paměť. Soubory virtuálního počítače neustále zabírají místo v datovém úložišti. To nemusí být praktické, pokud je pro převod použit produkční hostitel. Výkon virtuálního počítače je však omezen pouze zdroji hostitele.

Při použití druhé metody jsou zdroje spotřebovány pouze, když je spuštěn virtuální počítač. Prostor datového úložiště je vyžadován pouze k uchování změn na virtuálních discích. Virtuální počítač však může pracovat pomaleji, protože hostitel nemá přímý přístup k virtuálním diskům, ale komunikuje s agentem, který čte data ze zálohy. Virtuální počítač je navíc pouze dočasný. Vytvoření trvalého počítače je možné pouze při použití konfigurace ESXi.

6.9.2 Převod na virtuální počítač v rámci plánu ochrany

Převod na virtuální počítač můžete konfigurovat z libovolného umístění zálohy nebo replikace, které se nachází v plánu ochrany. Převod se provede po každé záloze nebo replikaci.

Informace o požadavcích a omezeních najdete v tématu Co potřebujete vědět o převodu (str. 156).

Nastavení převodu na virtuální počítač v plánu ochrany

1. Vyberte umístění zálohy, ze kterého chcete provést převod.
2. Na panelu plánu ochrany klikněte na tlačítko **Převést na VM** pod tímto umístěním.
3. Zapněte přepínač **Převod**.
4. V poli **Převést na** vyberte typ cílového virtuálního počítače. Je možné vybrat jednu z následujících možností:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **Soubory VHDX**
5. Proveďte jeden z následujících úkonů:
   - VMware ESXi a Hyper-V: Klikněte na **Hostitel**, vyberte cílového hostitele a pak určete novou šablonu názvu počítače.
   - Ostatní typy virtuálních počítačů: Do pole **Cesta** zadejte, kam chcete uložit soubory virtuálního počítače, a šablonu názvu souboru.

   Výchozí název je **[Název počítače]_converted**.
6. [Volitelné] Klikněte na možnost **Agent, který provede převod** a potom vyberte požadovaného agenta.

   Převod může provádět agent, který provádí zálohování (výchozí nastavení), nebo agent nainstalovaný v jiném počítači. V případě agenta nainstalovaného v jiném počítači je třeba zálohy uložit do sdíleného umístění, například do síťové složky, aby k nim měly ostatní počítače přístup.
7. [Volitelné] Pro VMware ESXi a Hyper-V můžete také provést toto:
   - Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.
   - Změňte režim poskytování disku. Ve výchozím nastavení je pro VMware ESXi nastavena možnost **Tenké** a pro Hyper-V možnost **Dynamicky se rozšiřující**.

- Klikněte na **Nastavení virtuálního počítače** a změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.

8. Klikněte na tlačítko **Hotovo**.

6.9.3 Jak funguje typický převod do virtuálního počítače

Fungování opakovaných převodů závisí na vybraném umístění virtuálního počítače.

- **Pokud vyberete uložení virtuálního počítače jako sady souborů:** každý převod znovu vytvoří nový virtuální počítač.
- **Pokud zvolíte vytvoření virtuálního počítače na virtualizačním serveru:** při převodu přírůstkové nebo rozdílové zálohy aktualizuje software existující virtuální počítač místo jeho nového vytvoření. Takový převod je obvykle rychlejší. Šetří síťový provoz a prostředky procesoru na hostiteli, který provádí převod. Pokud není aktualizace virtuálního počítače možná, vytvoří jej software znovu od začátku.

Následuje podrobný popis obou případů.

Pokud vyberete uložení virtuálního počítače jako sady souborů

Výsledkem prvního převodu bude vytvoření nového virtuálního počítače. Každý další převod znovu vytvoří tento počítač od začátku. Nejprve je starý počítač dočasně přejmenován. Poté je vytvořen nový virtuální počítač s názvem starého počítače. Pokud se tato operace zdaří, dojde k odstranění původního počítače. Jestliže se tato operace nezdaří, nový počítač se odstraní a starému počítači bude navrácen jeho předchozí název. Tímto způsobem převod vždy skončí s jedním počítačem. Během převodu je však potřeba úložiště navíc pro uložení starého počítače.

Pokud zvolíte vytvoření virtuálního počítače na virtualizačním serveru:

První převod vytvoří nový virtuální počítač. Následné převody pracují následovně:

- Pokud od posledního převodu byla vytvořena *plná záloha*, bude virtuální počítač vytvořen znovu od začátku, jak bylo popsáno dříve v tomto tématu.
- Jinak se existující virtuální počítač aktualizuje podle změn od posledního převodu. Pokud není aktualizace možná (například pokud jste odstranili přechodný snímek, další informace naleznete níže), vytvoří software virtuální počítač znovu od začátku.

Přechodné snímky

Software ukládá několik přechodných snímků, aby mohl aktualizovat virtuální počítač. Jejich názvy budou **Záloha…** a **Replika…** a měli byste je zachovat. Nepotřebné snímky budou smazány automaticky.

Poslední snímek **Replika…** odpovídá výsledku posledního převodu. Tento snímek můžete použít, pokud chcete vrátit počítač do tohoto stavu, například pokud jste s počítačem pracovali a nyní chcete zrušit provedené změny.

Ostatní snímky jsou pro vnitřní potřeby aplikace.

6.10 Replikace

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

V této části je popsána replikace záloh jako součást plánu ochrany. Informace o vytvoření zvláštního plánu replikace naleznete v části Zpracování dat mimo hostitele (str. 224).

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

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

Příklady použití

- **Spolehlivá obnova po havárii**

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

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

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

Podporovaná umístění

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

- místní složka,
- síťová složka,
- Secure Zone
- Server SFTP
- Umístění spravovaná pomocí uzlu úložišť

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

- místní složka,
- síťová složka,
- cloudové úložiště.
- Server SFTP
- Umístění spravovaná pomocí uzlu úložišť
- páskové zařízení,

Jak povolit replikaci záloh

1. Na panelu plánu ochrany klikněte na položku **Přidat umístění**.

   Ovládací prvek **Přidat umístění** se zobrazí, pouze pokud je replikace podporována *z* naposledy vybraného umístění.
2. Zadejte umístění, kam se vytvořená záloha bude replikovat.
3. [Volitelné] V okně **Jak dlouho uchovávat** změňte pravidla zachování pro zvolené umístění podle postupu popsaného v části Pravidla zachování (str. 152).
4. [Volitelné] V části **Převést na VM** zadejte nastavení pro převod na virtuální počítač podle postupu popsaného v části Převod na virtuální počítač (str. 155).
5. [Volitelné] Klikněte na ikonu ozubeného kola > **Výkon a okno pro zálohování** a potom nastavte okno pro zálohování pro zvolené umístění způsobem popsaným v části Výkon a okno pro zálohování (str. 182). Tato nastavení definují výkon replikace.
6. [Volitelné] Kroky 1–5 zopakujte u všech umístění, kde chcete replikovat zálohy. Je podporováno až pět následných umístění včetně primárního.

6.10.1 Co je potřeba zvážit u uživatelů s licencí Advanced

Tip

Vytvořením samostatného plánu replikace můžete nastavit replikaci záloh *z* cloudového úložiště. Další informace najdete v tématu Zpracovávání dat mimo hostitele (str. 224).

Omezení

- Replikování záloh *z* umístění spravovaného uzlem úložišť to místní složky není podporováno. Místní složka představuje složku v počítači s agentem, který zálohu vytvořil.
- Replikování záloh *do* spravovaného umístění s povolenou deduplikací není podporováno pro zálohy, které mají formát záloh (str. 167) **Verze 12**.

Který počítač provádí operaci?

Replikování zálohy *z* jakéhokoliv umístění je spuštěno agentem, který vytvořil zálohu, a je provedeno:

- Agentem, pokud umístění *není* spravováno uzlem úložiště.
- Odpovídajícím uzlem úložišť, pokud je umístění spravované. Replikace zálohy ze spravovaného úložiště do cloudového úložiště se však provádí pomocí agenta, který zálohu vytvořil.

Jak vyplývá z popisu výše, operace může být provedena pouze v případě, že je počítač s agentem zapnut.

Replikování záloh mezi spravovanými umístěními

Replikování zálohy z jednoho spravovaného umístění do jiného se provádí pomocí uzlu úložišť.

Pokud je pro cílové úložiště povolena deduplikace (možná v jiném uzlu úložišť), zdrojový uzel úložišť odešle pouze ty bloky dat, které se nenacházejí v cílovém umístění. Jinými slovy uzel úložišť provádí (podobně jako agent) deduplikaci ve zdroji. To snižuje zatížení sítě při replikaci dat mezi geograficky oddělenými uzly úložišť.

6.11 Spouštění zálohy ručně

1. Vyberte počítač, který má alespoň jeden použitý plán ochrany.
2. Klikněte na možnost **Zálohovat**.
3. Pokud je použito více plánů ochrany, vyberte příslušný plán.
4. Proveďte jeden z následujících úkonů:
   - Klikněte na možnost **Spustit**. Vytvoří se přírůstková záloha.
   - Pokud schéma zálohování obsahuje několik metod zálohování, můžete zvolit metodu, kterou chcete použít. Klikněte na šipku tlačítka **Spustit** a potom vyberte **Plná, Přírůstková** nebo **Rozdílová**.

První záloha vytvořená v plánu ochrany je vždy plná.

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

6.12 Možnosti zálohování

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

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

Dostupnost možností zálohování

Sada dostupných možností zálohování závisí na:

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

Následující tabulka shrnuje dostupnost možností zálohování.

	Záloha na úrovni disku			Záloha na úrovni souborů			Virtuální počítače			SQL a Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Computing	Windows
Výstrahy (str. 163)	+	+	+	+	+	+	+	+	+	+
Slučování záloh (str. 163)	+	+	+	+	+	+	+	+	+	-
Název souboru zálohy (str. 164)	+	+	+	+	+	+	+	+	+	+
Formát zálohy (str. 167)	+	+	+	+	+	+	+	+	+	+
Ověření zálohy (str. 168)	+	+	+	+	+	+	+	+	+	+
Sledování změněných bloků (CBT) (str. 169)	+	-	-	-	-	-	+	+	+	+
Režim zálohování clusteru (str. 169)	-	-	-	-	-	-	-	-	-	+
Úroveň komprese (str. 170)	+	+	+	+	+	+	+	+	+	+
E-mailová upozornění (str. 170)	+	+	+	+	+	+	+	+	+	+
Zpracování chyb (str. 171)										
Pokud dojde k chybě, pokusit se znovu	+	+	+	+	+	+	+	+	+	+
Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)	+	+	+	+	+	+	+	+	+	+
Ignorovat chybné sektory	+	+	+	+	+	+	+	+	+	-
Pokusit se znovu, pokud dojde k chybě při tvorbě snímku virtuálního počítače	-	-	-	-	-	-	+	+	+	-

Rychlá přírůstková/rozdílová záloha (str. 172)	+	+	+	-	-	-	-	-	-	-
Filtry souborů (str. 172)	+	+	+	+	+	+	+	+	+	-
Snímky záloh na úrovni souborů (str. 174)	-	-	-	+	+	+	-	-	-	-
Zkrácení protokolu (str. 181)	-	-	-	-	-	-	+	+	-	Pouze SQL
Zachycování snímků LVM (str. 181)	-	+	-	-	-	-	-	-	-	-
Přípojné body (str. 181)	-	-	-	+	-	-	-	-	-	-
Snímek více svazků (str. 182)	+	+	-	+	+	-	-	-	-	-
Výkon a okno pro zálohování (str. 182)	+	+	+	+	+	+	+	+	+	+
Odesílání fyzických dat (str. 185)	+	+	+	+	+	+	+	+	+	-
Příkazy před-po (str. 186)	+	+	+	+	+	+	+	+	+	+
Příkazy před/po získání dat (str. 188)	+	+	+	+	+	+	+	-	-	+
Snímky hardwaru SAN (str. 189)	-	-	-	-	-	-	+	-	-	-
Plánování (str. 189)										
Rozložit čas spuštění do časového rámce	+	+	+	+	+	+	+	+	+	+
Omezení počtu souběžně spuštěných záloh	-	-	-	-	-	-	+	+	+	-
Zálohování sektor po sektoru (str. 190)	+	+	-	-	-	-	+	+	+	-
Rozdělování (str. 191)	+	+	+	+	+	+	+	+	+	+
Správa pásek (str. 191)	+	+	+	+	+	+	+	+	+	+
Zpracování selhání úlohy (str. 193)	+	+	+	+	+	+	+	+	+	+
Podmínky spuštění úlohy (str. 194)	+	+	-	+	+	-	+	+	+	+
Služba Stínová kopie svazku (VSS) (str. 194)	+	-	-	+	-	-	-	+	-	+
Služba Stínová kopie svazku (VSS) pro virtuální počítače (str. 195)	-	-	-	-	-	-	+	+	+	-

Týdenní zálohování (str. 195)	+	+	+	+	+	+	+	+	+	+
Protokol událostí systému Windows (str. 196)	+	-	-	+	-	-	+	+	+	+

6.12.1 Výstrahy

Žádné úspěšné zálohy po určený počet po sobě jdoucích dní

Výchozí nastavení: **Zakázáno**.

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

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

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

6.12.2 Slučování záloh

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

Výchozí nastavení: **Zakázáno**.

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

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

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

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

Tato možnost *není* účinná, pokud:

- Záloha je umístěna na páskovém zařízení nebo v cloudovém úložišti.
- Schéma zálohování je nastaveno na možnost **Vždy přírůstkový (jeden soubor)**.
- Formát zálohy (str. 167) je nastavený na **Verze 12**.

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

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

Ve všech ostatních případech budou zálohy s odloženým odstraněním v GUI označeny ikonou odpadkového koše (). Pokud takovou zálohu odstraníte kliknutím na znak X, proběhne sloučení. Zálohy uložené na pásce zmizí z GUI až po přepsání nebo smazání pásky.

6.12.3 Název souboru zálohy

Tato možnost určuje názvy souborů záloh vytvořené plánem ochrany.

Tyto názvy se zobrazují při prohlížení umístění zálohy ve správci souborů.

Co je soubor zálohy?

Každý plán ochrany vytváří v umístění zálohy jeden nebo více souborů v závislosti na použitém schématu zálohování a formátu zálohy (str. 167). Následující tabulka uvádí soubory, které může vytvořit počítač nebo poštovní schránka.

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

Všechny soubory mají stejný název, ale mohou mít navíc časové razítko nebo pořadové číslo. Tento název (jinak také název souboru zálohy) můžete určit při vytváření nebo úpravě plánu ochrany.

Poznámka *Časové razítko se k souboru zálohy přidá pouze ve formátu zálohy* ***Verze 11****.*

Pokud nezměníte název souboru zálohy na název již existující zálohy stejného počítače, bude další zálohou plná záloha. Když použijete již existující název, provede se záloha (plná, přírůstková nebo rozdílová) podle harmonogramu plánu ochrany.

Názvy souborů zálohy je možné nastavit pro umístění, které nelze procházet správcem souborů (jako je cloudové úložiště nebo páskové zařízení). To je vhodné v případě, že chcete na kartě **Úložiště záloh** vidět vlastní názvy.

Kde mohu vidět názvy souboru zálohy?

Vyberte kartu **Úložiště záloh** a pak vyberte skupinu záloh.

- Na panelu **Podrobnosti** se zobrazí výchozí název souboru zálohy.
- Pokud nastavíte nevýchozí název souboru zálohy, zobrazí se přímo na kartě **Úložiště záloh** ve sloupci **Název**.

Omezení názvů souborů záloh

- Název souboru zálohy nesmí končit číslicí.

  Aby se zabránilo tomu, že bude název souboru zálohy končit číslicí, připojuje se k názvu souboru zálohy ve výchozím nastavení písmeno A. Když budete vytvářet vlastní název, dávejte vždy pozor na to, aby nekončil číslicí. Při používání proměnných nesmí název proměnnou končit, protože proměnná by mohla končit číslicí.
- Název souboru zálohy nesmí obsahovat následující symboly: **()&?*$<>":\|/#**, znaky konce řádku (**\n**) ani tabulátory (**\t**).

Výchozí název souboru zálohy

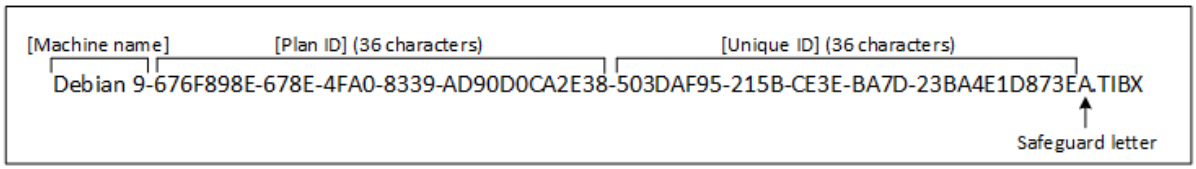
Výchozí název souboru zálohy je **[Machine Name]-[Plan ID]-[Unique ID]A**.

Výchozí název souboru zálohy pro zálohu poštovní schránky je **[Mailbox ID]_mailbox_[Plan ID]A**.

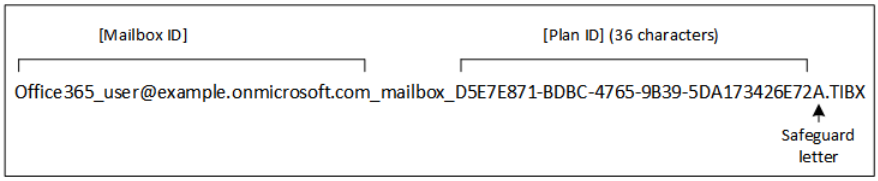
Název se skládá z následujících proměnných:

- **[Machine Name]** Za tuto proměnnou se dosazuje název počítače (je to stejný název, jaký se zobrazuje ve webové konzoli Cyber Protect) pro všechny typy zazálohovaných dat, kromě poštovních schránek Office 365. Pro poštovní schránky Office 365 se za tuto proměnnou dosazuje hlavní název (UPN) uživatele poštovní schránky.
- **[Plan ID]**: Za tuto proměnnou se dosazuje jedinečný identifikátor plánu ochrany. Tato hodnota se v případě přejmenování plánu nemění.
- **[Unique ID]**: Za tuto proměnnou se dosazuje jedinečný identifikátor vybraného počítače nebo poštovní schránky. Tato hodnota se v případě přejmenování počítače nebo změně hlavního názvu uživatele (UPN) poštovní schránky nemění.
- **[Mailbox ID]**: Za tuto proměnnou se dosazuje hlavní název uživatele (UPN) poštovní schránky.
- **"A"** je písmeno, které se pro jistotu připojuje k názvu, aby se zabránilo tomu, že bude končit číslicí.

V níže uvedeném diagramu vidíte výchozí název souboru zálohy.



V níže uvedeném diagramu vidíte výchozí název souboru zálohy pro poštovní schránky.



Názvy bez proměnných

Pokud změníte název souboru zálohy na **MyBackup**, budou soubory záloh vypadat tak, jak vidíte v následujících příkladech. U obou příkladů se předpokládají každodenní přírůstkové zálohy naplánované na 14:40 počínaje 13. zářím 2016.

Pro formát **Verze 12** se schématem zálohování **Vždy přírůstkový (jeden soubor)**:

```
MyBackup.tibx
```

Pro formát **Verze 12** s jinými schématy zálohování:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Pro formát **Verze 11** se schématem zálohování **Vždy přírůstkový (jeden soubor)**:

```
MyBackup.xml
MyBackup.tib
```

Pro formát **Verze 11** s jinými schématy zálohování:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Používání proměnných

Kromě proměnných, které se používají ve výchozím nastavení, můžete použít proměnnou **[Plan name]**, za kterou se dosazuje název plánu ochrany.

Pokud je pro zálohu vybráno více počítačů nebo poštovních schránek, musí název souboru zálohy obsahovat proměnnou **[Machine Name]**, **[Mailbox ID]** nebo **[Unique ID]**.

Název souboru zálohy vs. zjednodušené pojmenovávání souborů

Pomocí prostého textu a/nebo proměnných můžete vytvářet stejné názvy souborů jako v předchozích verzích Acronis Cyber Protect. Není však možné dosáhnout zjednodušených názvů souborů – ve verzi 12 bude mít název souboru časovou značku, pokud nebude použit formát jednoho souboru.

Příklady použití

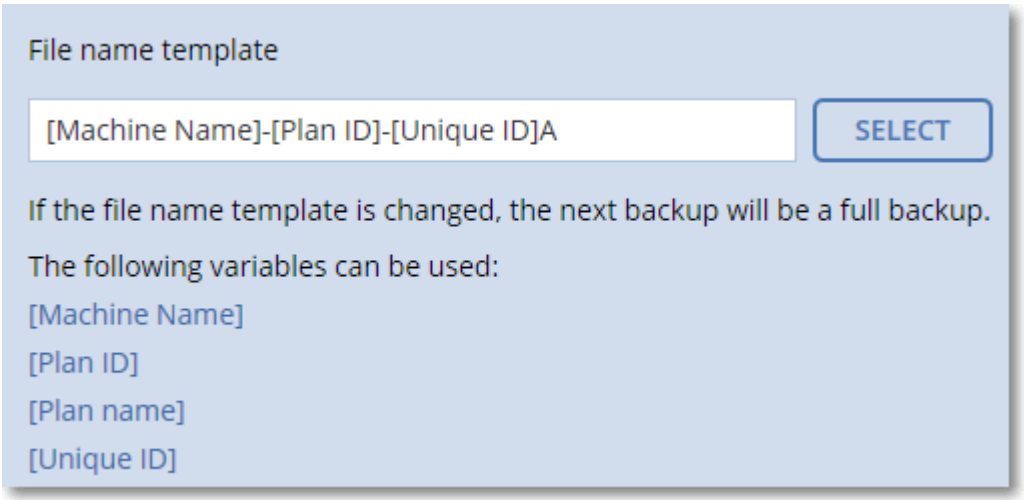
- **Zobrazení uživatelsky přívětivých názvů souborů**

  Při procházení umístění záloh pomocí správce souborů je důležité, abyste od sebe zálohy dokázali snadno rozlišit.

- **Pokračování v existující sekvenci záloh**

  Předpokládejme, že je plán ochrany použitý pro jediný počítač a vy tento počítač musíte odebrat z webové konzole Cyber Protect nebo musíte odinstalovat agenta společně s jeho konfiguračním nastavením. Po opětovném přidání počítače nebo přeinstalaci agenta můžete vynutit, aby plán ochrany pokračoval v zálohování do stejné zálohy nebo podle stejné sekvence zálohování. Stačí vybrat tuto volbu, kliknout na **Vybrat** a vybrat požadovanou zálohu.

  Tlačítkem **Procházet** zobrazíte zálohy v umístění vybraném v části **Kam se má zálohovat** panelu plánu ochrany. Neumožňuje zobrazit obsah žádného jiného umístění.



- **Upgrade z předchozích verzí produktu**

Pokud se během upgradu plán ochrany nemigroval automaticky, vytvořte ho znovu a přesměrujte ho na původní soubor zálohy. Pokud je pro zálohování vybraný jenom jeden počítač, klikněte na **Procházet** a vyberte požadovanou zálohu. Pokud je pro zálohování vybraných více počítačů, vytvořte znovu původní soubor zálohy pomocí proměnných.

Poznámka *Tlačítko* ***Vybrat*** *je aktivní pouze pro plány ochrany, které jsou vytvořeny a použity pro jedno zařízení.*

6.12.4 Formát zálohy

Tato možnost určuje formát záloh vytvořených plánem ochrany. K dispozici je pouze pro plány ochrany, které používají starší formát zálohy **Verze 11**. V tomto případě ho můžete změnit na nový formát **Verze 12**. Po této změně nebude už tato možnost dostupná.

Tato možnost *není* dostupná pro zálohy poštovních schránek. Zálohy poštovních schránek budou mít vždy nový formát.

Výchozí nastavení: **Automatický výběr**.

Je možné vybrat jednu z následujících možností:

- **Automatický výběr**

  Pokud plán ochrany nepřipojuje zálohy k zálohám vytvořeným staršími verzemi produktu, použije se formát Verze 12.
- **Verze 12**

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

  Při použití tohoto formátu není pravidlo **Podle celkové velikosti záloh** platné.
- **Verze 11**

  Starší formát zachovaný za účelem zpětné kompatibility. Můžete připojit zálohy k zálohám vytvořeným staršími verzemi produktu.

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

  Tento formát se automaticky vybere, pokud je cílem zálohy (nebo replikace) spravované umístění s povolenou deduplikací. Pokud formát změníte na formát **Verze 12**, zálohy selžou.

  Poznámka *Skupiny dostupnosti databáze (DAG) nelze zálohovat pomocí formátu archivu Verze 11. Zálohování DAG je podporováno pouze ve formátu archivu Verze 12.*

Formát a soubory záloh

U umístění záloh, které je možné procházet pomocí správce souborů (například místní nebo síťové složky), určuje formát záloh počet souborů a jejich přípony. Názvy souborů můžete definovat mocí volby název souboru zálohy (str. 164). Následující tabulka uvádí soubory, které může vytvořit počítač nebo poštovní schránka.

	Vždy přírůstková (jeden soubor)	**Jiná schémata zálohování**
Formát zálohy **Verze 11**	Jeden soubor TIB a jeden soubor metadat XML	Několik souborů TIB a jeden soubor metadat XML (běžný formát)

Formát zálohy **Verze 12**	Jeden soubor TIBX pro každý řetězec záloh (plná nebo rozdílová záloha a všechny závislé přírůstkové zálohy)

Změna formátu zálohy na verzi 12 (.tibx)

Pokud změníte formát zálohy z **Verze 11** (formát .tib) na **Verze 12** (formát .tibx):

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

Deduplikace v archivu

Formát **Verze 12** podporuje deduplikaci v archivu, která přináší následující výhody:

- Desetinásobně menší velikost záloh s integrovanou deduplikací libovolného typu dat na úrovni bloku
- Díky efektivnímu zpracování pevných odkazů nejsou v úložištích duplicitní položky
- Dělení na základě hodnot hash

Poznámka *Ve výchozím nastavení je pro všechny zálohy ve formátu .tibx povolena deduplikace v archivu. Není nutné ji povolit v možnostech zálohování a nelze ji zakázat.*

6.12.5 Ověření zálohy

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

Výchozí nastavení: **Zakázáno**.

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

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

Zatímco úspěšné ověření znamená vysokou pravděpodobnost úspěšné obnovy, nekontrolují se všechny faktory, které ovlivňují proces obnovy. Pokud zálohujete operační systém, doporučujeme provést zkušební obnovení se spouštěcím médiem na náhradní pevný disk nebo spuštění virtuálního počítače z této zálohy (str. 326) v prostředí ESXi nebo Hyper-V.

6.12.6 Sledování změněných bloků (CBT)

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

Výchozí nastavení: **Povoleno**.

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

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

6.12.7 Režim zálohování clusteru

Tyto možnosti platí pro zálohy Microsoft SQL Serveru a Microsoft Exchange Serveru na úrovni databází.

Tyto možnosti platí pouze v případě, že nejsou pro zálohování vybrané jednotlivé uzly nebo databáze v rámci clusteru, ale cluster samotný (skupiny dostupnosti Always On Microsoft SQL Serveru (AAG) nebo skupina dostupnosti databáze Microsoft Exchange Serveru (DAG)). Pokud vyberete jednotlivé položky v clusteru, nebude záloha podporovat cluster a budou se zálohovat pouze vybrané kopie těchto položek.

Microsoft SQL Server

Tato možnost určuje režim zálohování pro skupiny dostupnosti Always On SQL Serveru (AAG). Aby byla tato možnost účinná, musí být ve všech uzlech AAG nainstalován agent pro SQL. Další informace o zálohování skupin AAG najdete v části Ochrana skupin dostupnosti AAG (Always On Availability Groups) (str. 305).

Výchozí nastavení: **Sekundární replika, pokud je to možné.**

Můžete si vybrat jeden z úkonů níže:

- **Sekundární replika, pokud je to možné**

  Pokud jsou všechny sekundární repliky offline, je zálohována primární replika. Zálohování primární repliky může zpomalit výkon SQL Serveru, ale data budou zálohována v nejaktuálnějším stavu.
- **Sekundární replika**

  Pokud jsou všechny sekundární repliky offline, zálohování se nezdaří. Záloha sekundárních replik neovlivňuje výkon SQL Serveru a umožňuje zvětšit okno pro zálohování. Pasivní repliky však mohou obsahovat neaktuální informace, protože jsou takové repliky často aktualizovány asynchronně (opožděně).
- **Primární replika**

  Pokud je primární replika offline, zálohování se nezdaří. Zálohování primární repliky může zpomalit výkon SQL Serveru, ale data budou zálohována v nejaktuálnějším stavu.

Aby byla zajištěna konzistence databáze, software bez ohledu na hodnotu této možnosti přeskočí databáze, které při zahájení zálohování *nejsou* ve stavu **SYNCHRONIZOVÁNO** nebo **PROBÍHÁ SYNCHRONIZACE**. Pokud by byly přeskočeny všechny databáze, zálohování se nezdaří.

Aplikace Microsoft Exchange Server

Tato možnost určuje režim zálohování pro skupinu dostupnosti databáze Exchange Serveru (DAG). Aby byla tato možnost účinná, musí být ve všech uzlech DAG nainstalován agent pro Exchange. Další informace o zálohování skupin DAG najdete v části Ochrana skupin dostupnosti databáze (DAG) (str. 306).

Výchozí nastavení: **Pasivní kopie, je-li to možné.**

Můžete si vybrat jeden z úkonů níže:

- **Pasivní kopie, je-li to možné**

  Pokud jsou všechny pasivní kopie offline, je zálohována aktivní kopie. Zálohování aktivní kopie může zpomalit výkon Exchange Serveru, ale data budou zálohována v nejaktuálnějším stavu.
- **Pasivní kopie**

  Pokud jsou všechny pasivní kopie offline, zálohování se nezdaří. Záloha pasivních kopií neovlivňuje výkon serveru Exchange a umožňuje zvětšit okno pro zálohování. Pasivní kopie však mohou obsahovat neaktuální informace, protože jsou takové kopie často aktualizovány asynchronně (opožděně).
- **Aktivní kopie**

  Pokud je aktivní kopie offline, zálohování se nezdaří. Zálohování aktivní kopie může zpomalit výkon Exchange Serveru, ale data budou zálohována v nejaktuálnějším stavu.

Aby byla zajištěna konzistence databáze, software bez ohledu na hodnotu této možnosti přeskočí databáze, které při zahájení zálohování *nejsou* ve stavu **V POŘÁDKU** nebo **AKTIVNÍ**. Pokud by byly přeskočeny všechny databáze, zálohování se nezdaří.

6.12.8 Úroveň komprese

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

Výchozí nastavení: **Normální** –

Při vyšší úrovni komprese bude zálohování trvat déle, ale výsledná záloha zabere méně místa. Úrovně Vysoká a Maximální momentálně pracují podobně.

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

6.12.9 E-mailová upozornění

Pomocí této možnosti lze nastavit e-mailová upozornění týkající se událostí, ke kterým dochází při zálohování.

Tato možnost je dostupná pouze při místním nasazení. Při cloudovém nasazení se výchozí nastavení konfigurují pro každý účet při vytváření daného účtu.

Výchozí nastavení: **Použít nastavení systému**.

Můžete použít nastavení systému nebo je můžete přepsat vlastními hodnotami, které budou platit jen pro tento plán. Nastavení systému se konfigurují podle popisu v části E-mailová upozornění (str. 440).

***Důležité** Změna nastavení systému ovlivní všechny plány ochrany, které tato nastavení používají.*

Před zapnutím této možnosti se přesvědčte, zda jsou nakonfigurována nastavení **e-mailového serveru** (str. 441).

Úprava e-mailových upozornění pro plán ochrany

1. Vyberte možnost **Přizpůsobit nastavení pro tento plán ochrany**.
2. Do pole **E-mailové adresy příjemců** zadejte cílovou e-mailovou adresu. Je možné zadat více adres oddělených středníky.
3. [Volitelné] V poli **Předmět** změňte předmět e-mailového upozornění.

   Můžete použít následující proměnné:
   - **`[Alert]`** – shrnutí výstrah
   - **`[Device]`** – název zařízení
   - **`[Plan]`** – název plánu, který vygeneroval výstrahu
   - **`[ManagementServer]`** – název hostitele počítače, ve kterém je server pro správu nainstalován
   - **`[Unit]`** – název jednotky, do které počítač náleží

   Výchozí předmět je **`[Alert]`Zařízení: `[Device]` Plán: `[Plan]`**
4. Zaškrtněte políčka u událostí, na které chcete dostávat upozornění. Můžete vybírat ze seznamu výstrah, ke kterým dochází při zálohování, seskupených podle závažnosti.

6.12.10 Zpracování chyb

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

Pokud dojde k chybě, pokusit se znovu

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

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

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

Cloudové úložiště

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

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

Příklady:

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

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

Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)

Výchozí nastavení: **Povoleno**.

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

Ignorovat chybné sektory

Výchozí nastavení: **Zakázáno**.

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

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

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

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

6.12.11 Rychlá přírůstková/rozdílová záloha

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

Tato možnost neplatí (je vždy zakázána) pro svazky formátované pomocí systému souborů JFS, ReiserFS3, ReiserFS4, ReFS nebo XFS.

Výchozí nastavení: **Povoleno**.

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

6.12.12 Filtry souborů

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

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

Jak zapnout filtry souborů

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

Vyloučit soubory splňující konkrétní kritéria

Existují dvě možnosti, které mají opačný účinek.

- **Zálohovat jen soubory splňující následující kritéria**

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

  Poznámka: *Tento filtr nemá vliv na zálohy na úrovni souborů, pokud je jako **formát zálohy** (str. 167) vybrána možnost **Verze 11** a cílové umístění zálohy NENÍ cloudové úložiště.*

- **Nezálohovat soubory splňující následující kritéria**

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

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

Kritéria

- **Úplná cesta**

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

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

- **Název**

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

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

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

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

[Pouze pro zálohy ve formátu **Verze 12**] Dvě hvězdičky (*) v názvu souboru a cestě nahrazují nula nebo více znaků, včetně lomítka. Například kritérium ****/Docs/**.txt** zahrnuje všechny soubory txt ve všech podsložkách všech složek **Docs**.

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

Vyloučit skryté soubory a složky

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

Vyloučit systémové soubory a složky

Tato možnost platí pouze systémy souborů podporované systémem Windows. Výběrem tohoto zaškrtávacího políčka přeskočíte soubory a složky s nastaveným atributem **Systémový**. Jestliže má

složka atribut **systémový**, veškerý její obsah (včetně souborů, které nemají atribut **systémové**) se vyloučí.

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

6.12.13 Snímky záloh na úrovni souborů

Tato možnost platí pouze pro zálohy na úrovni souborů.

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

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

Výchozí nastavení:

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

Je možné vybrat jednu z následujících možností:

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

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

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

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

6.12.14 Kontrola záloh

Viry, malware a ransomware mohou na počítači provádět škodlivé aktivity. Další případ, který může vyžadovat šetření, je odcizení nebo změna dat na počítači s využitím různých programů. Šetření těchto aktivit je ale možné, pouze pokud si na počítači uchováte digitální důkazy. Důkazy (soubory, trasování atd.) mohou být ale bohužel vymazány nebo počítač nemusí být dostupný.

Možnost zálohování s názvem **Forenzní data** vám umožňuje shromažďovat digitální důkazy, které lze použít při forenzním šetření. Jako digitální důkaz lze použít následující položky: snímek nevyužitého místa na disku, výpisy z paměti a snímek spuštěných procesů. Funkce **Forenzní data** je k dispozici pouze pro zálohu celého počítače.

Možnost **Forenzní data** je momentálně k dispozici pouze pro počítače se systémem Windows s následujícími verzemi OS:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Poznámka
• Jakmile na počítač použijete plán ochrany s modulem zálohování, nastavení forenzních dat nelze změnit. Chcete-li použít jiné nastavení forenzních dat, vytvořte nový plán ochrany.
• Zálohy s kolekcemi forenzních dat nejsou podporovány pro počítače, které jsou k vaší síti připojeny prostřednictvím VPN a nemají přímý přístup k internetu.

Podporovaná umístění pro zálohy s forenzními daty jsou:

- Cloudové úložiště
- Místní složka

  Poznámka
  1. Místní složka je podporována pouze na externím pevném disku připojeném prostřednictvím USB.
  2. Místní dynamické disky nejsou jako umístění forenzních záloh podporovány.

- Síťová složka

Zálohy s forenzními daty jsou automaticky notarizovány. Forenzní zálohy umožní vyšetřovatelům analyzovat oblasti disku, které obvykle nejsou zahrnuty do pravidelných záloh disku.

Proces forenzní zálohy

Systém během procesu forenzní zálohy provede následující kroky:

1. Shromáždí neupravený výpis z paměti a seznam spuštěných procesů.
2. Automaticky restartuje počítač na spustitelném médiu.
3. Vytvoří zálohu, která zahrnuje využívaný i nepřiřazený prostor.
4. Notarizuje zálohované disky.
5. Restartuje počítač do operačního systému v produkčním provozu a pokračuje v provádění plánu (například replikace, uchování, ověření a další kroky).

Konfigurace shromažďování forenzních dat

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Všechna zařízení**. Plán ochrany lze alternativně vytvořit na kartě **Plány**.
2. Vyberte zařízení a klikněte na položku **Chránit**.
3. V plánu ochrany povolte modul **Zálohování**.
4. V okně **Co se má zálohovat** vyberte možnost **Celý počítač**.
5. V nabídce **Možnosti zálohy** klikněte na příkaz **Změnit**.
6. Najděte možnost **Forenzní data**.
7. Povolte možnost **Shromáždit forenzní data**. Systém automaticky shromáždí výpis z paměti a vytvoří snímek spuštěných procesů.

   Poznámka *Úplný výpis z paměti může obsahovat citlivé údaje, například hesla.*

8. Určete umístění.
9. Kliknutím na tlačítko **Spustit nyní** ihned vytvořte zálohu s forenzními daty nebo počkejte, dokud se záloha nevytvoří podle harmonogramu.
10. Přejděte do nabídky **Kontrolní panel** > **Aktivity** a ověřte, zda byla záloha s forenzními daty úspěšně vytvořena.

Zálohy tak budou zahrnovat forenzní data a budete je moct načíst a analyzovat. Zálohy s forenzními daty jsou označeny a mohou být filtrovány mezi dalšími zálohami v nabídce **Úložiště záloh** > **Umístění** pomocí možnosti **Pouze s forenzními daty**.

Jak načíst forenzní data ze zálohy?

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Úložiště záloh** a vyberte umístění se zálohami, které zahrnují forenzní data.
2. Vyberte zálohu s forenzními daty a klikněte na položku **Zobrazit zálohy**.
3. U zálohy s forenzními daty klikněte na položku **Obnovit**.
   - Pokud chcete načíst pouze forenzní data, klikněte na položku **Forenzní data**.

Systém zobrazí složku s forenzními daty. Vyberte soubor s výpisem z paměti nebo jiný forenzní soubor a klikněte na tlačítko **Stáhnout**.

- Chcete-li obnovit úplnou forenzní zálohu, klikněte na tlačítko **Celý počítač**. Systém obnoví zálohu bez režimu restartování. Bude tak možné zkontrolovat, zda byl disk změněn.

K další analýze paměti můžete použít poskytnutý výpis z paměti s forenzním softwarem třetích stran. Můžete například využít Volatility Framework na adrese https://www.volatilityfoundation.org/.

6.12.14.1 Notarizace záloh s forenzními daty

Za účelem ověření, že záloha s forenzními daty je stejná bitová kopie, která byla pořízena, a nebyla kompromitována, poskytuje modul zálohování notarizaci záloh s forenzními daty.

Jak to funguje

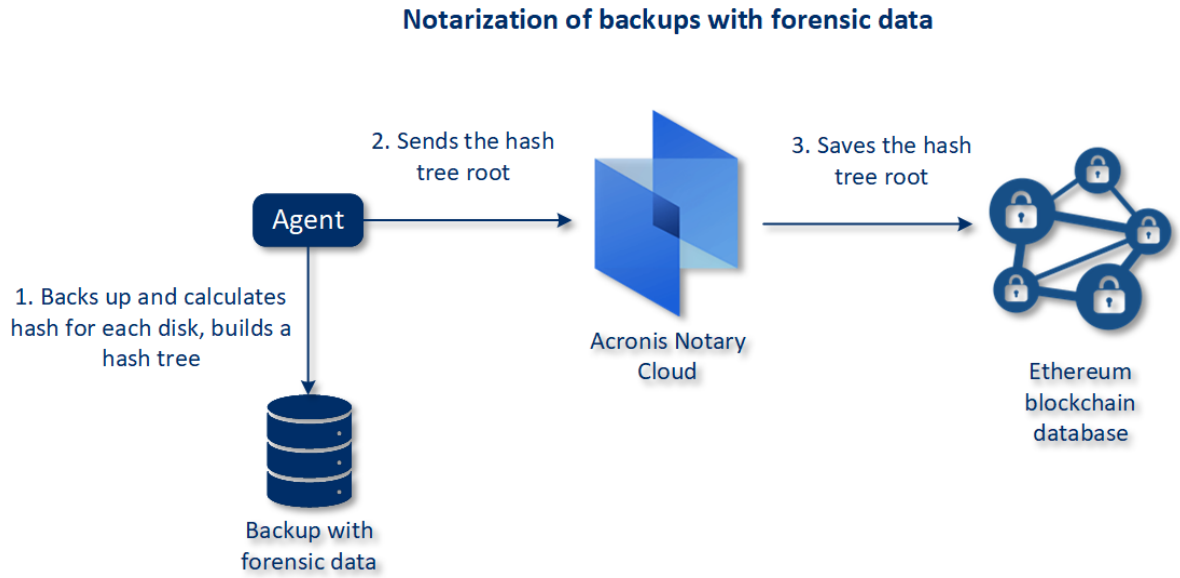
Notarizace umožňuje potvrdit, že disk s forenzními daty je autentický a nebyl od zálohy změněn.

Během zálohování agent vypočítá kódy hash zálohovaných disků, vytvoří hashovací strom, uloží ho do zálohy a odešle kořenový hashovací strom notářské službě. Notářská služba uloží kořenový hashovací strom v databázi blockchain Ethereum, čímž se zajistí, že tato hodnota se nezmění.

Při ověřování pravosti disku s forenzními daty agent vypočítá hash disku a porovná ho s kódem hash, který je uložen v hashovacím stromu uvnitř zálohy. Pokud se kódy hash neshodují, disk není považován za autentický. V opačném případě je autenticita disku zaručena hashovacím stromem.

Chcete-li ověřit, že samotný hashovací strom nebyl zfalšován, agent odešle kořenový hashovací strom notářské službě. Notářská služba jej porovná se stromem uloženým v databázi blockchain. Když se kódy hash shodují, je zaručena autenticita vybraného disku. V opačném případě se zobrazí zpráva s upozorněním, že disk není autentický.

Schéma níže stručně ukazuje notarizační proces pro zálohy s forenzními daty.



Chcete-li notarizovanou zálohu disku ručně ověřit, můžete načíst certifikát zálohy a provést zobrazený postup ověření pomocí certifikátu za použití nástroje tibxread (p. 177).

Získání certifikátu pro zálohy s forenzními daty

Certifikát pro zálohu s forenzními daty z konzole získáte následovně:

1. Přejděte do nabídky **Úložiště záloh** a vyberte zálohu s forenzními daty.
2. Obnovte celý počítač.
3. Systém otevře zobrazení **Mapování disku**.
4. U disku klikněte na ikonu **Získat certifikát**.
5. Systém vygeneruje certifikát a v prohlížeči otevře nové okno s certifikátem. Pod certifikátem uvidíte pokyny k ručnímu ověření notarizované zálohy disku.

6.12.14.2 Nástroj „tibxread" pro načtení zálohovaných dat

Cyber Protect poskytuje nástroj s názvem **tibxread** pro ruční kontrolu integrity zálohovaného disku. Pomocí nástroje můžete načíst data ze zálohy a vypočítat hodnotu hash zadaného disku. Nástroj se nainstaluje automaticky s následujícími součástmi: Agent pro Windows, Agent pro Linux a Agent pro Mac. Umístění je následující: **C:\Program Files\Acronis\BackupAndRecovery**.

Podporovaná umístění:

- Místní disk
- Síťová složka (CIFS/SMB), která je přístupná bez pověření.

  Pokud je síťová složka chráněná heslem, můžete ji pomocí nástrojů OS vložit do místní složky a místní složku použít jako zdroj pro tento nástroj.
- cloudové úložiště.

  Měli byste zadat adresu URL, port a certifikát. Adresu URL a port lze získat z klíče registru systému Windows nebo z konfiguračních souborů na počítačích Linux/Mac.

  Pro Windows:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
  ```

  Pro Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Pro macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Certifikát naleznete v následujících umístěních:

  Pro Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Pro Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Pro macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

Nástroj má následující příkazy:

- list backups
- list content
- get content
- calculate hash

list backups

Zobrazí body obnovy v záloze.

PŘEHLED:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Možnosti

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

Output template:

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – identifikátor GUID zálohy.

<datum> – datum vytvoření zálohy. Formát je: DD.MM.RRRR HH24:MM:SS. Ve výchozím nastavení v místním časovém pásmu (lze změnit pomocí možnosti --utc).

Příklad výstupu:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Zobrazí obsah v bodě obnovy.

PŘEHLED:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password
--backup=RECOVERY_POINT_ID --raw --log=PATH
```

Možnosti

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Šablona výstupu:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<číslo> – identifikátor disku.

<velikost> – velikost v bajtech.

<stav_notarizace> – dostupné jsou následující stavy: Bez notarizace, Notarizováno, Příští záloha.

Příklad výstupu:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

Zapíše obsah zadaného disku v bodě obnovy ve formě standardního výstupu (stdout).

PŘEHLED:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER --raw --log=PATH --progress
```

Možnosti

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Vypočítá hodnotu hash zadaného disku v bodě obnovy pomocí algoritmu SHA-256 a zapíše ho ve formě standardního výstupu (stdout).

PŘEHLED:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password
--backup=RECOVERY_POINT_ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Možnosti

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Popis možností

Volba	Popis
--arc=NÁZEV_ZÁLOHY	Název souboru zálohy, který můžete načíst z vlastností zálohy ve webové konzoli. Soubor zálohy musí být zadán s příponou .tibx.
--backup=ID_BODU_OBNOVY	Identifikátor bodu obnovy
--disk=ČÍSLO_DISKU	Číslo disku (stejné jako číslo zapsané ve výstupu příkazu „get content“)

--loc=URI	Identifikátor URI umístění zálohy. Možné formáty možnosti „--loc“: ▪ Název místní cesty (Windows) **c:/upload/backups** ▪ Název místní cesty (Linus) **/var/tmp** ▪ SMB/CIFS **\\server\folder** ▪ Cloudové úložiště **--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]** **<IP_address>** – naleznete v klíči registru v systému Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<přihlášení_tenanta>\FesUri **<path_to_certificate>** – cesta k souboru certifikátu pro přístup na platformu Cyber Cloud. Například v systému Windows se tento certifikát nachází v umístění **C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt** kde <uživatelské_jméno> je název vašeho účtu pro přístup na platformu Cyber Cloud.
--log=CESTA	Umožňuje zápis do protokolů zadaným parametrem CESTA (pouze místní cesta, formát je stejný jako pro parametr **--loc=URI**). Úroveň protokolování je DEBUG.
--password=HESLO	Šifrovací heslo k záloze. Pokud záloha není šifrovaná, ponechte tuto hodnotu prázdnou.

--raw	Skryje hlavičky (první dva řádky) ve výstupu příkazu. Používá se, když je třeba analyzovat výstup příkazu.
	Příklad výstupu bez „**--raw**“:
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Příklad výstupu s „**--raw**“:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Zobrazí data v UTC.

--progress	Zobrazí průběh operace.
	Například:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

6.12.15 Zkrácení protokolu

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

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

Výchozí nastavení: **Povoleno**.

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

6.12.16 Zachycování snímků LVM

Tato možnost platí pouze pro fyzické počítače.

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

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

Výchozí nastavení: **Softwarem pro zálohování**.

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

6.12.17 Přípojné body

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

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

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

Obnovení obsahu přípojného bodu během obnovy nadřazené složky závisí na tom, jestli je zapnuta nebo vypnuta možnost obnovy **Přípojné body** (str. 216).

- Pokud vyberete přímo přípojný bod nebo složku v připojeném svazku, budou vybrané složky považovány za běžné složky. Budou zálohovány nezávisle na stavu možnosti **Přípojné body** a obnoveny nezávisle na stavu možnosti obnovy**Přípojné body** (str. 216).

Výchozí nastavení: **Zakázáno**.

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

Příklad

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

Pokud vyberete svazek C a zapnete možnost **Přípojné body**, složka **C:\Data1** v záloze bude obsahovat složky **Složka1** a **Složka2**. Při obnově zálohovaných dat dávejte pozor na správné použití **možnosti obnovy** Přípojné body (str. 216).

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

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

6.12.18 Snímek více svazků

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

Tato možnost platí pro zálohy na úrovni disku. Platí také pro zálohy na úrovni souborů v případě, že jsou prováděny pořízením snímků. (Možnost Snímky záloh na úrovni souborů (str. 174) určuje, zda bude při zálohování na úrovni souborů pořízen snímek.)

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

Výchozí nastavení:

- Je-li k zálohování vybrán alespoň jeden počítač se systémem Windows: **Povoleno**.
- Pokud nejsou vybrané žádné počítače (tato situace nastává při vytváření plánu ochrany ze stránky **Plány** > **Zálohování**): **Povoleno**.
- Ostatní případy: **Zakázáno**.

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

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

6.12.19 Výkon a okno pro zálohování

Tato možnost umožňuje nastavit jednu ze tří úrovní výkonu zálohování (vysoká, nízká, zakázaná) pro každou hodinu během týdne. Tímto způsobem můžete definovat časové období, kdy je povoleno

spuštění a provádění zálohování. Vysoké a nízké úrovně výkonu jsou konfigurovatelné z hlediska priority procesu a rychlosti výstupu.

Tato možnost není k dispozici pro zálohy prováděné cloudovými agenty, jako jsou například zálohy webových stránek nebo zálohy serverů umístěné na cloudovém serveru pro obnovení.

Tuto možnost můžete nakonfigurovat zvlášť pro každé umístění zadané v plánu ochrany. Chcete-li tuto možnost konfigurovat pro umístění replikace, klikněte na ikonu ozubeného kola vedle názvu umístění a potom klikněte na **Výkon a okno pro zálohování**.

Tato možnost platí pouze pro procesy zálohování a replikace záloh. Příkazy po zálohování a další operace zahrnuté do plánu ochrany (ověření, převod na virtuální počítač) budou spuštěny bez ohledu na tuto možnost.

Výchozí nastavení: **Zakázáno**.

Pokud je tato možnost zakázána, je možné zálohování spustit kdykoli s následujícími parametry (bez ohledu na to, zda byly parametry změněny oproti výchozí hodnotě):

- Priorita CPU: **Nízká** (odpovídá nastavení **Nižší než normální** ve Windows).
- Rychlost výstupu: **Neomezená**

Pokud je tato možnost zapnuta, naplánované zálohy jsou povoleny nebo blokovány podle parametrů výkonu zadaných pro aktuální hodinu. Na začátku hodiny, když jsou zálohy zablokovány, se proces zálohování automaticky zastaví a vygeneruje se výstraha.

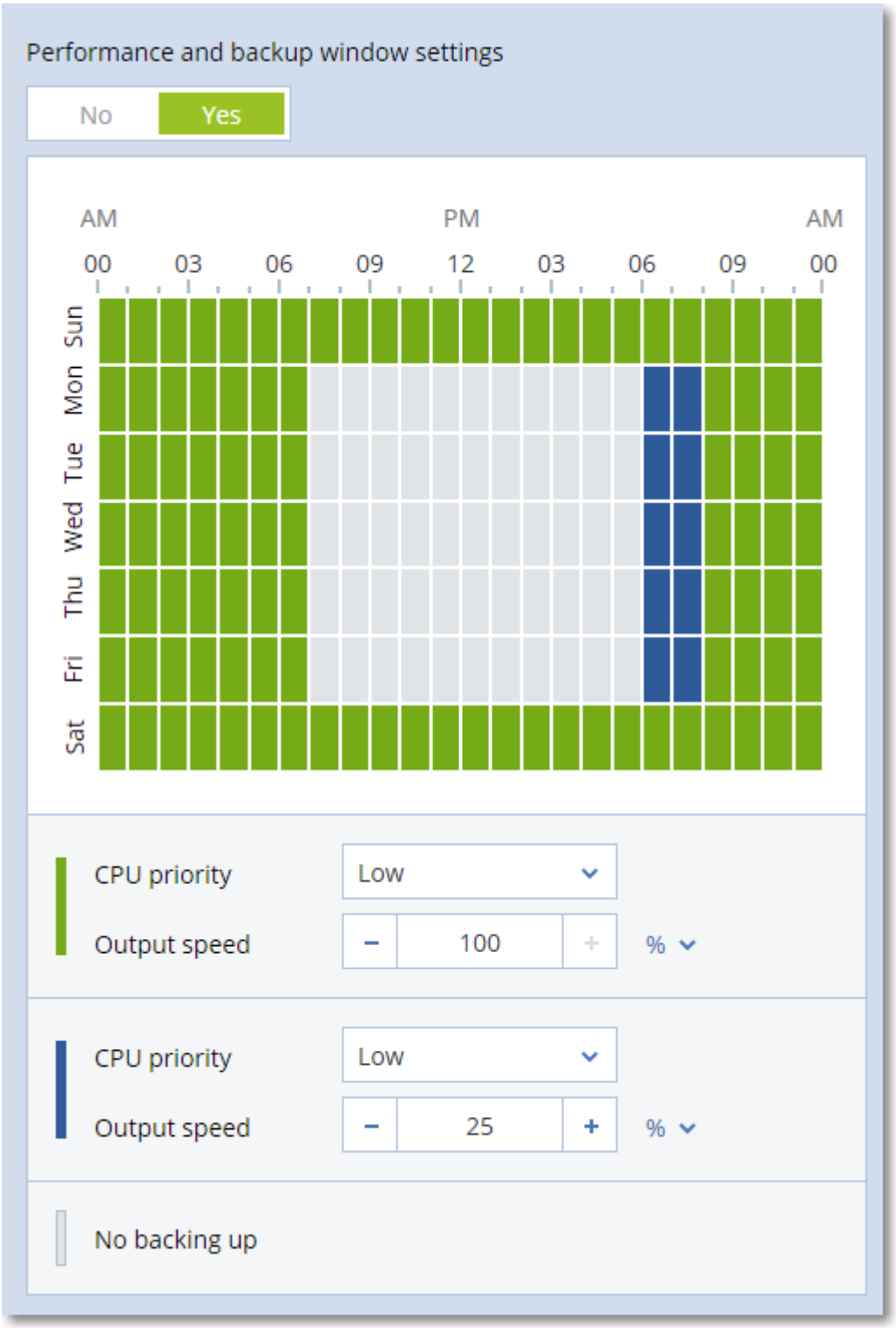
I v případě, kdy jsou naplánované zálohy zablokovány, lze zálohování spustit ručně. V takovém případě se použijí parametry výkonu poslední hodiny, kdy byly zálohy povoleny.

Okno pro zálohování

Každý obdélník představuje hodinu v rámci pracovního dne. Kliknutím na obdélník můžete procházet následující stavy:

- **Zelená:** zálohování je povoleno s parametry uvedenými v zelené části níže.
- **Modrá:** zálohování je povoleno s parametry uvedenými v modré části níže.
  Tento stav není k dispozici, když je formát zálohy nastavený na **Verze 11**.
- **Šedá:** zálohování je blokováno.

Kliknutím a přetažením můžete změnit stav více obdélníků současně.



Priorita CPU

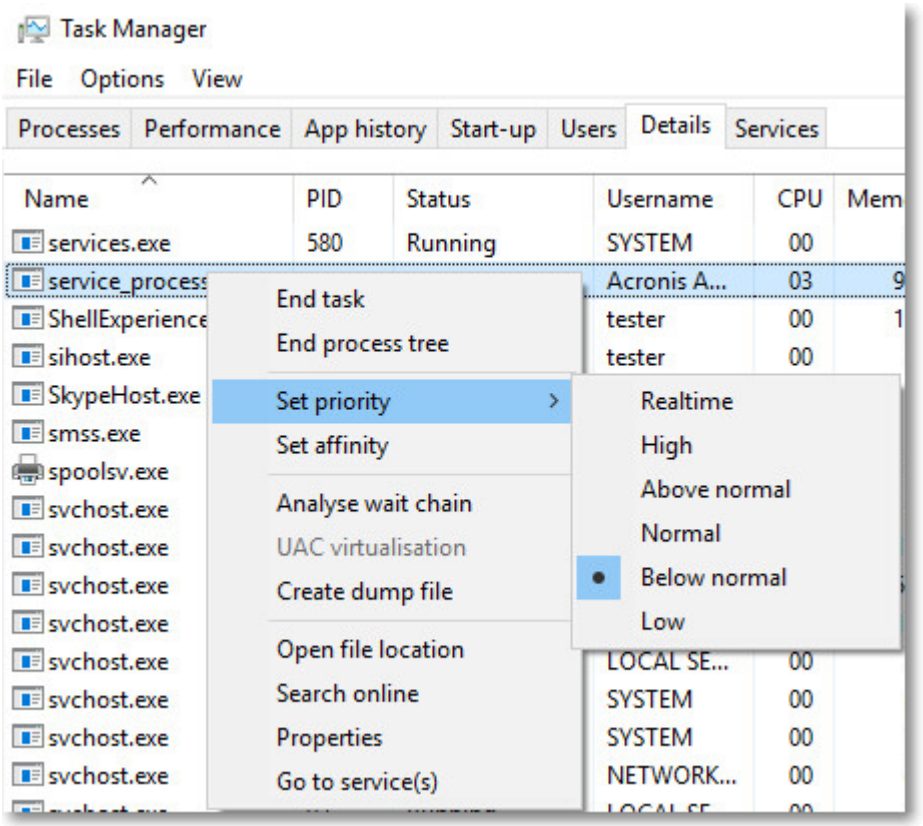
Tento parametr definuje prioritu procesu zálohování v operačním systému.

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

Priorita procesu běžícího v systému určuje množství CPU a systémových zdrojů poskytnutých procesu. Snížením priority zálohy uvolníte více zdrojů pro další aplikace. Zvýšení priority zálohování může

zrychlit proces zálohování žádostí, aby operační systém přidělil zálohovací aplikaci více zdrojů, například procesor. Výsledek ovšem závisí na celkovém zatížení procesoru a dalších faktorech, například rychlosti čtení/zápisu disku nebo síťovém provozu.

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



Výstupní rychlost při zálohování

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

Když je tato možnost zapnutá, můžete zadat maximální povolenou výstupní rychlost:

- Jako procento odhadované rychlosti zápisu cílového pevného disku (při zálohování do lokální složky) nebo odhadované maximální rychlosti síťového připojení (při zálohování do sdíleného síťového nebo cloudového úložiště).

  Toto nastavení funguje, pouze pokud je agent spuštěn v systému Windows.
- V kB/s (pro všechna umístění).

6.12.20 Odesílání fyzických dat

Tato možnost je účinná, pokud je cílem umístěním zálohy cloudové úložiště a formát zálohy (str. 167) je nastaven na **verzi 12**.

Tato možnost je platná pro zálohy na úrovni disků a zálohy souborů vytvořené agentem pro Windows, agentem pro Linux, agentem pro Mac, agentem pro VMware a agentem pro Hyper-V. Zálohy vytvořené pomocí spouštěcího média nejsou podporovány.

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

Výchozí nastavení: **Zakázáno**.

Informace o službě Odesílání fyzických dat

Webové rozhraní služby Odesílání fyzických dat je k dispozici pouze správcům organizace (str. 444) při místních nasazeních a správcům při cloudových nasazeních.

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

Přehled procesu odesílání fyzických dat

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

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

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

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

   Chcete-li přejít do webového rozhraní, proveďte jeden z následujících úkonů:

   - Místní nasazení: Přihlaste se ke svému účtu Acronis a potom v části **Odesílání fyzických dat** klikněte na **Přejít na konzolu sledování**.
   - Cloudové nasazení: přihlaste se k portálu pro správu, klikněte na kartu **Přehled** > **Použití** a poté v části **Odesílání fyzických dat** klikněte na možnost **Spravovat službu**.

3. Zabalte jednotky a odešlete je do datového centra.

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

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

6.12.21 Příkazy před-po

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

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

Příkaz před zálohou	Zálohování	Příkaz po záloze

Příklady, jak můžete používat příkazy před/po záloze:

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

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

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

6.12.21.1 Příkaz před zálohou

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

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

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

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

6.12.21.2 Příkaz po záloze

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

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

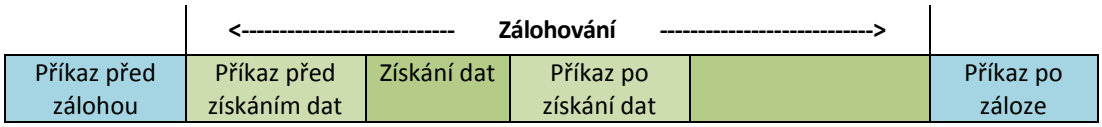
   Jestliže není toto políčko zaškrtnuto, výsledek provedení příkazu neovlivní úspěch nebo selhání zálohy. Výsledky spuštění příkazu můžete sledovat na kartě **Aktivity**.

6. Klikněte na tlačítko **Hotovo**.

6.12.22 Příkazy před/po získání dat

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

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



Pokud je zapnutá možnost (str. 194) stínové kopie svazku, spuštění příkazů a akcí VSS bude uspořádáno následovně:

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

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

6.12.22.1 Příkaz před získáním dat

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

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

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

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

6.12.22.2 Příkaz po získání dat

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

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

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

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

6.12.23 Snímky hardwaru SAN

Tato možnost je aktivní pro zálohy virtuálních počítačů VMware ESXi.

Výchozí nastavení: **Zakázáno**.

Tato možnost určuje, zda se při provádění zálohy použijí snímky SAN.

Pokud je tato možnost zapnutá, načte se obsah virtuálního disku ze snímku VMware. Snímek bude zachován po celou dobu trvání zálohy.

Pokud je tato možnost zapnutá, načte se obsah virtuálního disku ze snímku SAN. Bude vytvořen snímek VMware a uchová se po krátkou dobu, než se virtuální disky uvedou do konzistentního stavu. Pokud není možné čtení snímku SAN, zálohování se nezdaří.

Před povolením této možnosti zkontrolujte a proveďte požadavky uvedené v tématu Použití snímků hardwaru SAN (str. 337).

6.12.24 Plánování

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

Výchozí nastavení:

- Místní nasazení: **Spustit všechny zálohy přesně podle plánu**
- Cloudové nasazení: **Rozložit čas spuštění zálohy do časového rámce Maximální prodleva: 30 minut.**

Je možné vybrat jednu z následujících možností:

- **Spustit všechny zálohy přesně podle harmonogramu**

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

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

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

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

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

  Počet virtuálních počítačů, které bude agent současně zálohovat, lze změnit. Maximální hodnota je 10. Pokud však agent provádí více plánů ochrany, které se překrývají v čase, sčítají se čísla uvedená v jejich možnostech zálohování. Můžete omezit celkový počet virtuálních počítačů (str. 350), které může agent současně zálohovat, bez ohledu na to, kolik plánů ochrany je spuštěno.

  Zálohování fyzických počítačů začne přesně podle plánu.

6.12.25 Zálohování sektor po sektoru

Tato možnost má vliv pouze na zálohy na úrovni disku.

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

Výchozí nastavení: **Zakázáno**.

Pokud je tato možnost zapnutá, budou se zálohovat všechny sektory disku nebo svazku včetně nepřiděleného místa a volných sektorů. Výsledná záloha bude mít stejnou velikost jako zálohovaný disk (pokud je možnost Úroveň komprese (str. 170) nastavena na **Žádná**). Software automaticky zapne režim sektor po sektoru při zálohování disků s nerozpoznanými nebo nepodporovanými systémy souborů.

***Poznámka**: Obnovení dat aplikací ze záloh, které byly vytvořeny v režimu Sektor po sektoru, nebude možné.*

6.12.26 Rozdělování

Tato možnost platí pro schémata zálohování **Vždy plná**; **Týdenní plná, denní přírůstková**; **Měsíčně plná, týdně rozdílová, denně přírůstková (GFS)** a **Vlastní**.

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

Výchozí nastavení: **Automaticky**.

K dispozici jsou následující nastavení:

- **Automaticky**

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

  Zadejte požadovanou velikost souboru nebo ji vyberte v rozevíracím seznamu.

6.12.27 Správa pásek

Tato nastavení jsou účinná, pokud je záloha umístěna na páskovém zařízení.

Povolit obnovu souborů z diskových záloh uložených na páskách

Výchozí nastavení: **Zakázáno**.

Pokud je toto políčko zaškrtnuto, software při každé záloze vytvoří dodatečné soubory na pevném disku počítače, ke kterému je připojeno páskové zařízení. Dokud budou tyto dodatečné soubory zachovány, je možné provést obnovení souborů z diskových záloh. Soubory jsou automaticky odstraněny v případě, že páska s příslušnými zálohami je smazána (str. 431), odebrána (str. 432) nebo přepsána.

Dodatečné soubory jsou umístěny na následujících místech:

- V systému Windows XP a Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- V systému Windows Vista a novějších verzích systému Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- V Linuxu: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Místo obsazené těmito dodatečnými soubory závisí na počtu souborů v záloze. U plné zálohy disku obsahujícího přibližně 20 000 souborů (typická záloha disku pracovní stanice) mají tyto dodatečné soubory velikost asi 150 MB. Při plné záloze serveru s 250 000 soubory může vzniknout asi 700 MB dodatečných souborů. Pokud si tedy jste jistí, že nebude nutné obnovovat jednotlivé soubory, můžete zaškrtnutí políčka zrušit a ušetřit tak místo na disku.

Jestliže dodatečné soubory nebyly při zálohování vytvořeny nebo byly smazány, můžete je stále vytvořit překontrolováním (str. 430) pásek, na kterých je záloha umístěna.

Po každé úspěšné záloze každého počítače přesunout pásku zpět do slotu

Výchozí nastavení: **Povoleno**.

Jestliže tuto možnost vypnete, páska po dokončení operace s páskou zůstane v jednotce. Jinak software přesune pásku zpět do slotu, kde byla před operací. Jestliže podle plánu ochrany za zálohou následují další operace (například ověření zálohy nebo replikace do jiného umístění), přesune se páska zpět do slotu po jejich dokončení.

Pokud je zapnuta tato možnost a možnost **Po každé úspěšné záloze každého počítače vysunout pásky**, páska se vysune.

Po každé úspěšné záloze každého počítače vysunout pásky

Výchozí nastavení: **Zakázáno**.

Pokud je toto políčko zaškrtnuto, software vysune pásky po každém úspěšném zálohování každého počítače. Jestliže podle plánu ochrany za zálohou následují další operace (například ověření nebo replikace do jiného umístění), budou pásky vysunuty po jejich dokončení.

Při vytváření plné zálohy přepsat pásku v samostatné jednotce

Výchozí nastavení: **Zakázáno**.

Tato možnost platí pouze pro samostatné páskové jednotky. Když je tato možnost zapnuta, páska vložená do jednotky bude přepsána při každém vytvoření plné zálohy.

Použít následující pásková zařízení a jednotky

Pomocí této možnosti můžete určit pásková zařízení a páskové jednotky, které se použijí v plánu ochrany.

Fond pásek obsahuje pásky ze všech páskových zařízení připojených k počítači, ať už jde o uzel úložišť, počítač s nainstalovaným agentem pro ochranu, nebo obojí. Při výběru fondu pásek jako umístění zálohy nepřímo vybíráte počítač, ke kterému je páskové zařízení připojeno. Ve výchozím nastavení lze zálohy zapsat na pásky pomocí jakékoli páskové jednotky v jakémkoli páskovém zařízení připojeném k danému počítači. Pokud některá zařízení nebo jednotky chybí nebo nefungují, použije plán ochrany ty dostupné.

Můžete kliknout na možnost **Pouze vybraná zařízení a jednotky** a potom vybrat pásková zařízení a jednotky ze seznamu. Vybráním celého zařízení vyberete všechny jeho jednotky. To znamená, že v plánu ochrany lze použít jakoukoli z těchto jednotek. Pokud vybrané zařízení nebo jednotka chybí nebo nefunguje a nejsou vybraná žádná další zařízení, zálohování se nezdaří.

Díky této možnosti můžete řídit zálohování prováděná více agenty do velké páskové knihovny s více jednotkami. Například zálohování velkého souborového serveru nebo sdílené složky se nemusí spustit, jestliže ve stejném okně pro zálohování zálohuje více agentů počítače, a tím zabírají všechny jednotky. Pokud agentům povolíte použití jednotky 2 a 3, zůstane jednotka 1 rezervovaná pro agenta zálohujícího sdílenou složku.

Použít sady pásek s fondem pásek vybraným pro zálohu

Výchozí nastavení: **Zakázáno**.

Pásky v rámci jednoho fondu mohou být seskupeny do takzvaných **sad pásek**.

Pokud necháte tuto možnost zakázanou, data budou zálohována na všechny pásky, které náleží fondu. Pokud je tato možnost povolena, můžete zálohy rozdělit podle předem definovaných nebo vlastních pravidel.

- **Použít oddělenou sadu pásek pro každý** (zvolte pravidlo: **typ zálohy**, **typ zařízení**, **název zařízení**, **den v měsíci**, **den v týdnu**, **měsíc v roce**, **rok**, **datum**)

  Vyberete-li tuto variantu, můžete uspořádat sady pásek podle předem definovaného pravidla. Například můžete mít samostatné sady pásek pro každý den v týdnu nebo ukládat zálohy z jednotlivých počítačů na samostatnou sadu pásek.
- **Určit vlastní pravidlo pro sady pásek**

Vyberete-li tuto variantu, určíte si vlastní pravidlo pro organizaci sad pásek. Pravidlo může obsahovat následující proměnné:

Syntaxe proměnné	Popis proměnné	Dostupné hodnoty
[Resource Name]	Zálohy každého počítače se uloží na samostatnou sadu pásek.	Názvy počítačů registrovaných na serveru pro správu
[Backup Type]	Plné, přírůstkové a rozdílové zálohy se budou ukládat na samostatné sady pásek.	**full**, **inc**, **diff**
[Resource Type]	Zálohy počítačů jednotlivých typů se uloží na samostatnou sadu pásek.	**Server essentials**, **Server**, **Workstation**, **Physical machine**, **VMware Virtual Machine**, **Virtual-PC Virtual Machine**, **Virtual Server Virtual Machine**, **Hyper-V Virtual Machine**, **Parallels Virtual Machine**, **XEN Virtual Machine**, **KVM Virtual Machine**, **RHEV Virtual Machine**, **Parallels Cloud Virtual Machine**
[Day]	Zálohy vytvořené v jednotlivých dnech v měsíci se uloží na samostatnou sadu pásek.	**01**, **02**, **03**, ..., **31**
[Weekday]	Zálohy vytvořené v jednotlivých dnech v týdnu se uloží na samostatnou sadu pásek.	**Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**
[Month]	Zálohy vytvořené v jednotlivých měsících v roce se uloží na samostatnou sadu pásek.	**January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, **December**
[Year]	Zálohy vytvořené v každém roce se uloží na samostatnou sadu pásek.	**2017**, **2018**, ...

Například když pravidlo specifikujete takto: **[Resource Name]-[Backup Type]**, budete mít samostatnou sadu pásek pro každou plnou, přírůstkovou a rozdílovou zálohu jednotlivých počítačů, na které se tento plán ochrany vztahuje.

Také můžete pro jednotlivé pásky určit sady pásek (str. 432). V tomto případě bude software nejprve zapisovat zálohy na pásky, jejichž hodnota sady pásek se shoduje s hodnotou výrazu zadanou v plánu ochrany. Další pásky budou vybrány ze stejného fondu, až to bude nezbytné. Je-li fond obnovitelný, použijí se potom pásky z fondu **Volné pásky**.

Když například zadáte sadu pásek **Monday** pro pásku 1, **Tuesday** pro pásku 2 atd. a zadáte v možnostech zálohování **[Weekday]**, bude pro každý den v týdnu použita odpovídající páska.

6.12.28 Zpracování selhání úlohy

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

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

Výchozí nastavení: **Zakázáno**.

6.12.29 Podmínky spuštění úlohy

Tato možnost má vliv v operačních systémech Windows a Linux.

Tato možnost určuje chování programu v případě, že má být spuštěna úloha (nastane naplánovaný čas nebo dojde k zadané události v plánu), ale podmínka (nebo více podmínek) není splněna. Další informace o podmínkách najdete v části Podmínky spuštění (str. 147).

Výchozí nastavení: **Počkat, dokud nejsou splněny podmínky plánu.**

Počkat, dokud nejsou splněny podmínky plánu

V případě tohoto nastavení začne plánovač monitorovat podmínky, a jakmile budou splněny, spustí úlohu. Pokud podmínky nebudou splněny nikdy, úloha se nikdy nespustí.

K vyřešení situace, kdy podmínky nejsou splněny příliš dlouho a další odklad úlohy je rizikový, můžete nastavit časový interval, po jehož uplynutí bude úloha spuštěna bez ohledu na podmínku. Zaškrtněte políčko **Spustit úlohu i tak po** a zadejte časový interval. Úloha se spustí, jakmile budou splněny podmínky NEBO jakmile uplyne maximální doba prodlevy (podle toho, co nastane jako první).

Přeskočit spuštění úlohy

Zpoždění úlohy může být nepřijatelné, pokud například úlohu potřebujete spustit v přesně určený čas. V takovém případě může být namísto čekání na splnění podmínek vhodnější úlohu přeskočit, a to zejména pokud úloha probíhá relativně často.

6.12.30 Služba Stínová kopie svazku (VSS)

Tato možnost platí pouze pro operační systémy Windows.

Možnost určuje, zda zprostředkovatel služby VSS musí upozorňovat aplikace se službou VSS, že bude spuštěno zálohování. Tím je zajištěn konzistentní stav dat používaných danou aplikací a zvláště dokončení všech transakcí databáze v okamžiku pořízení snímku dat pomocí softwaru pro zálohování. Konzistence dat pak zajišťuje, že aplikace bude obnovena do správného stavu a bude funkční okamžitě po obnově.

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

Je možné vybrat jednu z následujících možností:

- **Automaticky vybrat zprostředkovatele snímku**

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

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

Vypněte ji, pokud není vaše databáze kompatibilní se službou VSS. Pořizování snímků je rychlejší, ale konzistenci dat aplikací, jejichž operace nejsou dokončeny v čase vytvoření snímku, nelze zaručit. Pokud chcete zajistit zálohování dat v konzistentním stavu, můžete použít příkazy před/po získání dat (str. 188). Například zadejte příkazy před zachycením dat, které pozastaví databázi a vyprázdní všechny mezipaměti, aby bylo zajištěno, že veškeré transakce jsou dokončeny, a zadejte příkazy po zachycení dat, které po pořízení snímku opět spustí operace databáze.

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

Zapnout úplné zálohování služby VSS

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

Výchozí nastavení: **Zakázáno**.

Tuto možnost ponechte zakázanou v následujících případech:

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

Povolení této možnosti nezkrátí protokoly aplikace Microsoft SQL Server. Chcete-li po zálohování zkrátit protokol SQL Serveru, zapněte možnost zálohy Zkrácení protokolu (str. 181).

6.12.31 Služba Stínová kopie svazku (VSS) pro virtuální počítače

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

Výchozí nastavení: **Povoleno**.

Pokud je tato možnost zapnutá, provedou se před pořízením snímku transakce všech aplikací s podporou VSS ve virtuálním počítači. Pokud tvorba snímku ve stavu nečinnosti selže po provedených opakovaných pokusech v počtu určeném v možnosti Zpracování chyb (str. 171) a zálohování aplikací je vypnuto, vytvoří se snímek mimo stav nečinnosti. Pokud je zapnuto zálohování aplikací, záloha selže.

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

Poznámka *Tato možnost nemá vliv na virtuální počítače Scale Computing HC3. U těchto počítačů závisí uvedení do stavu nečinnosti na tom, zda jsou na virtuálním počítači nainstalovány nástroje Scale, nebo ne.*

6.12.32 Týdenní zálohování

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

Výchozí nastavení: **Pondělí**.

6.12.33 Protokol událostí systému Windows

Tato možnost platí pouze pro operační systémy Windows.

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

Výchozí nastavení: **Zakázáno**.

7 Obnova

7.1 Shrnutí metod obnovy

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

Co obnovovat	Metoda obnovení
Fyzický počítač (Windows nebo Linux)	Pomocí webového rozhraní (str. 198) Pomocí spouštěcích médií (str. 203)
Fyzický počítač (Mac)	Pomocí spouštěcích médií (str. 203)
Virtuální počítač (VMware, Hyper-V nebo Scale Computing HC3)	Pomocí webového rozhraní (str. 202) Pomocí spouštěcích médií (str. 203)
Konfigurace ESXi	Pomocí spouštěcích médií (str. 211)
Soubory/složky	Pomocí webového rozhraní (str. 207) Stahování souborů z cloudového úložiště (str. 208) Pomocí spouštěcích médií (str. 210) Extrahování souborů z místních záloh (str. 211)
Stav systému	Pomocí webového rozhraní (str. 211)
Databáze SQL	Pomocí webového rozhraní (str. 310)
Databáze Exchange	Pomocí webového rozhraní (str. 313)
Poštovní schránky Exchange	Pomocí webového rozhraní (str. 316)
Poštovní schránky Office 365	Pomocí webového rozhraní (str. 323)
Databáze Oracle	Použití nástroje Oracle Explorer (str. 326)

Poznámka pro uživatele počítačů Mac

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

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

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

7.2 Bezpečné obnovení

Zálohovaný obraz operačního systému může být napaden malwarem a může infikovat počítač, ve kterém je obnoven.

Funkce bezpečného obnovení umožňuje zabránit opakovanému infikování pomocí integrované antimalwarové kontroly (p. 372) a detekce malwaru během procesu obnovení.

Omezení:

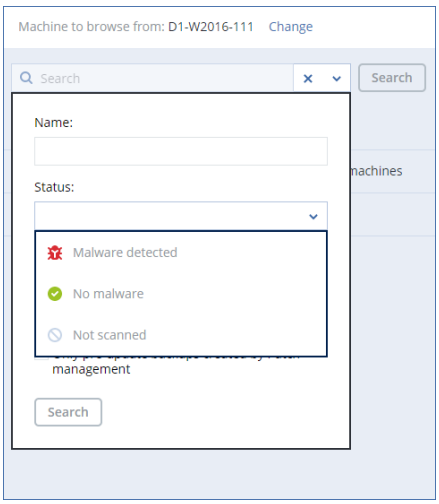
- Bezpečné obnovení je podporováno pouze u fyzických nebo virtuálních počítačů se systémem Windows, na kterých je nainstalován Agent pro Windows.
- Podporovány jsou pouze zálohy typu **Celý počítač** a **Disky/svazky**.
- Podporovány jsou pouze svazky se systémem souborů NTFS. Oddíly mimo systém NTFS budou obnoveny bez antimalwarové kontroly.
- Bezpečné obnovení není podporováno pro zálohy souvislé ochrany dat (p. 133). Počítač bude obnoven na základě poslední běžné zálohy bez dat v záloze souvislé ochrany dat. Chcete-li obnovit data souvislé ochrany dat, spusťte obnovení **souborů/složek**.

Jak to funguje

Pokud možnost Bezpečné obnovení povolíte během procesu obnovení, systém provede následující akce:

1. Zkontroluje, zda záloha bitové kopie neobsahuje malware, a označí infikované soubory. Záloze bude přidělen jeden z následujících stavů:
   - **Žádný malware** – během kontroly nebyl v záloze zjištěn žádný malware.
   - **Zjištěn malware** – během kontroly byl v záloze zjištěn malware.
   - **Nekontrolováno** – záloha nebyla kontrolována, zda neobsahuje malware.
2. Obnoví zálohu na vybraném počítači.
3. Odstraní zjištěný malware.

Zálohy můžete filtrovat pomocí parametru **Stav**.



7.3 Tvorba spouštěcího média

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

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

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

Jak vytvořit spouštěcí média v systému Windows nebo Linux

1. Stáhněte si soubor ISO spouštěcího média. Chcete-li stáhnout soubor, klikněte na ikonu účtu v pravém horním rohu stránky > **Stažené soubory Spouštěcí médium**.
2. Proveďte jeden z následujících úkonů:
   - Vypalte CD nebo DVD pomocí souboru ISO.
   - Vytvořte spouštěcí USB flash disk pomocí souboru ISO a některého z nástrojů volně dostupných online.

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

Spouštěcí médium lze také vytvořit pomocí Tvůrce spouštěcích médií (str. 231).

Vytvoření spouštěcího média v systém macOS

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

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

7.4 Obnovení počítače

7.4.1 Fyzický počítač

Tato část popisuje obnovu fyzických počítačů pomocí webového rozhraní.

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

- macOS
- Jakýkoli operační systém na holé železo nebo na počítač ve stavu offline.
- Struktura logických svazků (svazků vytvořených správcem Logical Volume Manager v Linuxu). Médium vám umožňuje vytvořit strukturu logických svazků automaticky.

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

Jak obnovit fyzický počítač

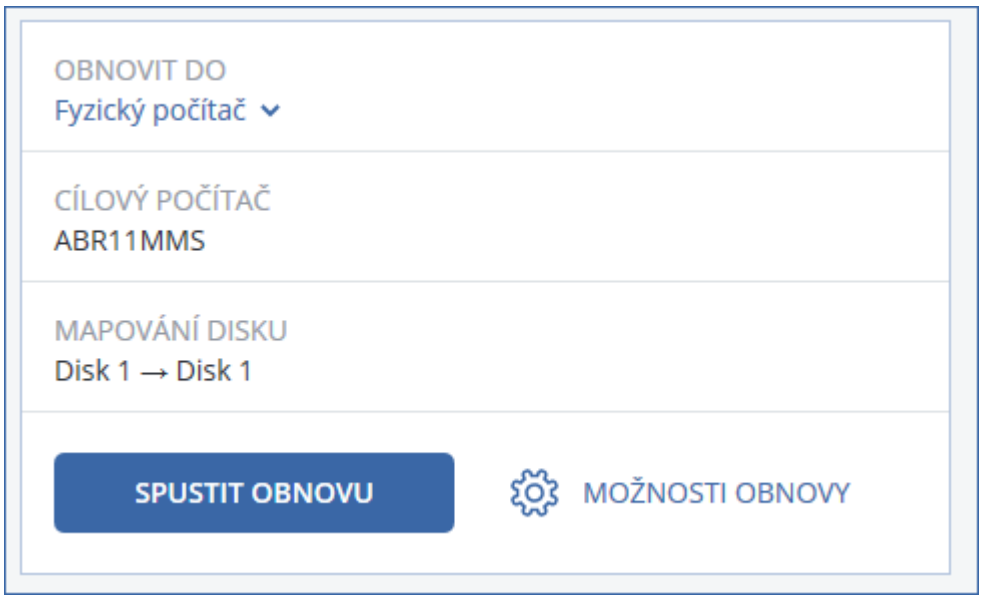
1. Vyberte zálohovaný počítač.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

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

   - Pokud se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte cílový počítač ve stavu online a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).
   - Obnovte počítač podle postupu popsaného v tématu Obnova disků pomocí spouštěcího média (str. 203).
4. Klikněte na **Obnovit** > **Celý počítač**.

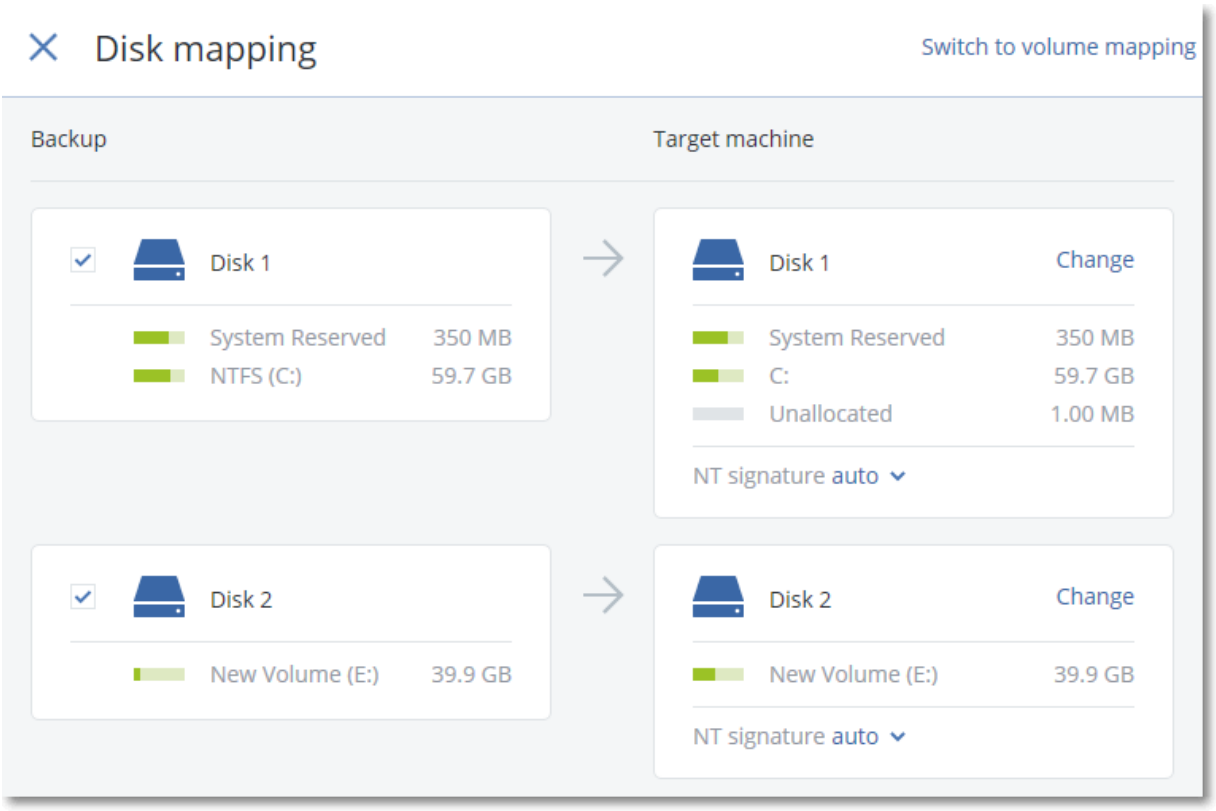
   Software automaticky namapuje disky ze zálohy na disky cílového počítače.

   Chcete-li obnovit další fyzický počítač, klikněte na možnost **Cílový počítač** a poté vyberte cílový počítač ve stavu online.



5. Pokud nejste spokojeni s výsledkem mapování nebo pokud mapování disku selže, můžete disky mapovat znovu ručně kliknutím na **Mapování disku**.

Oddíl mapování umožňuje také vybrat jednotlivé disky nebo svazky pro obnovu. Přepínat mezi obnovou disků a svazků můžete pomocí odkazu **Přepnout na...** v pravém horním rohu.



6. [Volitelné] Chcete-li zkontrolovat, zda záloha neobsahuje malware, zapněte přepínač **Bezpečné obnovení**. Pokud je malware detekován, bude v záloze označen a ihned po dokončení procesu obnovení bude odstraněn.
7. Klikněte na možnost **Spustit obnovu**.
8. Potvrďte, že chcete přepsat disky jejich zálohovanými verzemi. Vyberte, zda se má počítač automaticky restartovat.

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

7.4.2 Fyzický počítač na virtuální

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

Další informace o migraci P2V naleznete v tématu Migrace počítače (str. 351).

Jak obnovit fyzický počítač jako virtuální počítač

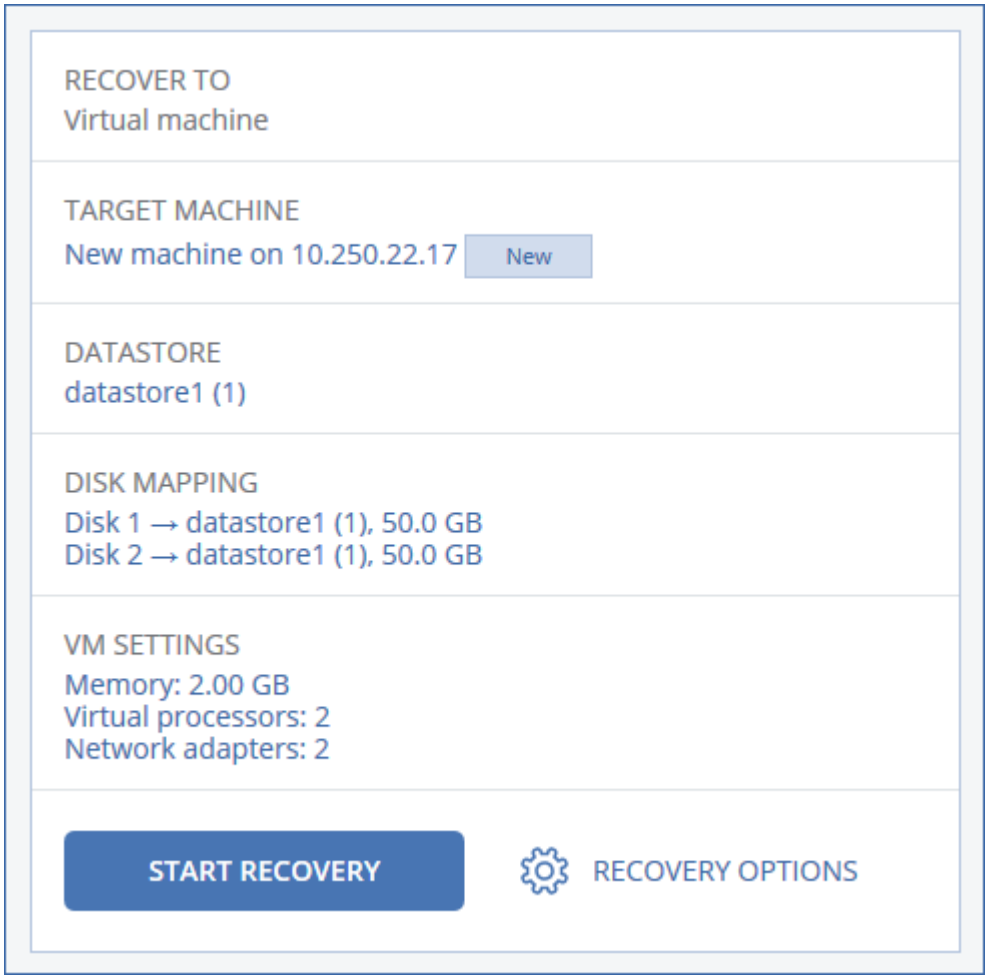
1. Vyberte zálohovaný počítač.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

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

   - Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

- Obnovte počítač podle postupu popsaného v tématu Obnova disků pomocí spouštěcího média (str. 203).

4. Klikněte na **Obnovit** > **Celý počítač**.
5. V poli **Obnovit na** vyberte **Virtuální počítač**.
6. Klikněte na možnost **Cílový počítač**.
   a. Vyberte hypervisor (**VMware ESXi** nebo **Hyper-V**).
      Je nutné, aby byl nainstalován alespoň jeden agent pro VMware nebo agent pro Hyper-V.
   b. Vyberte, zda se má provést obnova na nový, nebo existující počítač. Je doporučena možnost nového počítače, protože nevyžaduje, aby se konfigurace disků cílového počítače přesně shodovala s konfigurací disku v záloze.
   c. Vyberte hostitele a určete název nového počítače, případně vyberte existující cílový počítač.
   d. Klikněte na tlačítko **OK**.
7. [Volitelné] Při obnově na nový počítač je také možné provést následující úkony:
   - Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.
   - Kliknutím na **Mapování disku** vyberte datové úložiště, rozhraní a režim poskytování pro každý virtuální disk. Oddíl mapování umožňuje také vybrat jednotlivé disky pro obnovu.
   - Klikněte na **Nastavení virtuálního počítače** a změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.



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

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

7.4.3 Virtuální počítač

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

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

Jak obnovit virtuální počítač

1. Proveďte jeden z následujících úkonů:
   - Vyberte zálohovaný počítač, klikněte na možnost **Obnova** a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).
2. Klikněte na **Obnovit** > **Celý počítač**.
3. Pokud chcete obnovit fyzický počítač, vyberte možnost **Fyzický počítač** v okně **Obnovit do**. Jinak tento krok přeskočte.

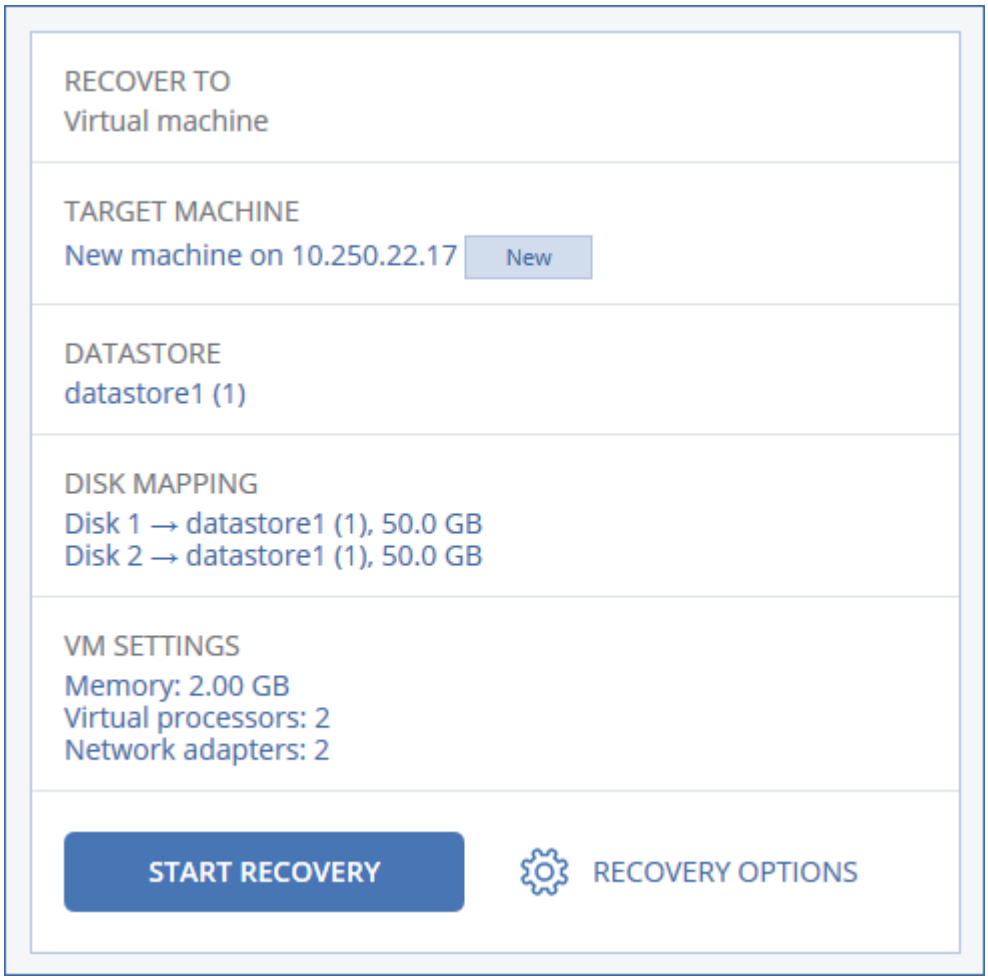
   Obnova na fyzický počítač je možná pouze, pokud se konfigurace disku cílového počítače přesně shoduje s konfigurací disku v záloze.

   V takovém případě pokračujte krokem 4 v části Fyzický počítač (str. 198). Jinak doporučujeme provést V2P migraci pomocí spouštěcího média (str. 203).
4. Software automaticky vybere původní počítač jako cílový.

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

   a. Vyberte hypervisor (**VMware ESXi**, **Hyper-V** nebo **Scale Computing HC3**).
   b. Vyberte, zda se má provést obnova na nový, nebo existující počítač.
   c. Vyberte hostitele a určete název nového počítače, případně vyberte existující cílový počítač.
   d. Klikněte na tlačítko **OK**.
5. [Volitelné] Při obnově na nový počítač je také možné provést následující úkony:
   - Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a Scale Computing HC3 a vyberte datové úložiště virtuálního počítače.
   - Kliknutím na **Mapování disku** vyberte datové úložiště, rozhraní a režim poskytování pro každý virtuální disk. Oddíl mapování umožňuje také vybrat jednotlivé disky pro obnovu.

- Klikněte na **Nastavení virtuálního počítače** a změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.



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

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

7.4.4 Obnovení disků pomocí spouštěcího média

Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 198).

Jak obnovit disky pomocí spouštěcích médií

1. Spusťte cílový počítač pomocí spouštěcích médií.
2. [Pouze při obnově počítače Mac] Pokud obnovujete disky/svazky formátu APFS na jiný než původní počítač nebo na počítač bez operačního systému, ručně znovu vytvořte původní konfiguraci disků:
   a. Klikněte na možnost **Nástroj Disk**.
   b. Znovu vytvořte původní konfiguraci disků. Další informace naleznete na stránce https://support.apple.com/guide/disk-utility/welcome.
   c. Klikněte na možnost **Nástroj Disk** > **Ukončit nástroj Disk**.
3. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).

4. Pokud je v síti zapnutý proxy server, klikněte na možnosti **Nástroje** > **Proxy server** a zadejte název hostitele či IP adresu a port proxy serveru. Jinak tento krok přeskočte.
5. V uvítacím okně klikněte na možnost **Obnovit**.
6. Klikněte na **Označit data** a poté klikněte na **Procházet**.
7. Určete umístění zálohy:
   - Chcete-li provést obnovení z cloudového úložiště, vyberte možnost **Cloudové úložiště**. Zadejte pověření k účtu, ke kterému je zálohovaný počítač přiřazen.
   - Pokud chcete provést obnovení z místní nebo síťové složky, vyhledejte ji v části **Místní složky** nebo **Síťové složky**.

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

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

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

7.4.5 Použití technologie Universal Restore

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

Funkci Universal Restore lze použít v systémech Windows a Linux.

Jak použít funkci Universal Restore

1. Spusťte počítač ze spouštěcího média.
2. Klikněte na možnost **Použít doplněk Universal Restore**.
3. Pokud máte v počítači více operačních systémů, vyberte si jeden z nich, na který se použije nástroj Universal Restore.
4. [Pouze ve Windows] Nakonfigurujte další nastavení (str. 205).
5. Klikněte na tlačítko **OK**.

7.4.5.1 Nástroj Universal Restore v systému Windows

Příprava

Příprava ovladačů

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

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

Kontrola přístupu k ovladačům ve spouštěcím prostředí

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

Nastavení nástroje Universal Restore

Automatické vyhledání ovladačů

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

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

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

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

V každém případě instalovat ovladače velkokapacitních zařízení

Toto nastavení potřebujete v následujících případech:

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

- Pokud automatické vyhledání ovladačů nepomůže spustit systém.

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

Proces používání nástroje Universal Restore

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

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

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

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

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

7.4.5.2 Nástroj Universal Restore v systému Linux

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

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

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

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

Nástroj Universal Restore nikdy neupravuje jádro systému Linux.

Návrat k původnímu počátečnímu disku RAM

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

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

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

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

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

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

7.5 Obnova souborů

7.5.1 Obnovení souborů pomocí webového rozhraní

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

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

   - [Doporučeno] Pokud se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte cílový počítač, který je online, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).
   - Stáhněte soubory z cloudového úložiště (str. 208).
   - Použijte spouštěcí médium (str. 210).
4. Klikněte na **Obnovit** > **Soubory/složky**.
5. Přejděte do požadované složky nebo pomocí vyhledávání získejte seznam požadovaných souborů a složek.

   Je možné použít více zástupných znaků (* a ?). Více informací o používání zástupných znaků naleznete v části Filtry souborů (str. 172).

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

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

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

   - Počítač, který původně obsahoval soubory, jež chcete obnovit (pokud je na počítači nainstalován agent).
   - Počítač, kde je nainstalován Agent pro VMware, Agent pro Hyper-V nebo Agent pro Scale Computing HC3 (pokud soubory pocházejí z virtuálního počítače ESXi, Hyper-V nebo Scale Computing HC3).

   Toto je cílový počítač pro obnovu. Pokud je to nutné, můžete vybrat jiný počítač.
9. V části **Cesta** vyberte cílové umístění obnovy. Je možné vybrat jednu z následujících možností:

   - Původní umístění (při obnově na původní počítač)
   - Místní složka v cílovém počítači

     Poznámka *Symbolické odkazy nejsou podporovány.*
   - Síťová složka, která je přístupná z cílového počítače
1. Klikněte na možnost **Spustit obnovu**.
2. Vyberte jednu z možností pro přepis souborů:

   - **Přepsat existující soubory**
   - **Přepsat existující soubor, pokud je starší**
   - **Nepřepisovat existující soubory**

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

7.5.2 Stahování souborů z cloudového úložiště

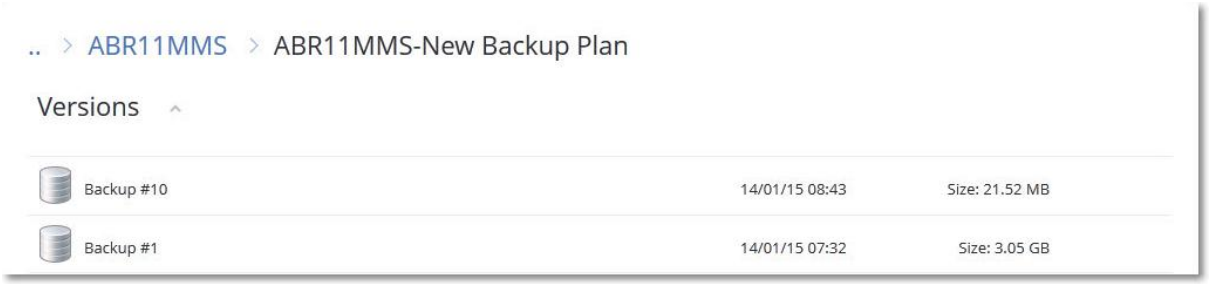
Je možné procházet cloudové úložiště, zobrazovat obsah záloh a stahovat potřebné soubory.

Omezení

- Zálohy stavu systému, databáze SQL a databáze Exchange není možné procházet.
- Pokud chcete zlepšit stahování, nestahujte najednou více než 100 MB dat. Chcete-li rychle načíst větší množství dat z cloudu, použijte postup pro obnovení souborů (str. 207).

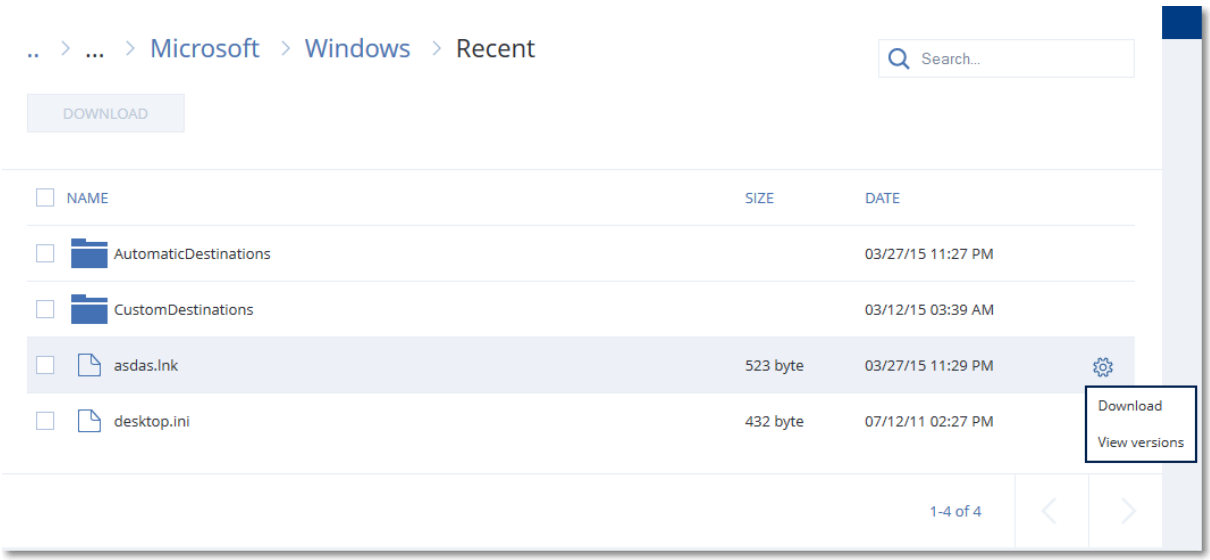
Jak stáhnout soubory z cloudového úložiště

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



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

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



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

   Pokud vyberete jeden soubor, stáhne se tak, jak je. Jinak se vybraná data archivují do souboru .zip

7. Vyberte umístění k uložení dat a klikněte na tlačítko **Uložit**.

7.5.3 Ověřování autenticity souboru pomocí služby Notary

Pokud byla během zálohování zapnutá notarizace (str. 155), můžete ověřit autenticitu souboru.

Jak ověřit autenticitu souboru

1. Soubor vyberte podle kroků 1–6 v části Obnovení souborů pomocí webového rozhraní (str. 207) nebo podle kroků 1–5 v části Stahování souborů z cloudového úložiště (str. 208).
2. Zkontrolujte, zda je vybraný soubor označený následující ikonou:  . To znamená, že soubor je notarizován.
3. Proveďte jeden z následujících úkonů:
   - Klikněte na možnost **Ověřit**.

     Software zkontroluje autenticitu souboru a zobrazí výsledek.
   - Klikněte na možnost **Získat certifikát**.

     V okně webového prohlížeče se zobrazí certifikát potvrzující notarizaci souboru. Okno také obsahuje pokyny, které vám umožní ověřit autenticitu souboru ručně.

7.5.4 Podepsání souboru pomocí služby ASign

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

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

Například můžete ASign použít k elektronickému podpisu následujících souborů:

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

Jak podepsat verzi souboru

1. Soubor vyberte podle kroků 1–6 v části Obnovení souborů pomocí webového rozhraní (str. 207).
2. Ověřte, zda je v levém panelu vybráno správné datum a čas.
3. Pokračujte kliknutím na možnost **Podepsat tuto verzi souboru**.

4. Zadejte heslo pro účet cloudového úložiště, ve kterém je záloha uložena. Přihlášení k účtu se zobrazí v okně s výzvou.

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

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

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

7.5.5 Obnovení souborů pomocí spouštěcího média

Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 198).

Jak obnovit soubory pomocí spouštěcího média

1. Spusťte cílový počítač pomocí spouštěcího média.
2. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).
3. Pokud je v síti zapnutý proxy server, klikněte na možnosti **Nástroje** > **Proxy server** a zadejte název hostitele či IP adresu a port proxy serveru. Jinak tento krok přeskočte.
4. V uvítacím okně klikněte na možnost **Obnovit**.
5. Klikněte na **Označit data** a poté klikněte na **Procházet**.
6. Určete umístění zálohy:
   - Chcete-li provést obnovení z cloudového úložiště, vyberte možnost **Cloudové úložiště**. Zadejte pověření k účtu, ke kterému je zálohovaný počítač přiřazen.
   - Pokud chcete provést obnovení z místní nebo síťové složky, vyhledejte ji v části **Místní složky** nebo **Síťové složky**.

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

Poznámka *Umístění pásky zabírá hodně místa a v případě opětovné kontroly a obnovení v rámci spouštěcího média pro Linux nebo spouštěcího média pro WinPE se nemusí vejít do paměti RAM. V případě Linuxu je nutné připojit další umístění a ušetřit tak data na disku nebo ve sdílené složce. Viz Acronis Cyber Backup Advanced: Změna složky umístění pásky (KB 27445). Pro systém Windows PE momentálně neexistuje žádné alternativní řešení.*

7.5.6 Extrahování souborů z místních záloh

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

Požadavky

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

Jak extrahovat soubory ze zálohy

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

7.6 Obnova stavu systému

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

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

7.7 Obnova konfigurace ESXi

Chcete-li obnovit konfiguraci ESXi, budete potřebovat spouštěcí média systému Linux. Informace o tvorbě spouštěcích médií naleznete v tématu Tvorba spouštěcího média (str. 198).

Pokud obnovujete konfiguraci ESXi do jiného než původního hostitele a původní hostitel ESXi je k serveru vCenter stále připojen, ze serveru jej odeberte, aby při obnově nedocházelo k nečekaným potížím. Pokud chcete původního hostitele ponechat spolu s obnoveným, můžete jej znovu přidat, až bude obnova dokončena.

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

Jak obnovit konfiguraci ESXi

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

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

7.8 Možnosti obnovy

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

Dostupnost možností obnovení

Dostupné možnosti obnovení závisí na:

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

Následující tabulka shrnuje dostupnosti možností obnovení.

	Disky			**Soubory**				**Virtuální počítače**	**SQL a Exchange**
	Windows	Linux	Spouštěcí médium	Windows	Linux	macOS	Spouštěcí médium	ESXi, Hyper-V, Scale Computing HC3	Windows

	Disky			Soubory				Virtuální počítače	SQL a Exchange
	Windows	Linux	Spouštěcí médium	Windows	Linux	macOS	Spouštěcí médium	ESXi, Hyper-V, Scale Computing HC3	Windows
Ověření zálohy (str. 213)	+	+	+	+	+	+	+	+	+
Režim spouštění (str. 214)	+	-	-	-	-	-	-	+	-
Datum a čas pro soubory (str. 215)	-	-	-	+	+	+	+	-	-
Zpracování chyb (str. 215)	+	+	+	+	+	+	+	+	+
Vyloučení souborů (str. 216)	-	-	-	+	+	+	+	-	-
Flashback (str. 216)	+	+	+	-	-	-	-	+	-
Obnova úplné cesty (str. 216)	-	-	-	+	+	+	+	-	-
Přípojné body (str. 216)	-	-	-	+	-	-	-	-	-
Výkon (str. 217)	+	+	-	+	+	+	-	+	+
Příkazy před-po (str. 217)	+	+	-	+	+	+	-	+	+
Změna SID (str. 218)	+	-	-	-	-	-	-	-	-
Správa napájení virtuálního počítače (str. 219)	-	-	-	-	-	-	-	+	-
Protokol událostí systému Windows (str. 219)	+	-	-	+	-	-	-	Pouze Hyper-V	+

7.8.1 Ověření zálohy

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

Výchozí nastavení: **Zakázáno**.

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

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

Poznámka *Ověření je k dispozici pro cloudové úložiště v datovém centru Acronis poskytnuté partnery Acronis.*

7.8.2 Režim spouštění

Tato možnost platí pouze pro obnovu fyzického nebo virtuálního počítače ze zálohy na úrovni disku obsahující operační systém Windows.

Tato volba umožňuje vybrat režim spouštění (BIOS nebo UEFI), který systém Windows použije po obnovení. Pokud se režim spouštění původního počítače liší od vybraného režimu spouštění, provede software následující akce:

- Inicializuje disk, na který obnovujete systémový svazek podle vybraného režimu spouštění (MBR pro BIOS, GPT pro UEFI).
- Upraví operační systém Windows tak, aby bylo možné jej spustit pomocí vybraného režimu spouštění.

Výchozí nastavení: **Jako na cílovém počítači.**

Můžete si vybrat jeden z úkonů níže:

- **Jako na cílovém počítači**

  Agent spuštěný v cílovém počítači zjistí režim spouštění aktuálně používaný v systému Windows a provede úpravy podle zjištěného režimu spouštění.

  To je nejjistější hodnota, díky které se automaticky vytvoří spustitelný systém, pokud neplatí níže uvedená omezení. Protože v rámci spouštěcího média není k dispozici možnost **Režim spouštění**, chová se agent, jako kdyby byla tato hodnota již zvolená.
- **Jako na zálohovaném počítači**

  Agent spuštěný v cílovém počítači přečte režim spouštění ze zálohy a provede úpravy podle zjištěného režimu spouštění. Můžete tak obnovit systém v jiném počítači i v případě, že daný počítač používá jiný režim spouštění, a potom nahradit disk v zálohovaném počítači.
- **BIOS**

  Agent spuštěný v cílovém počítači provede úpravy k použití systému BIOS.
- **UEFI**

  Agent spuštěný v cílovém počítači provede úpravy k použití systému UEFI.

Po změně nastavení se bude opakovat postup mapování disku. Tato operace bude chvíli trvat.

Doporučení

Pokud potřebujete přenést Windows mezi rozhraním UEFI a systémem BIOS:

- Obnovte celý disk, na kterém je umístěn systémový svazek. Pokud obnovíte pouze systémový svazek na již existujícím svazku, nebude agent moci správně inicializovat cílový disk.
- Mějte na paměti, že systém BIOS neumožňuje využít více jak 2 TB místa.

Omezení

- Přenos mezi rozhraním UEFI a systémem BIOS je podporován v těchto systémech:
  - 64bitové operační systémy Windows počínaje systémem Windows Vista SP1
  - 64bitové operační systémy Windows Server počínaje systémem Windows Server 2008 SP1
- Přenos mezi rozhraním UEFI a systémem BIOS není podporován, jestliže je záloha uložena na páskovém zařízení.

Pokud není přenos mezi rozhraním UEFI a systémem BIOS podporován, chová se agent, jako kdyby bylo vybráno nastavení **Jako na zálohovaném počítači**. Pokud cílový počítač podporuje rozhraní UEFI i systém BIOS, je nutné ručně povolit režim spouštění odpovídající původnímu počítači. Jinak se systém nespustí.

7.8.3 Datum a čas pro soubory

Tato možnost je účinná pouze při obnově souborů.

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

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

Výchozí nastavení: **Povoleno**.

7.8.4 Zpracování chyb

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

Pokud dojde k chybě, pokusit se znovu

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

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

Při zpracování nezobrazovat zprávy a dialogová okna (tichý režim)

Výchozí nastavení: **Zakázáno**.

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

Uložení informací o systému, pokud selže obnovení s restartováním

Tato možnost platí pro obnovu disků nebo svazků do fyzických počítačů se systémem Windows nebo Linux.

Výchozí nastavení: **Zakázáno**.

Je-li tato možnost povolena, můžete určit složku na místním disku (včetně flash disků nebo pevných disků připojených k cílovému počítači) nebo v síťovém úložišti, kde budou uloženy soubory protokolů, systémové informace a výpisy stavu systému. Tento soubor pomůže pracovníkům technické podpory identifikovat problém.

7.8.5 Vyloučení souborů

Tato možnost je účinná pouze při obnově souborů.

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

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

7.8.6 Zabezpečení na úrovni souborů

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

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

Výchozí nastavení: **Povoleno**.

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

7.8.7 Flashback

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

Pokud je tato možnost zapnutá, obnoví se jen rozdíly mezi daty v záloze a na cílovém disku. Tím se urychlí obnova dat na stejný disk, který byl zálohován, zvláště pokud se nezměnilo rozvržení svazků na disku. Data se porovnávají na úrovni bloků.

U fyzických počítačů je porovnávání dat na úrovni bloků časově náročná operace. Pokud je připojení k úložišti záloh rychlé, bude obnovení celého disku trvat kratší dobu než výpočet datových rozdílů. Proto doporučujeme povolit tuto možnost pouze v případě, že připojení k úložišti záloh je pomalé (například pokud je záloha uložena v cloudovém úložišti nebo ve vzdálené síťové složce).

Při obnovení fyzického počítače výchozí nastavení závisí na umístění zálohy:

- Pokud se umístění zálohy nachází v cloudovém úložišti, je výchozí nastavení: **Povoleno**.
- Pro ostatní umístění zálohy je výchozí nastavení: **Zakázáno**.

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

7.8.8 Obnova úplné cesty

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

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

Výchozí nastavení: **Zakázáno**.

7.8.9 Přípojné body

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

Tuto možnost zapněte, chcete-li obnovit soubory a složky, které byly uloženy na připojených svazcích a zálohovány se zapnutou možností Přípojné body (str. 181).

Výchozí nastavení: **Zakázáno**.

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

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

7.8.10 Výkon

Tato možnost definuje prioritu procesu obnovy v operačním systému.

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

Výchozí nastavení: **Normální**–

Priorita procesu běžícího v systému určuje množství CPU a systémových zdrojů poskytnutých procesu. Snížením priority obnovy uvolníte více zdrojů pro další aplikace. Pokud zvýšíte prioritu obnovy, může to celý proces urychlit, protože operační systém bude moci přidělit více prostředků aplikaci, která bude obnovu provádět. Výsledek ovšem závisí na celkovém zatížení procesoru a dalších faktorech, například rychlosti čtení/zápisu disku nebo síťovém provozu.

7.8.11 Příkazy před-po

Tato volba vám umožňuje určit příkazy, které se provedou automaticky před a po obnově dat.

Příklad, jak můžete používat příkazy před/po:

- Můžete spustit příkaz **Checkdisk** s cílem najít a opravit logické chyby systému souborů, fyzické chyby nebo vadné sektory před zahájením obnovy nebo po dokončení obnovy.

Tento program nepodporuje interaktivní příkazy. To jsou příkazy, které vyžadují zásah uživatele (například "pause").

Příkazy po obnově nebudou vykonány, pokud obnova pokračuje restartováním.

7.8.11.1 Příkaz před obnovením

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

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

Políčko	Nastavení			
Nechat selhat obnovu, pokud selže vykonávání příkazu*	Zaškrtnuto	Nezaškrtnuto	Zaškrtnuto	Nezaškrtnuto
S obnovou počkejte až na dokončení provádění příkazu	Zaškrtnuto	Zaškrtnuto	Nezaškrtnuto	Nezaškrtnuto
Výsledek				
	Přednastaveno Provést obnovu pouze po úspěšném vykonání příkazu. Nechat selhat obnovu, pokud selže vykonávání příkazu.	Provést obnovu po vykonání příkazu, ať už vykonání příkazů bylo nebo nebylo úspěšné.	N/A	Provést obnovu současně s vykonáváním příkazu a bez ohledu na výsledku provedení příkazu.

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

7.8.11.2 Příkaz po obnovení

Jak zadat příkaz/spustitelný soubor, aby byl spuštěn po dokončení obnovení

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

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

Poznámka *Příkazy po obnově nebudou vykonány, pokud obnova pokračuje restartováním.*

7.8.12 Změna SID

Tato možnost platí při obnově systému Windows 8.1/Windows Server 2012 R2 nebo staršího.

Tato možnost nefunguje, když se provádí obnova na virtuální počítač pomocí Agenta pro VMware, Agenta pro Hyper-V nebo Agenta pro Scale Computing HC3.

Výchozí nastavení: **Zakázáno**.

Software může vygenerovat jedinečný bezpečnostní identifikátor (SID počítače) pro obnovený operační systém. Touto možností můžete zajistit provozuschopnost softwaru třetích stran závisejícího na SID počítače.

Společnost Microsoft oficiálně nepodporuje změnu SID v nasazeném nebo obnoveném systému. Tuto možnost používáte na vlastní nebezpečí.

7.8.13 Správa napájení virtuálního počítače

Tyto možnosti fungují, když se provádí obnovení do virtuálního počítače pomocí Agenta pro VMware, Agenta pro Hyper-V nebo Agenta pro Scale Computing HC3.

Vypnout cílové virtuální počítače při spuštění obnovení

Výchozí nastavení: **Povoleno**.

Obnovení do existující virtuálního počítače není možné, pokud je online, a proto je tento počítač při zahájení obnovy automaticky vypnut. Uživatelé budou od počítače odpojeni a veškerá neuložená data budou ztracena.

Zrušte zaškrtnutí políčka pro toto nastavení, pokud před obnovením preferujete ruční vypnutí virtuálního počítače.

Zapnout cílový virtuální počítač po dokončení obnovení

Výchozí nastavení: **Zakázáno**.

Po obnovení počítače ze zálohy na jiný počítač existuje šance, že se v síti objeví replika existujícího počítače. Bezpečný provoz zajistíte ručním zapnutím obnoveného virtuálního počítače po provedení nezbytných opatření.

7.8.14 Protokol událostí systému Windows

Tato možnost platí pouze pro operační systémy Windows.

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

Výchozí nastavení: **Zakázáno**.

8 Obnovení po havárii

Tato funkce je dostupná pouze v cloudových nasazeních aplikace Acronis Cyber Protect. Podrobný popis této funkce viz Argentina/support/documentation/DisasterRecovery/index.html#43224.html.

9 Operace se zálohami

9.1 Karta Úložiště záloh

Na kartě **Úložiště záloh** jsou uvedeny zálohy všech počítačů, které kdy byly registrovány na serveru pro správu. Toto se týká i počítačů ve stavu offline a počítačů, které již nejsou dále registrovány.

Zálohy uložené ve sdílených umístěních (například ve sdílených složkách SMB nebo NFS) jsou viditelné všem uživatelům, kteří mají pro dané umístění oprávnění ke čtení.

V případě cloudového úložiště mají uživatelé přístup pouze ke svým zálohám. Při cloudovém nasazení si správce může zobrazit zálohy jakéhokoli účtu, který patří ke stejné skupině a jejím podřízeným skupinám. Tento účet se nepřímo vybere v okně **Počítač k procházení**. Karta **Úložiště záloh** zobrazuje zálohy všech počítačů registrovaných pod stejným účtem, pod kterým je registrován počítač.

Umístění zálohy použitá v plánech ochrany se automaticky přidají na kartu **Úložiště záloh**. Chcete-li přidat vlastní složku (například vyměnitelné zařízení USB) do seznamu umístění záloh, klikněte na tlačítko **Procházet** a určete cestu ke složce.

Postup výběru bodu obnovy pomocí karty Úložiště záloh

1. Na kartě **Úložiště záloh** vyberte umístění, kde jsou uloženy zálohy.

   Software zobrazí všechny zálohy, u kterých má váš účet oprávnění je zobrazit v daném umístění. Zálohy jsou seskupeny do skupin. Názvy skupin se tvoří podle následující šablony:

   `<název počítače> – <název plánu ochrany>`
2. Vyberte skupinu, ze které chcete obnovit data.
3. [Volitelné] Klikněte na tlačítko **Změnit** vedle položky **Počítač k procházení** a poté vyberte jiný počítač. Některé zálohy smí procházet pouze určití agenti. Například pokud chcete procházet zálohy databází aplikace Microsoft SQL Server, je nutné vybrat počítač, na kterém běží Agent pro SQL.

   Důležité *Mějte na vědomí, že* ***Počítač k procházení*** *je výchozí umístění zálohy fyzického počítače, ze které se provede obnova. Po výběru bodu obnovy a kliknutí na možnost* ***Obnovit*** *zkontrolujte nastavení u položky* ***Cílový počítač****, abyste se ujistili, že chcete provést obnovu na tento konkrétní počítač. Chcete-li změnit umístění obnovy, vyberte jiný počítač pomocí možnost* ***Počítač k procházení****.*
4. Klikněte na možnost **Zobrazit zálohy**.
5. Vyberte bod obnovy.

9.2 Připojování svazků ze zálohy

Když připojíte svazek ze zálohy na úrovni disku, budete k němu moct přistupovat, jako by se jednalo o fyzický disk.

Připojení svazků v režimu pro čtení/zápis vám umožňuje upravovat obsah zálohy, tedy ukládat, přesouvat, vytvářet a mazat soubory nebo složky a spouštět spustitelné soubory skládající se

z jednoho souboru. V tomto režimu vytvoří software přírůstkovou zálohu obsahující změny, které v obsahu zálohy provedete. Mějte na paměti, že tyto změny nebude obsahovat žádná z následujících záloh.

Požadavky

- Tato funkce je dostupná jen ve Windows v Průzkumníku souborů.
- Na počítači, na kterém chcete svazek připojit, musí být nainstalovaný Agent pro Windows.
- Zálohovaný systém souborů musí být podporován tou verzí Windows, kterou váš počítač používá.
- Záloha musí být uložená v místní složce, v síťovém umístění (SMB/CIFS) nebo v oddílu Secure Zone.

Scénáře použití

- **Sdílení dat**

  Obsah připojených svazků se dá snadno sdílet přes síť.

- **„Náplasťové“ řešení obnovy databáze**

  Připojte svazek obsahující databázi SQL počítače, který havaroval. Tím umožníte přístup k databázi, dokud nebude počítač obnoven. Tento přístup lze využít i ke granulární obnově dat z Microsoft Sharepointu pomocí aplikace SharePoint Explorer.

- **Offline likvidace virů**

  Máte-li nakažený počítač, připojte jeho zálohu, vyčistěte ji pomocí antivirového programu (anebo najděte nejnovější nenakaženou databázi) a potom počítač obnovte z této zálohy.

- **Kontrola chyb**

  Pokud selhala obnova se změnou velikosti svazku, může to být kvůli chybě v zálohovaném systému souborů. Připojte zálohu v režimu pro čtení/zápis. Potom zkontrolujte chyby na připojeném svazku příkazem **chkdsk /r**. Až budou chyby opravené a vytvoří se nová přírůstková záloha, obnovte systém z této zálohy.

Jak připojit svazek ze zálohy

1. V Průzkumníku souborů přejděte do umístění se zálohou.
2. Dvakrát klikněte na soubor zálohy. Ve výchozím nastavení se názvy souborů tvoří podle následující šablony:

   `<název počítače> – <GUID plánu ochrany>`
3. Pokud je záloha zašifrovaná, zadejte šifrovací heslo. Jinak tento krok přeskočte.

   Průzkumník souborů zobrazí body obnovy.
4. Dvakrát klikněte na požadovaný bod obnovy.

   Průzkumník souborů zobrazí zálohované svazky.

   Tip: *Když na svazek dvakrát kliknete, můžete procházet jeho obsah. Soubory a složky ze zálohy se dají kopírovat do jakékoli složky ve vašem systému souborů.*
5. Klikněte na svazek pravým tlačítkem a vyberte některou z těchto akcí:
   - **Připojit**
   - **Připojit v režimu jen pro čtení**
6. Pokud je záloha uložená v síťovém umístění, zadejte pověření k přístupu. Jinak tento krok přeskočte.

   Software připojí vybraný svazek. Svazku bude přiděleno první nepoužité písmeno.

Jak odpojit svazek

1. V Průzkumníku souborů přejděte na **Počítač** (respektive **Tento počítač** v systému Windows 8.1 a starším).
2. Klikněte pravým tlačítkem na připojený svazek.
3. Klikněte na **Odpojit**.
4. Pokud byl svazek připojený v režimu pro čtení/zápis a došlo ke změně jeho obsahu, zvolte, zda chcete vytvořit přírůstkovou zálohu obsahující tyto změny. Jinak tento krok přeskočte.

   Software odpojí vybraný svazek.

9.3 Export záloh

Operace exportu vytvoří soběstačnou kopii zálohy do vámi určeného umístění. Původní záloha zůstává nedotčena. Export umožňuje z řetězce přírůstkových a rozdílových záloh oddělit určitou zálohu pro rychlou obnovu, nebo rychlý zápis na vyměnitelná média, odnímatelná média a pro další účely.

Výsledkem operace exportu je vždy plná záloha. Chcete-li replikovat celý řetězec záloh do jiného umístění a zachovat několik bodů obnovy, použijte plán replikace záloh (str. 225).

Název souboru zálohy (str. 164) exportované zálohy závisí na hodnotě formátu zálohy (str. 167):

- Pro formát **Verze 12** s libovolným schématem zálohování je název souboru zálohy stejný jako název původní zálohy, s výjimkou pořadového čísla. Pokud je do stejného umístění exportováno více záloh ze stejného řetězce záloh, připojí se k názvům souborů všech záloh čtyřmístné pořadové číslo, s výjimkou prvního souboru.
- Pro formát **Verze 11** se schématem zálohování **Vždy přírůstkový (jeden soubor)** název souboru zálohy přesně odpovídá názvu souboru zálohy původní zálohy. Pokud je do stejného umístění exportováno více záloh ze stejného řetězce záloh, každá operace exportu přepíše dříve exportovanou zálohu.
- Pro formát **Verze 11** s jinými schématy zálohování je název souboru zálohy stejný jako název původní zálohy, s výjimkou časového razítka. Časová razítka exportovaných záloh odpovídají době, kdy je prováděn export.

Exportovaná záloha zdědí nastavení šifrování a heslo z původní zálohy. Při exportu šifrované zálohy musíte zadat heslo.

Export zálohy

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

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

   - Pokud se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte cílový počítač ve stavu online a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).
4. Klikněte na ikonu ozubeného kola a potom klikněte na **Export**.
5. Vyberte agenta, který provede export.
6. Pokud je záloha šifrovaná, zadejte heslo. Jinak tento krok přeskočte.
7. Vyberte cílové umístění exportu.
8. Klikněte na **Spustit**.

9.4 Odstranění záloh

Upozornění *Po odstranění zálohy jsou všechna data trvale vymazána. Odstraněná data nelze obnovit.*

Odstranění záloh počítače, který je ve stavu online a je přítomný ve webové konzoli Cyber Protect

1. Na kartě **Všechna zařízení** vyberte počítač, jehož zálohy chcete odstranit.
2. Klikněte na možnost **Obnova**.
3. Vyberte umístění, ze kterého chcete odstranit úlohy.
4. Proveďte jeden z následujících úkonů:
   - Chcete-li odstranit jednu zálohu, vyberte ji a klikněte na ikonu ozubeného kola a potom na možnost **Odstranit**.
   - Všechny zálohy ve vybraném umístění odstraníte kliknutím na **Odstranit vše**.
5. Potvrďte své rozhodnutí.

Jak odstranit zálohy libovolného počítače

1. Na kartě **Úložiště záloh** vyberte umístění, ze kterého chcete odstranit zálohy.

   Software zobrazí všechny zálohy, u kterých má váš účet oprávnění je zobrazit v daném umístění. Zálohy jsou seskupeny do skupin. Názvy skupin se tvoří podle následující šablony:

   `<název počítače> – <název plánu ochrany>`
2. Vyberte skupinu.
3. Proveďte jeden z následujících úkonů:
   - Chcete-li odstranit jednu zálohu, klikněte na možnost **Zobrazit zálohy**, vyberte požadovanou zálohu, klikněte na ikonu ozubeného kola a potom na možnost **Odstranit**.
   - Kliknutím na tlačítko **Odstranit** odstraníte vybranou skupinu.
4. Potvrďte své rozhodnutí.

Odstranění záloh přímo z cloudového úložiště

1. Přihlaste se do cloudového úložiště způsobem popsaným v části Stahování souborů z cloudového úložiště (str. 208).
2. Klikněte na název počítače, jehož zálohy chcete odstranit.

   Software zobrazí jednu nebo více skupin záloh.
3. Klikněte na ikonu ozubeného kola u skupiny záloh, kterou chcete odstranit.
4. Klikněte na **Odebrat**.
5. Potvrďte operaci.

10 Karta Plány

Plány ochrany a další plány můžete spravovat na kartě **Plány**.

Každá část karty **Plány** obsahuje všechny plány konkrétního typu. Toto jsou všechny dostupné části:

- **Ochrana**
- **Kontrola záloh** (str. 224)
- **Replikace záloh** (str. 225)
- **Ověřování** (str. 226)
- **Vyčištění** (str. 228)

- **Převod do VM** (str. 228)
- **Replikace virtuálního počítače** (str. 330)
- **Spouštěcí médium**. V této části jsou uvedeny plány ochrany, které byly vytvořeny pro počítače spouštěné ze spouštěcího média (str. 253) a které lze použít pouze na těchto počítačích.

Plány pro replikaci, ověřování, vyčištění a převod záloh na virtuální počítač jsou k dispozici pouze s licencí Advanced. Pokud nemáte licenci Advanced, je možné tyto akce provádět pouze jako součást plánu ochrany.

V každé části můžete plán vytvořit, upravit, zakázat, povolit, odstranit a spustit a můžete zkontrolovat stav provádění plánu.

Klonování a zastavování je dostupné pouze pro plány ochrany. Na rozdíl od zastavení zálohování z karty **Zařízení** bude plán ochrany zastaven na všech zařízeních, na kterých je spuštěn. Pokud je spuštění zálohování pro různá zařízení naplánováno na různou dobu, zastavení plánu ochrany také zabrání spuštění zálohování na zařízeních, na kterých ještě není spuštěno.

Plán můžete také exportovat do souboru nebo importovat dříve exportovaný plán.

10.1 Zpracovávání dat mimo hostitele

Většina akcí, které jsou součástí plánu ochrany, jako je replikace, ověřování a použití pravidel zachování, je prováděna agentem, který provádí zálohování. Tím dochází k dalšímu zatížení počítače, ve kterém je agent spuštěný, i po dokončení procesu zálohování.

Oddělením plánů antimalwarové kontroly, replikace, ověřování, vyčištění a převodu od plánů ochrany získáte následující flexibilitu:

- Zvolit pro tyto operace jiného agenta nebo agenty
- Naplánovat tyto operace na časy mimo pracovní špičku kvůli minimalizaci spotřeby šířky pásma sítě
- Přesunout tyto operace mimo pracovní dobu, pokud neplánujete zřídit vyhrazeného agenta

Pokud používáte uzel úložišť, má instalace vyhrazeného agenta na stejný počítač smysl.

Na rozdíl od plánů zálohování a replikace virtuálních počítačů, které používají časové nastavení z počítačů, kde běží agenti, běží plány zpracovávání dat mimo hostitele podle časových nastavení počítače se serverem pro správu.

10.1.1 Plán kontroly zálohy

Podporovaná umístění

Malware můžete v zálohách vyhledávat v následujících umístěních: **Cloudové úložiště**, **místní složka** a **síťová složka**. Do umístění **Místní složka** má přístup pouze agent nainstalovaný na kontrolovaném počítači.

Další informace o kontrole záloh a souvisejících omezeních naleznete v tématu „Antimalwarová kontrola záloh (p. 372)“.

Vytvoření plánu kontroly zálohy

1. Ve webové konzoli Cyber Protect klikněte na položky **Plány** > **Kontrola záloh**.
2. Klikněte na **Vytvořit plán**.
3. [Volitelné] Chcete-li upravit název plánu, klikněte na ikonu tužky vedle výchozího názvu.

4. Vyberte agenta kontroly.
5. Vyberte umístění zálohy nebo jednotlivé zálohy, které chcete kontrolovat.

   Současně můžete vybrat několik umístění zálohy. Chcete-li do jednoho plánu zahrnout několik individuálních záloh, musíte zálohy přidávat postupně.
6. [Pokud je vybrána možnost **Cloudové úložiště** nebo **Síťová složka**] Pokud se zobrazí výzva, zadejte pověření k úložišti záloh.
7. [Pokud je vybrána šifrovaná záloha] Zadejte heslo pro přístup k záloze. Pokud vyberete úložiště nebo více šifrovaných záloh, můžete zadat jedno heslo. Pokud heslo není pro konkrétní zálohu správné, zobrazí se výstraha. Kontrolovány budou pouze zálohy, pro které bude zadáno správné heslo.
8. Nakonfigurujte harmonogram kontroly.
9. Jakmile budete hotovi, klikněte na tlačítko **Vytvořit**.

Vytvoří se plán kontroly zálohy.

10.1.2 Replikace záloh

Podporovaná umístění

Následující tabulka shrnuje umístění záloh podporovaná plány replikace záloh.

Umístění záloh	Podporováno jako zdroj	Podporováno jako cíl
Cloudové úložiště	+	+
Místní složka	+	+
Síťová složka	+	+
Složka NFS	–	–
Secure Zone	–	–
Server SFTP	–	–
Spravované umístění	+	+
Páskové zařízení	–	+

Vytvoření plánu replikace záloh

1. Klikněte na **Plány** > **Replikace záloh**.
2. Klikněte na **Vytvořit plán**.

   Software zobrazí šablonu nového plánu.
3. [Volitelné] Chcete-li upravit název plánu, klikněte na výchozí název.
4. Klikněte na možnost **Agent** a potom vyberte agenta, který provede replikaci.

   Můžete vybrat jakéhokoli agenta, který má přístup ke zdrojovému a cílovému umístění zálohy.
5. Klikněte na možnost **Položky k replikaci** a vyberte zálohy, které bude tento plán replikovat.

   Přepínat mezi výběrem záloh a výběrem celých umístění můžete pomocí přepínače **Umístění/Zálohy** v pravém horním rohu.

   Pokud jsou vybrané zálohy šifrované, musí všechny používat stejné heslo. Pro zálohy, které používají různá hesla pro šifrování, vytvořte samostatné plány.
6. Klikněte na **Cíl** a pak zadejte cílové umístění.

7. [Volitelné] V části **Jak replikovat** vyberte, které zálohy chcete replikovat. Je možné vybrat jednu z následujících možností:
   - **Všechny zálohy** (výchozí nastavení)
   - **Jen plné zálohy**
   - **Pouze poslední zálohu**
8. [Volitelné] Klikněte na možnost **Plán** a změňte plán.
9. [Volitelné] Klikněte na **Pravidla zachování** a pak určete pravidla zachování pro cílové umístění podle postupu popsaného v části Pravidla zachování (str. 152).
10. Pokud jsou zálohy vybrané v kroku **Položky k replikaci** zašifrovány, klikněte na možnost **Heslo zálohy** a poté zadejte heslo. Jinak tento krok přeskočte.
11. [Volitelné] Pokud chcete upravit možnosti plánu, klikněte na ikonu ozubeného kola.
12. Klikněte na tlačítko **Vytvořit**.

10.1.3 Ověření

Ověřování je operace, která kontroluje možnost obnovy dat ze zálohy.

Ověřování umístění zálohy ověřuje všechny zálohy uložené v daném umístění.

Jak to funguje

Plán ověřování nabízí dvě metody ověření. Pokud vyberete obě metody, operace budou prováděny postupně.

- **Výpočet kontrolního součtu pro každý blok dat uložený v záloze.**

  Další informace o ověření výpočtem kontrolního součtu naleznete v části Ověření zálohy (str. 168).
- **Spuštění virtuálního počítače ze zálohy**

  Tato metoda funguje pouze pro zálohy na úrovni disku, které obsahují operační systém. Chcete použít tuto metodu, potřebujete hostitele ESXi nebo Hyper-V a agenta pro ochranu (Agent pro VMware nebo Agent pro Hyper-V), který spravuje tohoto hostitele.

  Agent spustí virtuální počítač ze zálohy a potom se připojí k VMware Tools nebo službě prezenčního signálu Hyper-V kvůli ověření úspěšného spuštění operačního systému. Pokud se připojení nezdaří, agent se pokusí připojit každé dvě minuty a to celkem pětkrát. Není-li žádný z pokusů úspěšný, ověření se nezdaří.

  Bez ohledu na počet plánů ověření a ověřených záloh, agent, který provádí ověření, spustí vždy jeden virtuální počítač současně. Jakmile je výsledek ověření jasný, agent odstraní aktuální virtuální počítač a spustí další.

Pokud se ověření nezdaří, můžete si prohlédnout podrobnosti v části **Aktivity** na kartě **Přehled**.

Podporovaná umístění

Následující tabulka shrnuje umístění záloh podporovaná plány ověřování.

Umístění záloh	Výpočet kontrolního součtu	Spuštění virtuálního počítače
Cloudové úložiště	+	+
Místní složka	+	+
Síťová složka	+	+

Složka NFS	–	–
Secure Zone	–	–
Server SFTP	–	–
Spravované umístění	+	+
Páskové zařízení	+	–

Vytvoření nového plánu ověřování

1. Klikněte na možnost **Plány** > **Ověřování**.
2. Klikněte na **Vytvořit plán**.

   Software zobrazí šablonu nového plánu.
3. [Volitelné] Chcete-li upravit název plánu, klikněte na výchozí název.
4. Klikněte na možnost **Agent** a potom vyberte agenta, který provede ověření.

   Chcete-li provést ověření spuštěním virtuálního počítače ze zálohy, musíte vybrat Agenta pro WMware nebo Agenta pro Hyper-V. V opačném případě vyberte libovolného agenta, který je zaregistrovaný na serveru pro správu a má přístup k umístění zálohy.
5. Klikněte na možnost **Položky k ověření** a vyberte zálohy, které má tento plán ověřit.

   Přepínat mezi výběrem záloh a výběrem celých umístění můžete pomocí přepínače **Umístění/Zálohy** v pravém horním rohu.

   Pokud jsou vybrané zálohy šifrované, musí všechny používat stejné heslo. Pro zálohy, které používají různá hesla pro šifrování, vytvořte samostatné plány.
6. [Volitelné] V části **Co ověřovat** vyberte, které zálohy chcete ověřit. Je možné vybrat jednu z následujících možností:
   - **Všechny zálohy**
   - **Pouze poslední zálohu**
7. [Volitelné] Klikněte na možnost **Jak ověřovat** a potom vyberte některou z následujících metod:
   - **Ověření kontrolního součtu**

     Software vypočítá kontrolní součet pro každý blok dat uložený v záloze.
   - **Spustit jako virtuální počítač**

     Software spustí virtuální počítač z každé zálohy.
8. Pokud zvolíte možnost **Spustit jako virtuální počítač**:
   a. Klikněte na možnost **Cílový počítač** a pak vyberte typ virtuálního počítače (ESXi nebo Hyper-V), hostitele a šablonu názvu počítače.

      Výchozí název je **[Název počítače]_validate**.
   b. U ESXi klikněte na možnost **Datové úložiště**, u Hyper-V klikněte na možnost **Cesta** a pak vyberte datové úložiště virtuálního počítače.
   c. [Volitelné] Změňte režim poskytování disku.

      Ve výchozím nastavení je pro VMware ESXi nastavena možnost **Tenké** a pro Hyper-V možnost **Dynamicky se rozšiřující**.
   d. Pokud potřebujete správný výsledek ověření, nechte povolený přepínač **Prezenční signál virtuálního počítače** Tento přepínač je určen pro budoucí verze.
   e. [Volitelné] Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti a síťová připojení virtuálního počítače.

      Ve výchozím nastavení virtuální počítač *není* připojen k síti a velikost paměti virtuálního počítače se rovná velikosti paměti původního počítače.

9. [Volitelné] Klikněte na možnost **Plán** a změňte plán.
10. Pokud jsou zálohy vybrané v kroku **Položky k ověření** zašifrovány, klikněte na možnost **Heslo zálohy** a poté zadejte heslo. Jinak tento krok přeskočte.
11. [Volitelné] Pokud chcete upravit možnosti plánu, klikněte na ikonu ozubeného kola.
12. Klikněte na tlačítko **Vytvořit**.

10.1.4 Vyčištění

Vyčištění je operace, která odstraňuje zastaralé zálohy podle pravidel zachování.

Podporovaná umístění

Plány vyčištění podporují všechna umístění záloh s výjimkou složek NFS, serverů SFTP a oblasti Secure Zone.

Vytvoření nového plánu vyčištění

1. Klikněte na **Plány** > **Vyčištění**.
2. Klikněte na **Vytvořit plán**.

   Software zobrazí šablonu nového plánu.
3. [Volitelné] Chcete-li upravit název plánu, klikněte na výchozí název.
4. Klikněte na možnost **Agent** a potom vyberte agenta, který provede vyčištění.

   Můžete vybrat jakéhokoli agenta, který má přístup k umístění zálohy.
5. Klikněte na **Položky k vyčištění** a vyberte zálohy, které tento plán vyčistí.

   Přepínat mezi výběrem záloh a výběrem celých umístění můžete pomocí přepínače **Umístění/Zálohy** v pravém horním rohu.

   Pokud jsou vybrané zálohy šifrované, musí všechny používat stejné heslo. Pro zálohy, které používají různá hesla pro šifrování, vytvořte samostatné plány.
6. [Volitelné] Klikněte na možnost **Plán** a změňte plán.
7. [Volitelné] Klikněte na **Pravidla zachování** a pak určete pravidla zachování podle postupu popsaného v části Pravidla zachování (str. 152).
8. Pokud jsou zálohy vybrané v kroku **Položky k vyčištění** zašifrovány, klikněte na možnost **Heslo zálohy** a poté zadejte heslo. Jinak tento krok přeskočte.
9. [Volitelné] Pokud chcete upravit možnosti plánu, klikněte na ikonu ozubeného kola.
10. Klikněte na tlačítko **Vytvořit**.

10.1.5 Převod na virtuální počítač

Můžete vytvořit zvláštní plán pro převod na virtuální počítač a spustit tento plán ručně nebo podle plánu.

Informace o požadavcích a omezeních najdete v tématu Co potřebujete vědět o převodu (str. 156).

Vytvoření plánu převodu na virtuální počítač

1. Klikněte na **Plány** > **Převod do VM**.
2. Klikněte na tlačítko **Vytvořit plán**.

   Software zobrazí šablonu nového plánu.
3. [Volitelné] Pokud chcete upravit název plánu, klikněte na výchozí název.
4. V poli **Převést na** vyberte typ cílového virtuálního počítače. Je možné vybrat jednu z následujících možností:

- **VMware ESXi**
- **Microsoft Hyper-V**
- **VMware Workstation**
- **Soubory VHDX**

5. Proveďte jeden z následujících úkonů:
   - VMware ESXi a Hyper-V: Klikněte na **Hostitel**, vyberte cílového hostitele a pak určete novou šablonu názvu počítače.
   - Ostatní typy virtuálních počítačů: Do pole **Cesta** zadejte, kam chcete uložit soubory virtuálního počítače, a šablonu názvu souboru.

   Výchozí název je **[Název počítače]_converted**.
6. Klikněte na možnost **Agent** a potom vyberte agenta, který provede převod.
7. Klikněte na možnost **Položky k převodu** a vyberte zálohy, které tento plán převede na virtuální počítače.

   Přepínat mezi výběrem záloh a výběrem celých umístění můžete pomocí přepínače **Umístění/Zálohy** v pravém horním rohu.

   Pokud jsou vybrané zálohy šifrované, musí všechny používat stejné heslo. Pro zálohy, které používají různá hesla pro šifrování, vytvořte samostatné plány.
8. [Pouze pro VMware ESXi a Hyper-V] Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.
9. [Volitelné] Pro VMware ESXi a Hyper-V můžete také provést toto:
   - Změňte režim poskytování disku. Ve výchozím nastavení je pro VMware ESXi nastavena možnost **Tenké** a pro Hyper-V možnost **Dynamicky se rozšiřující**.
   - Klikněte na **Nastavení virtuálního počítače** a změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.
10. [Volitelné] Klikněte na možnost **Plán** a změňte plán.
11. Pokud jsou zálohy vybrané v kroku **Položky k převodu** zašifrovány, klikněte na možnost **Heslo zálohy** a poté zadejte heslo. Jinak tento krok přeskočte.
12. [Volitelné] Pokud chcete upravit možnosti plánu, klikněte na ikonu ozubeného kola.
13. Klikněte na tlačítko **Vytvořit**.

11 Spouštěcí médium

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

Spouštěcí médium

Spouštěcí médium je fyzické médium (CD, DVD, jednotka USB Flash nebo jiné vyměnitelné médium, která BIOS počítače podporuje jako spouštěcí zařízení), které umožňuje spouštět agenta aplikace Acronis Cyber Protect bez pomoci operačního systému v prostředí založeném na Linuxu nebo na WinPE (Windows Preinstallation Environment).

Spouštěcí médium se nejčastěji používá k:

- Obnovení operačního systému, který nelze spustit
- Přístupu a zálohování dat, která zůstala zachována v poškozeném systému
- Nasazení operačního systému na zcela nový počítač
- Vytváření základních nebo dynamických svazků na holém železe

- Zálohování disků s nepodporovaným systémem souborů sektor po sektoru
- Offline zálohování jakýchkoliv dat, která nemohou být zálohována online, například protože jsou trvale blokována spuštěnou aplikací nebo z důvodu omezeného přístupu.

Počítač lze také spustit spouštěním ze sítě z PXE Serveru Acronis, pomocí služby WDS (Windows Deployment Services) nebo služby RIS (Microsoft Remote Installation Services). Tyto servery s nahranými spouštěcími součástmi lze považovat za jistý druh spouštěcího média. S pomocí stejného průvodce můžete nakonfigurovat PXE server, službu WDS/RIS nebo vytvořit spouštěcí médium.

Vytvořit spouštěcí médium nebo stáhnout připravené médium?

Pomocí Tvůrce spouštěcích médií (str. 231) můžete vytvořit vlastní spouštěcí médium (založené na Linuxu (str. 232) nebo založené na WinPE (p. 247)) pro počítače se systémem Windows, Linux nebo macOS. Potřebujete-li spouštěcí médium s kompletními funkcemi, zadejte licenční klíč Acronis Cyber Protect. Bez tohoto klíče bude vaše spouštěcí médium moct provádět pouze operace obnovy.

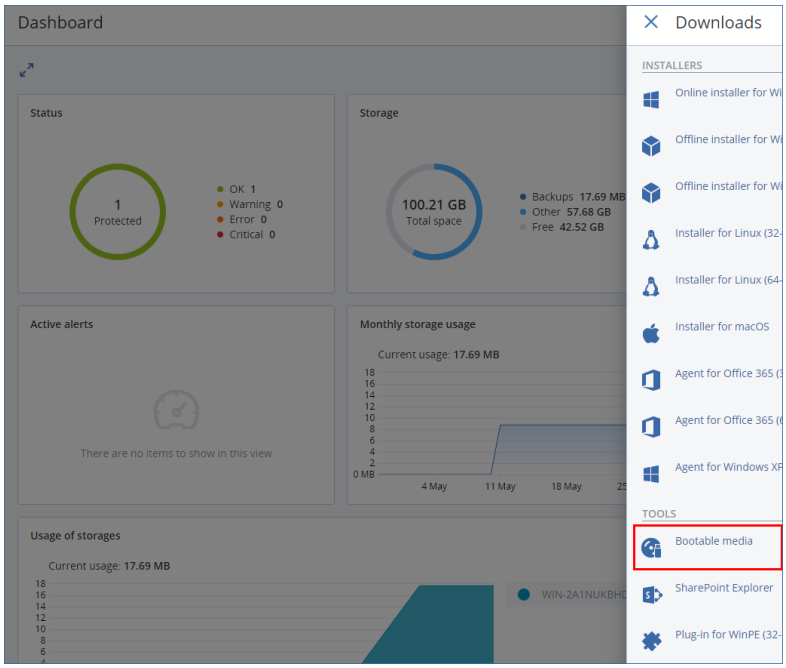
Poznámka *Spouštěcí médium nepodporuje hybridní jednotky.*

Můžete si také stáhnout připravené spouštěcí médium (pouze založené na Linuxu). Můžete si stáhnout spouštěcí médium pouze pro operace obnovy a přístup k Acronis Universal Restore. Pomocí média nemůžete zálohovat data, ověřovat nebo exportovat zálohy, spravovat disky ani používat skripty. Stažené spouštěcí médium není vhodné pro počítače se systémem macOS.

Poznámka *Připravené spouštěcí médium nepodporuje uzel úložišť, umístění pásek a umístění SFTP. Pokud chcete použít umístění úložiště v místním nasazení, musíte vytvořit vlastní spouštěcí médium pomocí nástroje Tvůrce spouštěcích médií. Viz https://kb.acronis.com/content/61566 https://kb.acronis.com/content/61566.*

Stažení připraveného spouštěcího média

1. Ve webové konzoli Cyber Protect klikněte na ikonu účtu v pravém horním rohu stránky a klikněte na položku **Stažené soubory**.
2. Vyberte položku **Spouštěcí médium**.



Stažený soubor ISO můžete vypálit na CD/DVD nebo vytvořit spouštěcí jednotku USB Flash pomocí některého z nástrojů, které jsou zdarma k dispozici online. Použijte nástroj `ISO to USB` nebo RUFUS, pokud chcete spouštět počítač UEFI, nebo `Win32DiskImager` pro počítač, kde je BIOS. V Linuxu je možné použít nástroj `dd`.

Pokud je webová konzole Cyber Protect nedostupná, můžete si připravené spouštěcí médium stáhnout ze svého účtu na zákaznickém portálu Acronis.

1. Přejděte na adresu https://account.acronis.com.
2. Vyhledejte Acronis Cyber Protect a klikněte na položku **Stažené soubory**.
3. Na stránce, která se otevře, vyhledejte možnost **Další stažené soubory** a klikněte na položku **ISO spouštěcího média (pro Windows a Linux)**.

Spouštěcí média založená na Linuxu nebo WinPE?

Pro systém Linux

Spouštěcí médium založené na Linuxu (str. 232) obsahuje spouštěcího agenta aplikace Acronis Cyber Protect založeného na linuxovém jádru. Tohoto agenta lze spustit a provádět operace na hardwaru kompatibilním s PC, včetně zcela nových počítačů a počítačů s poškozeným nebo nepodporovaným systémem souborů. Operace lze s využitím webové konzole Cyber Protect nakonfigurovat a ovládat místně nebo vzdáleně.

Seznam hardwaru podporovaného médii založenými na Linuxu je k dispozici v následujícím článku: http://kb.acronis.com/content/55310.

Založeno na WinPE

Spouštěcí médium založené na WinPE (p. 247) obsahuje minimální systém Windows nazývaný WinPE (Windows Preinstallation Environment) s doplňkem Acronis pro WinPE, který je modifikací agenta aplikace Acronis Cyber Protect a který může být spuštěn v předinstalačním prostředí.

V rozsáhlých prostředích s různým hardwarem se WinPE ukázalo jako nejpohodlnější spouštěcí řešení.

Výhody:

- Aplikace Acronis Cyber Protect nabízí v prostředí Windows Preinstallation Environment více funkcí než při použití linuxového spouštěcího média. Po spuštění PC-kompatibilního hardwaru do WinPE můžete používat nejen agenta aplikace Acronis Cyber Protect, ale také příkazy a skripty PE a další doplňky, které přidáte do PE.
- Spouštěcí médium založené na prostředí PE vám pomůže vyřešit určité problémy, které se vyskytují u spouštěcích médií založených na systému Linux, například podporu určitých řadičů RAID nebo jen určitých úrovní polí RAID. Média založená na WinPE 2.x nebo novější verzi umožňují dynamické načtení potřebných ovladačů zařízení.

Omezení:

- Spouštěcí média založená na verzích WinPE starších než 4.0 nelze použít ke spuštění v počítačích, které používají rozhraní UEFI (Unified Extensible Firmware Interface).
- Pokud je počítač spuštěn ze zaváděcího média založeného na systému PE, nemůžete jako cílové umístění záloh vybrat optická média, jako jsou disky CD, DVD nebo Blu-ray (BD).

11.1 Tvůrce spouštěcích médií

Tvůrce spouštěcích médií je specializovaný nástroj na vytváření spouštěcích médií. K dispozici pouze pro místní nasazení.

Tvůrce spouštěcích médií se instaluje automaticky při instalaci serveru pro správu. Tvůrce médií můžete nainstalovat samostatně na libovolný počítač se systémem Windows nebo Linux. Podporované operační systémy jsou stejné jako pro odpovídající agenty.

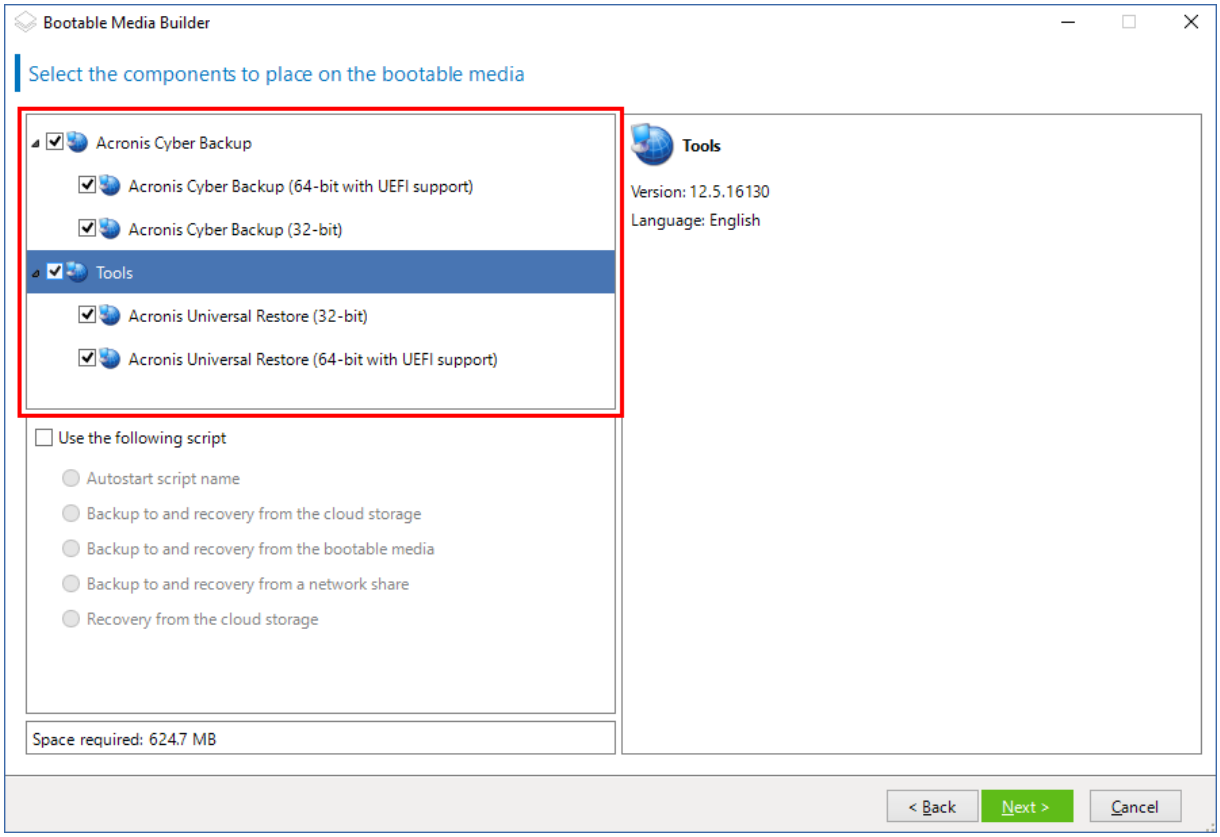
Proč používat tvůrce médií?

Připravené spouštěcí médium, které je dostupné ke stažení ve webové konzoli Cyber Protect, lze používat pouze k obnovování. Toto médium je založeno na jádru Linux. Na rozdíl od prostředí Windows PE neumožňuje vkládání vlastních ovladačů za chodu.

- Tvůrce médií umožňuje vytvoření přizpůsobeného spouštěcího média založeného na Linuxu (str. 232) nebo založeného na WinPE (p. 247) s podporou funkce zálohování.
- Kromě toho, že můžete vytvořit fyzické spouštěcí médium, můžete toto médium také nahrát do služby WDS (Windows Deployment Services) a používat spouštění ze sítě.
- Připravené spouštěcí médium nepodporuje uzel úložišť, umístění pásek a umístění SFTP. Pokud chcete použít umístění úložiště v místním nasazení, musíte vytvořit vlastní spouštěcí médium pomocí nástroje Tvůrce spouštěcích médií. Viz https://kb.acronis.com/content/61566 https://kb.acronis.com/content/61566.

32 nebo 64bitová verze?

Tvůrce spouštěcích médií vytváří média s 32bitovými i 64bitovými součástmi. Ve většině případů je ke spuštění počítače s rozhraním UEFI (Unified Extensible Firmware Interface) nutné použít 64bitové médium.

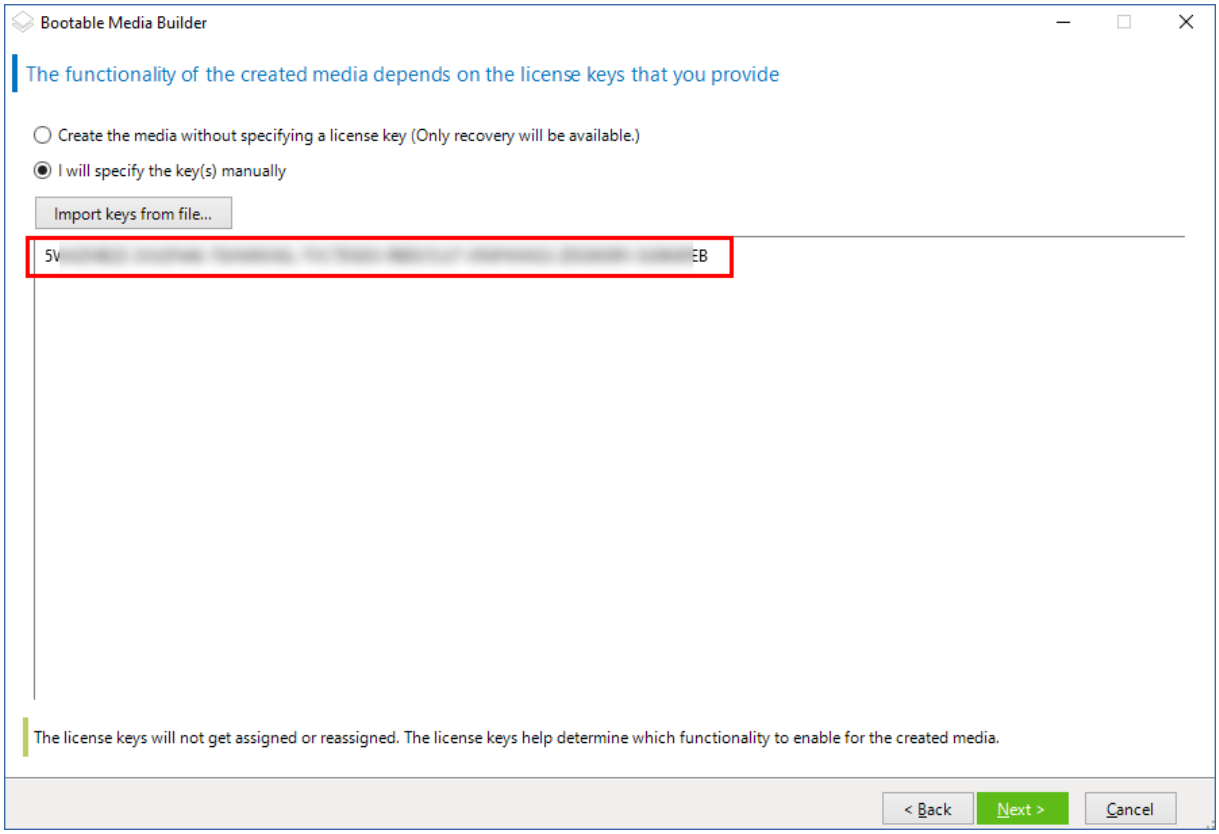


11.1.1 Spouštěcí média pro systém Linux

Vytvoření spouštěcího média pro systém Linux

1. Spusťte nástroj **Tvůrce spouštěcích médií**.
2. Chcete-li vytvořit spouštěcí médium s kompletními funkcemi, zadejte licenční klíč Acronis Cyber Protect. Tento klíč se používá k určení funkcí, které budou zahrnuty do spouštěcího média. Z počítačů nebudou odvolány žádné licence.

Pokud nezadáte licenční klíč, lze výsledné spouštěcí médium použít pouze pro operace obnovení a přístup k Acronis Universal Restore.

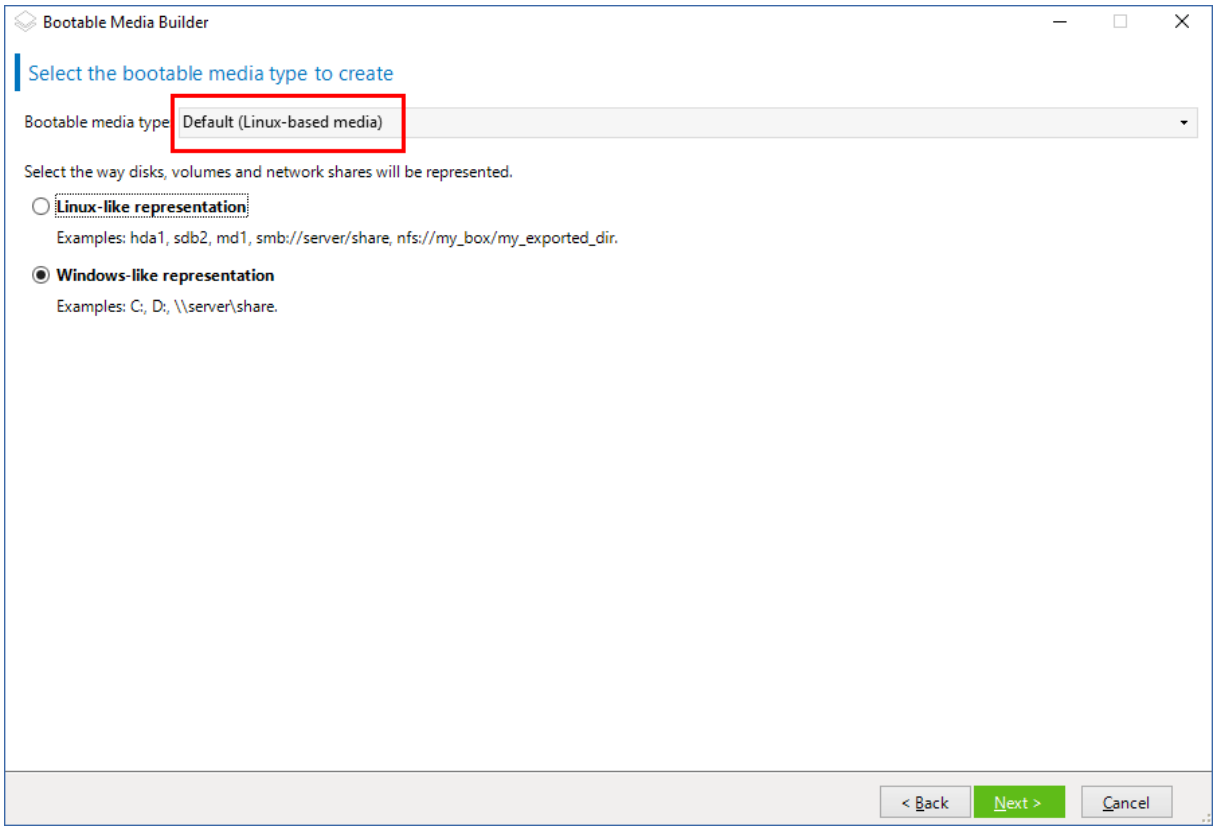


3. Vyberte možnost **Typ spouštěcího média: Výchozí (média založená na Linuxu)**.

   Vyberte, jak se zobrazí svazky a síťové prostředky:

   - Média se stylem zobrazení svazků jako v Linuxu zobrazují svazky například jako hda1 a sdb2. Toto médium se před zahájením obnovy pokusí obnovit zařízení MD a logické svazky (LVM).

- Média se stylem zobrazení svazků jako ve Windows zobrazují svazky například jako C: a D:. Toto médium poskytuje přístup k dynamickým svazkům (LDM).



4. [Volitelné] Zadejte parametry jádra systému Linux. Parametry oddělujte mezerami.

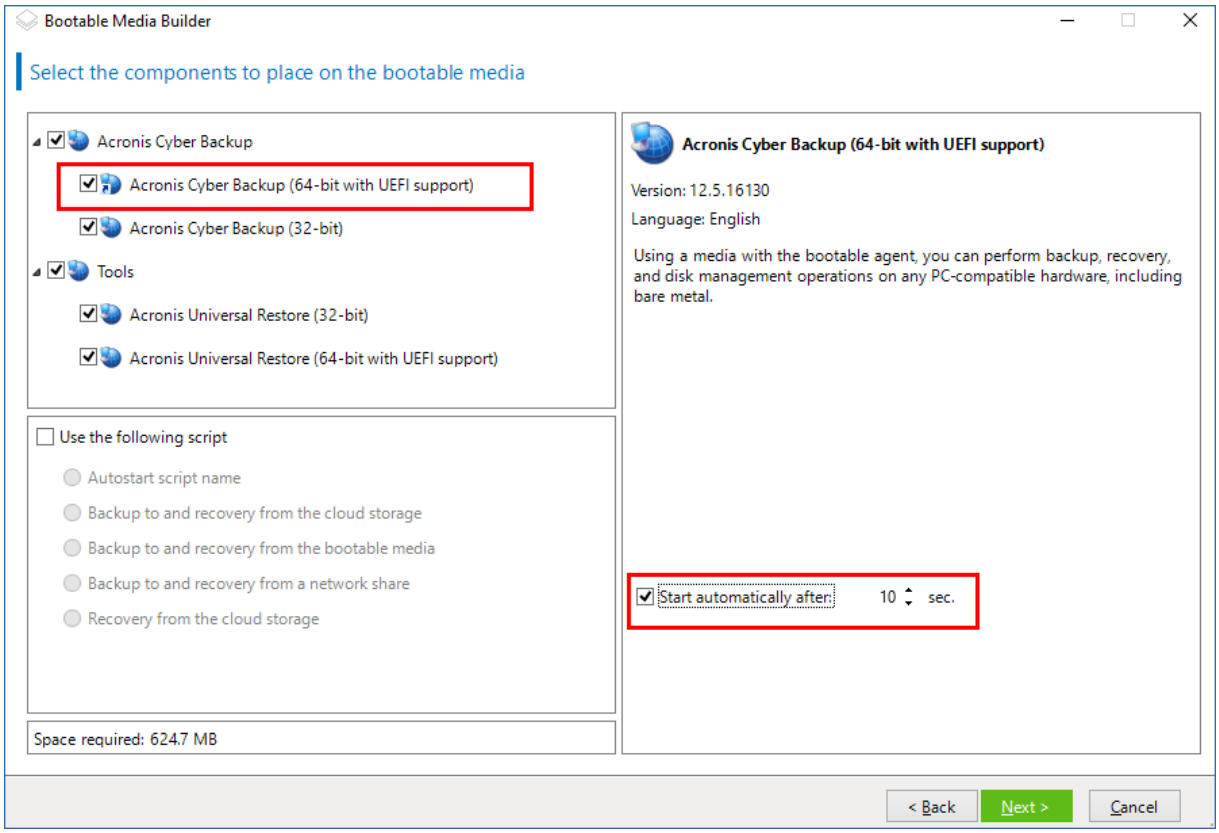
   Chcete-li mít například možnost vybrat při každém spuštění média režim zobrazení spouštěcího agenta, zadejte: **vga=ask**.

   Další informace o dostupných parametrech naleznete v tématu Parametry jádra (str. 236).
5. [Volitelné] Vyberte jazyk, který bude použit na spouštěcím médiu.
6. Vyberte součásti, které se mají umístit na médium: spouštěcí agent Acronis Cyber Protect nebo nástroj Universal Restore, pokud plánujete systém obnovit na odlišný hardware.

   Spouštěcí agent umožňuje provádět operace zálohování, obnovení a správy disků na libovolném hardwaru kompatibilním s PC včetně zcela nových počítačů.

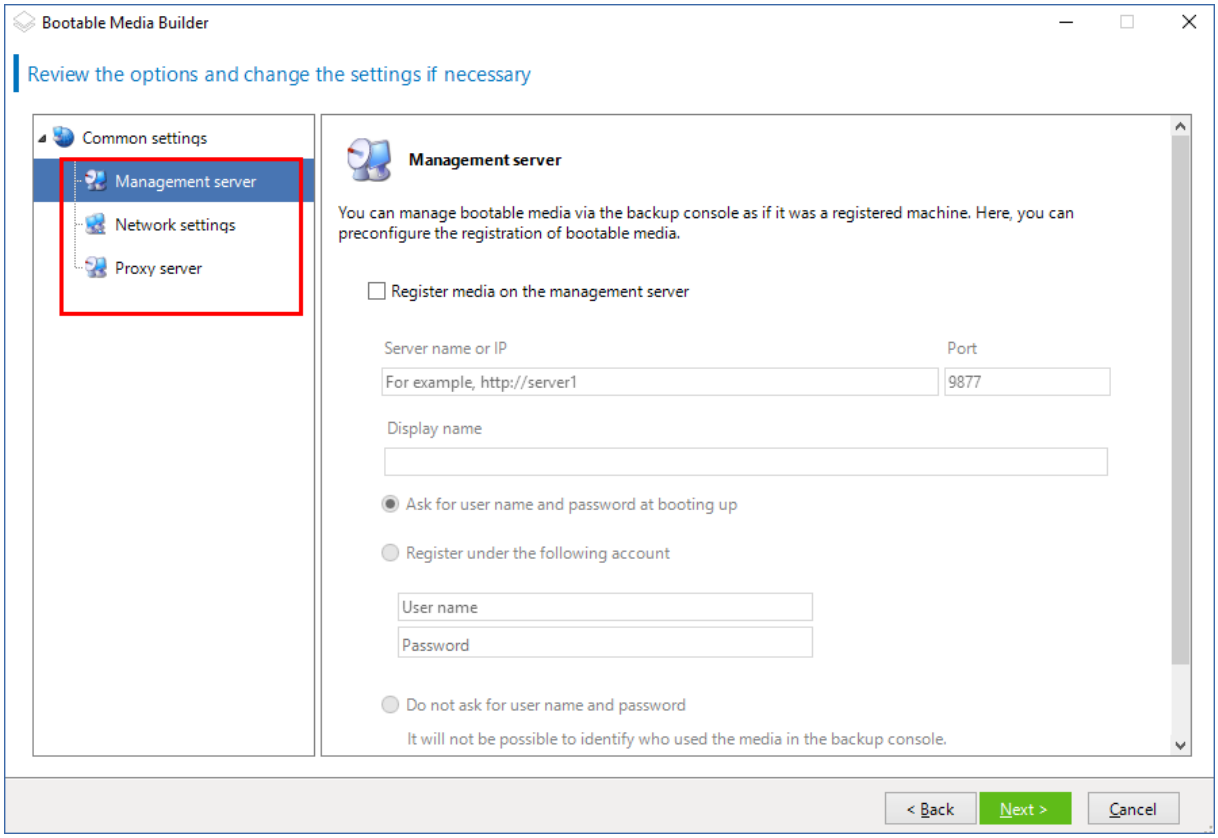
   Universal Restore (p. 204) umožňuje spuštění operačního systému obnoveného na odlišný hardware nebo do virtuálního počítače. Tento nástroj najde a nainstaluje ovladače pro zařízení, která jsou důležitá pro spuštění operačního systému, například ovladače úložiště, základní desky nebo čipové sady.

7. [Volitelné] Zadejte časový interval spouštěcí nabídky a součást, která se po uplynutí časového limitu automaticky spustí. Klikněte na požadovanou součást na panelu vlevo nahoře a nastavte pro ni interval. To umožňuje bezobslužné interní operace při spouštění z WDS/RIS.
Pokud toto nastavení není nakonfigurováno, počká zavaděč, dokud nevyberete, zda se má spustit operační systém (pokud existuje), nebo součást.



8. [Volitelné] Pokud chcete automatizovat operace spouštěcího agenta, zaškrtněte políčko **Použít následující skript**. Pak vyberte jeden ze skriptů (str. 239) a zadejte parametry skriptu.

9. [Volitelné] Vyberte, jak zaregistrovat médium na serveru pro správu při spouštění. Více informací o nastavení registrace naleznete v části Server pro správu (str. 244).



10. [Volitelné] Zadejte nastavení sítě (str. 245): Nastavení TCP/IP přiřazené síťovým adaptérům počítače.
11. [Volitelné] Zadejte síťový port (str. 246): TCP port, na kterém spouštěcí agent naslouchá pro příchozí spojení.
12. [Volitelné] Pokud máte v síti povolený proxy server, zadejte jeho název hostitele nebo IP adresu.
13. Vyberte typ média. Můžete:
    - Vytvořit obraz ISO. Obraz pak můžete vypálit na CD/DVD, použít ho k vytvoření spouštěcí jednotky USB Flash nebo ho připojit k virtuálnímu počítači.
    - Vytvořit soubor ve formátu ZIP.
    - Odeslat vybrané součástí na Server PXE Acronis.
    - Nahrát vybrané součásti na server WDS/RIS.
14. [Volitelné] Přidejte ovladače systému Windows, které budou používány nástrojem Universal Restore (str. 246). Toto okno se otevře, když je na médium přidán nástroj Universal Restore a je vybráno jiné médium než WDS/RIS.
15. Pokud se zobrazí výzva, zadejte název hostitele / IP adresu a pověření pro WDS/RIS nebo cestu k souboru ISO média.
16. V okně shrnutí zkontrolujte nastavení a poté klikněte na tlačítko **Pokračovat**.

11.1.1.1 Parametry jádra

Toto okno umožňuje určit jeden nebo více parametrů jádra Linuxu. Tyto parametry budou automaticky použity při spuštění ze spouštěcího média.

Tyto parametry se obvykle používají při problémech při práci se spouštěcím médiem. Normálně můžete toto pole nechat prázdné.

Některé z těchto parametrů můžete také zadat stisknutím klávesy F11 ve spouštěcí nabídce při spouštění počítače.

Parametry

Při zadávání více parametrů oddělte parametry mezerami.

acpi=off

Zakáže ACPI (Advanced Configuration and Power Interface). Tento parametr může být užitečný při problémech se speciální hardwarovou konfigurací.

noapic

Zakáže APIC (Advanced Programmable Interrupt Controller). Tento parametr může být užitečný při problémech se speciální hardwarovou konfigurací.

vga=ask

Výzva pro zobrazovací režim, který bude použit pro grafické uživatelské rozhraní spouštěcího média. Bez parametru **vga** se zobrazovací režim detekuje automaticky.

vga=*číslo_režimu*

Určuje zobrazovací režim, který bude použit pro grafické uživatelské rozhraní spouštěcího média. Číslo režimu je dáno parametrem *číslo_režimu* v hexadecimálním formátu – například: **vga=0x318**

Rozlišení obrazovky a počet barev odpovídající číslu režimu může být na různých počítačích odlišné. Před zvolením hodnoty parametru *číslo_režimu* se doporučuje nejdřív použít parametr **vga=ask**.

quiet

Zakáže zobrazování zpráv o spouštění při načítání jádra Linuxu a po načtení jádra spustí konzolu pro správu.

Tento parametr je implicitně zadán při vytváření spouštěcího média, tento parametr ale můžete odebrat při spuštění počítače ve spouštěcí nabídce.

Bez tohoto parametru se zobrazí všechny spouštěcí zprávy a budou následovány příkazovým řádkem. Chcete-li spustit konzolu pro správu z příkazového řádku, zadejte příkaz: **/bin/product**

nousb

Zakáže načtení podsystému USB (Universal Serial Bus).

nousb2

Vypne podporu USB 2.0. Zařízení standardu USB 1.1 při použití tohoto parametru stále fungují. Tento parametr umožňuje používat ovladače USB v režimu USB 1.1 v případě, že v režimu USB 2.0 nefungují.

nodma

Zakáže přímý přístup do paměti (DMA) pro všechny pevné disky IDE. Zabraňuje zamrznutí jádra při použití určitého hardwaru.

nofw

Vypne podporu rozhraní FireWire (IEEE1394).

nopcmcia

Vypne detekci hardwaru PCMCIA.

nomouse

Vypne podporu myši.

název_modulu=**off**

Vypne modul, jehož název je dán parametrem *název_modulu*. Například chcete-li zakázat použití modulu SATA, zadejte: **sata_sis=off**

pci=bios

Vynutí použití PCI systému BIOS místo přímého přístupu k hardwarovému zařízení. Tento parametr můžete použít, pokud má počítač nestandardní přemostění hostitelského PCI.

pci=nobios

Vypne použití PCI systému BIOS; povoleny budou pouze metody přímého přístupu k hardwaru. Tento parametr lze použít, když selže spuštění spouštěcího média, což může být způsobeno BIOSem.

pci=biosirq

K získání tabulky směrování přerušení se použijí volání PCI systému BIOS. Tento parametr může být užitečný, pokud jádro není schopno přidělit požadavky na přerušení (IRQ) nebo nalézt sekundární sběrnice PCI.

Tato volání nemusí na některých počítačích fungovat. Může to být ale jediný způsob, jak získat tabulku směrování přerušení.

LAYOUTS=en-US, de-DE, fr-FR, ...

Určuje rozložení kláves, která je možné použít v grafickém uživatelském rozhraní spouštěcího média.

Bez tohoto parametru lze použít pouze dvě rozložení: Anglické (USA) a rozložení odpovídající jazyku vybranému ve spouštěcí nabídce média.

Můžete zadat některé z následujících rozložení:

belgické: **be-BE**

české: **cz-CZ**

anglické: **en-GB**

anglické (USA): **en-US**

francouzské: **fr-FR**

francouzské (Švýcarsko): **fr-CH**

německé: **de-DE**

německé (Švýcarsko): **de-CH**

italské: **it-IT**

polské: **pl-PL**

portugalské: **pt-PT**

portugalské (Brazílie): **pt-BR**

ruské: **ru-RU**

srbské (cyrilice): **sr-CR**

srbské (latinka): **sr-LT**

španělské: **es-ES**

Při práci v rámci spouštěcího média můžete procházet dostupnými rozloženími pomocí CTRL + SHIFT.

11.1.1.2 Skripty ve spouštěcích médiích

Chcete-li, aby spouštěcí médium provedlo určenou sadu operací, můžete při vytváření média v Tvůrci spouštěcích médií zadat skript. Tento skript se spustí při každém spuštění média namísto zobrazí uživatelského rozhraní.

Můžete si vybrat některý z předem definovaných skriptů nebo si vytvořit vlastní při dodržení skriptovacích konvencí.

Předdefinované skripty

Tvůrce spouštěcích médií nabízí následující předdefinované skripty:

- Zálohování a obnova pomocí cloudového úložiště (**entire_pc_cloud**)
- Zálohování a obnova pomocí spouštěcího média (**entire_pc_local**)
- Zálohování a obnova pomocí sdíleného síťového umístění (**entire_pc_share**)
- Obnova z cloudového úložiště (**golden_image**)

Skripty se nacházejí na počítači, na kterém je nainstalován Tvůrce spouštěcích médií, v následujících adresářích:

- Ve Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- V Linuxu: **/var/lib/Acronis/MediaBuilder/scripts/**

Zálohování a obnova pomocí cloudového úložiště

Tento skript provádí zálohování počítače do cloudového úložiště nebo obnovu počítače z jeho poslední zálohy, kterou tento skript vytvořil v cloudovém úložišti. Skript po svém spuštění vyzve uživatele k výběru mezi zálohováním, obnovou a spuštěním uživatelského rozhraní.

V Tvůrci spouštěcích médií zadejte následující parametry skriptu:

1. Uživatelské jméno a heslo pro cloudové úložiště
2. [Volitelné] Heslo, které skript použije k šifrování nebo přístupu k zálohám

Zálohování a obnova pomocí spouštěcího média

Tento skript provádí zálohování počítače na spouštěcí médium nebo obnovu počítače z jeho poslední zálohy, kterou tento skript vytvořil na stejném médiu. Skript po svém spuštění vyzve uživatele k výběru mezi zálohováním, obnovením a spuštěním uživatelského rozhraní.

V Tvůrci spouštěcích médií můžete zadat heslo, které skript použije k šifrování nebo přístupu k zálohám.

Zálohování a obnova pomocí sdíleného síťového umístění

Tento skript provádí zálohování počítače do sdíleného síťového umístění nebo obnovu počítače z jeho poslední zálohy, která se nachází ve sdíleném síťovém umístění. Skript po svém spuštění vyzve uživatele k výběru mezi zálohováním, obnovou a spuštěním uživatelského rozhraní.

V programu pro tvorbu spouštěcích médií zadejte následující parametry skriptu:

1. Cesta ke sdílenému síťovému umístění
2. Uživatelské jméno a heslo pro sdílené síťové umístění

3. [Volitelné] Název záložního souboru. Výchozí hodnota je **AutoBackup**. Pokud chcete, aby skript připojoval zálohy k již existující záloze nebo aby prováděl obnovu ze zálohy s názvem, který není výchozí, změňte výchozí hodnotu na název souboru s touto zálohou.

   Zjištění názvu záložního souboru

   1. Ve webové konzoli Cyber Protect přejděte do nabídky **Úložiště záloh** > **Umístění**.
   2. Vyberte sdílenou síťovou složku (pokud sdílená složka není uvedená, klikněte na **Přidat umístění**).
   3. Vyberte zálohu.
   4. Klikněte na **Podrobnosti**. Název souboru se zobrazí v poli **Název záložního souboru**.
4. [Volitelné] Heslo, které skript použije k šifrování nebo přístupu k zálohám

Obnova z cloudového úložiště

Tento skript provádí obnovu počítače z jeho poslední zálohy, která se nachází v cloudovém úložišti. Skript po svém spuštění vyzve uživatele k zadání těchto položek:

1. Uživatelské jméno a heslo pro cloudové úložiště
2. Heslo, pokud je záloha šifrována

Doporučujeme, abyste pod tímto účtem cloudového úložiště ukládali zálohy pouze jednoho počítače. Jinak v případě, že je záloha jiného počítače novější než záloha aktuálního počítače, dojde k tomu, že skript vybere zálohu jiného počítače.

Vlastní skripty

Důležité: *Vytváření vlastních skriptů vyžaduje znalost příkazového jazyka Bash a JavaScriptového popisu objektů (JSON). Pokud jazyk Bash neznáte, můžete se jej naučit na adrese http://www.tldp.org/LDP/abs/html. Specifikace JSON je k dispozici na adrese http://www.json.org.*

Soubory skriptu

Skript se musí nacházet v následujících adresářích počítače, na kterém je nainstalován Tvůrce spouštěcích médií:

- Ve Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- V Linuxu: **/var/lib/Acronis/MediaBuilder/scripts/**

Skript se musí skládat alespoň ze tří souborů:

- **<script_file>.sh** – soubor se skriptem Bash. Během vytváření skriptu používejte pouze omezenou sadu příkazů příkazového řádku, kterou můžete najít na adrese https://busybox.net/downloads/BusyBox.html. Použít lze také následující příkazy:
  - **`acrocmd`** – nástroj příkazového řádku pro zálohování a obnovení
  - **`product`** – příkaz, který spustí uživatelské rozhraní spouštěcích médií

  Tento soubor a všechny ostatní soubory, které skript zahrnuje (například pomocí příkazu dot) musí být v podsložce **bin**. Ve skriptu zadejte cesty k ostatním souborům takto: **/ConfigurationFiles/bin/<soubor>**.
- **autostart**- soubor pro spuštění skriptu **<soubor_skriptu>.sh**. Obsah souboru musí být následující:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json**- soubor JSON obsahující následující:

- Název a popis skriptu, který se má zobrazovat ve Tvůrci spouštěcích médií.
- Názvy proměnných skriptu, které chcete nakonfigurovat pomocí Tvůrce spouštěcích médií.
- Parametry ovládacích prvků, které se budou zobrazovat v Tvůrci spouštěcích médií pro každou proměnnou.

Struktura souboru autostart.json

Objekt na nejvyšší úrovni

Pár		Vyžadováno	Popis
Název	**Typ hodnoty**		
displayName	string	Ano	Název skriptu, který se má zobrazovat ve Tvůrci spouštěcích médií.
description	string	Ne	Popis skriptu, který se má zobrazovat ve Tvůrci spouštěcích médií.
timeout	číslo	Ne	Časový limit (v sekundách) pro nabídku spuštění před spuštěním skriptu. Pokud není zadán pár, bude časový limit 10 sekund.
variables	objekt	Ne	Jakékoli proměnné **<soubor_skriptu>.sh** , které chcete nakonfigurovat přes Tvůrce spouštěcích médií. Hodnota se musí skládat z následujících párů: řetězcový identifikátor proměnné a objekt proměnné (viz tabulka níže).

Objekt proměnné

Pár		Vyžadováno	Popis
Název	**Typ hodnoty**		
displayName	string	Ano	Název proměnné použitý v názvu souboru **<soubor_skriptu>.sh**.
type	string	Ano	Typ ovládacího prvku, který se zobrazuje v Tvůrci spouštěcích médií. Tento ovládací prvek se používá ke konfiguraci hodnoty proměnné. Informace o všech podporovaných typech najdete v následující tabulce.
description	string	Ano	Popisek ovládacího prvku, který se zobrazuje nad ovládacím prvkem v Tvůrci spouštěcích médií.
default	řetězec, pokud má parametr **type** hodnotu **string**, **multiString** , **password** nebo **enum** číslo, pokud má parametr **type** hodnotu , **number**, **spinner** nebo **checkbox**	Ne	Výchozí hodnota ovládacího prvku. Pokud není zadán pár, bude výchozí hodnotou prázdný řetězec nebo nula (závisí na typu ovládacího prvku). Výchozí hodnotou zaškrtávacího políčka může být **0** (zrušené zaškrtnutí) nebo **1** (zaškrtnuté).

Pár		Vyžadováno	Popis
Název	**Typ hodnoty**		
order	číslo (nezáporné)	Ano	Pořadí ovládacího prvku v Tvůrci spouštěcích médií. Čím je hodnota vyšší, tím níže je ovládací prvek umístěn relativně k ostatním ovládacím prvkům definovaným v souboru **autostart.json**. Počáteční hodnota musí být **0**.
min (pouze pro **spinner**)	číslo	Ne	Minimální hodnota ovládacího pole číselníku. Pokud není zadán pár, bude mít hodnotu **0**.
max (pouze pro **spinner**)	číslo	Ne	Maximální hodnota ovládacího pole číselníku. Pokud není zadán pár, bude mít hodnotu **100**.
step (pouze pro **spinner**)	číslo	Ne	Hodnota step ovládacího pole číselníku. Pokud není zadán pár, bude mít hodnotu **1**.
items (pouze pro **enum**)	pole řetězců	Ano	Hodnoty v rozevíracím seznamu.
required (pro **string**, **multiString**, **password** a **enum**)	číslo	Ne	Určuje, jestli hodnota ovládacího prvku může být prázdná (**0**) nebo ne (**1**). Pokud není zadán pár, může být hodnota ovládacího prvku prázdná.

Typ ovládacího prvku

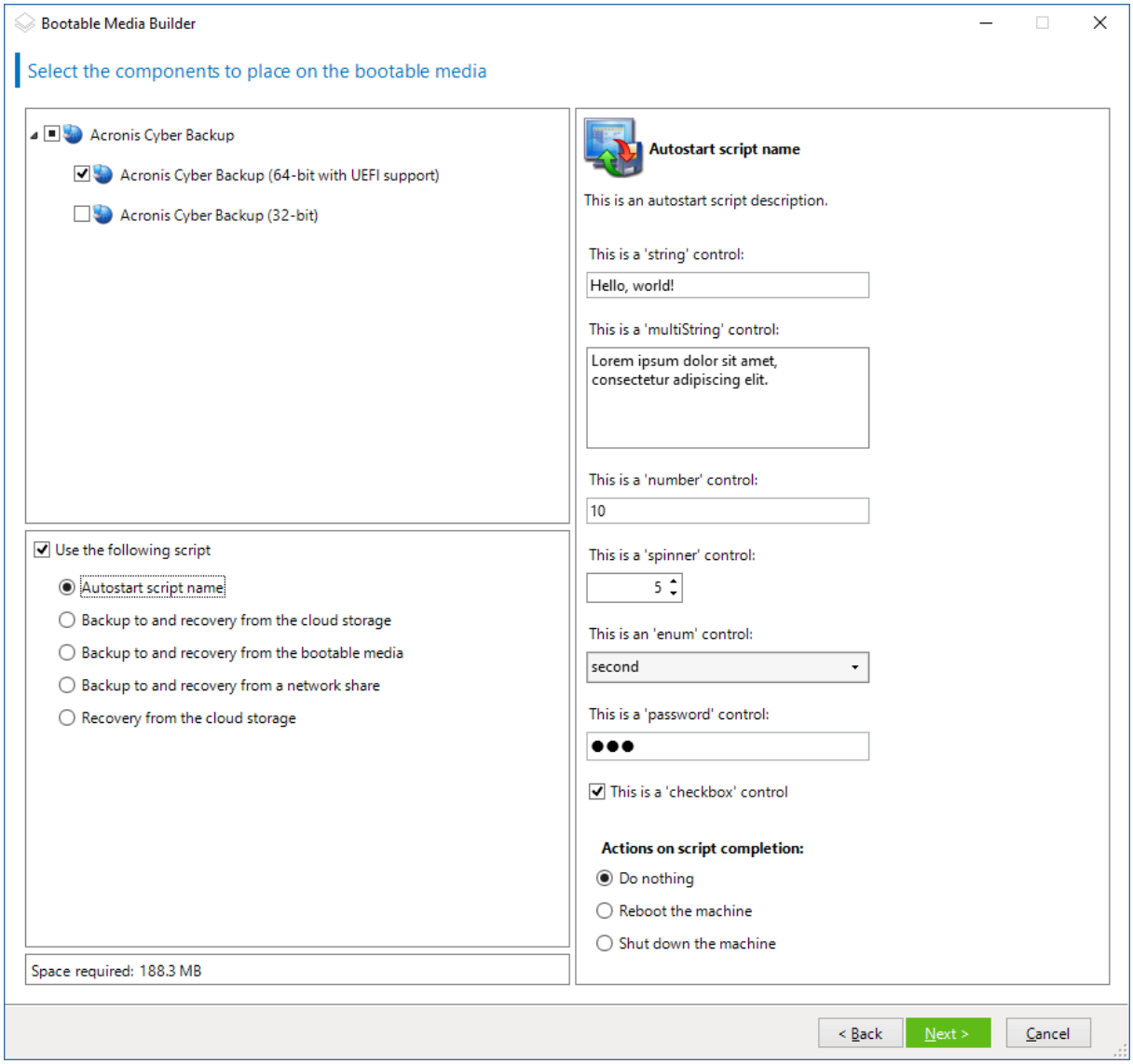
Název	Popis
string	Jednořádkové textové pole bez omezení sloužící k zadání nebo úpravě krátkých řetězců.
multiString	Víceřádkové textové pole bez omezení sloužící k zadání nebo úpravě dlouhých řetězců.
password	Jednořádkové textové pole bez omezení sloužící k bezpečnému zadání hesel.
number	Jednořádkové textové pole, do kterého lze zadat pouze číselné hodnoty, sloužící k zadání nebo úpravě čísel.
spinner	Jednořádkové textové pole s číselníkem, do kterého lze zadat pouze číselné hodnoty, sloužící k zadání nebo úpravě čísel. Používá se pro něj také označení číselník.
enum	Standardní rozevírací seznam s pevně danou sadou předem určených hodnot.
checkbox	Zaškrtávací políčko se dvěma stavy – zaškrtnuté nebo nezaškrtnuté.

Ukázkový soubor **autostart.json** uvedený níže obsahuje všechny platné typy ovládacích prvků, které je možné použít k nakonfigurování proměnných pro soubor **<soubor_skriptu>.sh**.

```
{
   "displayName": "Autostart script name",
   "description": "This is an autostart script description.",
   "variables": {
      "var_string": {
         "displayName": "VAR_STRING",
         "type": "string", "order": 1,
         "description": "This is a 'string' control:", "default": "Hello,
         world!"
      },
```

```
      "var_multistring": {
         "displayName": "VAR_MULTISTRING",
         "type": "multiString", "order": 2,
         "description": "This is a 'multiString' control:",
         "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
      },
      "var_number": {
         "displayName": "VAR_NUMBER",
         "type": "number", "order": 3,
         "description": "This is a 'number' control:", "default": 10
      },
      "var_spinner": {
         "displayName": "VAR_SPINNER",
         "type": "spinner", "order": 4,
         "description": "This is a 'spinner' control:",
         "min": 1, "max": 10, "step": 1, "default": 5
      },
      "var_enum": {
         "displayName": "VAR_ENUM",
         "type": "enum", "order": 5,
         "description": "This is an 'enum' control:",
         "items": ["first", "second", "third"], "default": "second"
      },
      "var_password": {
         "displayName": "VAR_PASSWORD",
         "type": "password", "order": 6,
         "description": "This is a 'password' control:", "default": "qwe"
      },
      "var_checkbox": {
         "displayName": "VAR_CHECKBOX",
         "type": "checkbox", "order": 7,
         "description": "This is a 'checkbox' control", "default": 1
      }
   }
}
```

Takto to vypadá v Tvůrci spouštěcích médií.



11.1.1.3 Server pro správu

Při vytváření spouštěcího média máte možnost předem nakonfigurovat registraci média na serveru pro správu.

Registrace média vám umožní spravovat dané médium prostřednictvím webové konzole Cyber Protect, jako kdyby se jednalo o registrovaný počítač. Kromě pohodlí vzdáleného přístupu to správci umožní sledovat všechny operace prováděné pod spouštěcím médiem. Operace se zapisují do **Aktivit**, takže je možné zjistit, kdo a kdy operaci spustil.

Pokud registrace není předem nakonfigurovaná, je stále možné médium zaregistrovat po spuštění počítače z média (str. 253).

Pokud chcete registraci předem nakonfigurovat na serveru pro správu:

1. Zaškrtněte políčko **Zaregistrovat médium na serveru pro správu**.
2. Do pole **Název nebo IP adresa serveru** zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován. Můžete použít jeden z následujících formátů:
   - `http://<server>`, Například `http://10.250.10.10` nebo `http://server1`

- `<IP adresa>`, například `10.250.10.10`
- `<název hostitele>`, Například `server1` nebo `server1.example.com`

3. V poli **Port** zadejte port, který bude používán pro přístup k serveru pro správu. Výchozí hodnota je 9877.
4. Do pole **Zobrazený název** zadejte název, pod kterým se má tento počítač zobrazovat ve webové konzoli Cyber Protect. Pokud toto pole necháte prázdné, nastaví se jako zobrazený název jeden z těchto názvů:
   - Pokud byl počítač už předtím zaregistrován na serveru pro správu, bude mít stejný název.
   - Jinak se použije plně kvalifikovaný název domény (FQDN) nebo IP adresa počítače.
5. Vyberte, který účet se použije pro registraci média na serveru pro správu. Dostupné jsou následující možnosti:
   - **Při spouštění požadovat uživatelské jméno a heslo**

     Pověření je nutné zadat při každém spuštění počítače z média.

     Aby byla registrace úspěšná, musí být účet v seznamu správců serveru pro správu (**Nastavení** > **Účty**). Ve webové konzoli Cyber Protect bude dané médium k dispozici na základě pověření zadaného účtu pod organizací nebo pod konkrétní jednotkou.

     V rozhraní spouštěcího média bude možné změnit uživatelské jméno a heslo kliknutím na **Nástroje** > **Zaregistrovat médium na serveru pro správu**.
   - **Registrovat pod následujícím účtem**

     Počítač se automaticky zaregistruje při každém spuštění z média.

     Zadaný účet musí být v seznamu správců serveru pro správu (**Nastavení** > **Účty**). Ve webové konzoli Cyber Protect bude dané médium k dispozici na základě pověření zadaného účtu pod organizací nebo pod konkrétní jednotkou.

     V rozhraní spouštěcího média *nebude* možné změnit registrační parametry.
   - **Nepožadovat uživatelské jméno a heslo**

     Počítač bude registrován anonymně, pokud není anonymní registrace na serveru pro správu zakázána (str. 443).

     Na kartě **Aktivity** webové konzole Cyber Protect nebude zobrazeno, kdo médium použil.

     Ve webové konzoli Cyber Protect bude dané médium k dispozici pod organizací.

     V rozhraní spouštěcího média bude možné změnit uživatelské jméno a heslo kliknutím na **Nástroje** > **Zaregistrovat médium na serveru pro správu**.

11.1.1.4 Nastavení sítě

Při tvorbě spouštěcího média máte možnost předem nakonfigurovat síťová připojení, která budou použita spouštěcím agentem. Předem nakonfigurovat lze následující parametry:

- IP adresa
- Maska podsítě
- Brána
- DNS server
- Server WINS

Jakmile se v počítači spustí spouštěcí agent, použije se konfigurace na síťovou kartu počítače. Nebyla-li nastavení předem nakonfigurována, použije agent automatickou konfiguraci DHCP. Běží-li v počítači spouštěcí agent, můžete nastavení sítě nakonfigurovat také ručně.

Předběžná konfigurace více síťových připojení

Je možné předem nakonfigurovat nastavení TCP/IP pro až deset síťových karet. Aby bylo zaručeno, že všem síťovým kartám budou přidělena příslušná nastavení, vytvořte médium na serveru, pro který je médium přizpůsobené. Když v okně průvodce vyberete existující síťovou kartu, její nastavení se uloží na médium. Na médium se také uloží adresa MAC všech existujících síťových karet.

Nastavení, vyjma adresy MAC, je možné změnit. V případě potřeby je také možné nakonfigurovat nastavení pro neexistující síťovou kartu.

Jakmile se na serveru spustí spouštěcí agent, hned načte seznam dostupných síťových karet. Tento seznam je seřazen podle slotů, ve kterých jsou síťové karty zasunuty: na prvním místě seznamu je slot nejblíže k procesoru.

Spouštěcí agent všem známým síťovým kartám přiřadí příslušné nastavení, přičemž síťové karty identifikuje podle jejich adres MAC. Po nakonfigurování síťových karet se známými adresami MAC jsou zbývajícím síťovým kartám přidělena nastavení, která jste vytvořili pro neexistující síťové karty, počínaje nepřidělenou síťovou kartou na prvním místě seznamu.

Spouštěcí médium můžete přizpůsobit pro libovolný počítač, ne jenom pro počítač, na kterém bylo vytvořeno. V takovém případě nakonfigurujte síťové karty podle pořadí jejich slotů v daném počítači: Síťová karta 1 je zasunutá ve slotu nejblíž procesoru, síťová karta 2 je ve vedlejším slotu atd. Když se na tomto počítači spustí spouštěcí agent, nenajde žádné síťové karty se známými adresami MAC a nakonfiguruje je ve stejném pořadí, jako vy.

Příklad

Spouštěcí agent by jeden ze síťových adaptérů mohl použít pro komunikaci s konzolou pro správu prostřednictvím produkční sítě. Pro toto připojení lze provést automatickou konfiguraci. Přes druhou síťovou kartu, zahrnutou prostřednictvím statického nastavení TCP/IP ve vyhrazené záložní síti, můžou být přenášeny velké objemy dat pro obnovu.

11.1.1.5 Síťový port

Při vytváření spustitelného média máte možnost předem nakonfigurovat síťový port, na kterém spouštěcí agent sleduje příchozí připojení z nástroje **acrocmd**. Můžete použít některou z těchto možností:

- výchozí port,
- právě používaný port,
- nový port (zadejte číslo portu).

Pokud port nebude předem nakonfigurován, agent použije port 9876.

11.1.1.6 Ovladače pro nástroj Universal Restore

Při vytváření zaváděcího média máte možnost přidat na médium ovladače systému Windows. Nástroj Universal Restore tyto ovladače použije ke spuštění operačního systému Windows přesunutého na odlišný hardware.

Nástroj Universal Restore budete moci nakonfigurovat tak, aby:

- na médiu vyhledal ovladače, které nejlépe vyhovují cílovému hardwaru,

- z média získal ovladače velkokapacitního paměťového zařízení, které výslovně určíte. Toto je nutné, pokud cílový hardware obsahuje specifický řadič velkokapacitního paměťového zařízení (například SCSI, RAID nebo adaptér Fiber Channel) pro pevný disk.

Tyto ovladače budou umístěny do viditelné složky Drivers na spouštěcím médiu. Tyto ovladače se nenačtou do paměti RAM cílovéhopočítače, proto musí v průběhu celé operace nástroje Universal Restore médium zůstat vloženo nebo připojeno.

Přidání ovladačů na zaváděcí médium je k dispozici, když vytváříte vyměnitelné médium nebo jeho bitovou kopii ISO či vyměnitelné médium, například flash disk. Ovladače nelze nahrát na WDS/RIS.

Ovladače mohou být přidány na seznam pouze ve skupinách, přidáním souborů INF nebo složek, které tyto soubory obsahují. Ze souborů INF nelze vybrat jednotlivé ovladače, tvůrce médií však pro informaci obsah souboru zobrazí.

Přidání ovladačů:

1. Klikněte na tlačítko **Přidat** a vyhledejte soubor INF nebo složku, která soubory INF obsahuje.
2. Vyberte soubor INF nebo složku.
3. Klikněte na tlačítko **OK**.

Ovladače lze ze seznamu odebrat pouze ve skupinách – odebráním souborů INF.

Odebrání ovladačů:

1. Vyberte soubor INF.
2. Klikněte na tlačítko **Odebrat**.

11.1.2 Spouštěcí média založená na prostředí WinPE

Tvůrce spouštěcích médií nabízí dvě metody integrace aplikace Acronis Cyber Protect s prostředím WinPE:

- Vytvoření nového souboru PE ISO s doplňkem.
- Přidání doplňku Acronis k souboru WIM pro budoucí účely (ruční sestavení ISO, přidání dalších nástrojů k obrazu atd.).

Obrazy PE založené na WinRE můžete vytvořit bez další přípravy. Popřípadě je můžete vytvořit po instalaci sad Windows Automated Installation Kit (AIK) (p. 248) nebo Windows Assessment and Deployment Kit (ADK) (p. 248).

Obrazy PE založené na WinRE

Vytvoření obrazů založených na WinRE je podporováno pro následující operační systémy:

- Windows 7 (64bitová verze)
- Windows 8, 8.1, 10 (32bitová a 64bitová verze)
- Windows Server 2012, 2016, 2019 (64bitová verze)

Obrazy PE

Po instalaci sady Windows Automated Installation Kit (AIK) nebo Windows Assessment and Deployment Kit (ADK) podporuje tvůrce spouštěcích médií distribuce WinPE, které jsou založeny na některém z následujících jader:

- Windows Vista (PE 2.0)
- Windows Vista SP1 a Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) s doplňkem nebo bez doplňku pro systém Windows 7 SP1 (PE 3.1)

- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE pro Windows 10)

Tvůrce spouštěcích médií podporuje 32bitové i 64bitové distribuce WinPE. 32bitové distribuce mohou pracovat i na 64bitovém hardwaru. Ke spuštění počítače s rozhraním UEFI (Unified Extensible Firmware Interface) je ovšem nutné použít 64bitovou distribuci.

Bitové kopie prostředí PE založené na WinPE verze 4 nebo novější vyžadují ke správné činnosti alespoň 1 GB paměti RAM.

11.1.2.1 Příprava: Prostředí WinPE 2.x a 3.x

Aby bylo možné vytvářet nebo upravovat diskový obraz PE 2.x nebo 3.x, nainstalujte Tvůrce spouštěcích médií do počítače, ve kterém je nainstalována sada AIK (Windows Automated Installation Kit). Pokud nemáte počítač se sadou AIK, připravte následující prostředí.

Jak připravit počítač se sadou AIK

1. Stáhněte a nainstalujte sadu Windows Automated Installation Kit.

   Sada Automated Installation Kit (AIK) pro Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=cs

   Sady Automated Installation Kit (AIK) pro Windows Vista SP1 a Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=cs

   Sada Automated Installation Kit (AIK) pro Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=cs

   Doplněk sady Automated Installation Kit (AIK) pro Windows 7 SP1 (PE 3.1):

   http://www.microsoft.com/cs-cz/download/details.aspx?id=5188

   Systémové požadavky na instalaci naleznete v odkazech výše.
2. [Nepovinné] Vypalte sadu WAIK na disk DVD nebo jej zkopírujte na flash disk.
3. Nainstalujte prostředí Microsoft .NET Framework z této sady (NETFXx86 nebo NETFXx64 podle hardwaru).
4. Nainstalujte Microsoft Core XML (MSXML) 5.0 nebo 6.0 Parser z této sady.
5. Z této sady nainstalujte sadu Windows AIK.
6. Nainstalujte do tohoto počítače Tvůrce spouštěcích médií.

Doporučuje se seznámit se s dokumentací dodávanou k sadě Windows AIK. Tuto dokumentaci lze zobrazit výběrem příkazů **Microsoft Windows AIK -> Documentation** v nabídce Start.

11.1.2.2 Příprava: WinPE 4.0 a novější

Aby bylo možné vytvářet nebo upravovat obrazy PE 4 nebo novější, nainstalujte Tvůrce spouštěcích medií do počítače, ve kterém je nainstalována sada ADK (Windows Assessment and Deployment Kit). Pokud nemáte počítač se sadou ADK, připravte následující prostředí.

Jak připravit počítač se sadou ADK

1. Stáhněte instalační program sady ADK.

Sada ADK (Assessment and Deployment Kit) pro Windows 8 (PE 4,0):
http://www.microsoft.com/en-us/download/details.aspx?id=30652.

Sada ADK (Assessment and Deployment Kit) pro Windows 8.1 (PE 5,0):
http://www.microsoft.com/en-US/download/details.aspx?id=39982.

Sada ADK (Assessment and Deployment Kit) pro Windows 10 (PE pro Windows 10):
https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

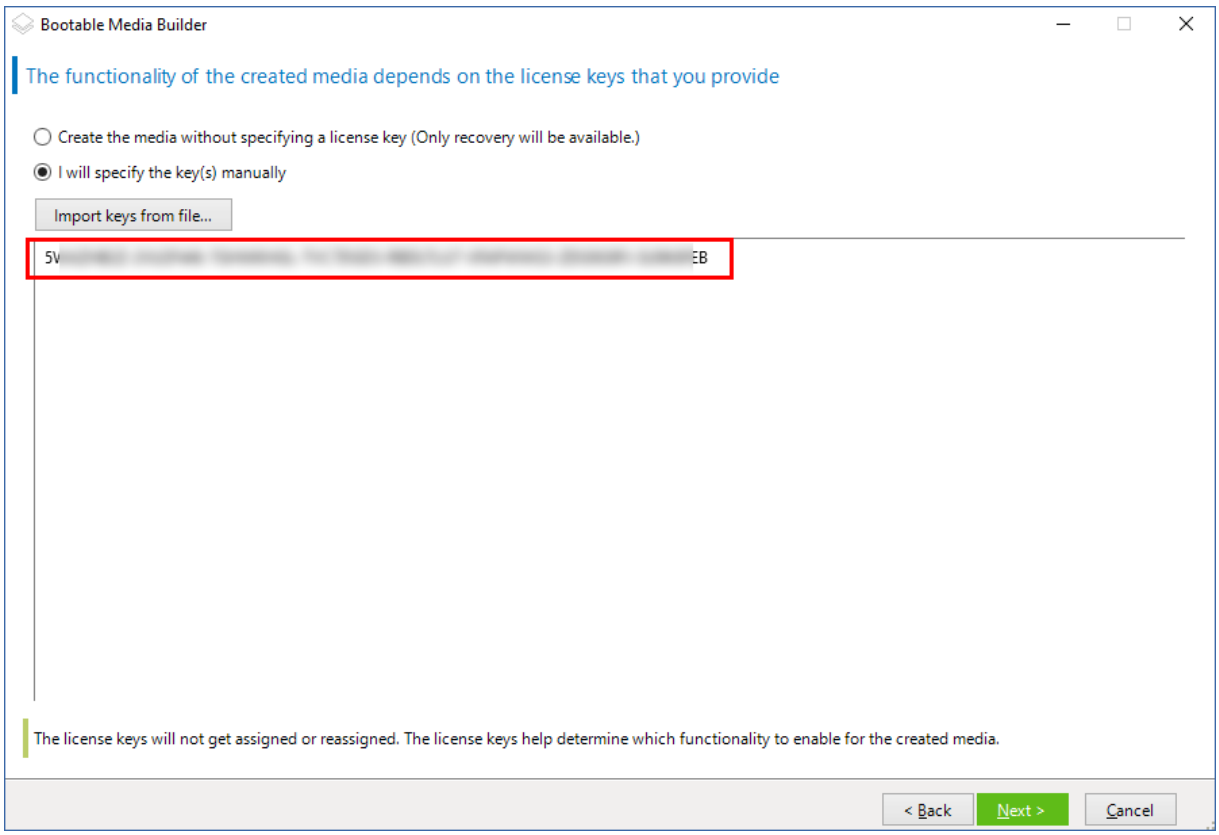
Systémové požadavky na instalaci naleznete v odkazech výše.

2. Nainstalujte do počítače sadu Assessment and Deployment Kit.
3. Nainstalujte do tohoto počítače Tvůrce spouštěcích médií.

11.1.2.3 Přidání doplňku Acronis do prostředí WinPE

Přidání doplňku Acronis do prostředí WinPE:

1. Spusťte tvůrce spouštěcích médií.
2. Chcete-li vytvořit spouštěcí médium s kompletními funkcemi, zadejte licenční klíč Acronis Cyber Protect. Tento klíč se používá k určení funkcí, které budou zahrnuty do spouštěcího média. Z počítačů nebudou odvolány žádné licence.
   Pokud nezadáte licenční klíč, lze výsledné spouštěcí médium použít pouze pro operace obnovení a přístup k Acronis Universal Restore.



3. Vyberte možnost **Typ spouštěcího média: Windows PE** nebo **Typ spouštěcího média: Windows PE (64bitová verze)**. Ke spuštění počítače s rozhraním UEFI (Unified Extensible Firmware Interface) je nutné použít 64bitové spouštěcí médium.

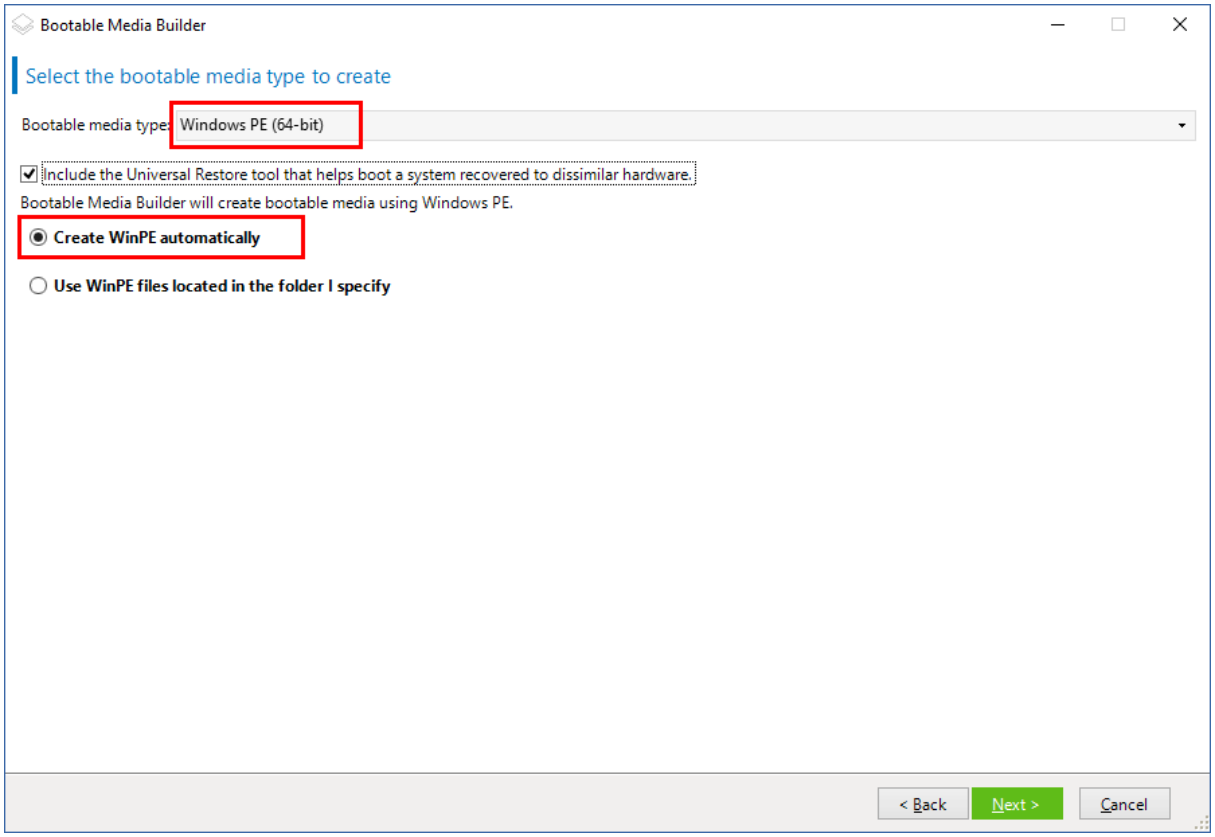
   Pokud jste vybrali možnost **Typ spouštěcího média: Windows PE**, proveďte nejdříve následující:

   - Klikněte na **Stáhnout doplněk pro WinPE (32bitová verze)**.
   - Uložte doplněk do složky **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

Pokud plánujete obnovení operačního systému na odlišný hardware nebo do virtuálního počítače a chcete zajistit spustitelnost systému, zaškrtněte políčko **Zahrnout nástroj Universal Restore**.

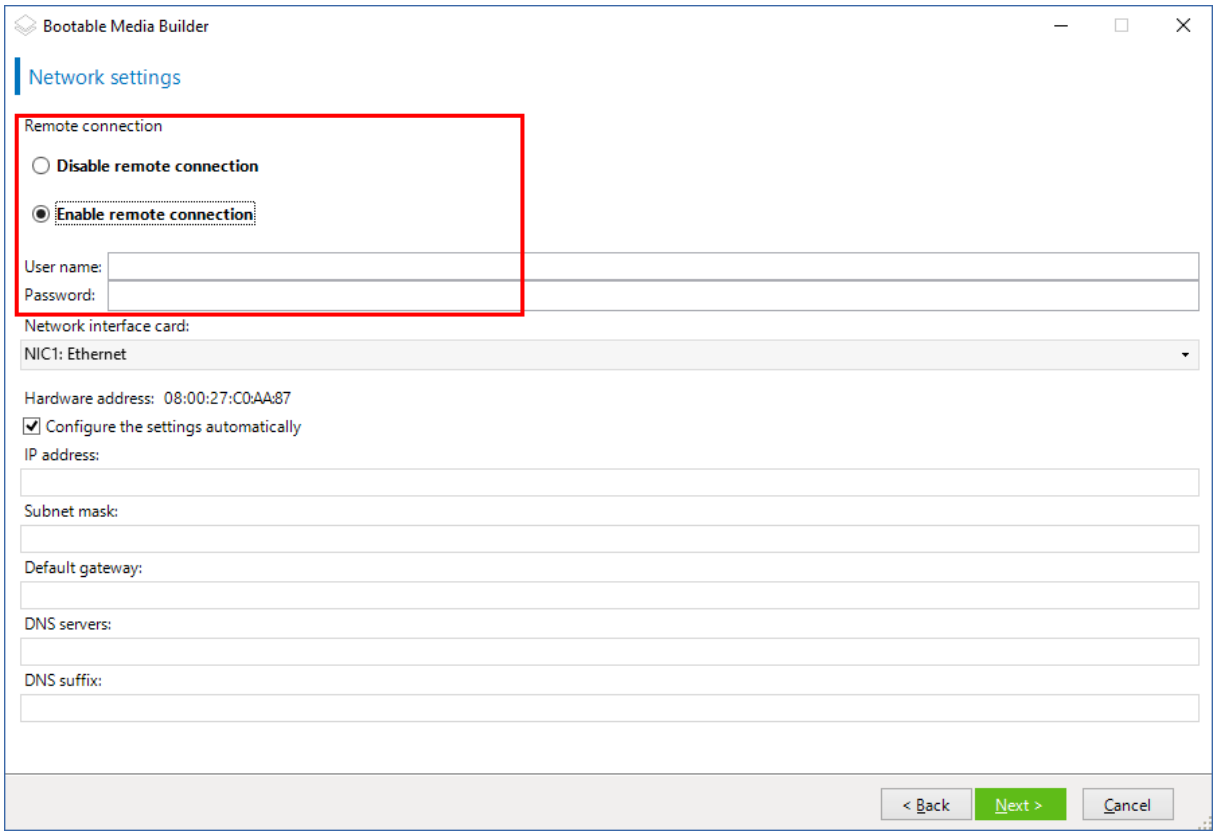
4. Vyberte **Vytvořit prostředí WinPE automaticky**.

   Software spustí příslušný skript a přepne se do dalšího okna.



5. Vyberte jazyk, který bude použit na spouštěcím médiu.
6. Vyberte, zda má být povoleno nebo zakázáno vzdálené připojení k počítači spuštěného z média. Pokud je povoleno, zadejte uživatelské jméno a heslo, které má být určeno na příkazovém řádku, když nástroj **acrocmd** běží v jiném počítači. Tato pole můžete také ponechat prázdná. Budete pak moct využít vzdálené připojení prostřednictvím rozhraní příkazového řádku bez zadání přihlašovacích údajů.

   Tyto přihlašovací údaje jsou také požadovány, když si zaregistrujete médium na serveru pro správu z webové konzole Cyber Protect (str. 253).



[Volitelné] Vyberte

7. Určete nastavení sítě (str. 245) pro síťové adaptéry v počítačích nebo vyberte automatickou konfiguraci DHCP.
8. [Volitelné] Vyberte, jak zaregistrovat médium na serveru pro správu při spouštění. Více informací o nastavení registrace naleznete v části Server pro správu (str. 244).
9. [Nepovinné] Určete ovladače systému Windows, které se mají přidat do prostředí Windows PE.

   Po spuštění počítače v prostředí Windows PE vám mohou ovladače pomoci v přístupu k zařízení, ve kterém je umístěna záloha. Přidejte 32bitové ovladače, pokud používáte 32bitovou distribuci prostředí WinPE, nebo 64bitové ovladače, pokud používáte 64bitovou distribuci prostředí WinPE.

   Přidané ovladače budete také moci využít při konfiguraci nástroje Universal Restore pro Windows. Chcete-li používat funkci Universal Restore, přidejte 32bitové nebo 64bitové ovladače podle toho, zda plánujete obnovovat 32bitový nebo 64bitový operační systém Windows.

   Přidání ovladačů:

   - Klikněte na tlačítko **Přidat** a určete cestu k potřebnému souboru .inf příslušného řadiče SCSI, RAID, SATA, síťového adaptéru, páskové jednotky nebo jiného zařízení.
   - Opakujte tento postup u všech ovladačů, které chcete přidat na výsledné médium s prostředím WinPE.
10. Vyberte, zda chcete vytvořit obraz ISO nebo WIM, nebo zda chcete médium odeslat na server (WDS nebo RIS).
11. Zadejte úplnou cestu k výslednému souboru bitové kopie včetně názvu souboru nebo určete server a zadejte uživatelské jméno a heslo pro přístup.
12. V okně shrnutí zkontrolujte nastavení a poté klikněte na tlačítko **Pokračovat**.
13. Vypalte soubor .ISO na disk CD nebo DVD pomocí nástroje od jiného výrobce nebo připravte spouštěcí flash disk.

Po spuštění počítače do prostředí WinPE se agent spustí automaticky.

Jak vytvořit obraz PE (soubor ISO) z výsledného souboru WIM:

- Nahraďte výchozí soubor boot.wim ve složce Windows PE nově vytvořeným souborem WIM. U výše uvedeného příkladu zadejte:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- Použijte nástroj **Oscdimg**. U výše uvedeného příkladu zadejte:

  ```
  oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

  Nekopírujte a nevkládejte tento příklad. Zadejte příkaz ručně, jinak selže.

Další informace o přizpůsobení Windows PE 2.x a 3.x naleznete v uživatelské příručce pro Windows Preinstallation Environment (Winpe.chm). Informace o přizpůsobování prostředí Windows PE 4.0 a novějšího jsou k dispozici v knihovně Microsoft TechNet.

11.2 Připojení k počítači spuštěnému ze spouštěcího média

Jakmile se počítač spustí ze spouštěcího média, terminál počítače zobrazí spouštěcí obrazovku s IP adresami získanými ze serveru DHCP nebo nastavenými podle přednastavených hodnot.

Konfigurace síťových nastavení

Chcete-li změnit síťová nastavení pro aktuální relaci, klikněte na položku **Konfigurovat síť** na spouštěcí obrazovce. Zobrazené okno **Nastavení sítě** umožní nakonfigurovat nastavení sítě pro každou síťovou kartu (NIC) v počítači.

Změny provedené během relace budou po restartu počítače ztraceny.

Přidání sítí VLAN

V okně **Nastavení sítě** můžete přidat virtuální místní sítě (VLAN). Tuto funkci použijte, pokud je nutné získat přístup k umístění záloh, které se vyskytují v určité síti VLAN.

Sítě VLAN se používají zejména k rozdělení místní sítě do segmentů. NIC, která je připojena k *přístupovému* portu přepínače má vždy přístup k síti VLAN určené v konfiguraci portu. NIC připojená ke *kmenovému* portu přepínače může k sítím VLAN povoleným v konfiguraci portu přistupovat pouze tehdy, určíte-li tyto sítě VLAN v síťovém nastavení.

Jak zapnout přístup k síti VLAN prostřednictvím kmenového portu

1. Klikněte na **Přidat síť VLAN**.
2. Zvolte síťovou kartu, která poskytuje přístup k místní síti obsahující požadovanou síť VLAN.
3. Určete identifikátor sítě VLAN.

Po kliknutí na tlačítko **OK** se v seznamu síťových adaptérů zobrazí nová položka.

Pokud potřebujete odebrat síť VLAN, klikněte na položku požadované sítě VLAN a poté klikněte na tlačítko **Odebrat síť VLAN**.

Místní připojení

Má-li fungovat přímo v počítači spuštěném ze spouštěcího média, klikněte na položku **Místní správa tohoto počítače** na spouštěcí obrazovce.

Vzdálené připojení

Pokud se chcete k médiu připojit vzdáleně, zaregistrujte ho na serveru pro správu, jak je popsáno v tématu Registrace média na serveru pro správu (str. 253).

11.3 Registrace média na serveru pro správu

Registrace spouštěcího média vám umožní spravovat dané médium prostřednictvím webové konzole Cyber Protect, jako kdyby se jednalo o registrovaný počítač. Týká se to všech spouštěcích médií, bez ohledu na metodu spouštění (fyzická média, Startup Recovery Manager, Acronis PXE Server, WDS nebo RIS). Nelze však registrovat spouštěcí médium, které bylo vytvořeno v systému macOS.

Registrace média je možná pouze v případě, že je na server pro správu přidaná alespoň jedna licence Advanced pro aplikaci Acronis Cyber Protect.

Médium můžete zaregistrovat v uživatelském rozhraní média.

Parametry registrace lze v Tvůrci spouštěcích médií předkonfigurovat pomocí možnosti Server pro správu (str. 244). Pokud jsou všechny parametry registrace předkonfigurované, zobrazí se médium ve webové konzoli Cyber Protect automaticky. Pokud jsou předkonfigurované některé parametry registrace, nemusí být některé kroky v následujících postupech dostupné.

Registrace média v uživatelském rozhraní média

Médium lze stáhnout nebo vytvořit pomocí Tvůrce spouštěcích médií (str. 231).

Registrace média v uživatelském rozhraní média

1. Spusťte počítač pomocí média.
2. Proveďte jeden z následujících úkonů:
   - Ve spouštěcím okně klikněte pod položkou **Server pro správu** na možnost **Upravit**.
   - V rozhraní spouštěcího média klikněte na možnost **Nástroje** > **Zaregistrovat médium na serveru pro správu**.
3. V poli **Zaregistrovat na** zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován. Můžete použít jeden z následujících formátů:
   - `http://<server>`, Příklad: **`http://10.250.10.10`** nebo **`http://server`**
   - `<IP adresa>`, Příklad: **`10.250.10.10`**
   - `<název hostitele>`, Příklad: **`server`** nebo **`server.example.com`**
4. Do polí **Uživatelské jméno** a **Heslo** zadejte pověření k účtu, který je v seznamu správců serveru pro správu (**Nastavení** > **Účty**). Ve webové konzoli Cyber Protect bude dané médium k dispozici na základě pověření zadaného účtu pod organizací nebo pod konkrétní jednotkou.
5. Do pole **Zobrazený název** zadejte název, pod kterým se má tento počítač zobrazovat ve webové konzoli Cyber Protect. Pokud toto pole necháte prázdné, nastaví se jako zobrazený název jeden z těchto názvů:
   - Pokud byl počítač už předtím zaregistrován na serveru pro správu, bude mít stejný název.
   - Jinak se použije plně kvalifikovaný název domény (FQDN) nebo IP adresa počítače.
6. Klikněte na tlačítko **OK**.

11.4 Operace se spouštěcím médiem

Operace se spouštěcím médiem jsou podobné operacím zálohování a obnovy, které jsou prováděny se spuštěným operačním systémem. Existují zde následující rozdíly:

1. U spouštěcího média ve stylu Windows má svazek stejné písmeno jednotky jako ve Windows. Svazky, které nemají ve Windows písmena jednotek (například svazek rezervovaný systémem), mají přiřazena volná písmena v pořadí jejich výskytu na disku.

   Pokud spouštěcí médium nedokáže detekovat v počítači systém Windows nebo jich detekuje více, budou všem svazkům včetně těch bez písmen, přiřazena písmena jednotek podle jejich pořadí na disku. Písmena svazků se tak mohou lišit od zobrazení ve Windows. Například disk D: v rámci spouštěcího média může odpovídat disku E: v systému Windows.

   Poznámka *Doporučujeme přiřadit svazkům jedinečné názvy.*

2. Spouštěcí médium ve stylu Linuxu ukazuje místní disky a svazky jako nepřipojené (sda1, sda2, ...).
3. Zálohy vytvořené pomocí spouštěcího média mají zjednodušené názvy souborů. Standardní názvy jsou přiřazeny k zálohám pouze v případě, že jsou tyto zálohy přidávány do existujícího archivu se standardním pojmenováním souborů nebo pokud umístění nepodporuje zjednodušené názvy souborů.
4. Spouštěcí médium ve stylu Linuxu nemůže zapisovat zálohy do svazku ve formátu NTFS. Pokud potřebujete zapisovat do systému NTFS, použijte médium ve stylu Windows. Chcete-li přepnout reprezentace svazku spouštěcího média, klikněte na položky **Nástroje** > **Změnit reprezentaci svazků**.
5. Úlohy nelze naplánovat. Pokud operaci potřebujete zopakovat, nakonfigurujte ji od začátku.
6. Životnost protokolu je omezena na aktuální relaci. Celý protokol nebo jeho filtrované záznamy můžete uložit do souboru.
7. Ve stromu složek okna **Archiv** se nezobrazují centralizovaná úložiště.

   Pro přístup k spravovanému úložišti zadejte do pole **Cesta** následující řetězec:

   bsp://adresa_uzlu/název_úložiště/

   Pro přístup k centralizovanému úložišti bez správy zadejte úplnou cestu ke složce úložiště.

   Po zadání pověření pro přístup uvidíte seznam archivů umístěných v úložišti.

Nastavení režimu zobrazení

Když spustíte počítač ze spouštěcího média založeného na systému Linux, režim zobrazení se rozpozná automaticky podle hardwarové konfigurace (specifikací monitoru a grafické karty). Pokud se režim zobrazení neurčí správně, postupujte následovně:

1. Ve spouštěcí nabídce stiskněte klávesu F11.
2. Na příkazovém řádku zadejte: **vga=ask** a pokračujte ve spouštění.
3. Chcete-li zobrazit seznam podporovaných režimů zobrazení, vyberte příslušný režim zadáním jeho čísla (například **318**) a stiskněte klávesu **Enter**.

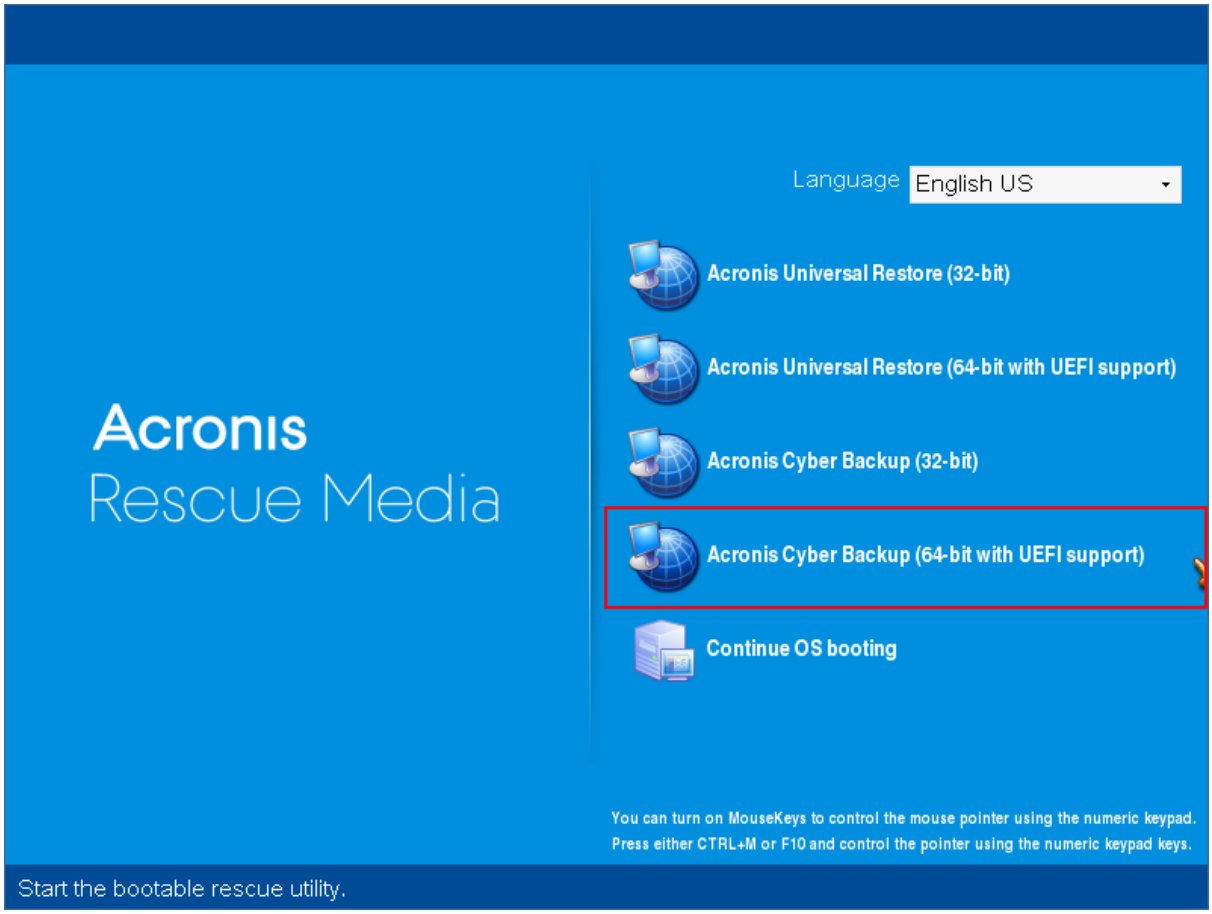
Jestliže nechcete tento postup provádět při každém spuštění dané hardwarové konfigurace, znovu vytvořte spouštěcí médium s příslušným číslem režimu (v případě výše **vga=0x318**) zadaným v okně **Parametry jádra**.

11.4.1 Zálohování

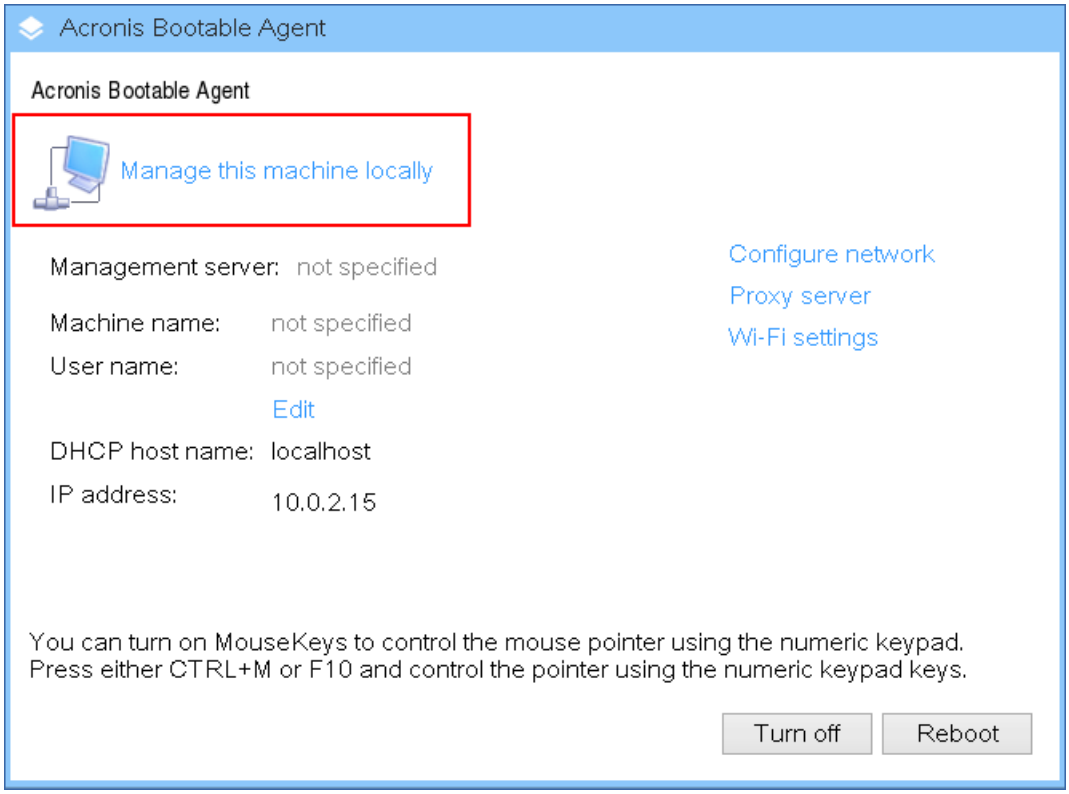
Data můžete zálohovat pouze s využitím spouštěcího média, které jste vytvořili pomocí Tvůrce spouštěcích médií a pomocí licenčního klíče k produktu Acronis Cyber Protect. Další informace o vytvoření spouštěcího média naleznete v tématu Spouštěcí média založená na systému Linux (str. 232) a Spouštěcí média založená na systému Windows-PE (p. 247).

Zálohování dat v rámci spouštěcího média

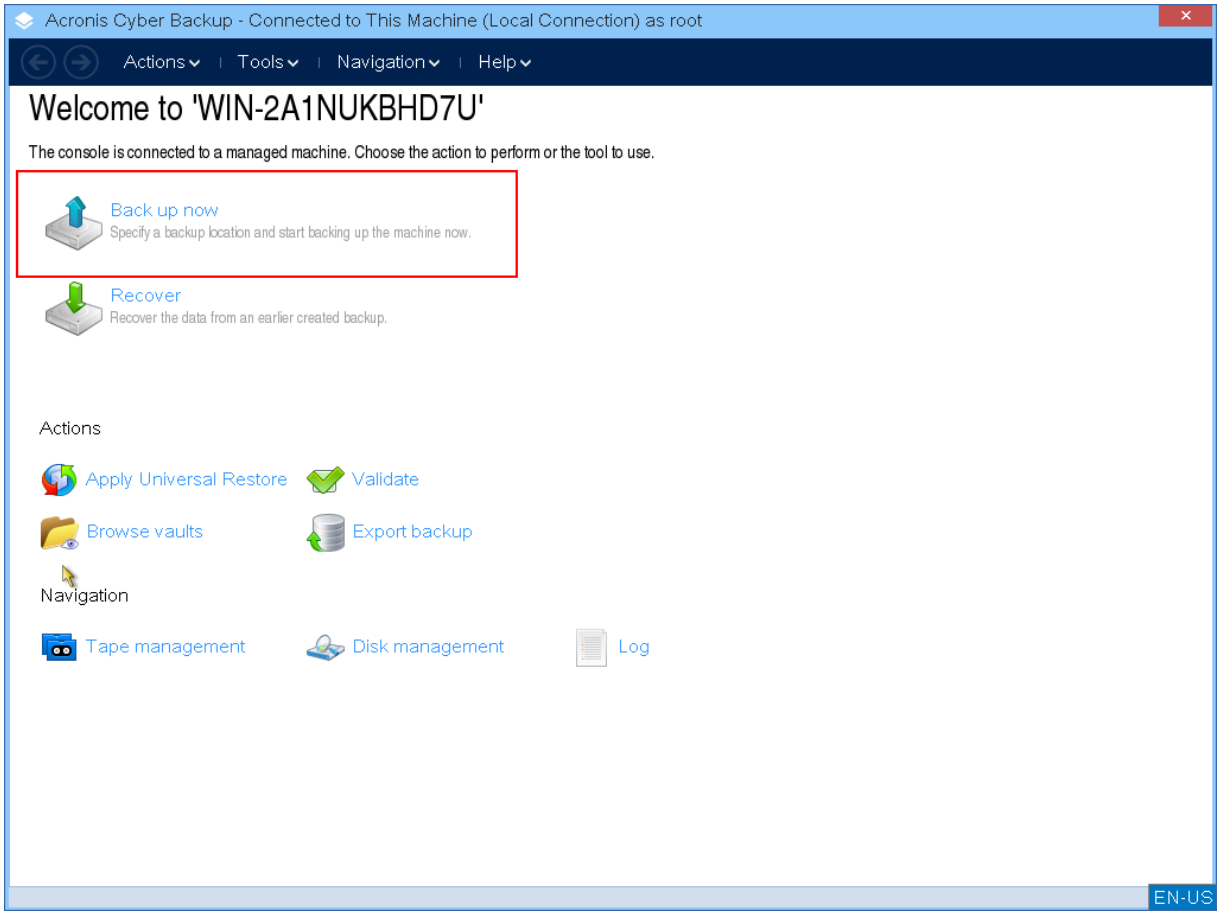
1. Proveďte spuštění ze záchranného spouštěcího média Acronis.



2. Chcete-li zálohovat místní počítač, klikněte na položku **Místní správa tohoto počítače**. V případě vzdáleného připojení si prostudujte téma Registrace média na serveru pro správu (str. 253).



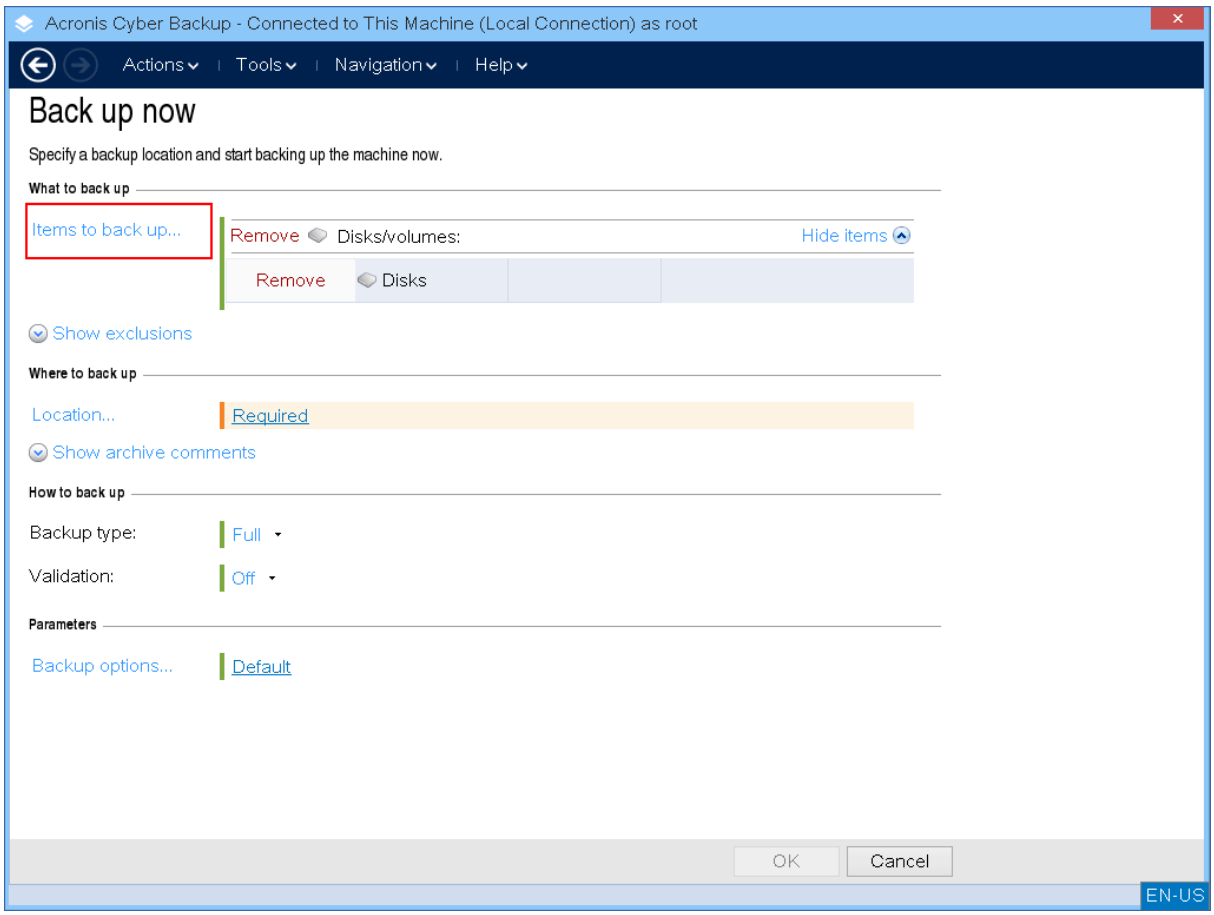
3. Klikněte na tlačítko **Zálohovat nyní**.



4. K zálohování se automaticky vyberou všechny nevyměnitelné disky počítače. Chcete-li změnit data, která se budou zálohovat, klikněte na možnost **Položky k zálohování** a vyberte požadované disky nebo svazky.

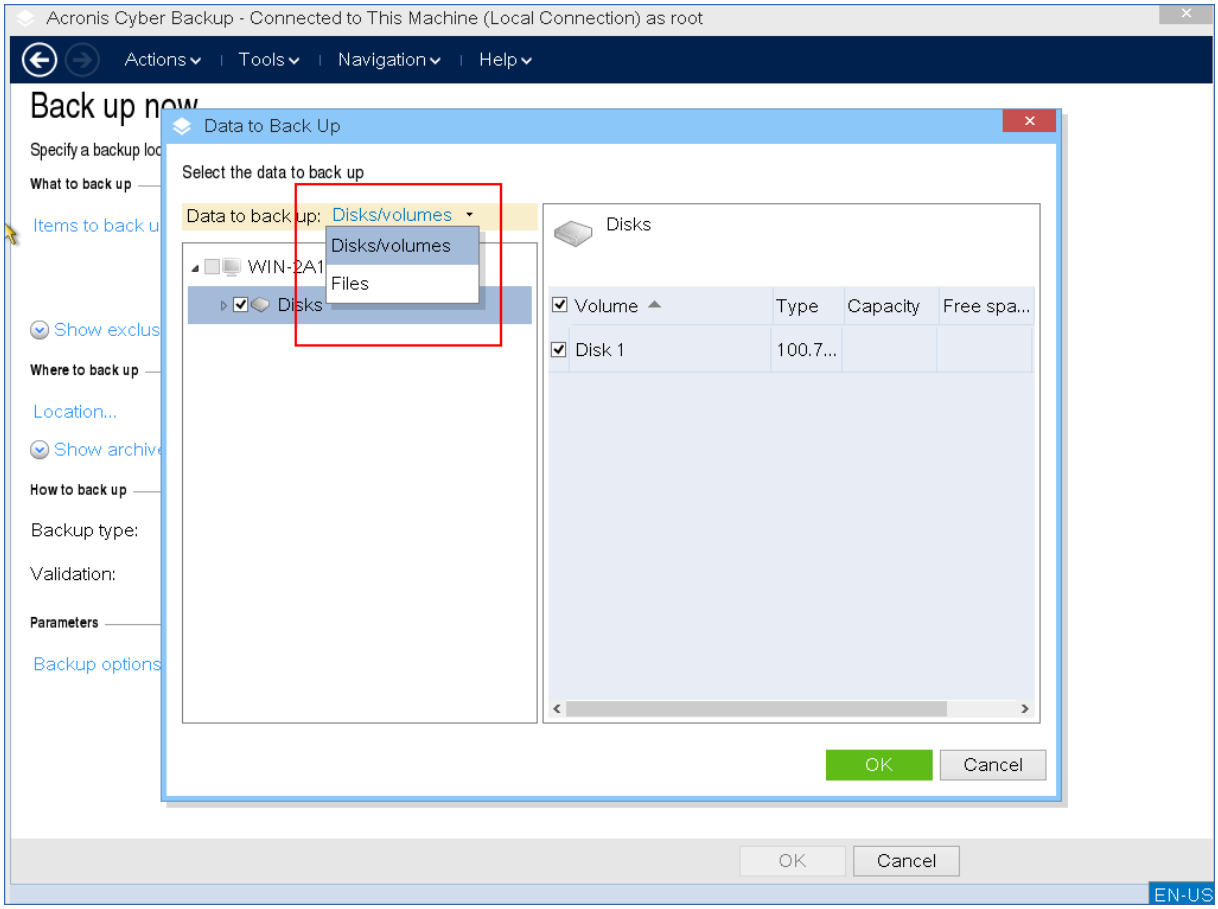
   Během vybírání dat k zálohování se může zobrazit následující zpráva: *„Tento počítač není možné vybrat přímo. Předchozí verze agenta je nainstalována v počítači. Tento počítač vyberete pro zálohování pomocí pravidel zásad.“* Jedná se o problém grafického uživatelského rozhraní, který lze bezpečně ignorovat. Pokračujte ve výběru jednotlivých disků nebo svazků, které chcete zálohovat.

Poznámka *V případě spouštěcího média založeného na systému Linux můžete vidět písmena jednotek, která se liší od písmen v systému Windows. Zkuste identifikovat požadovanou jednotku nebo oddíl podle velikosti nebo popisku.*

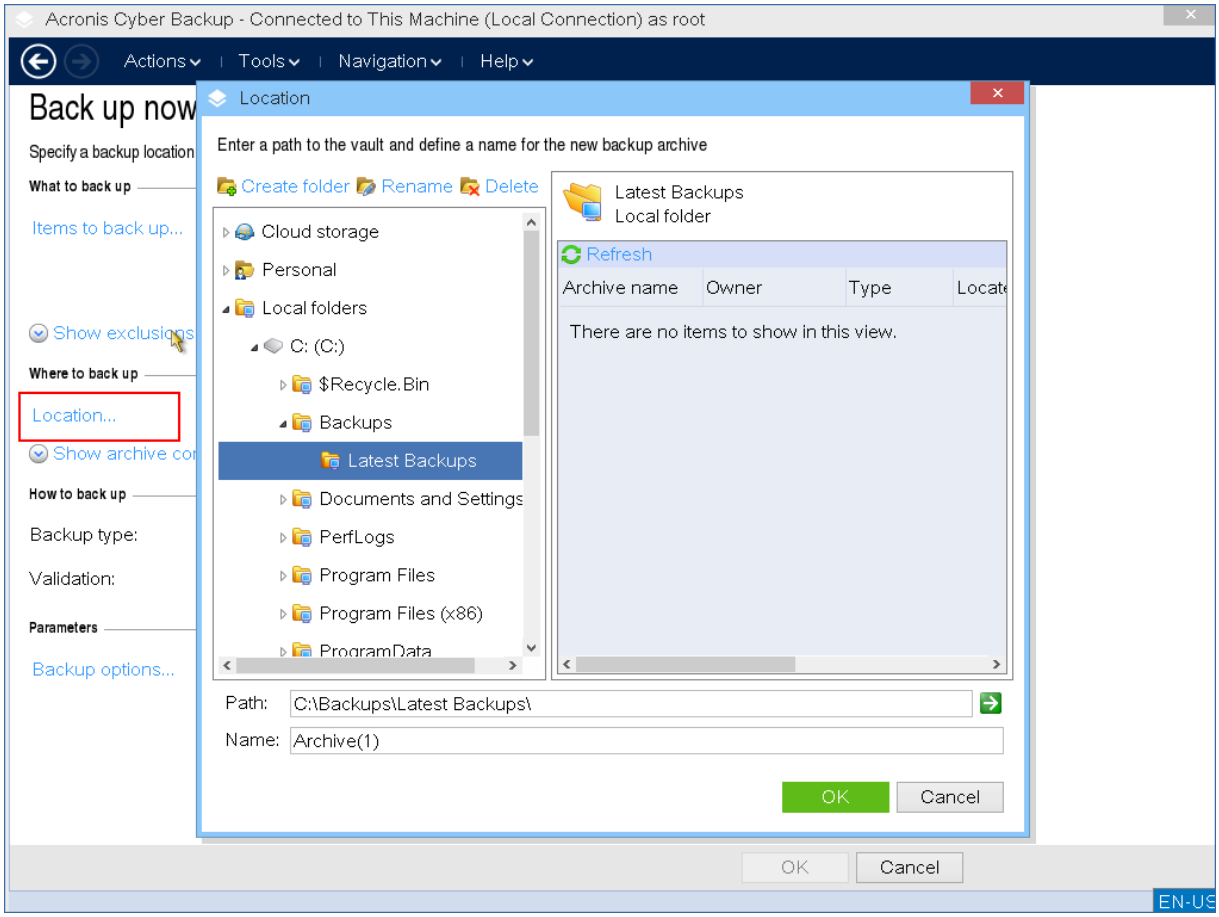


5. Pokud potřebujete zálohovat soubory nebo složky namísto disků, přepněte v části **Data pro zálohován** na možnost **Soubory**.

V rámci spouštěcího média lze provádět pouze zálohy disku/oddílu a souboru/složky. Další typy záloh, například zálohy databáze, jsou možné pouze v rámci spuštěného operačního systému.

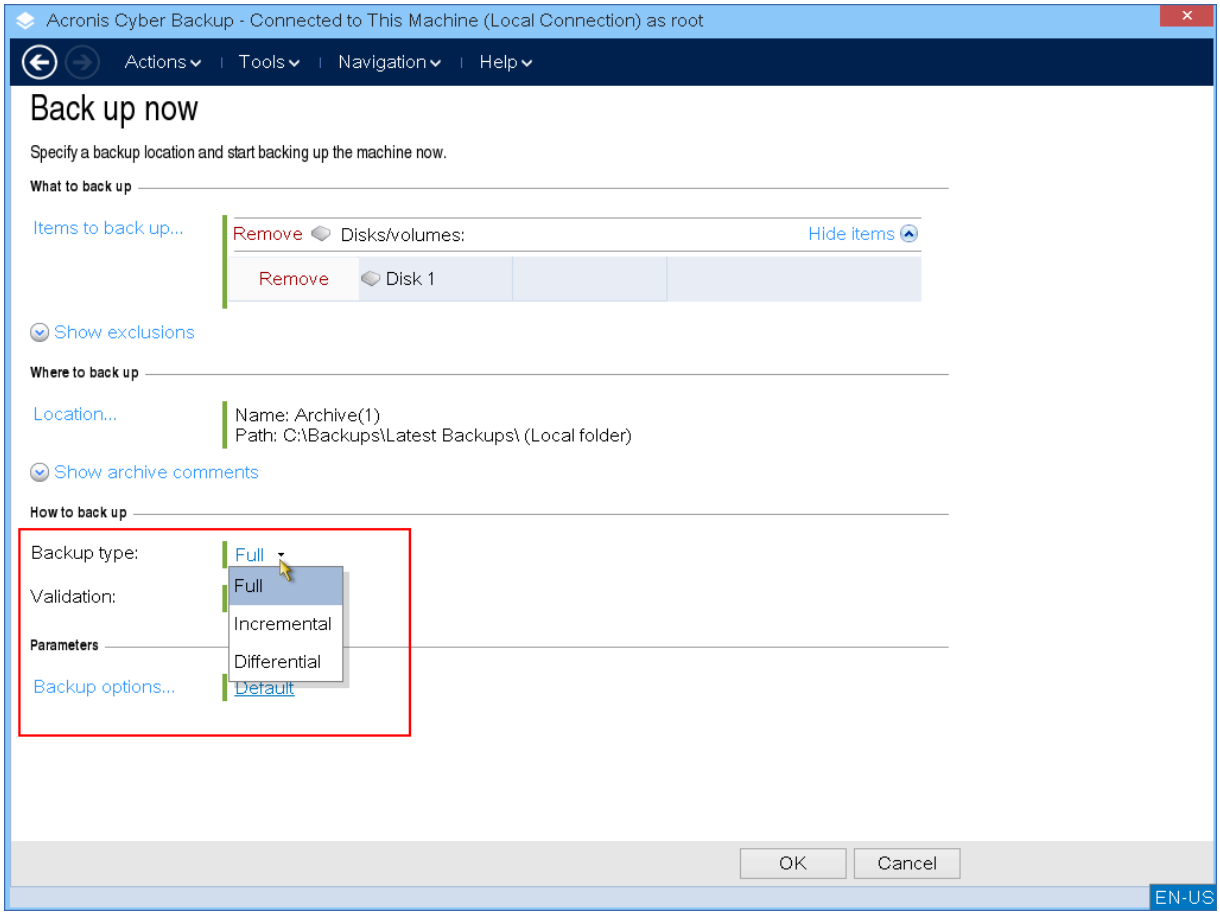


6. Klikněte na položku **Umístění** a vyberte umístění, do kterého chcete zálohu uložit.

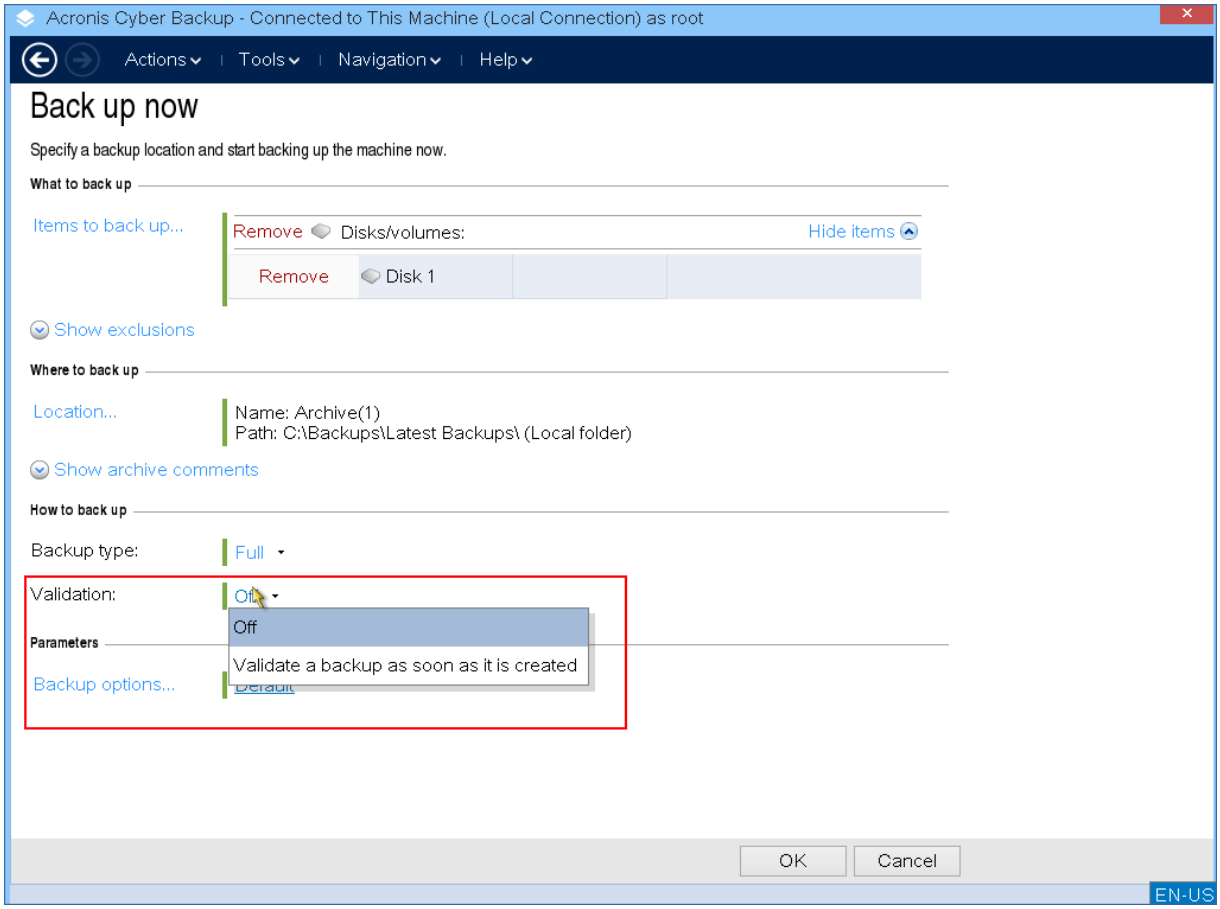


7. Zadejte umístění a název zálohy.

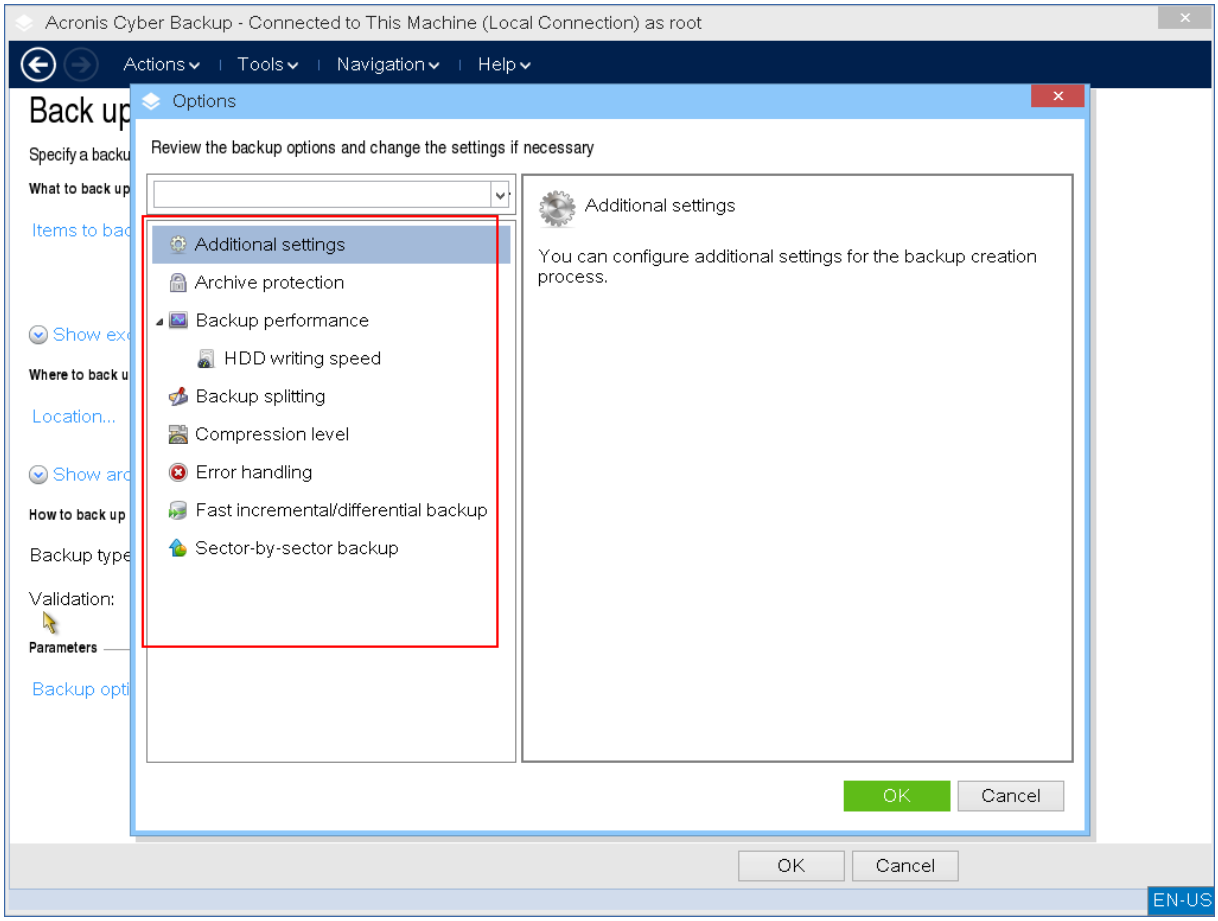
8. Zadejte typ zálohy. Pokud se jedná o první zálohu v tomto umístění, vytvoří se plná záloha. Pokud budete záloh dělat více, můžete vybrat **přírůstkovou** nebo **rozdílovou** zálohu a ušetřit místo. Další informace o typech záloh naleznete v tématu https://kb.acronis.com/content/1536 (https://kb.acronis.com/content/1536 - https://kb.acronis.com/content/1536).



9. [Volitelné] Pokud chcete ověřit soubor zálohy, vyberte možnost **Ověřit zálohu ihned po vytvoření**.



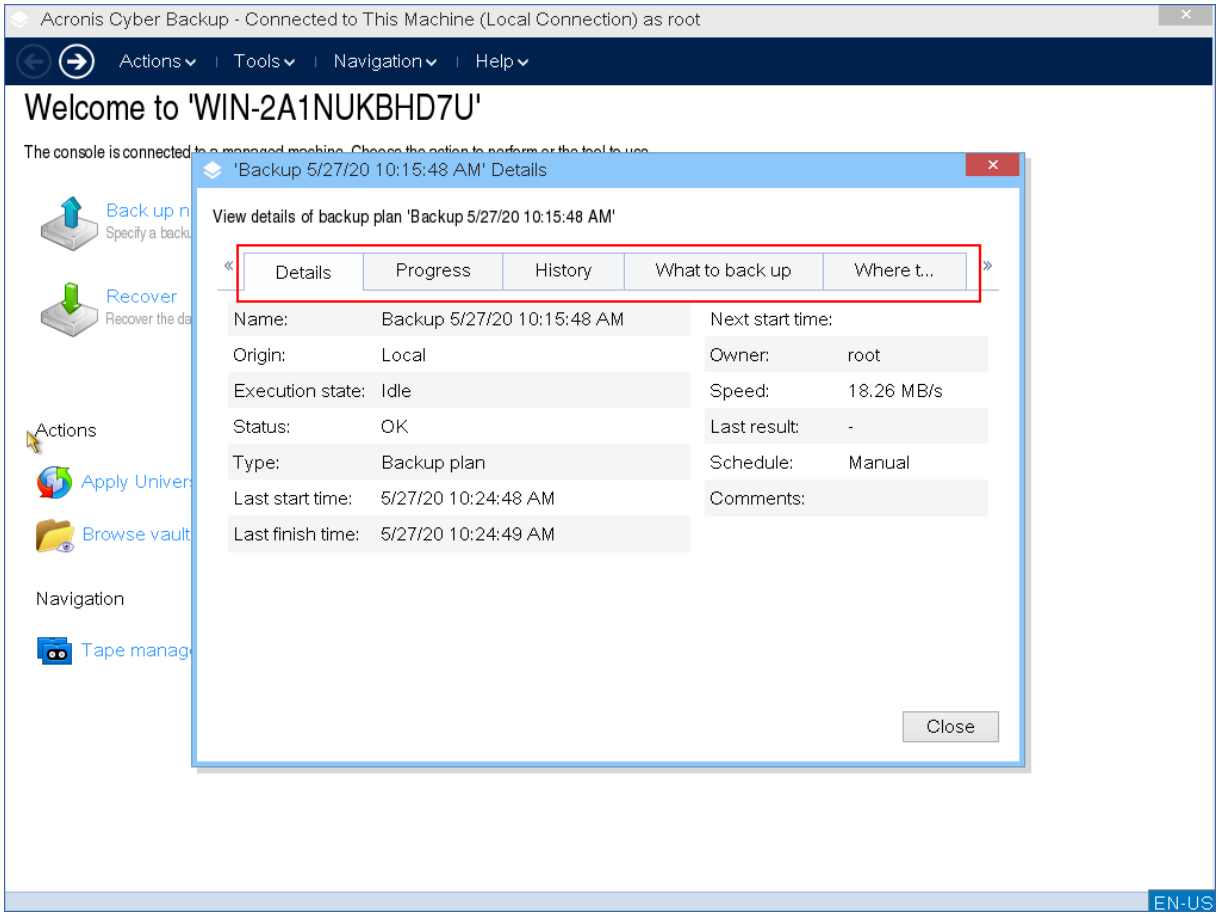
10. [Volitelné] Určete možnosti zálohování, které můžete potřebovat – například heslo pro soubor zálohy, rozdělení zálohy nebo řešení chyb.



11. Kliknutím na tlačítko **OK** spusťte zálohování.

    Spouštěcí médium přečte data z disku, komprimuje je do souboru .tib a tento soubor zapíše do vybraného umístění. Nevytvoří snímek disku, protože nejsou spuštěny žádné aplikace.

12. V okně, které se zobrazí, můžete zkontrolovat stav úlohy zálohování a další informace o záloze.

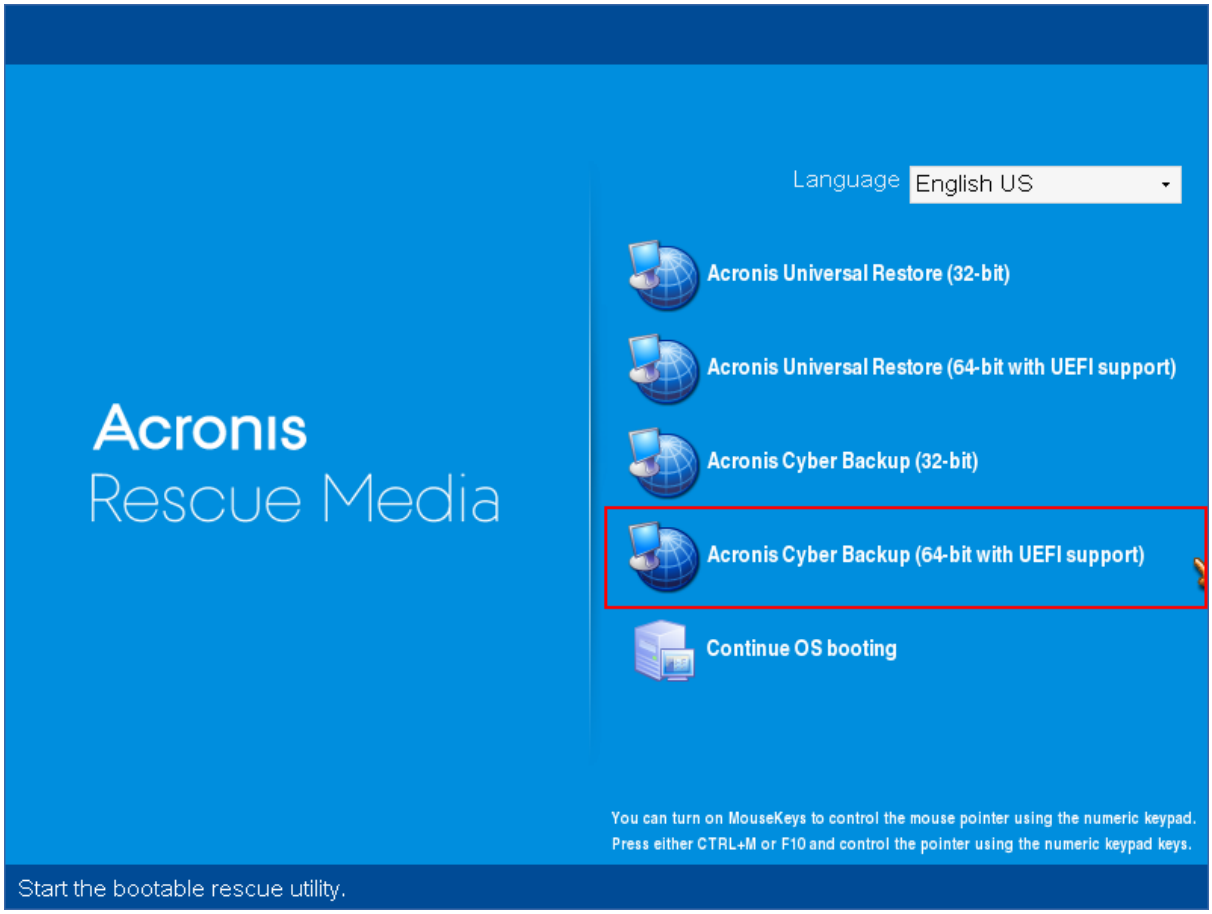


11.4.2 Obnova

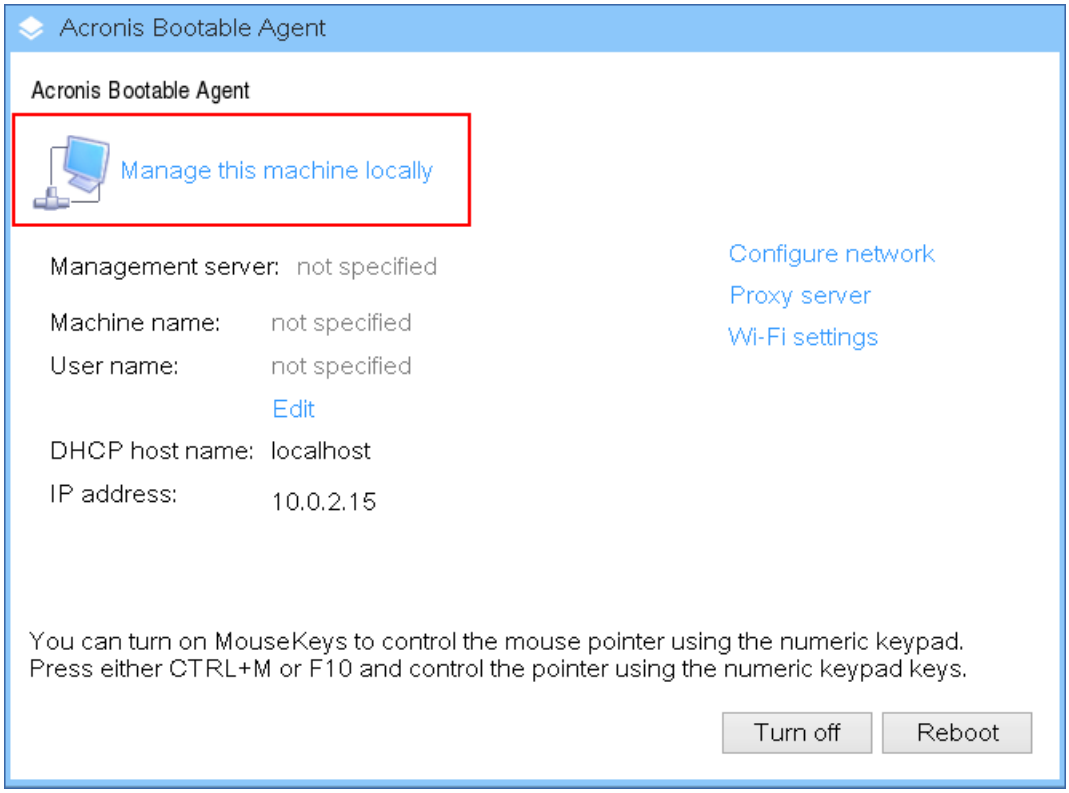
Operace obnovy je k dispozici pro spouštěcí médium vytvořené pomocí nástroje Tvůrce spouštěcích médií i pro stažené připravené spouštěcí médium.

Obnovení dat v rámci spouštěcího média

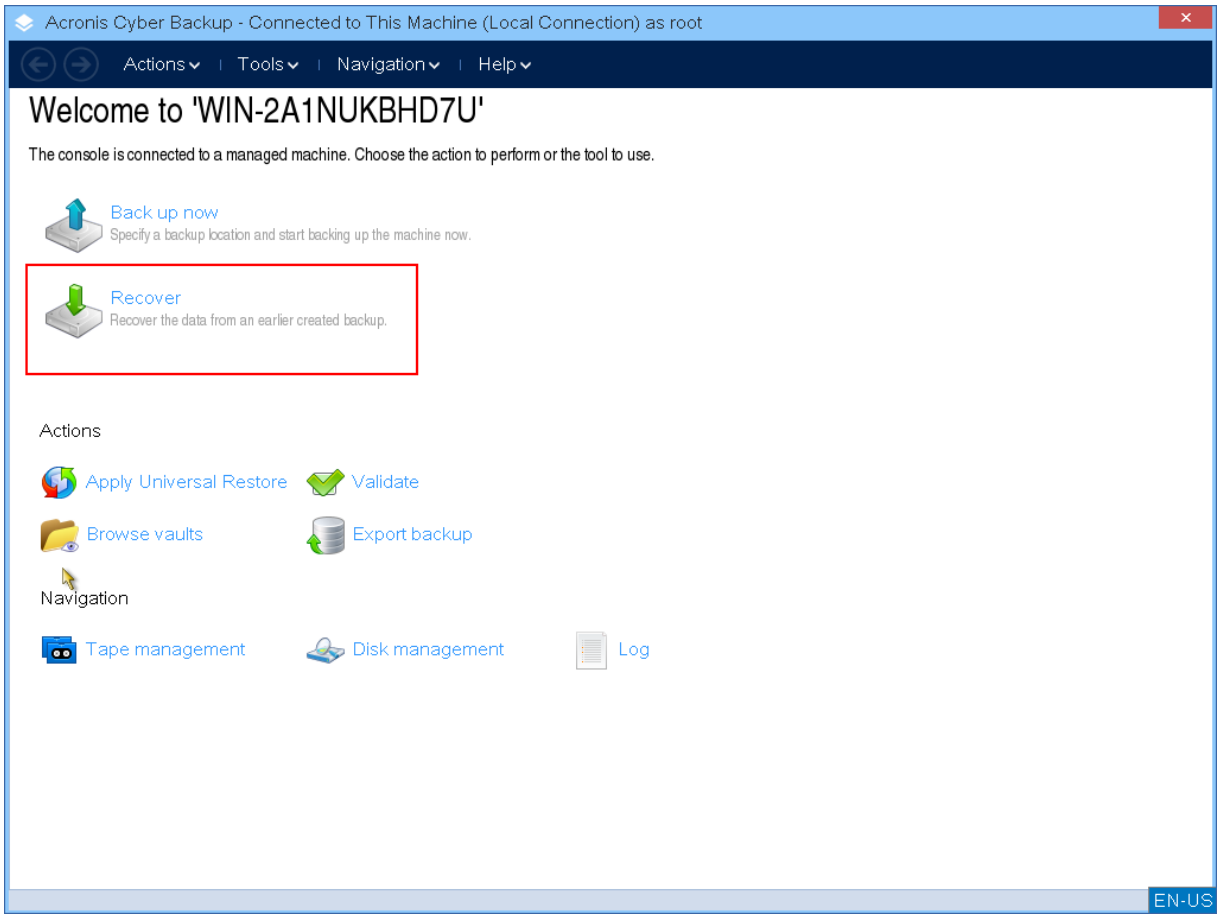
1. Proveďte spuštění ze záchranného spouštěcího média Acronis.



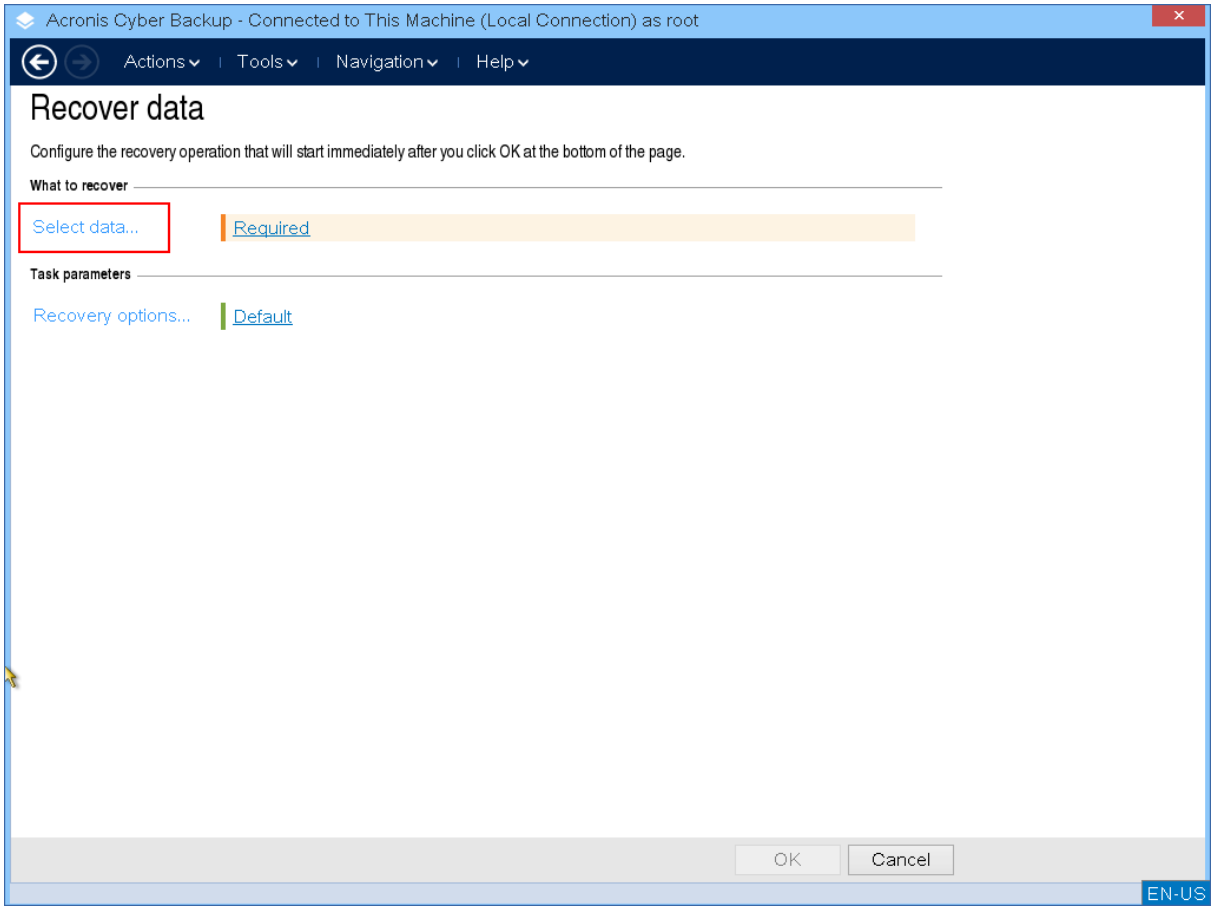
2. Chcete-li obnovit data do místního počítače, klikněte na položku **Místní správa tohoto počítače**. V případě vzdáleného připojení si prostudujte téma Registrace média na serveru pro správu (str. 253).



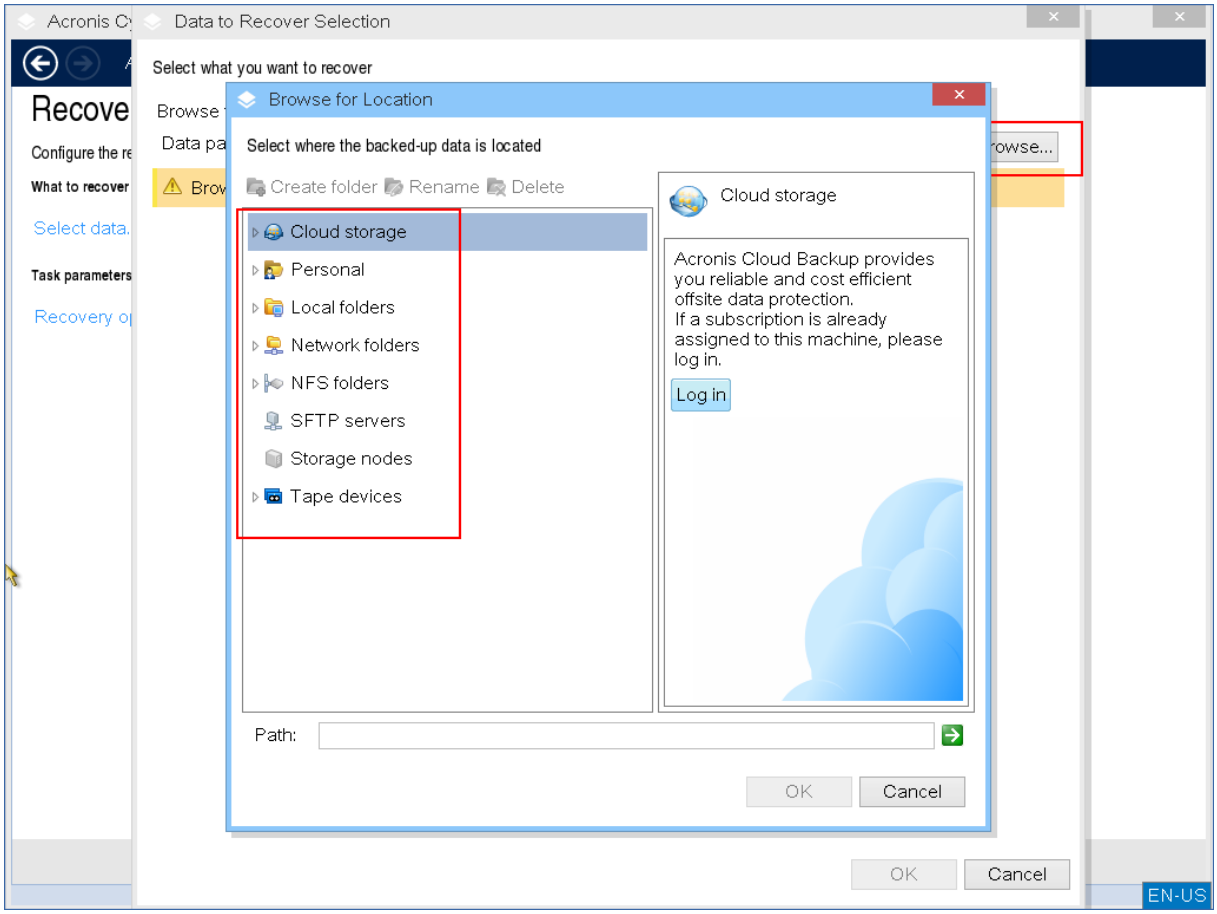
3. Klikněte na příkaz **Obnovit**.



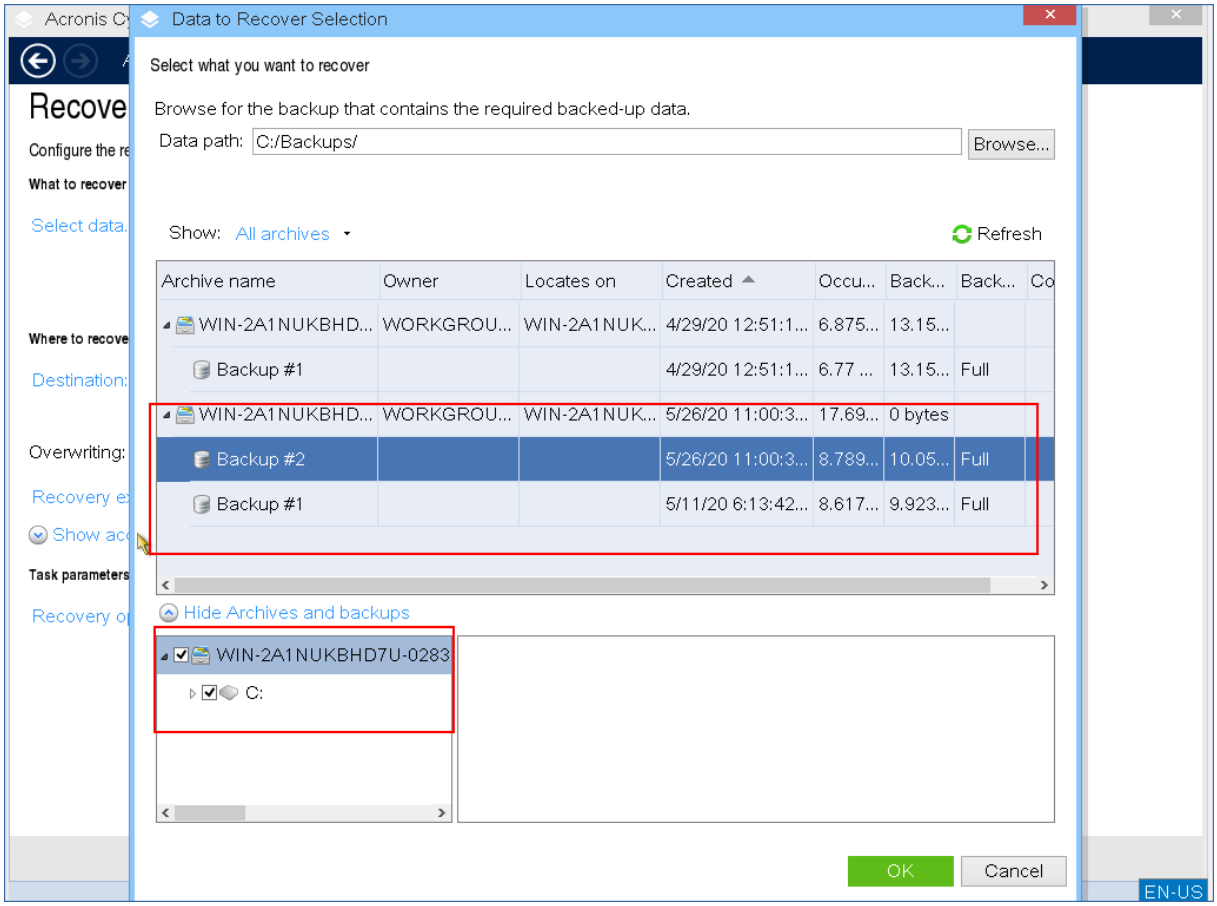
4. V části **Co obnovovat** klikněte na možnost **Vybrat data**.



5. Klikněte na tlačítko **Procházet** a vyberte umístění zálohy.

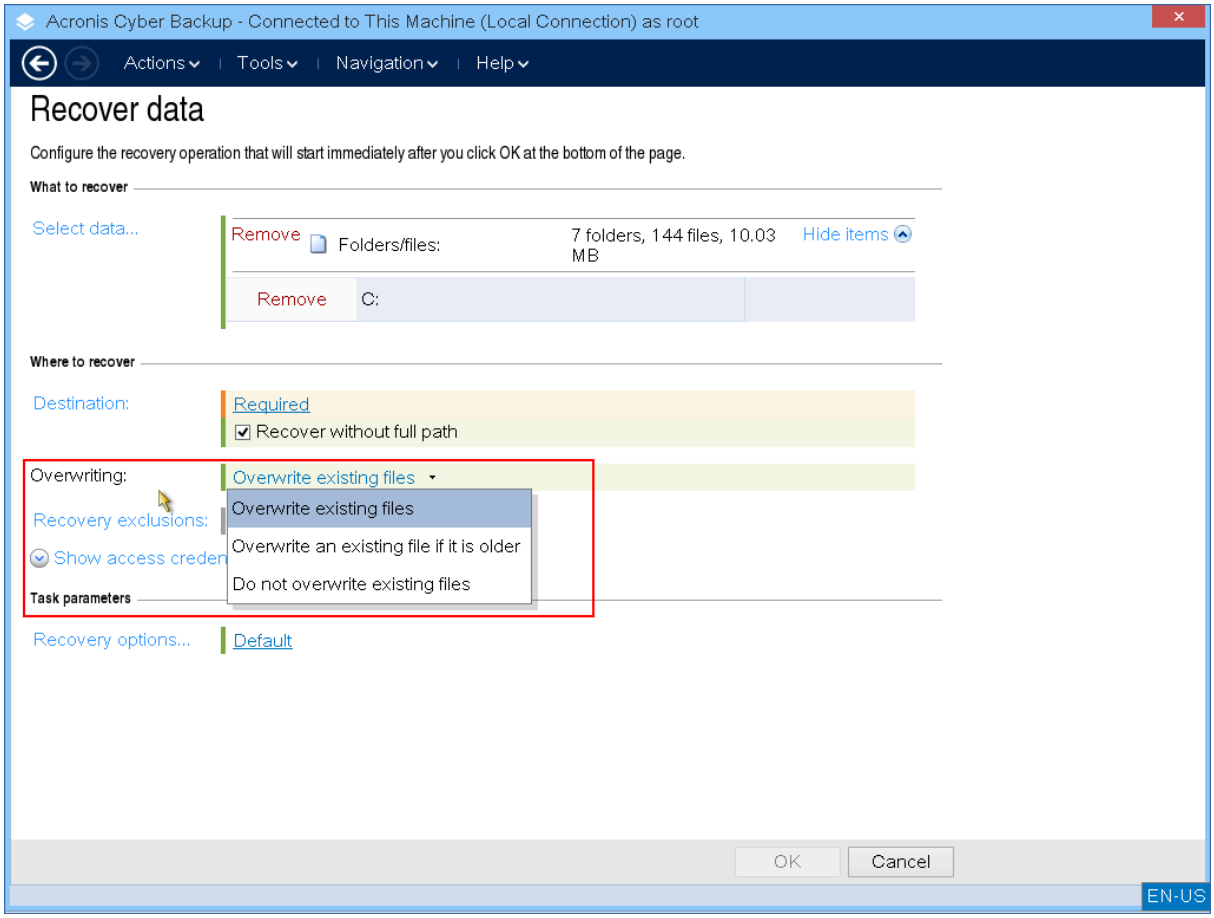


6. Vyberte soubor zálohy, ze kterého chcete data obnovit.

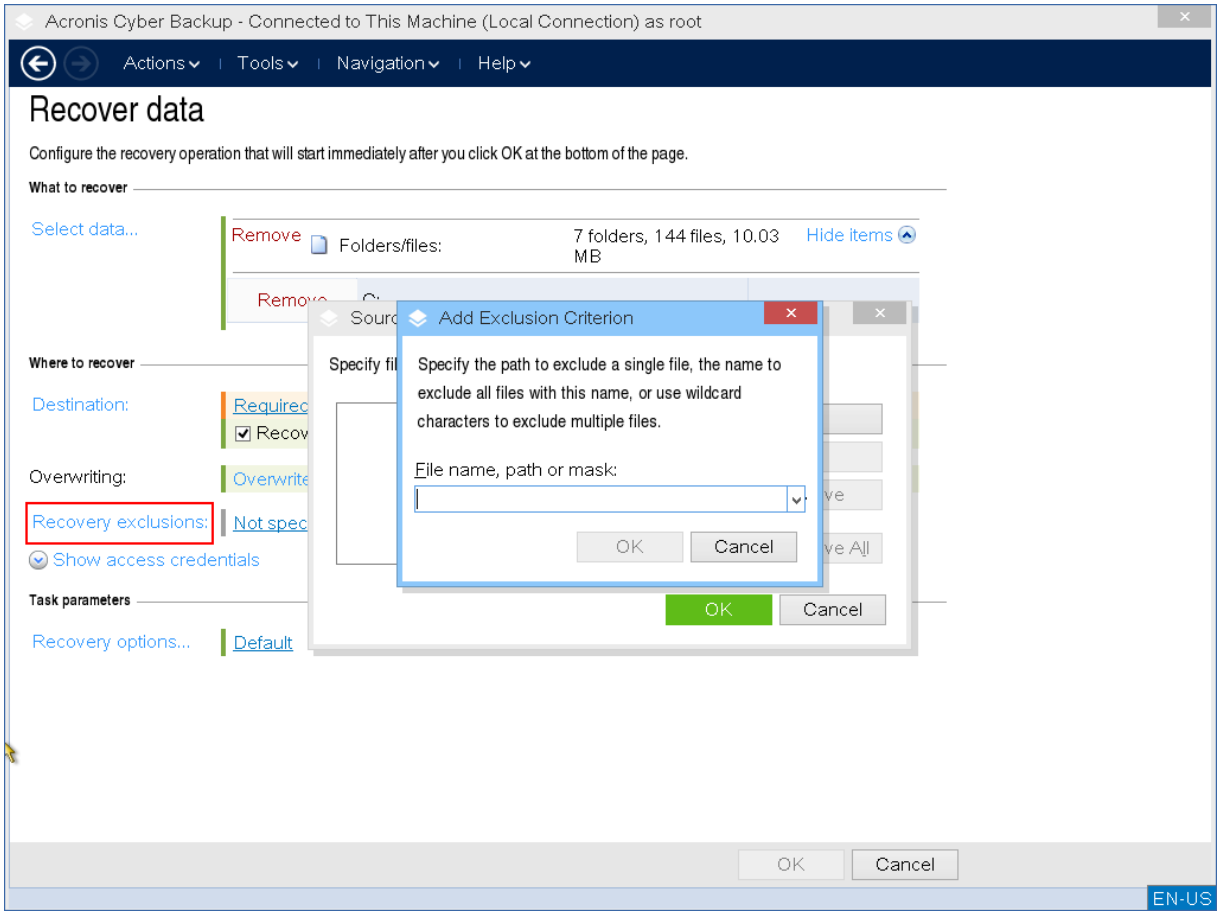


7. V levém dolním panelu vyberte jednotky/svazky (nebo soubory/složky), které chcete obnovit, a klikněte na tlačítko **OK**.

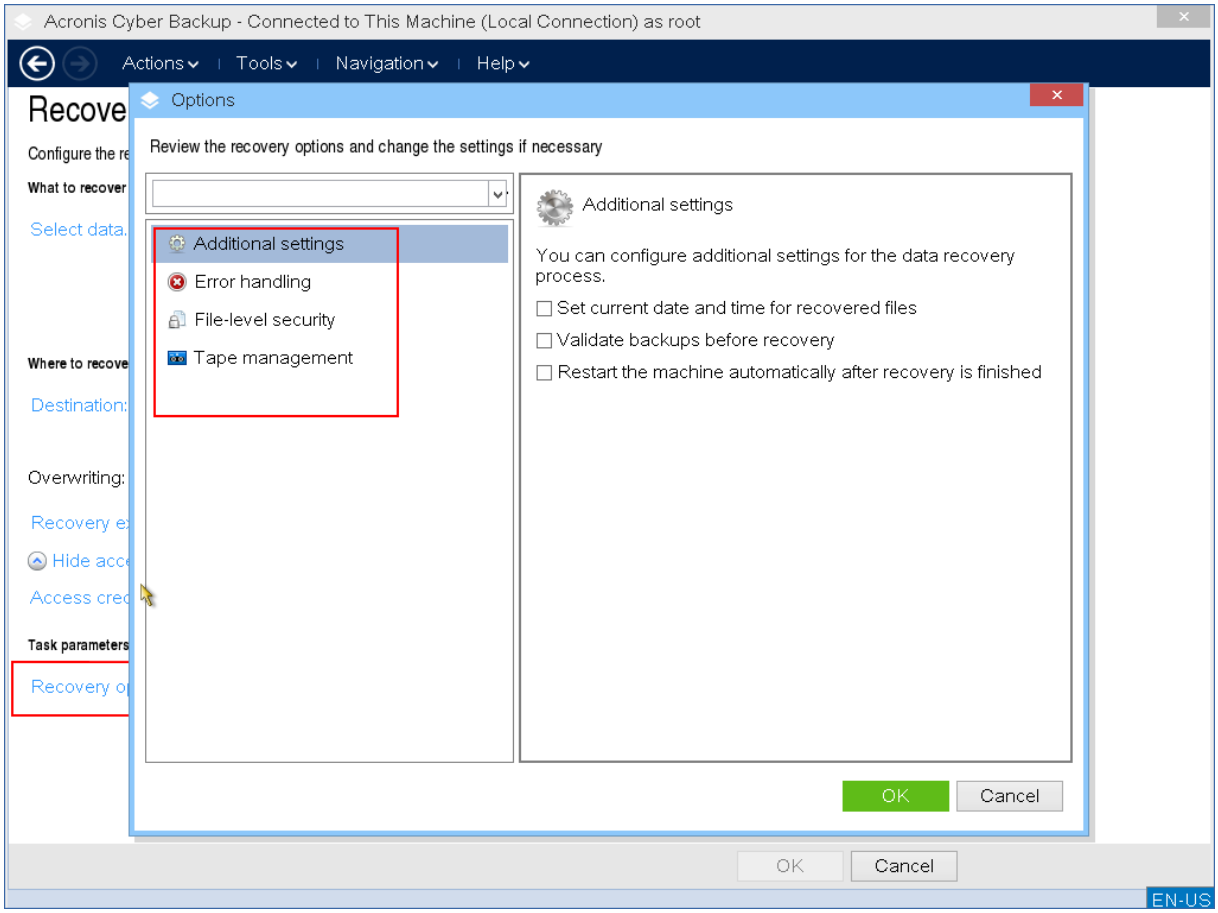
8. [Volitelné] Nakonfigurujte pravidla přepisu.



9. [Volitelné] Nakonfigurujte výjimky obnovení.



10. [Volitelné] Nakonfigurujte možnosti obnovení.



11. Zkontrolujte, zda je nastavení správné, a klikněte na tlačítko **OK**.

Poznámka *Chcete-li obnovit data na odlišný hardware, musíte použít Acronis Universal Restore (p. 204). Acronis Universal Restore není k dispozici, pokud se záloha nachází v Acronis Secure Zone.*

12 Správa disků

Pomocí spouštěcího média Acronis můžete připravit konfiguraci disku a svazku pro obnovení diskových obrazů svazku zálohovaných s použitím nástroje Acronis Cyber Protect.

Někdy, když je vytvořena záloha svazku a jeho diskový obraz je již umístěn do bezpečného úložiště, konfigurace disku počítače se může změnit, ať už kvůli nahrazení pevného disku nebo ztrátě hardwaru. V takovémto případě můžete znovu vytvořit nezbytnou konfiguraci disku, takže diskový obraz svazku může být obnoven přesně „tak, jak byl“, nebo s nějakou úpravou struktury disku nebo svazku, kterou uživatel považuje za nezbytnou.

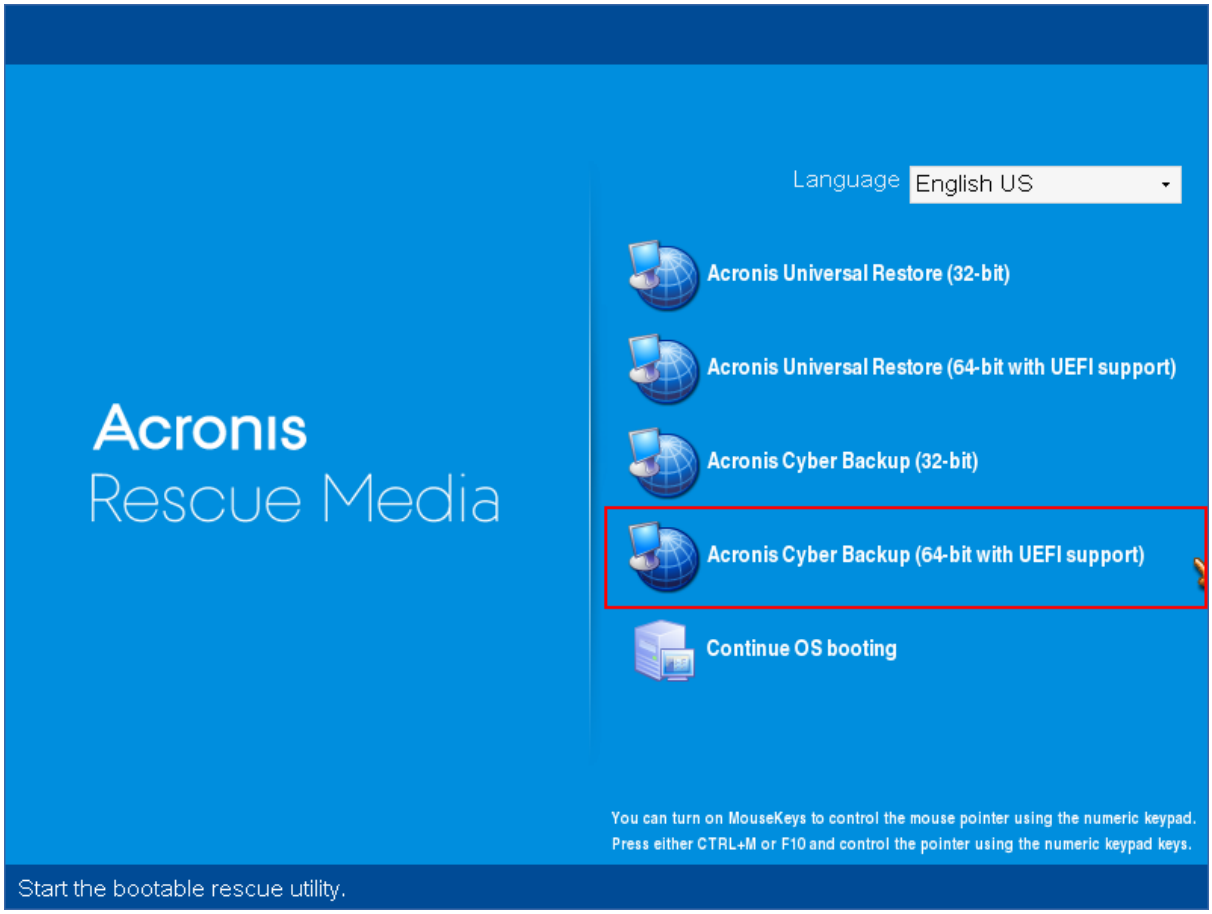
Pokud chcete zabránit možné ztrátě dat, proveďte všechna nezbytná preventivní opatření (str. 275).

Poznámka *Veškeré operace na discích a svazcích představují určité riziko poškození dat. Operace se systémovými, spouštěcími nebo datovými svazky je nutné provádět velice opatrně, abyste se vyhnuli možným problémům s procesem spouštění nebo s ukládáním dat pevného disku.*
Operace s pevnými disky a svazky vyžadují určitý čas, a jakýkoliv výpadek napájení, neúmyslné vypnutí počítače nebo náhodné zmáčknutí tlačítka Reset během procedury může vést k poškození svazku nebo ztrátě dat.

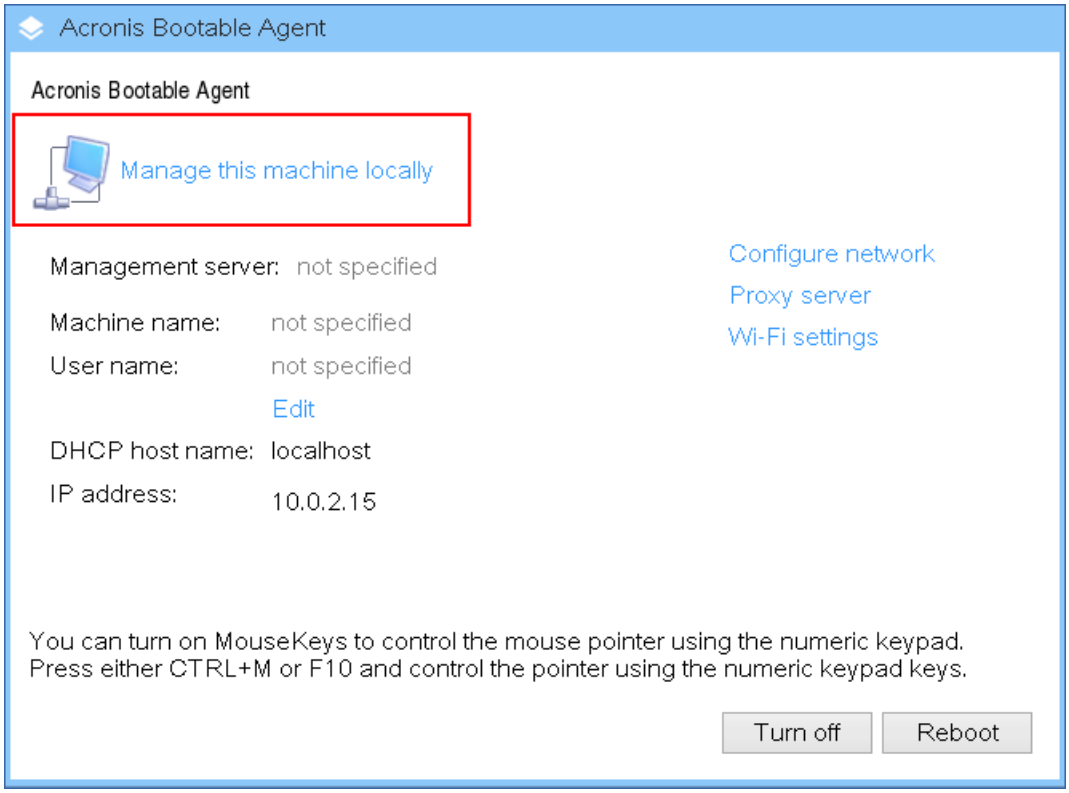
Operace správy disků můžete spustit v počítačích bez operačního systému, počítačích, které nelze spustit, a v počítačích se systémem jiným než Windows. Budete potřebovat spouštěcí médium, které jste vytvořili pomocí Tvůrce spouštěcích médií a pomocí licenčního klíče k produktu Acronis Cyber Protect. Další informace o vytvoření spouštěcího média naleznete v tématu Spouštěcí média založená na systému Linux (str. 232) a Spouštěcí média založená na systému Windows-PE (p. 247).

Provádění operací správy disků

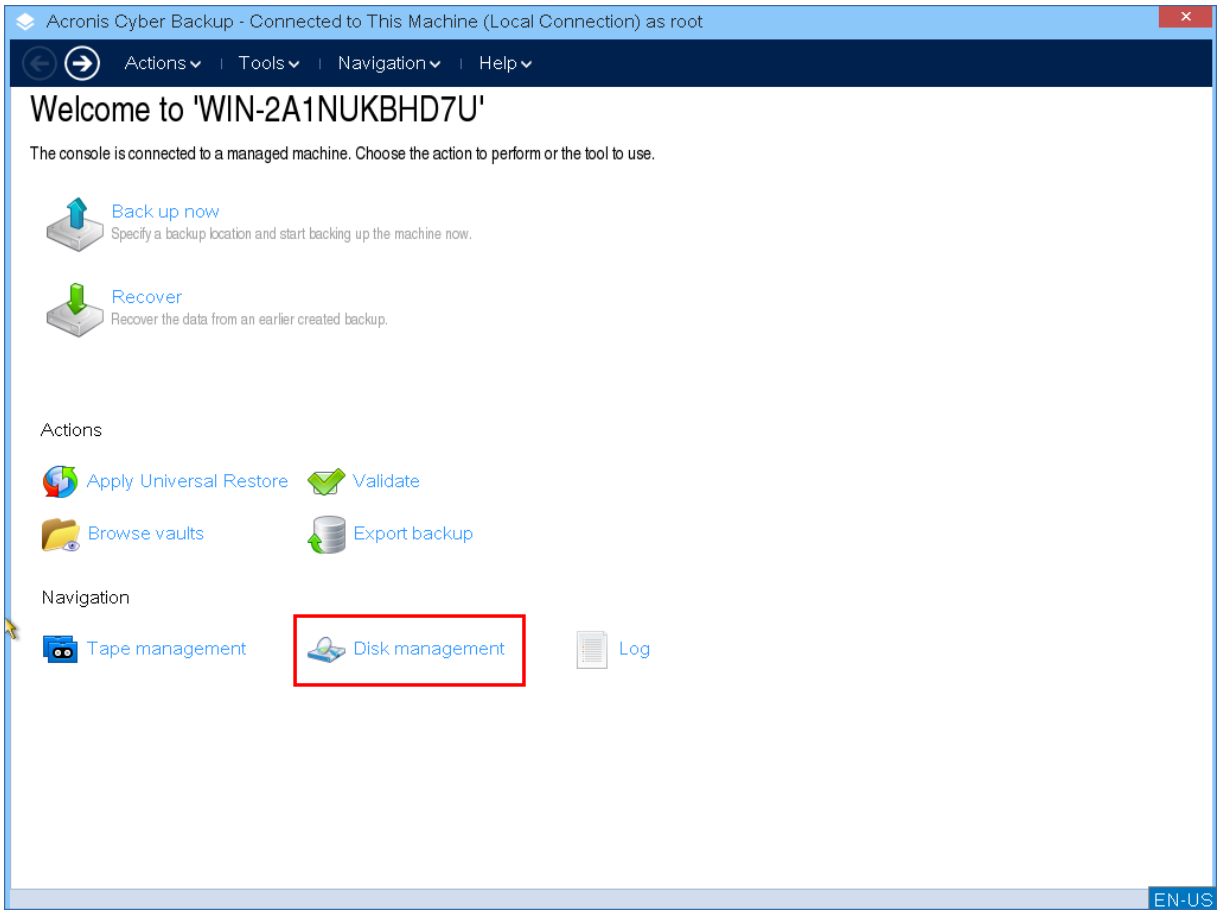
1. Proveďte spuštění ze záchranného spouštěcího média Acronis.



2. Chcete-li pracovat na místním počítači, klikněte na položku **Místní správa tohoto počítače**. V případě vzdáleného připojení si prostudujte téma Registrace média na serveru pro správu (str. 253).



3. Klikněte na položku **Správa disků**.



Poznámka *Operace správy disků založené na spouštěcím médiu mohou fungovat nesprávně, pokud jsou v počítači nakonfigurovány prostory úložišť.*

12.1.1.1 Podporované systémy souborů

Spouštěcí médium podporuje správu disků s následujícími systémy souborů:

- FAT 16/32
- NTFS

Pokud potřebujete provést operaci se svazkem s jiným systémem souborů, použijte Acronis Disk Director. Ta poskytuje více nástrojů a utilit pro správu disků a svazků s následujícími systémy souborů:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

12.1.1.2 Základní bezpečnostní opatření

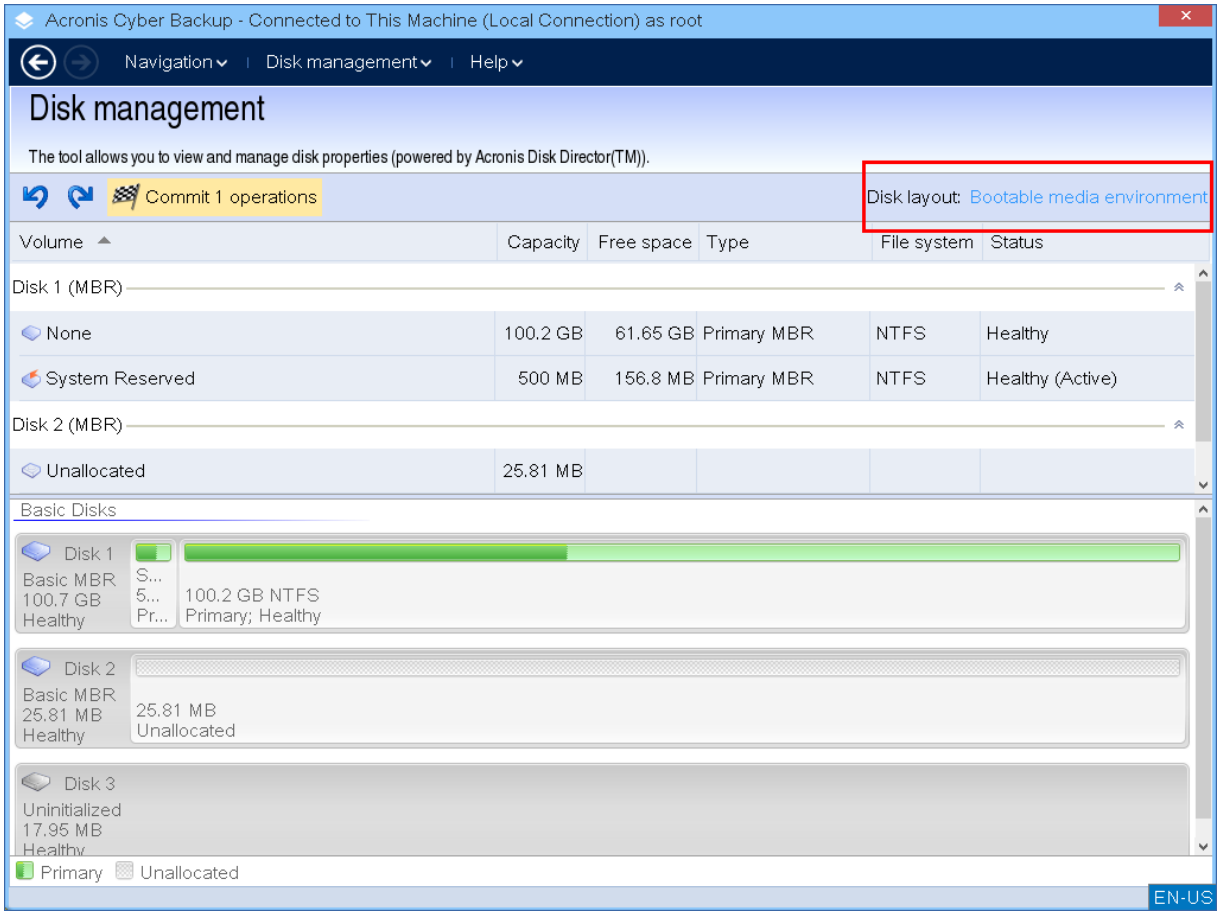
Chcete-li zabránit možnému poškození struktury disků nebo svazků a ztrátě dat, proveďte potřebná preventivní opatření a dodržujte tato pravidla:

1. Zálohujte disk, na němž chcete vytvářet nebo spravovat svazky. Pokud zálohujete nejdůležitější data na jiný pevný disk, síťové úložiště nebo vyměnitelná média, můžete se svazky na disku pracovat a budete mít jistotu, že jsou data v bezpečí.
2. Zkontrolujte, zda je disk plně funkční a zda neobsahuje vadné sektory nebo chyby v systému souborů.
3. Neprovádějte žádné operace s diskem či svazkem, pokud je spuštěn jiný software s přístupem k disku na nízké úrovni.

12.1.1.3 Výběr operačního systému pro správu disků

V počítači se dvěma nebo více operačními systémy závisí znázornění disků a svazků na tom, který operační systém je právě spuštěn. Stejný svazek může být v různých operačních systémech označen různými písmeny.

Když provedete operaci pro správu disků, musíte určit rozvržení disků, pro které bude zobrazen operační systém. Klikněte na název operačního systému vedle štítku **Rozvržení disku** a v okně, které se otevře, vyberte požadovaný operační systém.



12.1.1.4 Operace s disky

Se spouštěcím médiem můžete provádět následující operace správy disku:

- Inicializace disku (str. 276) – Inicializuje nový hardware, který byl přidán do systému.
- Klonování základních disků (str. 277) – Přenese kompletní data ze zdrojového základního disku typu MBR na cílový disk.
- Převod disku: MBR na GPT (str. 284) – Převede tabulku diskových oddílů MBR na GPT.
- Převod disku: GPT na MBR (str. 285) – Převede tabulku diskových oddílů GPT na MBR.
- Převod disku: Základní na dynamický (str. 285) – Převede základní disk na dynamický.
- Převod disku: Dynamický na základní (str. 285) – Převede dynamický disk na základní.

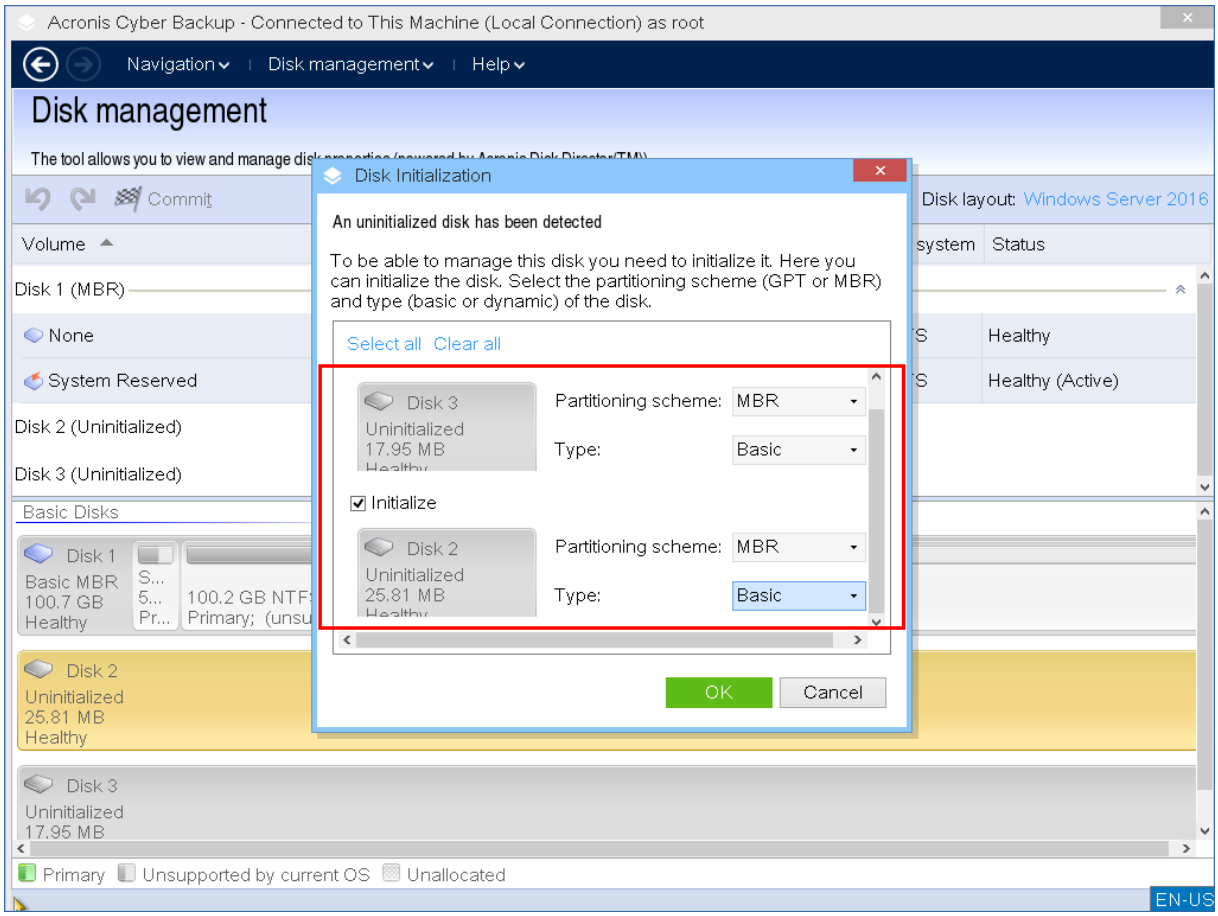
Inicializace disku

Spouštěcí médium ukazuje neinicializovaný disk jako šedý blok se zašedlou ikonou, což udává, že systém nemůže disk použít.

Inicializace disku

1. Klikněte pravým tlačítkem na požadovaný disk a vyberte příkaz **Inicializovat**.

2. V okně **Inicializace disku** nastavte schéma rozdělení na diskové oddíly (MBR nebo GPT) a typ disku (základní nebo dynamický).
3. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci inicializace disku.
4. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.
5. Po inicializaci zůstává prostor na disku nepřidělený. Chcete-li tento prostor využít, je třeba na něm vytvořit svazek (str. 287).



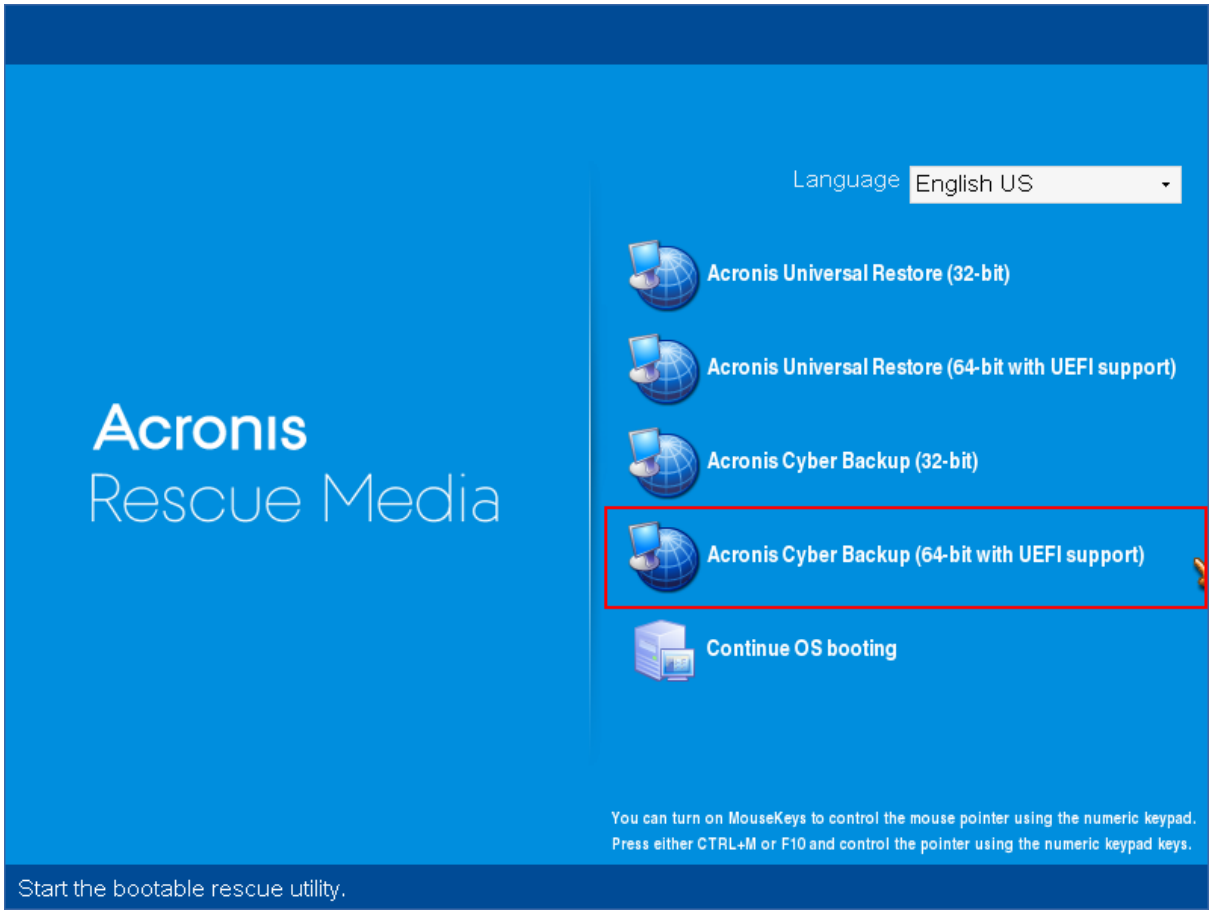
Klonování základních disků

Se spouštěcím médiem založeným na Linuxu s kompletními funkcemi můžete klonovat základní disky typu MBR. Klonování disku není k dispozici v připraveném spouštěcím médiu, které si můžete stáhnout, nebo ve spouštěcím médiu vytvořeném bez licenčního klíče.

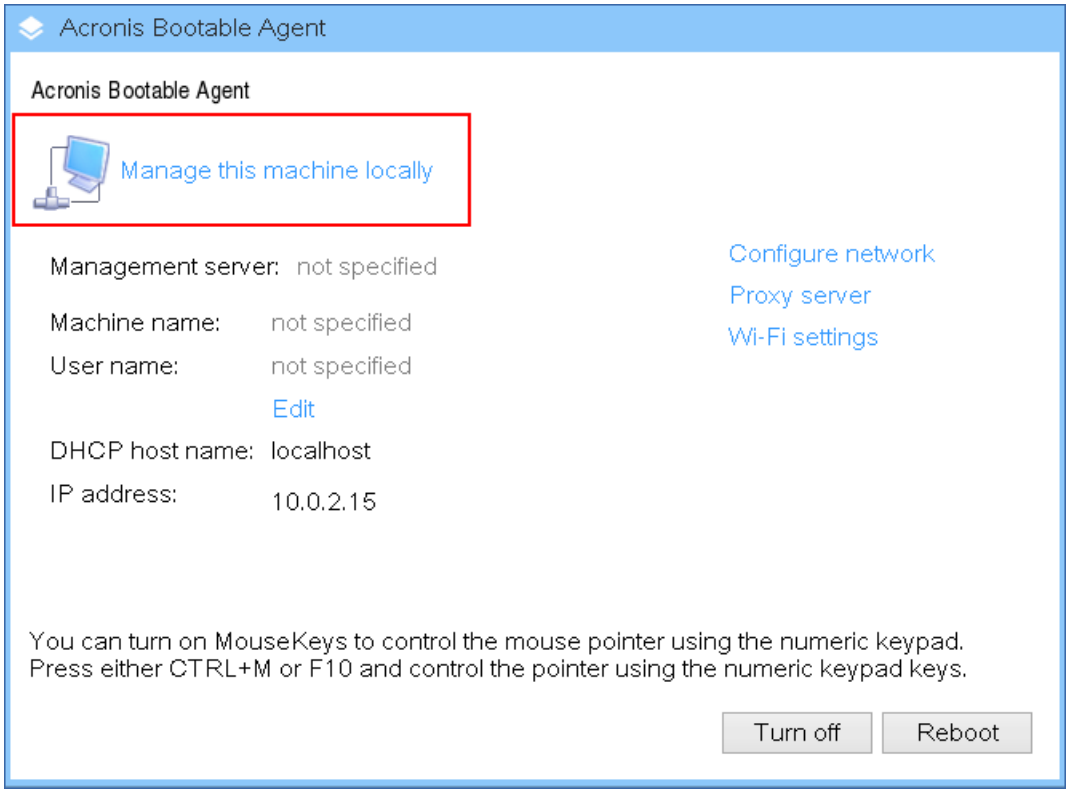
Poznámka *Disky můžete také klonovat pomocí nástroje příkazového řádku Acronis Cyber Protect https://www.acronis.com/en-us/support/documentation/AcronisBackup_12.5_Command_Line_Reference/index.html#15133.html.*

Klonování základních disků v rámci spouštěcího média

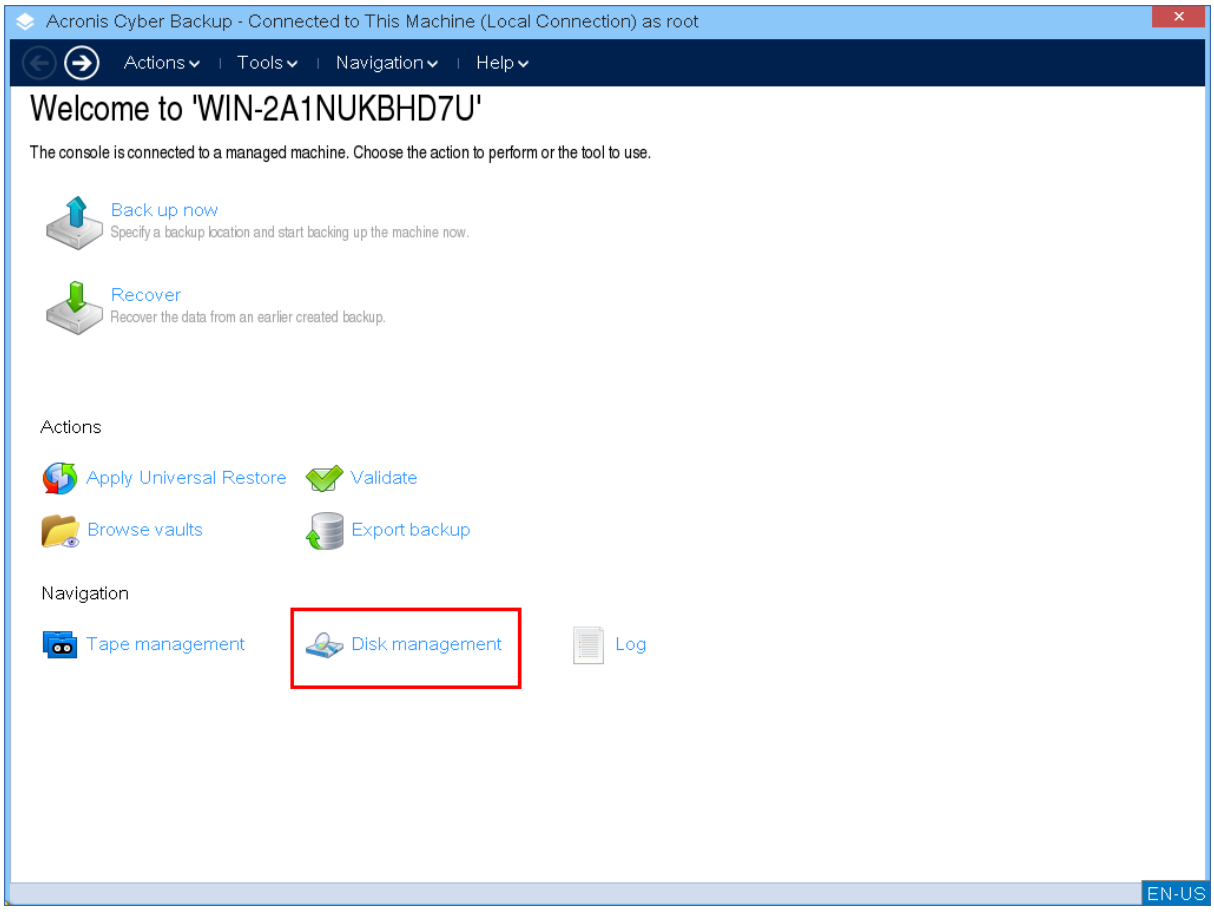
1. Proveďte spuštění ze záchranného spouštěcího média Acronis.



2. Chcete-li naklonovat disk místního počítače, klikněte na položku **Místní správa tohoto počítače**. V případě vzdáleného připojení si prostudujte téma Registrace média na serveru pro správu (str. 253).

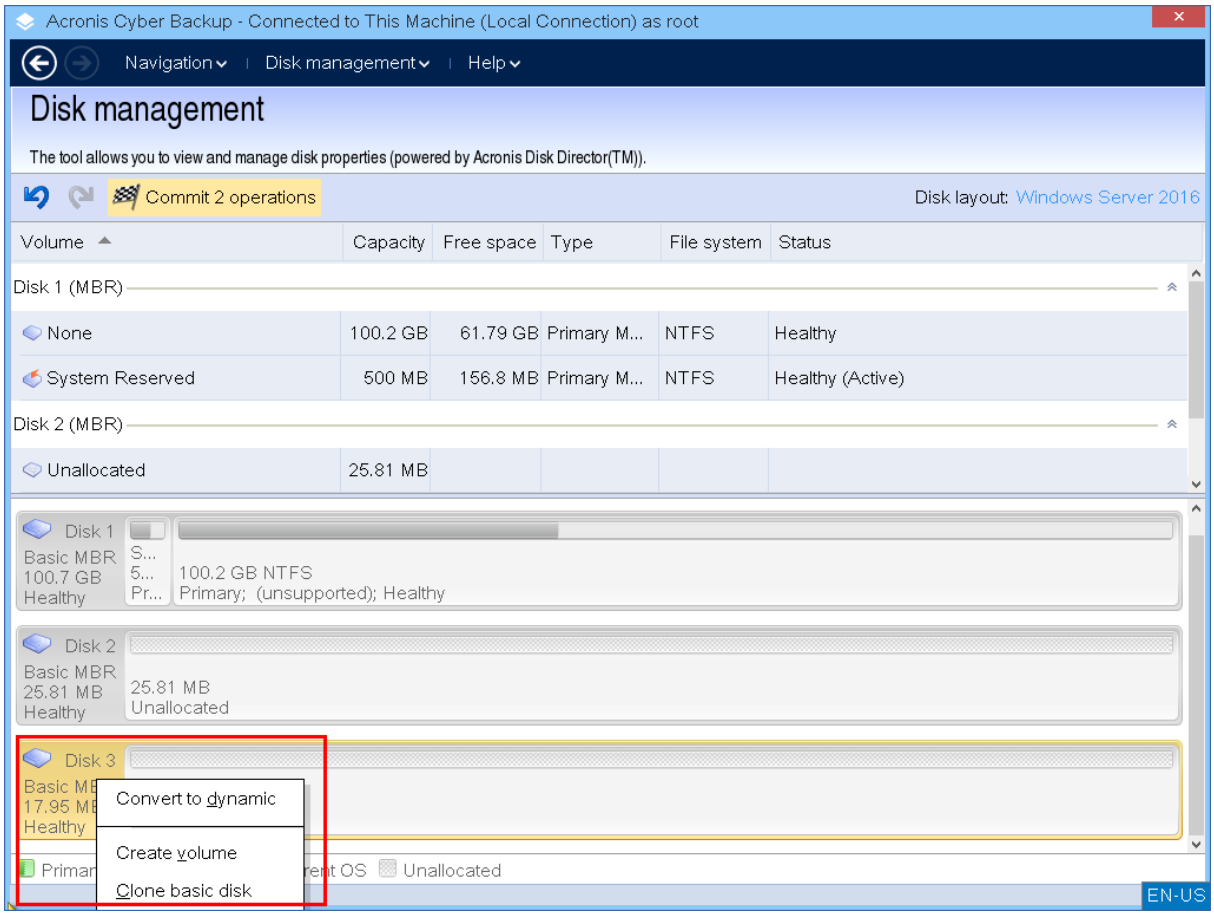


3. Klikněte na položku **Správa disků**.

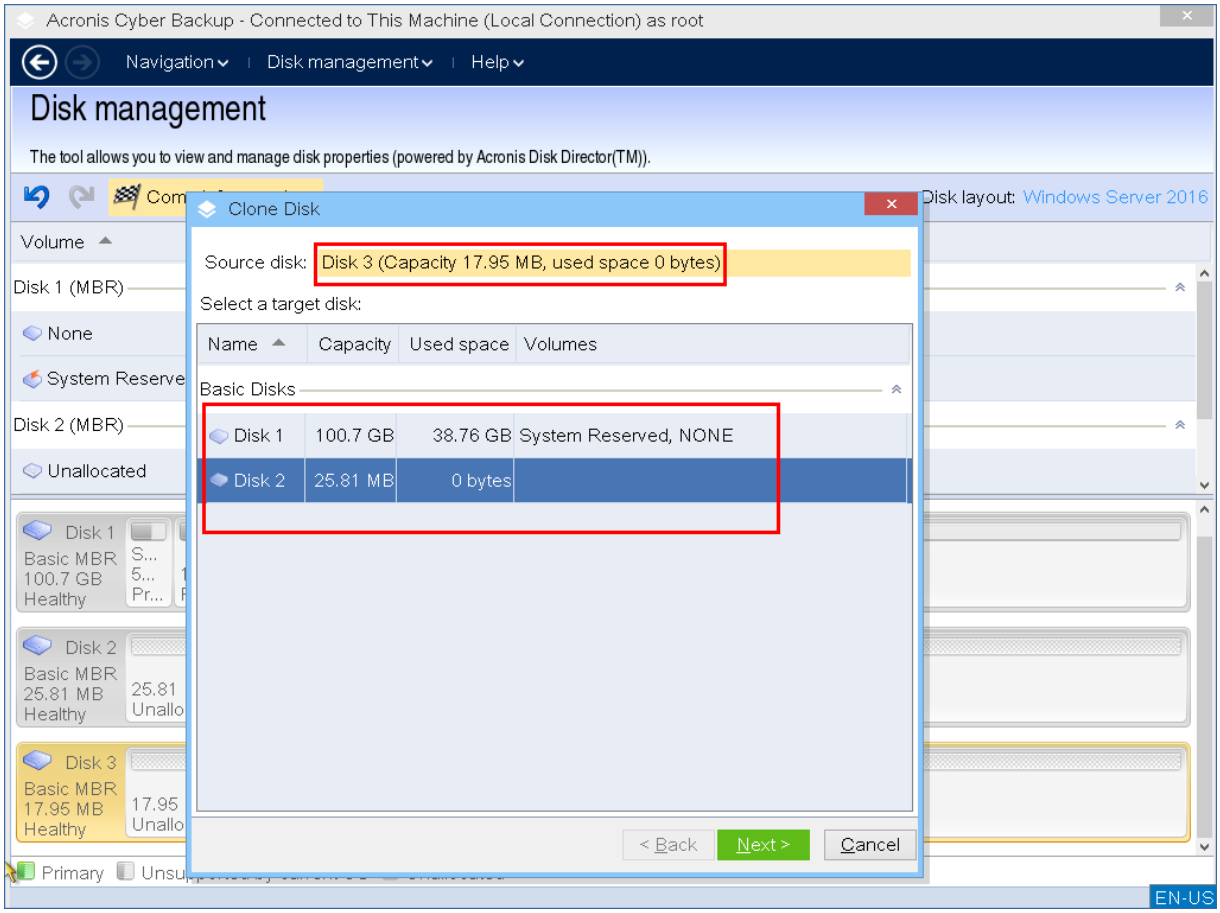


4. Zobrazí se dostupné disky. Klikněte pravým tlačítkem na disk, který chcete klonovat, a vyberte příkaz **Klonovat základní disk**.

Poznámka *Klonovat lze pouze celý disk. Klonování oddílů není k dispozici*

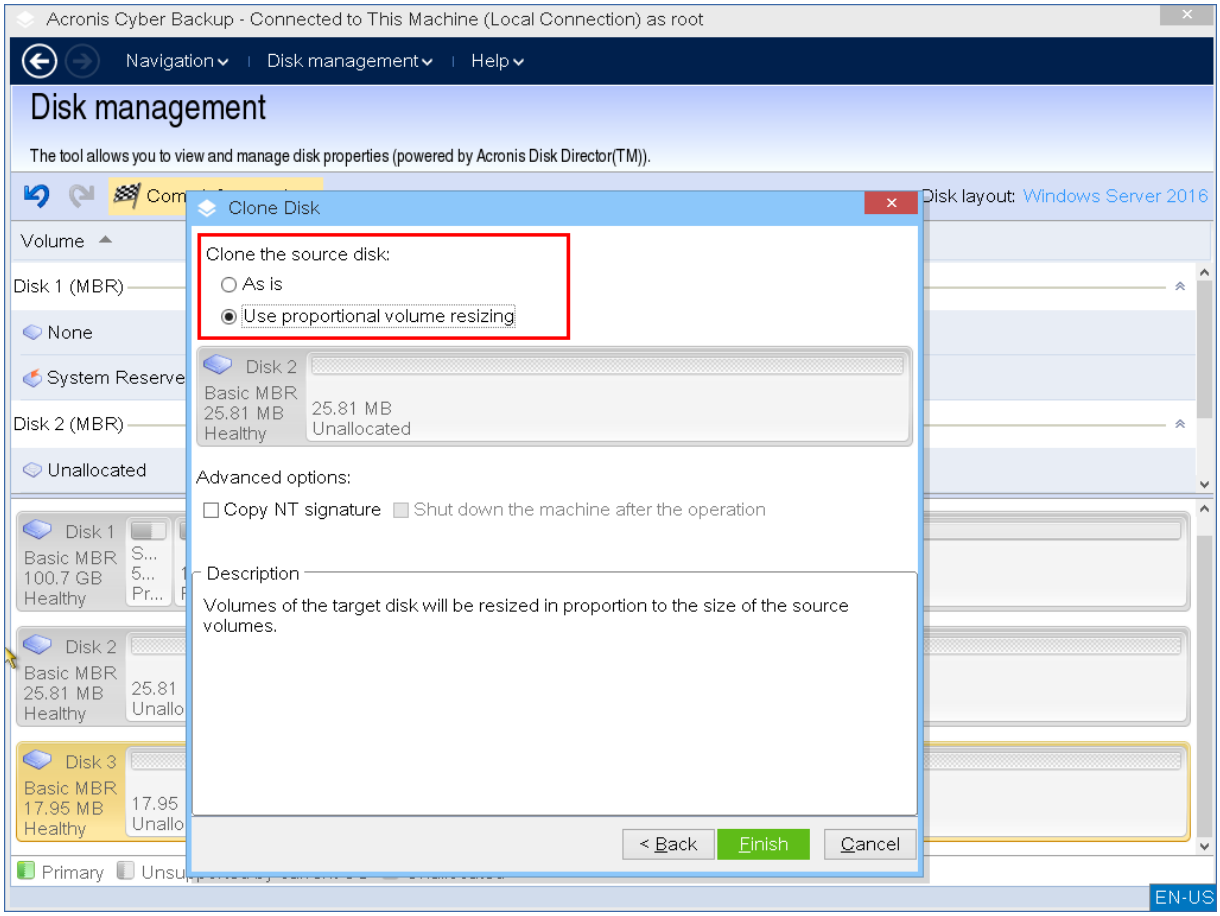


5. Zobrazí se seznam možných cílových disků. Program umožňuje vybrat cílový disk, jehož velikost je dostatečná k uchování všech dat ze zdrojového disku bez ztráty. Vyberte cílový disk a klikněte na tlačítko **Další**.

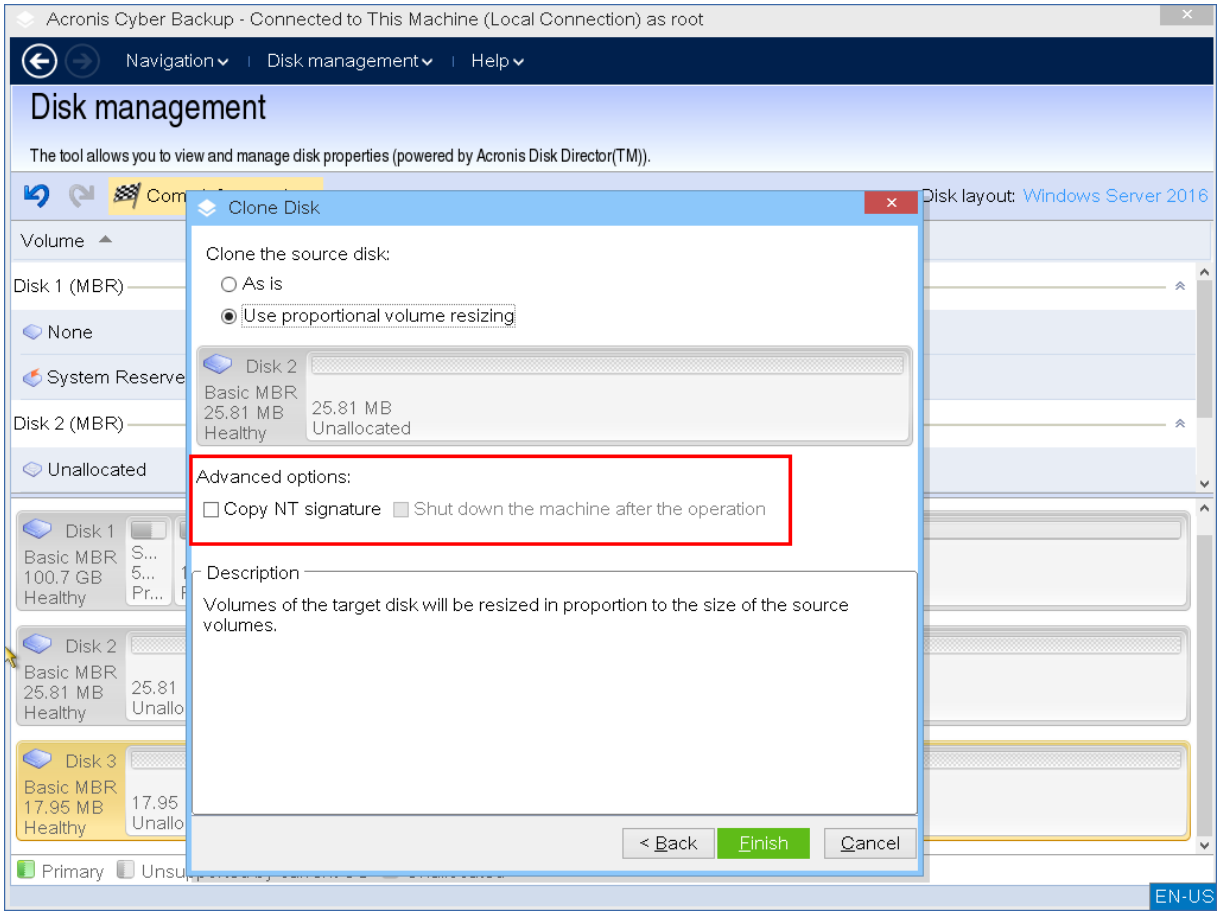


Pokud je cílový disk větší, můžete disk naklonovat tak, jak je, nebo změnit velikost svazků zdrojového disku (výchozí možnost), abyste se vyhnuli ponechání nepřiděleného místa na cílovém disku.
Pokud je disk menší, je k dispozici pouze proporcionální změna velikosti. Pokud bezpečné klonování není možné ani v případě proporcionální změny velikosti, nebude možné v operaci pokračovat.

Důležité *Jestliže jsou na cílovém disku data, zobrazí se upozornění: „*Vybraný cílový disk není prázdný. Data v jeho svazcích budou přepsána.“ *Pokud budete pokračovat, všechna data, která jsou momentálně na cílovém disku, budou nenávratně ztracena.*



6. Vyberte, zda chcete zkopírovat NT podpis.



Při klonování disku, který obsahuje systémový svazek, potřebujete zachovat spustitelnost operačního systému na cílovém svazku disku. To znamená, že operační systém musí mít informace systémového svazku (například písmeno svazku) shodující se s NT podpisem, který se uchovává v záznamu disku typu MBR. Dva disky se stejným NT podpisem však nemůžou správně fungovat pod jedním operačním systémem.

Pokud jsou na počítači dva disky se stejným NT podpisem obsahující systémový svazek, operační systém se spustí z prvního disku, nalezení stejného NT podpisu na druhém disku automaticky vygeneruje nový unikátní NT podpis a přiřadí ho ke druhému disku. Výsledkem je, že svazky druhého disku ztratí svá písmena, všechny cesty na disku už nebudou platné a programy nenaleznou své soubory. Operační systém na tomto disku nebude spustitelný.

Pro zachování spustitelnosti systému na svazku cílového disku máte následující možnosti:

a. **Zkopírovat NT podpis** – zajistit, aby cílový disk měl NT podpis zdrojového disku shodující se s klíči registrů, které budou také zkopírovány na cílový disk.

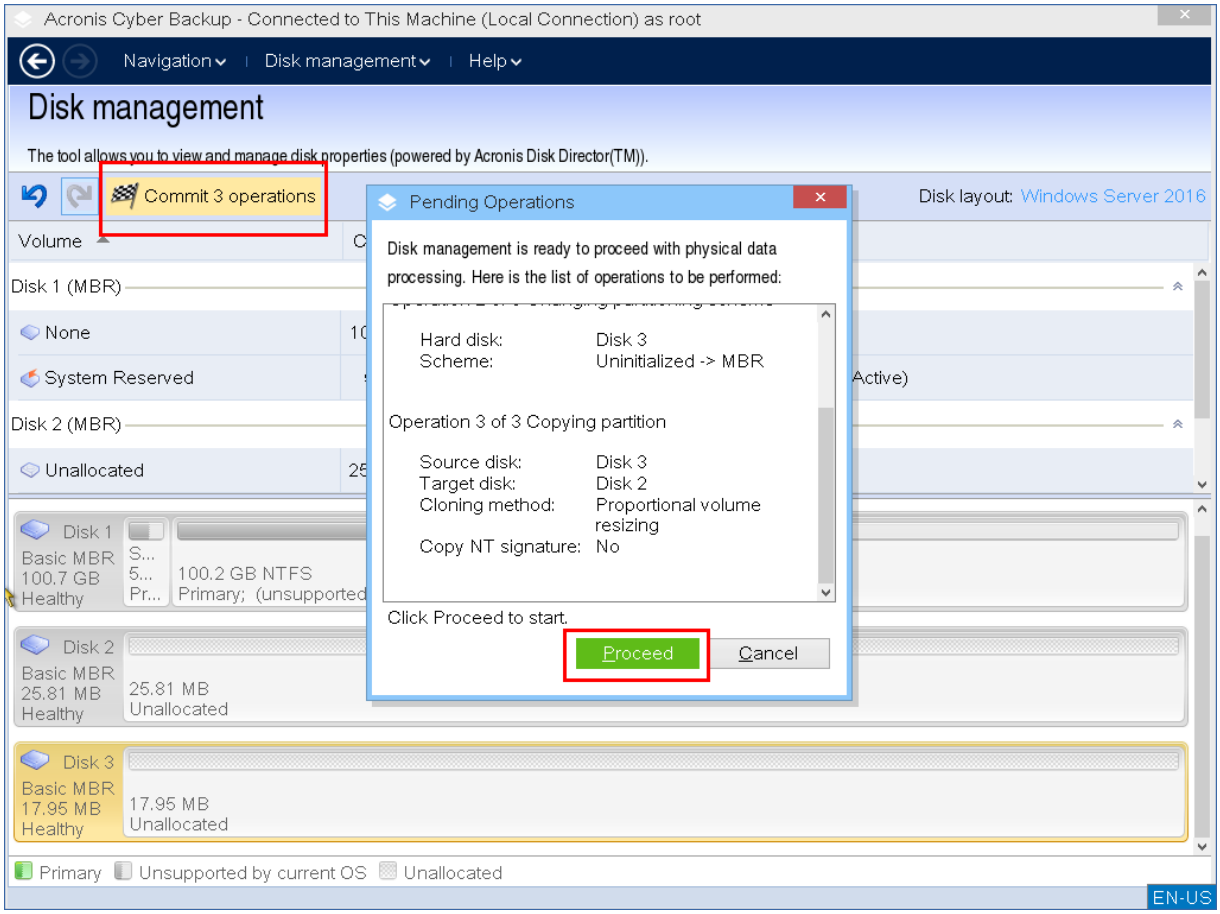
   Zaškrtněte políčko **Kopírovat NT podpis**.
   Zobrazí se upozornění: *„Pokud je na pevném disku operační systém, před spuštěním počítače znovu odinstalujte jednotky zdrojového i cílového pevného disku. Jinak se spustí OS na prvním disku a OS na druhém disku se stane nespustitelným.“*
   Políčko **Vypnout počítač po operaci** se vybírá a vypíná automaticky.

b. **Nechat NT podpis** – zachovat podpis starého cílového disku a podle podpisu aktualizovat operační systém.

   V případě potřeby kliknutím zrušte zaškrtnutí políčka **Kopírovat NT podpis**.
   Zaškrtnutí políčka **Vypnout počítač po operaci** se automaticky zruší.

7. Kliknutím na tlačítko **Dokončit** přidáte naplánovanou operaci klonování disku.

8. Klikněte na tlačítko **Provést** a pak v okně **Naplánované operace** klikněte na **Pokračovat**. Pokud program ukončíte bez provedení operace, operaci zrušíte.



9. Pokud se rozhodnete zkopírovat NT podpis, počkejte na dokončení operace a vypnutí počítače. Pak odpojte zdrojový, nebo cílový pevný disk z počítače.

Převod disku: MBR na GPT

Základní disk typu MBR můžete chtít převést na základní disk GPT, když potřebujete:

- Více než čtyři primární svazky na disku.
- Vyšší spolehlivost disku vůči případnému poškození dat.

Důležité *Základní disk typu MBR, který obsahuje spouštěcí svazek s aktuálně spuštěným operačním systémem, nelze převést na GPT.*

Převedení základního disku typu MBR na základní disk GPT

1. Klikněte pravým tlačítkem na disk, který chcete klonovat, a vyberte příkaz **Převést na GPT**.
2. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci převodu disku typu MBR na GPT.
3. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Poznámka *Disk GPT s diskovými oddíly obsahuje vyhrazené místo za oblastí s diskovými oddíly, které se využívá jako oblast pro záložní kopie záhlaví GPT a tabulky diskových oddílů. Pokud je disk plný a velikost svazku nelze automaticky zmenšit, převod disku typu MBR na GPT selže.*
Operaci nelze vrátit zpět. Pokud máte na disku typu MBR primární svazek a převedete tento disk nejprve na GPT a potom zpět na MBR, bude tento svazek logický a nebude ho možné použít jako systémový svazek.

Převod dynamického disku: MBR na GPT

Spouštěcí médium nepodporuje u dynamických disků přímý převod MBR na GPT. Stejného výsledku lze ale dosáhnout provedením následujících převodů:

1. Převod disku typu MBR: dynamického na základní (str. 285) pomocí operace **Převést na základní**.
2. Převod základního disku: MBR na GPT pomocí operace **Převést na GPT**.
3. Převod disku GPT: základního na dynamický (str. 285) pomocí operace **Převést na dynamický**.

Převod disku: GPT na MBR

Pokud plánujete instalaci operačního systému, který nepodporuje disky GPT, je možné disk GPT převést na MBR.

Důležité *Základní disk typu GPT, který obsahuje spouštěcí svazek s aktuálně spuštěným operačním systémem, nelze převést na MBR.*

Jak převést disk GPT na MBR

1. Klikněte pravým tlačítkem na disk, který chcete klonovat, a vyberte příkaz **Převést na MBR**.
2. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci převodu disku GPT na MBR.
3. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Poznámka *Po operaci budou svazky na tomto disku logické. Tuto změnu nelze vrátit zpět.*

Převod disku: základní na dynamický

Základní disk je vhodné převést na dynamický v následujících případech:

- Pokud plánujete disk použít jako součást skupiny dynamických disků.
- Pokud chcete dosáhnout vyšší spolehlivosti úložiště dat.

Jak převést základní disk na dynamický

1. Klikněte pravým tlačítkem na disk, který chcete převést, a vyberte příkaz **Převést na dynamický**.
2. Klikněte na tlačítko **OK**.

Převod se provede okamžitě a počítač se v případě potřeby restartuje.

Poznámka *Dynamický disk využívá poslední megabajt fyzického disku k uložení databáze včetně čtyřúrovňového popisu (svazek-součást-diskový oddíl-disk) pro všechny dynamické svazky. Jestliže se během převodu na dynamický disk ukáže, že základní disk je plný a velikost jeho svazků nelze automaticky zmenšit, operace se nezdaří.*
Převod disků obsahujících systémové svazky nějakou dobu trvá a jakýkoliv výpadek napájení, nechtěné vypnutí počítače nebo neúmyslné stisknutí tlačítka Reset během této operace může způsobit nemožnost spuštění z tohoto disku.

Na rozdíl od Správce disků Windows aplikace po operaci zajišťuje spustitelnost **offline operačního systému** na disku.

Převod disku: dynamický na základní

Dynamické disky je vhodné převést na základní například v případě, že v počítači chcete používat operační systém, který dynamické disky nepodporuje.

Převedení dynamického disku na základní:

1. Klikněte pravým tlačítkem na disk, který chcete převést, a vyberte příkaz **Převést na základní**.

2. Klikněte na tlačítko **OK**.

Převod se provede okamžitě a počítač se v případě potřeby restartuje.

Poznámka *Tato operace není dostupná pro dynamické disky obsahující rozložené, prokládané nebo RAID-5 svazky.*

Po převodu se posledních 8 MB místa na disku vyhradí pro budoucí převod tohoto disku ze základního na dynamický. V některých případech se možné nepřidělené místo může lišit od předpokládané maximální velikosti svazku (například když velikost jednoho zrcadlení určuje velikost druhého zrcadlení nebo je posledních 8 MB diskového prostoru vyhrazeno pro pozdější převod základního disku na dynamický).

Poznámka *Převod disků obsahujících systémové svazky nějakou dobu trvá a jakýkoliv výpadek napájení, nechtěné vypnutí počítače nebo neúmyslné stisknutí tlačítka Reset během této operace může způsobit nemožnost zavedení z tohoto disku.*

Na rozdíl od Správce disků Windows aplikace zajišťuje:

- bezpečný převod dynamického disku na základní, pokud obsahuje svazky **s daty** jednoduchých a zrcadlených svazků,
- možnost spuštění systému (v systémech s více možnostmi spuštění), který byl v průběhu operace **offline**.

12.1.1.5 Operace se svazky

Se spouštěcím médiem můžete provádět následující operace se svazky:

- Vytvořit svazek (str. 287) – vytvoří nový svazek
- Odstranit svazek (str. 290) – odstraní vybraný svazek
- Nastavit jako aktivní (str. 290) – nastaví vybraný svazek na aktivní, takže počítač bude možné spustit s operačním systémem, který je tam nainstalovaný
- Změnit písmeno (str. 291) – změní písmeno vybraného svazku
- Změnit jmenovku (str. 291) – změní jmenovku vybraného svazku
- Formátovat svazek (str. 291) – naformátuje svazek se systémem souborů

Typy dynamických svazků

Jednoduchý svazek

Svazek vytvořený z volného místa na jednom fyzickém disku. Může zahrnovat jednu oblast na disku nebo několik oblastí, které jsou virtuálně sjednoceny nástrojem Správce logických disků. Neposkytuje vyšší spolehlivost a rychlost ani více místa.

Rozložený svazek

Svazek vytvořený z volného místa na disku, které je virtuálně spojeno nástrojem Správce logických disků z několika fyzických disků. Do jednoho svazku lze zahrnout až 32 disků a překonat tak omezení velikosti hardwaru. Pokud ale selže jen jediný disk, ztracena budou všechna data. Také nelze odebrat jen určitou část rozloženého svazku bez zničení celého svazku. Rozložený svazek tak nenabízí vyšší spolehlivost ani vyšší rychlost I/O.

Prokládaný svazek

Svazek (označovaný také jako RAID-0), který se skládá z pásů dat o stejné velikosti zapsaných na všechny disky ve svazku. K vytvoření prokládaného svazku tak potřebujete dva a více dynamických disků. Disky v prokládaném svazku nemusí být identické, ale na každém disku, který

chcete do svazku zahrnout, musí být stejně velké bloky nepřiděleného místa. Velikost svazku bude záviset na velikosti nejmenšího místa. Přístup k datům na prokládaném svazku je většinou rychlejší než přístup ke stejným datům na jednom fyzickém disku, protože I/O operace jsou rozděleny na více než jeden disk.

Prokládané svazky se vytvářejí k zajištění vyššího výkonu, ne pro jejich vyšší spolehlivost – neobsahují redundantní informace.

Zrcadlený svazek

Jedná se o svazek označovaný také jako RAID 1. Je odolný proti chybám a jeho data jsou duplikována na dva stejné fyzické disky. Všechna data jednoho disku se zkopírují na druhý disk, aby byla zajištěna redundance dat. Zrcadlit lze téměř každý svazek včetně systémových a spouštěcích svazků a v případě, že jeden disk selže, lze k datům stále přistupovat na zbývajících discích. Hardwarová omezení velikosti a výkonu jsou při použití zrcadlených svazků bohužel ještě přísnější.

Zrcadlený-prokládaný svazek

Svazek s tolerancí chyb, který se označuje také jako RAID 1+0. Kombinuje výhodu vysoké rychlosti I/O prokládaného rozložení a redundanci typu zrcadlení. Nevýhodou je vlastnost zrcadlené architektury – nízký poměr zrcadlených disků na svazek.

RAID-5

Svazek s tolerancí chyb, jehož data jsou prokládána do pole tří nebo více disků. Disky nemusí být identické, ale na každém disku ve svazku musí být stejně velké bloky nepřiděleného místa. Parita (vypočítaná hodnota použitá při obnově dat po chybě) je také prokládána do pole disků a vždy se uchovává na jiném disku než samotná data. Pokud fyzický disk selže, část svazku RAID-5 na chybném disku lze obnovit ze zbývajících dat a parity. Svazek RAID-5 nabízí spolehlivost a může překonat i omezení velikosti fyzického disku díky většímu poměru zrcadlených disků na svazek.

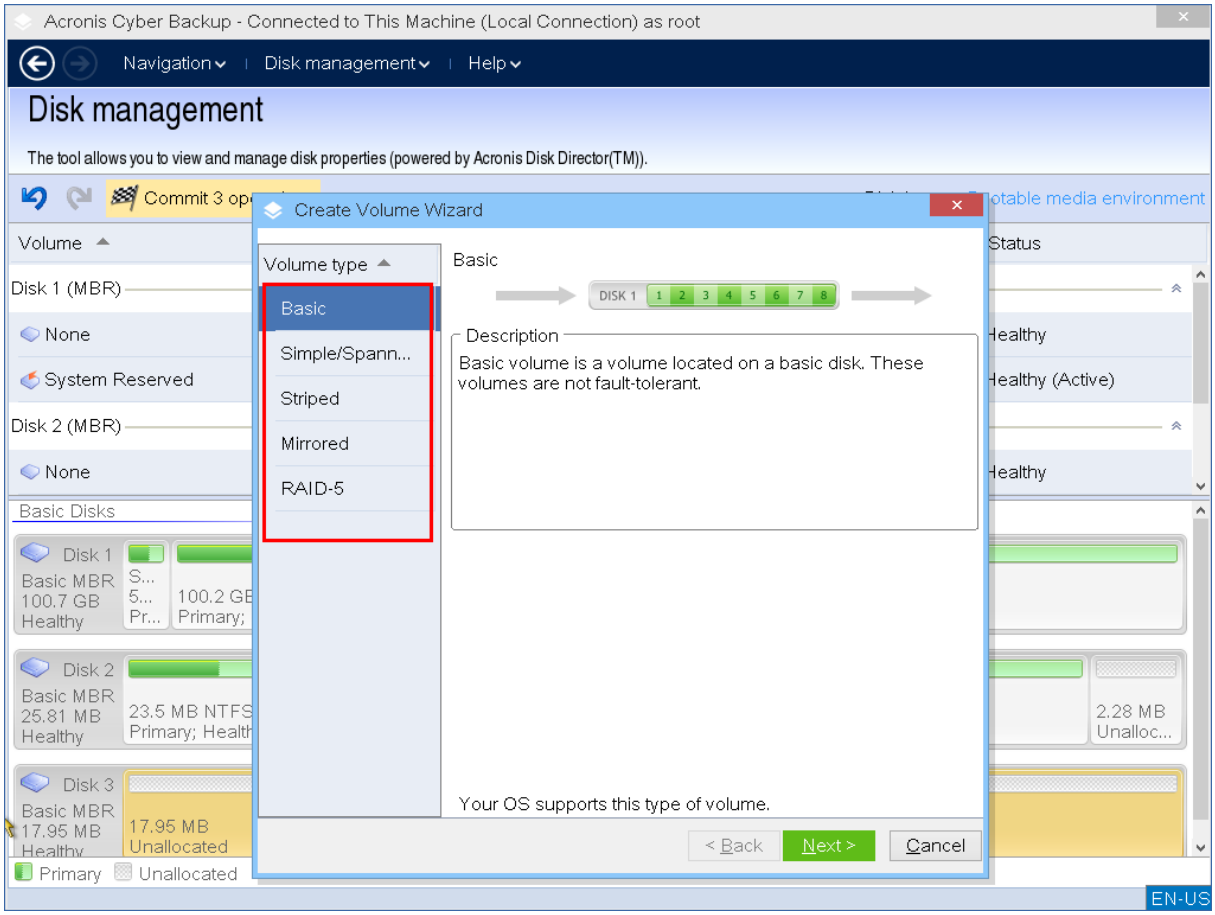
Vytvoření nového svazku

Nový svazek lze využít, pokud chcete:

- Obnovit dříve uloženou kopii zálohy v konfiguraci přesně „tak, jak byla“
- Uchovávat kolekce podobných souborů odděleně (například kolekci MP3 nebo video souborů na samostatném svazku)
- Uchovávat zálohy (obrazy) ostatních svazků/disků na speciálním svazku
- Nainstalovat nový operační systém (nebo odkládací soubor) na novém svazku
- Přidat do počítače nový hardware

Vytvoření svazku

1. Klikněte pravým tlačítkem na nepřidělené místo na disku a vyberte příkaz **Vytvořit svazek**. Otevře se průvodce **vytvořením svazku**.



2. Vyberte typ svazku. Dostupné jsou následující možnosti:
   - Základní
   - Jednoduchý/rozložený
   - Prokládaný
   - Zrcadlený
   - RAID-5

   Pokud aktuální operační systém vybraný typ svazku nepodporuje, zobrazí se upozornění a tlačítko **Další** bude zakázáno. Pokud chcete pokračovat, musíte vybrat jiný typ svazku.
3. Zadejte nepřidělené místo nebo vyberte cílové disky.
   - V případě základního svazku zadejte nepřidělené místo na vybraném disku.
   - V případě jednoduchého/rozloženého svazku vyberte jeden a více cílových disků.
   - V případě zrcadleného svazku vyberte dva cílové disky.
   - V případě prokládaného svazku vyberte dva a více cílových disků.
   - V případě svazku RAID-5 vyberte tři cílové disky.

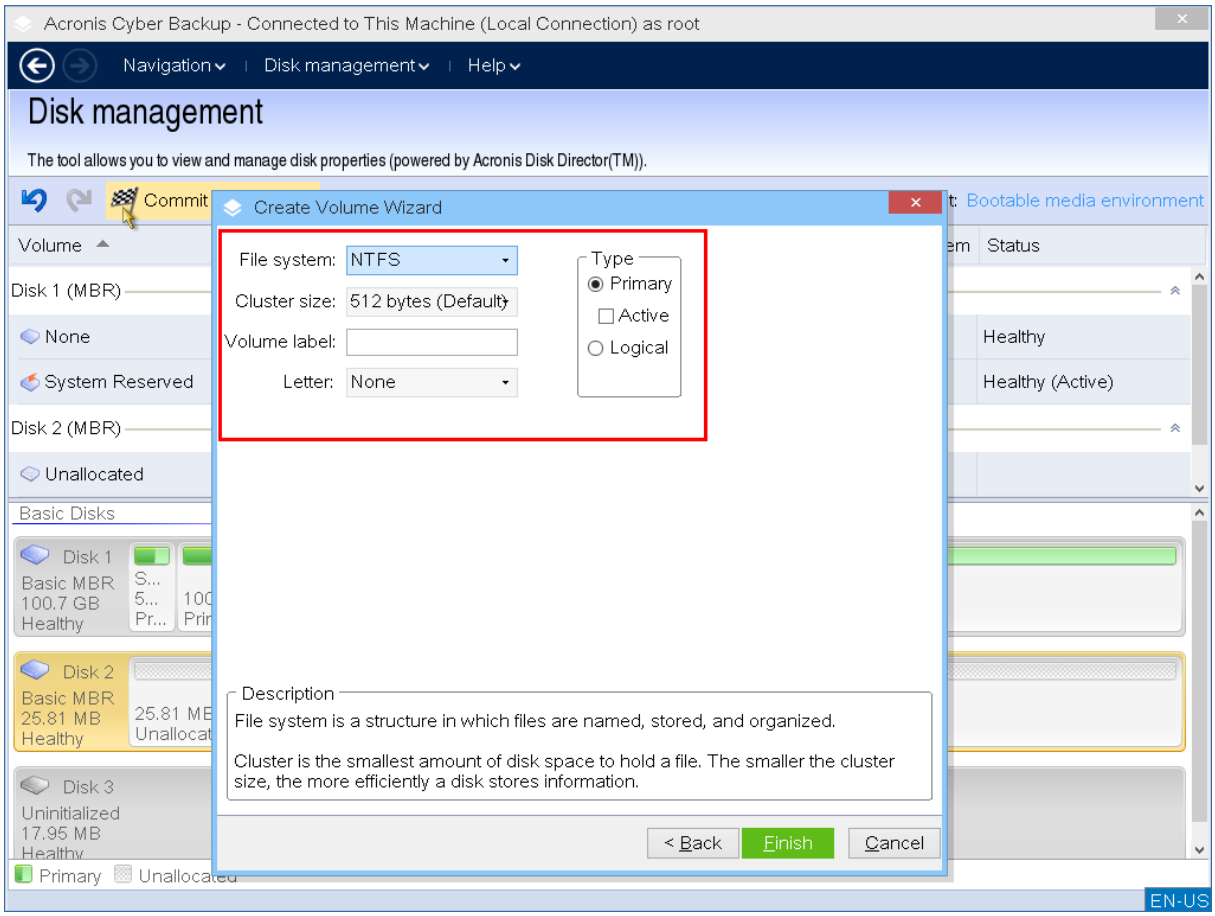
   Když vytváříte **dynamický** svazek a jako cíl vyberete jeden nebo více **základních** disků, zobrazí se upozornění, že vybraný disk se automaticky převede na dynamický.
4. Nastavení velikosti svazku.

   Maximální hodnota běžně odráží maximální možné nepřidělené místo. V některých případech se navržená maximální hodnota může lišit – například když velikost jednoho zrcadlení určuje

velikost druhého zrcadlení nebo je posledních 8 MB diskového prostoru vyhrazeno pro pozdější převod základního disku na dynamický.

Pokud je nepřidělené místo na disku větší než svazek, můžete na tomto disku vybrat pozici nového základního svazku.

5. Nastavte možnosti svazku.



Můžete přiřadit **písmeno** svazku (výchozí je první volné písmeno abecedy) a případně také **jmenovku** (výchozí je prázdná). Zadat musíte také **systém souborů** a **velikost clusteru**.

Dostupné možnosti systému souborů:

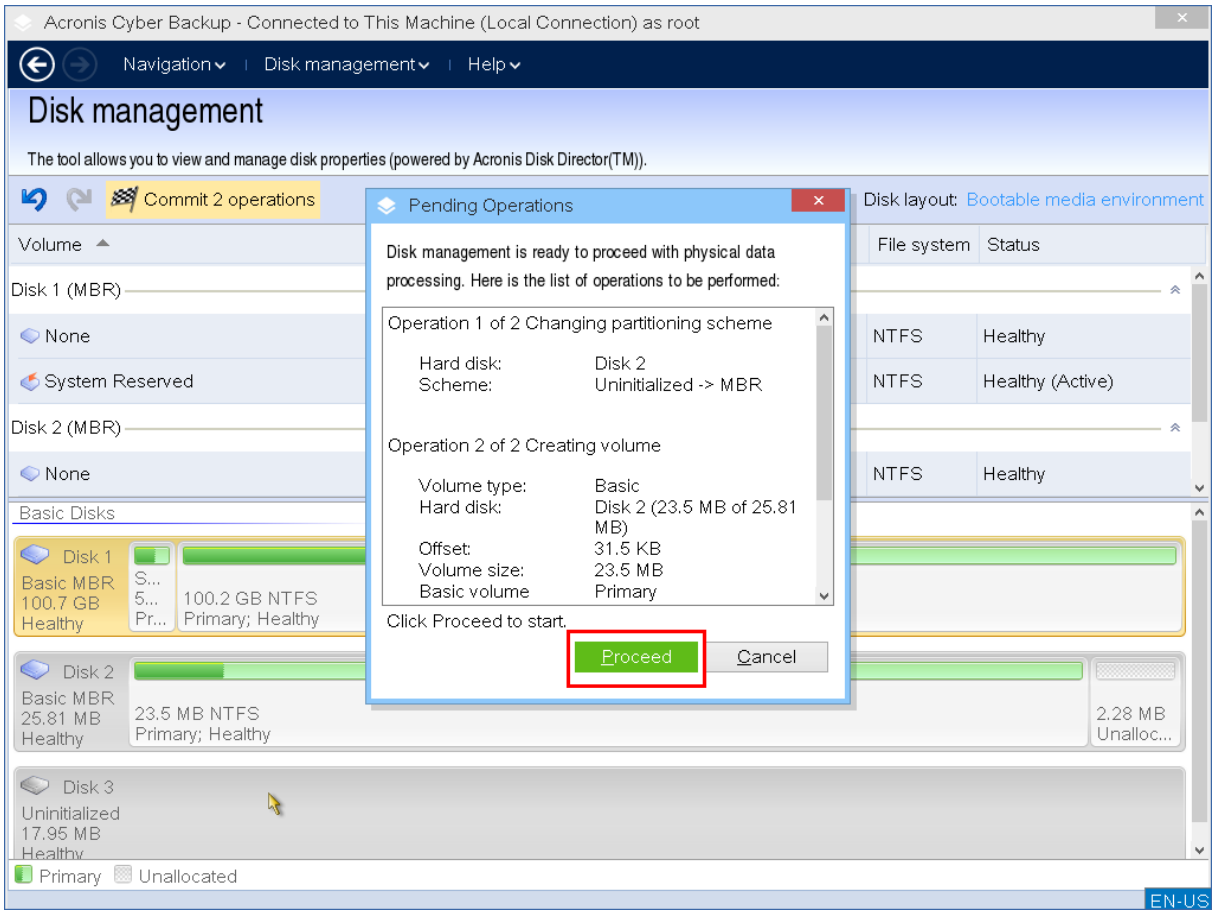
- FAT16 (vypnuto, pokud je velikost svazku nastavena na více než 2 GB)
- FAT32 (vypnuto, pokud je velikost svazku nastavena na více než 2 TB)
- NTFS
- Ponechat svazek neformátovaný.

Při nastavení velikosti clusteru můžete pro každý systém souborů vybrat libovolnou přednastavenou hodnotu. Velikost clusteru, která je navržena ve výchozím nastavení, je nejvhodnější pro svazek s vybraným systémem souborů. Jestliže nastavíte velikost clusteru 64 kB pro FAT16/FAT32 nebo 8 kB až 64 kB pro NTFS, Windows může svazek připojit, ale některé aplikace (například instalační programy) mohou nesprávně vypočítat místo v něm.

Pokud vytváříte základní svazek, který lze nastavit na systémový, můžete také vybrat typ svazku – **Primární** (**Aktivní primární**) nebo **Logický**. Typ **Primární** se běžně vybírá k instalaci operačního systému do svazku. Vyberte hodnotu **Aktivní** (výchozí), pokud chcete do tohoto svazku nainstalovat operační systém, který se má spustit při spuštění počítače. Jestliže není tlačítko **Primární** vybráno, možnost **Aktivní** nebude aktivní. Pokud je svazek zamýšlen k ukládání dat, vyberte možnost **Logický**.

Poznámka *Základní disk může obsahovat až čtyři primární svazky. Pokud již existují, disk bude nutné převést na dynamický, jinak budou možnosti **Aktivní** a **Primární** vypnuty a bude možné vybrat pouze typ svazku **Logický**.*

6. Klikněte na tlačítko **Provést** a pak v okně **Naplánované operace** klikněte na **Pokračovat**. Pokud program ukončíte bez provedení operace, operaci zrušíte.



Odstranění svazku

Jak odstranit svazek

1. Klikněte pravým tlačítkem na svazek, který chcete odstranit.
2. Klikněte na možnost **Odstranit svazek**.

Poznámka *Všechny informace v tomto svazku budou nenávratně ztraceny.*

3. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci odstranění svazku.
4. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Po odstranění svazku je jeho prostor přidán k nepřidělenému diskovému prostoru. Lze ho využít k tvorbě nového svazku nebo ke změně na jiný typ svazku.

Nastavení aktivního svazku

Pokud máte více primárních svazků, musíte jeden z nich určit jako spouštěcí svazek. To provedete tak, že svazek nastavíte jako aktivní. Na disku může být pouze jeden aktivní svazek.

Nastavení aktivního svazku:

1. Klikněte pravým tlačítkem na požadovaný primární svazek na základním MBR a klikněte na příkaz **Označit jako aktivní**.

   Pokud v systému není další aktivní svazek, operace nastavení aktivního svazku se přidá do naplánovaných operací. Jestliže je v systému další aktivní svazek, zobrazí se upozornění, že dříve aktivní svazek je třeba nejdříve nastavit jako pasivní.

   Poznámka *Pokud nastavíte jako aktivní nový svazek, písmeno dříve aktivního svazku se může změnit a některé nainstalované aplikace nemusí být možné spustit.*

2. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci nastavení aktivního svazku.

   Poznámka *I když je na novém aktivním svazku operační systém, nemusí být v některých případech možné ho v počítači spustit. Nastavení nového aktivního svazku je nutné potvrdit.*

3. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Změna písmena svazku

Operační systémy Windows při spuštění přiřazují svazkům pevného disku písmena (C:, D: atd.). Tato písmena využívají aplikace a operační systémy k nalezení souborů a složek ve svazcích. Připojením dalšího disku a vytvořením nebo odstraněním svazku na existujícím disku se může konfigurace systému změnit. To může způsobit, že některé aplikace přestanou správně fungovat nebo nemusí být možné automaticky vyhledávat a otevírat uživatelské soubory. Chcete-li tomu předejít, můžete písmena přiřazená svazkům operačním systémem ručně změnit.

Změna písmena přiřazeného svazku operačním systémem

1. Klikněte pravým tlačítkem na požadovaný svazek a vyberte příkaz **Změnit písmeno**.
2. V okně **Změnit písmeno** vyberte nové písmeno.
3. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci přiřazení písmena svazku.
4. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Změna jmenovky svazku

Jmenovka svazku není povinný atribut. Je to název přiřazený ke svazku pro snadnější rozpoznání.

Jak změnit jmenovku svazku

1. Klikněte pravým tlačítkem na požadovaný svazek a vyberte příkaz **Změnit jmenovku**.
2. Zadejte novou jmenovku do textového pole okna **Změnit jmenovku** .
3. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci změny jmenovky svazku.
4. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

Formátování svazku

Svazek můžete formátovat v případě, že chcete změnit systém souborů:

- abyste ušetřili další místo ztracené kvůli velikosti clusteru v systémech souborů FAT16 a FAT32,
- abyste mohli rychle a více či méně spolehlivě zničit data umístěná v tomto svazku.

Formátování svazku:

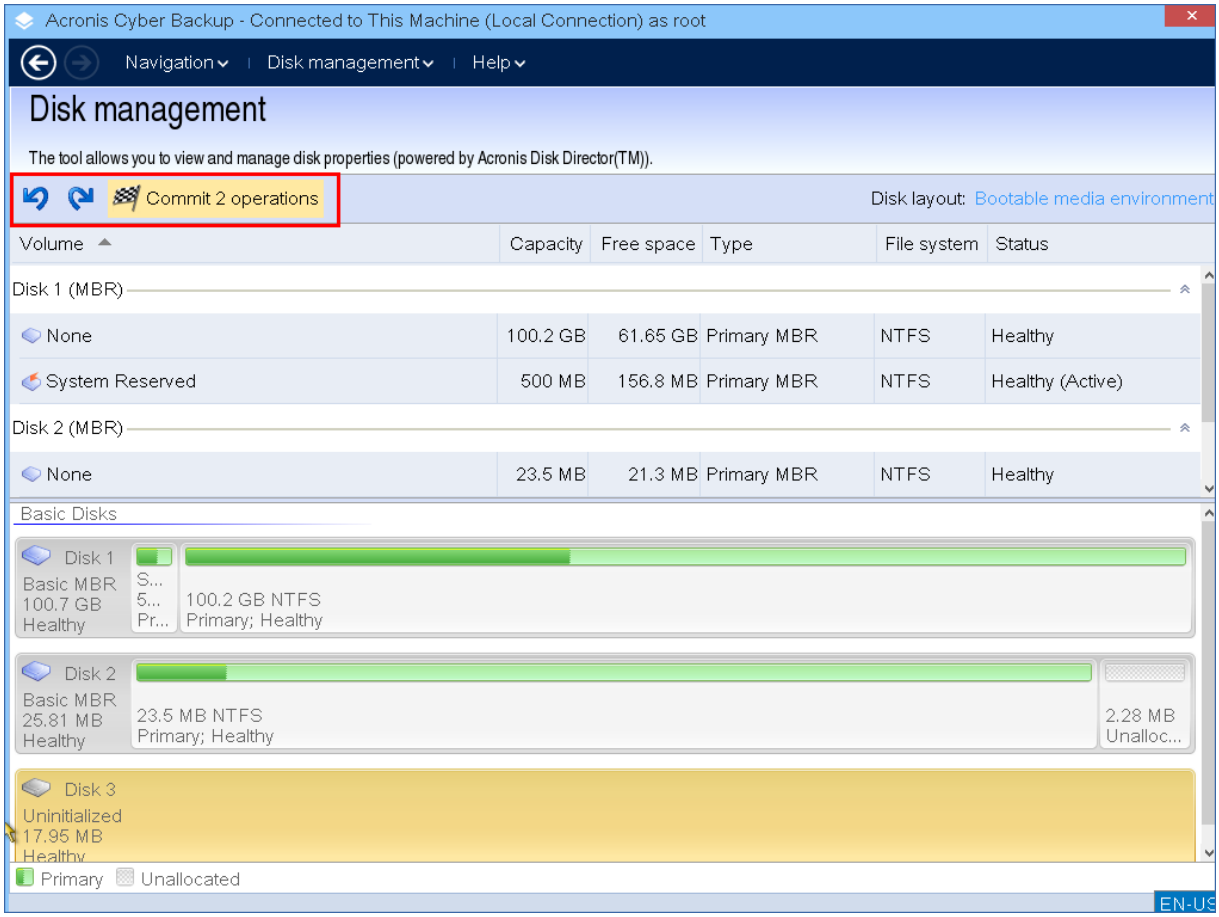
1. Klikněte pravým tlačítkem na požadovaný svazek a vyberte příkaz **Formátovat**.

2. Vyberte velikost clusteru a systém souborů. Dostupné možnosti systému souborů:
   - FAT16 (vypnuto, pokud je velikost svazku nastavena na více než 2 GB)
   - FAT32 (vypnuto, pokud je velikost svazku nastavena na více než 2 TB)
   - NTFS
3. Kliknutím na tlačítko **OK** přidáte naplánovanou operaci formátování svazku.
4. Chcete-li přidanou operaci dokončit, potvrďte (str. 292) ji. Pokud program ukončíte bez provedení operace, operaci zrušíte.

12.1.1.6 Naplánované operace

Všechny operace jsou považovány za naplánované, dokud nevydáte a nepotvrdíte příkaz **Provést**. Můžete tak řídit všechny naplánované operace, opakovaně kontrolovat zamýšlené změny a v případě potřeby operace zrušit ještě před jejich provedením.

Zobrazení **Správa disků** obsahuje panel nástrojů s ikonami pro akce **Zpět**, **Opakovat** a **Provést**, které jsou určeny pro naplánované operace. Tyto akce lze spustit také z nabídky **Správa disků**.



Všechny naplánované operace se přidají do seznamu naplánovaných operací.

Pomocí akce **Zpět** můžete vrátit poslední operaci v seznamu. Tato akce je dostupná vždy, když seznam operací není prázdný.

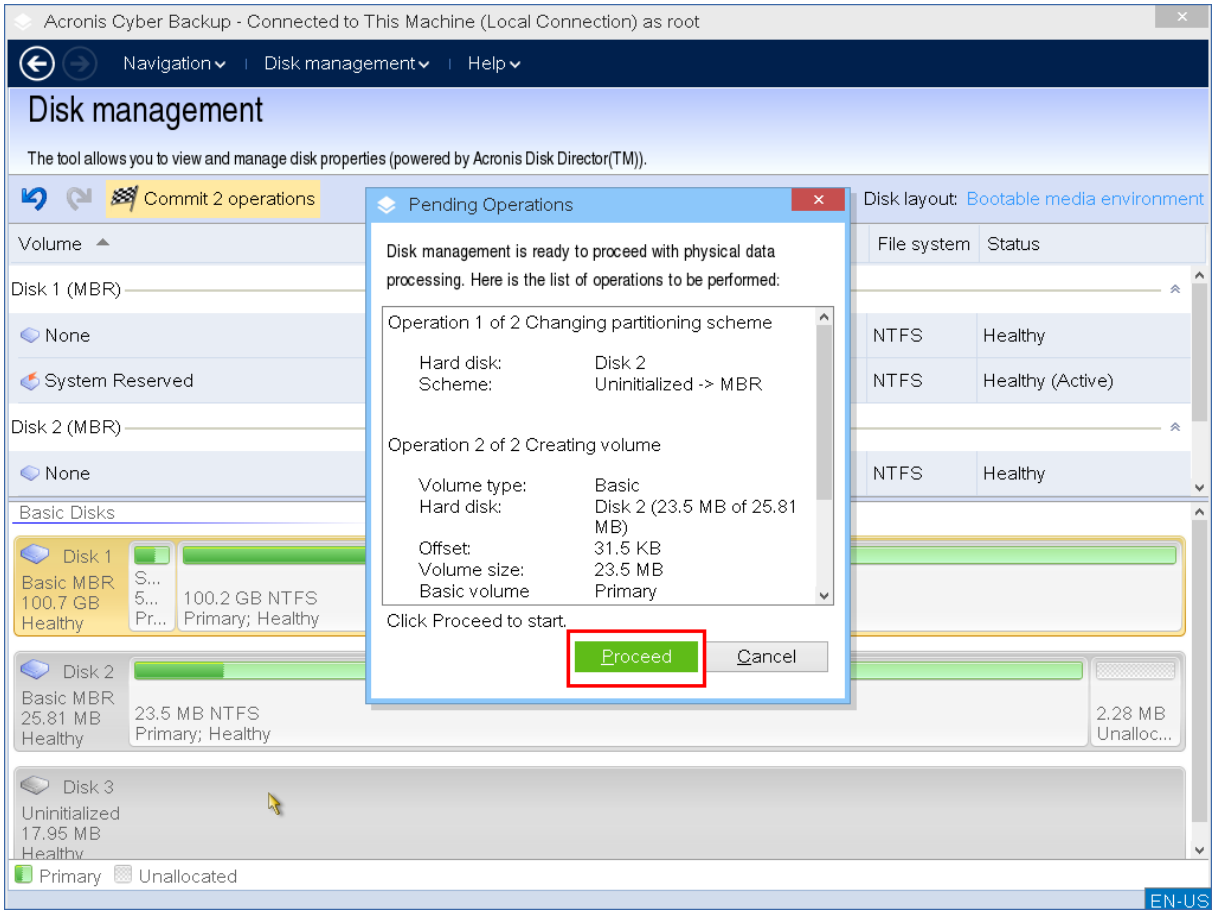
Pomocí akce **Opakovat** můžete znovu provést poslední zrušenou naplánovanou operaci.

Výběrem akce **Provést** přejdete do okna **Naplánované operace**, kde si můžete zobrazit seznam naplánovaných operací.

Chcete-li spustit jejich provedení, klikněte na možnost **Pokračovat**.

Poznámka *Pokud pro operaci vyberete možnost* ***Pokračovat****, nebude možné akce ani operace vrátit zpět.*

Pokud operace nechcete potvrdit, klikněte na tlačítko **Storno**. V tomto případě nebudou provedeny žádné změny seznamu naplánovaných operací. Jestliže aplikaci ukončíte bez provedení naplánovaných operací, operace se zruší.



12.2 Konfigurace zařízení iSCSI a NDAS

V tomto tématu je popsáno, jak konfigurovat zařízení iSCSI (Small Computer System Interface) a zařízení NDAS (Network Direct Attached Storage) při práci se spouštěcím médiem. Po provedení níže uvedených kroků budete tato zařízení moci používat, jako by byla místně připojená k počítači spuštěnému ze spouštěcího média.

Cílový server iSCSI (nebo **cílový portál**) je server, který je hostitelem zařízení iSCSI. **Cíl iSCSI** je součást na cílovém serveru. Tato součást sdílí zařízení a zobrazuje seznam iniciátorů iSCSI, které mají povolený přístup k zařízení. **Iniciátor iSCSI** je součástí počítače. Tato součást zajišťuje interakci mezi počítačem a cílem iSCSI. Při konfigurování přístupu k zařízení iSCSI na počítači spuštěném ze spouštěcího média musíte zadat cílový portál iSCSI zařízení a jeden z iniciátorů iSCSI uvedených v cíli. Pokud cílové zařízení sdílí více zařízení, získáte přístup ke všem zařízením.

Přidání zařízení iSCSI na spouštěcí médium založené na Linuxu

1. Klikněte na **Nástroje** > **Konfigurovat zařízení iSCSI/NDAS**.
2. Klikněte na **Přidat hostitele**.

3. Zadejte IP adresu a port cílového portálu iSCSI a název libovolného iniciátoru iSCSI, který má povolen přístup k zařízení.
4. Jestliže hostitel vyžaduje ověření, zadejte pro něj uživatelské jméno a heslo.
5. Klikněte na tlačítko **OK**.
6. Vyberte v seznamu cíl iSCSI a klikněte na **Připojit**.
7. Pokud je v nastaveních cíle iSCSI povoleno ověřování CHAP, budete vyzváni k zadání pověření pro přístup k cíli iSCSI. Zadejte uživatelské jméno a tajný klíč cíle shodné s nastavením cíle iSCSI. Klikněte na tlačítko **OK**.
8. Kliknutím na **Zavřít** zavřete okno.

Přidání zařízení iSCSI na spouštěcí médium založené na prostředí PE

1. Klikněte na **Nástroje** > **Spustit instalaci iSCSI**.
2. Klikněte na kartu **Hledání**.
3. V části **Cílové portály** klikněte na **Přidat** a pak zadejte IP adresu a port cílového portálu iSCSI. Klikněte na tlačítko **OK**.
4. Klikněte na kartu **Obecné**, klikněte na **Změnit** a zadejte název libovolného iniciátoru iSCSI, který má povolen přístup k zařízení.
5. Klikněte na kartu **Cíle**, klikněte na **Obnovit**, vyberte v seznamu cíl iSCSI a klikněte na **Připojit**. Kliknutím na **OK** se připojte k cíli iSCSI.
6. Pokud je v nastaveních cíle iSCSI povoleno ověřování CHAP, zobrazí se chyba **Ověřování selhalo**. V takovém případě klikněte na **Připojit**, poté klikněte na **Pokročilé**, vyberte **Povolit přihlášení CHAP** a potom zadejte uživatelské jméno a tajný klíč cíle shodné s nastavením cíle iSCSI. Kliknutím na tlačítko **OK** zavřete okno a poté se kliknutím na tlačítko **OK** připojte k cíli iSCSI.
7. Kliknutím na **OK** zavřete okno.

Přidání zařízení NDAS (pouze na spouštěcí médium založené na Linuxu)

1. Klikněte na **Nástroje** > **Konfigurovat zařízení iSCSI/NDAS**.
2. Klikněte na **Zařízení NDAS** a potom klikněte na **Přidat zařízení**.
3. Zadejte ID zařízení o délce 20 znaků.
4. Jestliže chcete povolit do zařízení zápis dat, zadejte klíč k zápisu o délce 5 znaků. Bez tohoto klíče bude zařízení dostupné v režimu pouze pro čtení.
5. Klikněte na tlačítko **OK**.
6. Kliknutím na **Zavřít** zavřete okno.

12.3 Startup Recovery Manager

Správce Startup Recovery Manager je spouštěcí součást umístěná na systémovém disku ve Windows nebo oddílu /boot v Linuxu a je nakonfigurován, aby se spustil stisknutím klávesy F11 při spouštění. To odstraňuje potřebu samostatného média nebo síťového připojení ke spuštění záchranného spouštěcího nástroje.

Správce Startup Recovery Manager je zvlášť praktický pro mobilní uživatele. Pokud dojde k selhání, restartujte počítač, počkejte na výzvu „Stisknutím klávesy F11 spustíte správce Acronis Startup Recovery Manager...“ a potom stiskněte klávesu F11. Aplikace se spustí a můžete provést obnovení.

Pomocí správce Startup Recovery Manager je možné provádět zálohování i na cestách.

V počítačích s nainstalovaným zavaděčem GRUB místo použití klávesy F11 spusťte správce Startup Recovery Manager ze spouštěcí nabídky.

Počítač spuštěný pomocí správce Startup Recovery Manager lze zaregistrovat na serveru pro správu podobně jako počítač spouštěný ze spouštěcího média. Chcete-li to provést, klikněte na možnost **Nástroje** > **Zaregistrovat médium na serveru pro správu** a potom použijte postup popsaný v části Registrace média na serveru pro správu (str. 253).

Aktivace správce Startup Recovery Manager

Správce Startup Recovery Manager lze aktivovat v počítači s nainstalovaným Agentem pro Windows nebo Agentem pro Linux pomocí webové konzole Cyber Protect.

Aktivace správce Startup Recovery Manager ve webové konzoli Cyber Protect

1. Vyberte počítač, na kterém chcete správce Startup Recovery Manager aktivovat.
2. Klikněte na **Podrobnosti**.
3. Zapněte přepínač **Startup Recovery Manager**.
4. Počkejte, až aplikace správce Startup Recovery Manager aktivuje.

Jak aktivovat správce Startup Recovery Manager v počítači bez agenta

1. Spusťte počítač ze spouštěcího média.
2. Klikněte na **Nástroje** > **Aktivovat Startup Recovery Manager**.
3. Počkejte, až software správce Startup Recovery Manager aktivuje.

Co se stane, když správce Startup Recovery Manager aktivujete

Aktivace zapne výzvu „Stisknutím klávesy F11 spustíte Acronis Startup Recovery Manager...“ (pokud nemáte zavaděč GRUB) nebo přidá položku „ Startup Recovery Manager“ do nabídky zavaděče GRUB (pokud GRUB máte).

Systémový disk (nebo oddíl /boot v Linuxu) by měl mít k aktivaci správce Startup Recovery Manager aspoň 100 MB volného místa.

Pokud nepoužíváte zavaděč GRUB a zavaděč je nainstalován v záznamu MBR (Master Boot Record), aktivace správce Startup Recovery Manager přepíše záznam MBR svým vlastním spouštěcím kódem. Pokud jsou nainstalovány zavaděče od jiných výrobců, bude možná nutná jejich reaktivace.

Pokud v Linuxu používáte jiný zavaděč než GRUB (jako například LILO), zvažte instalaci zavaděče do zaváděcího záznamu kořenového diskového oddílu Linuxu místo do MBR ještě před aktivací správce Startup Recovery Manager. Jinak zavaděč překonfigurujte ručně po aktivaci.

Deaktivace správce Startup Recovery Manager

Deaktivace se provádí podobně jako aktivace.

Deaktivace vypne výzvu „Stisknutím klávesy F11 spustíte Acronis Startup Recovery Manager…“ (nebo položku nabídky v zavaděči GRUB) při spuštění počítače. Pokud správce Startup Recovery Manager není aktivován, budete pro obnovu systému, který selže při spouštění, potřebovat provést následující:

- Spustit počítač ze samostatného spouštěcího média nebo
- Použít spuštění ze sítě ze serveru PXE nebo služby Microsoft RIS (Remote Installation Services).

12.4 Server PXE Acronis

Acronis PXE Server umožňuje spouštění počítačů do spouštěcích součástí aplikace Acronis pomocí sítě.

Síťové spouštění:

- Odstraňuje potřebu mít na místě technika, který vloží spouštěcí médium do systému, jenž má být spuštěn.
- Při skupinových operacích zkracuje oproti použití fyzických spouštěcích médií čas potřebný ke spuštění více počítačů.

Spouštěcí součásti se odesílají na Server PXE Acronis pomocí Tvůrce spouštěcích médií Acronis. Chcete-li odeslat spouštěcí součásti, spusťte Tvůrce spouštěcích médií a potom se řiďte postupem popsaným v tématu Spouštěcí média pro systém Linux (str. 232).

Spouštění více počítačů ze Serveru PXE Acronis má smysl v případě, že se v síti nachází server DHCP (Dynamic Host Control Protocol). V takovém případě síťová rozhraní spouštěných počítačů automaticky získají IP adresy.

Omezení:

Server PXE Acronis nepodporuje zavaděč UEFI.

12.4.1 Instalace serveru PXE Acronis

Instalace serveru PXE Acronis

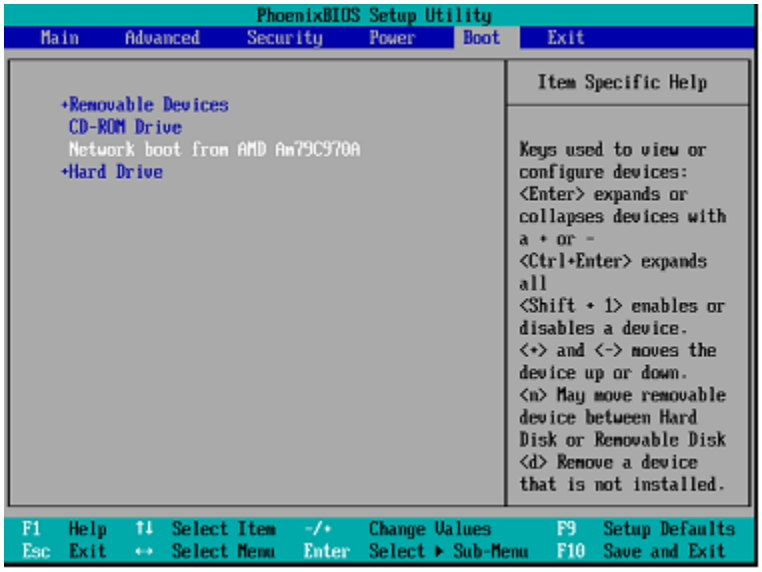
1. Přihlaste se jako správce a spusťte instalační program aplikace Acronis Cyber Protect.
2. [Volitelné] Pokud chcete změnit jazyk instalačního programu, klikněte na **Jazyk instalace**.
3. Vyjádřete souhlas s licenčními podmínkami a vyberte, jestli se počítač bude účastnit Programu zkušeností uživatelů Acronis (ACEP).
4. Klikněte na **Přizpůsobit nastavení instalace**.
5. Vedle možnosti **Co je nutno nainstalovat** klikněte na **Změnit**.
6. Zaškrtněte políčko **Server PXE**. Pokud do tohoto počítače nechcete instalovat žádné další součásti, zrušte zaškrtnutí příslušných políček. Pokračujte kliknutím na **Hotovo**.
7. [Volitelné] Změňte další nastavení instalace.
8. Kliknutím na **Instalovat** zahajte instalaci.
9. Po dokončení instalace klikněte na **Zavřít**.

Server PXE Acronis se ihned po instalaci spustí jako služba. Později se bude spouštět automaticky při každém spuštění systému. Server PXE Acronis můžete spouštět a zastavovat stejným způsobem jako jiné služby Windows.

12.4.2 Nastavení zavádění počítače z PXE

U počítačů bez systému stačí, aby BIOS počítače podporoval spouštění po síti.

Na počítači s nainstalovaným operačním systémem na pevném disku je nutné nastavit BIOS tak, aby byla síťová karta prvním zaváděcím zařízením nebo aby alespoň byla před pevným diskem. Následující příklad zobrazuje jednu z možných konfigurací BIOSu. Pokud nevložíte spouštěcí médium, zařízení se spustí ze sítě.



V některých verzích BIOSu je nutné po zapnutí síťové karty uložit změny BIOSu, aby se karta zobrazila v seznamu zaváděcích zařízení.

Pokud hardware obsahuje více síťových karet, zkontrolujte, zda je kabel připojen ke kartě podporované BIOSem.

12.4.3 Práce v podsítích

Aby mohl Acronis PXE Server pracovat v jiné podsíti (přes přepínač), nakonfigurujte přepínač tak, aby přenášel provoz PXE. IP adresy PXE serveru se nastavují podle rozhraní pomocí funkce IP helper stejně jako adresy DHCP serveru. Více informací naleznete na adrese: https://support.microsoft.com/en-us/help/257579/pxe-clients-do-not-receive-an-ip-address-from-a-dhcp-server.

13 Ochrana mobilních zařízení

Pomocí zálohovací aplikace můžete zálohovat svá data do cloudového úložiště a v případě ztráty nebo poškození si je opět stáhnout. K zálohování do cloudového úložiště potřebujete účet a předplatné služby Cloud.

Podporovaná mobilní zařízení

Zálohovací aplikaci můžete nainstalovat na mobilním zařízení s jedním z následujících operačních systémů:

- iOS 10.3 a novější (iPhone, iPod a iPad)
- Android 5.0 a novější

Co můžete zálohovat

- Kontakty

- Fotografie
- Videa
- Kalendáře
- Připomínky (jen na zařízeních se systémem iOS)

Co byste měli vědět

- Data se dají zálohovat jen do cloudového úložiště.
- Při každém otevření aplikace se zobrazí přehled změn, ke kterým v datech došlo, a vy budete moct ručně spustit zálohování.
- Funkce **Souvislá záloha** je ve výchozím nastavení zapnutá. Pokud je toto nastavení zapnuté:
  - V systému Android 7.0 a novějším: zálohovací aplikace automaticky průběžně zjišťuje nová data a nahraje je do služby Cloud.
  - V systému Android 5 a 6: aplikace kontroluje změny každé tři hodiny. Souvislé zálohování můžete vypnout v nastavení aplikace.
- Možnost **Použít pouze Wi-Fi** je ve výchozím nastavení zapnutá. Pokud je toto nastavení zapnuté, bude zálohovací aplikace zálohovat vaše data, pouze když je k dispozici připojení k Wi-Fi. Pokud je připojení k síti Wi-Fi ztraceno, proces zálohování se nespustí. Pokud chcete, aby zálohovací aplikace používala i mobilní data, tuto možnost vypněte.
- Energii můžete šetřit dvěma způsoby:
  - S využitím funkce **Zálohovat při nabíjení**, která je ve výchozím nastavení vypnutá. Pokud je toto nastavení zapnuté, bude zálohovací aplikace zálohovat vaše data, pouze když je zařízení připojeno ke zdroji napájení. Pokud je zařízení během souvislého zálohování odpojeno od zdroje napájení, zálohování se pozastaví.
  - Pomocí **režimu úspory energie**, který je ve výchozím nastavení zapnutý. Pokud je toto nastavení zapnuté, bude zálohovací aplikace zálohovat vaše data, pouze když je úroveň nabití baterie dostatečná. Jakmile se úroveň nabití baterie sníží, souvislé zálohování se pozastaví. Tato možnost je k dispozici pro zařízení se systémem Android 8 a novějším.
- K zálohovaným datům se dostanete z každého mobilního zařízení, které máte zaregistrované pod svým účtem. Díky tomu můžete snadno přenést data ze starého mobilního zařízení do nového. Kontakty a fotky ze zařízení se systémem Android nelze obnovit do systému iOS a naopak. Fotky, videa a kontakty si můžete stáhnout do libovolného zařízení, a to pomocí webové konzole Cyber Protect.
- K datům zálohovaným z mobilních zařízení registrovaných prostřednictvím vašeho účtu lze získat přístup pouze z tohoto účtu. Tato data nemůže zobrazit ani obnovit nikdo kromě vás.
- V zálohovací aplikaci lze obnovit jen nejnovější verze dat. Potřebujete-li obnovit data z konkrétní verze zálohy, použijte k tomu webovou konzoli Cyber Protect na tabletu nebo na počítači.
- [Pouze pro zařízení se systémem Android] Máte-li během zálohování v zařízení vloženou SD kartu, budou se zálohovat i data uložená na této kartě. Data budou obnovena na libovolnou SD kartu (do složky **Recovered by Backup** (Obnoveno ze zálohy), pokud je během obnovení vložena v zařízení, nebo aplikace požádá o zadání jiného umístění, do kterého mají být data obnovena.

Kde si můžete zálohovací aplikaci stáhnout

1. V mobilním zařízení otevřete prohlížeč a přejděte na adresu https://backup.acronis.com/.
2. Přihlaste se pomocí svého účtu.
3. Klikněte na **Všechna zařízení** > **Přidat**.
4. V části **Mobilní zařízení** vyberte typ zařízení.

   Podle typu zařízení budete přesměrováni do obchodu App Store nebo Google Play.

5. [Pouze zařízení se systémem iOS] Klikněte na tlačítko **Získat**.
6. Chcete-li nainstalovat zálohovací aplikaci, klikněte na **Instalovat**.

Spuštění zálohování dat

1. Otevřete aplikaci.
2. Přihlaste se pomocí svého účtu.

Klepnutím na tlačítko **Vytvořit** vytvořte první zálohu.

1. Vyberte kategorie dat, které chcete zálohovat. Ve výchozím nastavení jsou vybrané všechny kategorie.
2. [volitelný krok] Pokud chcete zálohu chránit šifrováním, povolte možnost **Zašifrovat zálohu**. V takovém případě také:
   1. Zadejte dvakrát šifrovací heslo.

      Heslo si budete muset zapamatovat, protože zapomenuté heslo nebude možné obnovit ani změnit.

   1. Klepněte na tlačítko **Šifrovat**.
1. Klepněte na tlačítko **Zálohovat**.
2. Povolte aplikaci přístup k osobním datům. Jestliže k některým kategoriím dat zakážete přístup, nebudou příslušná data zálohována.

Zálohování bude zahájeno.

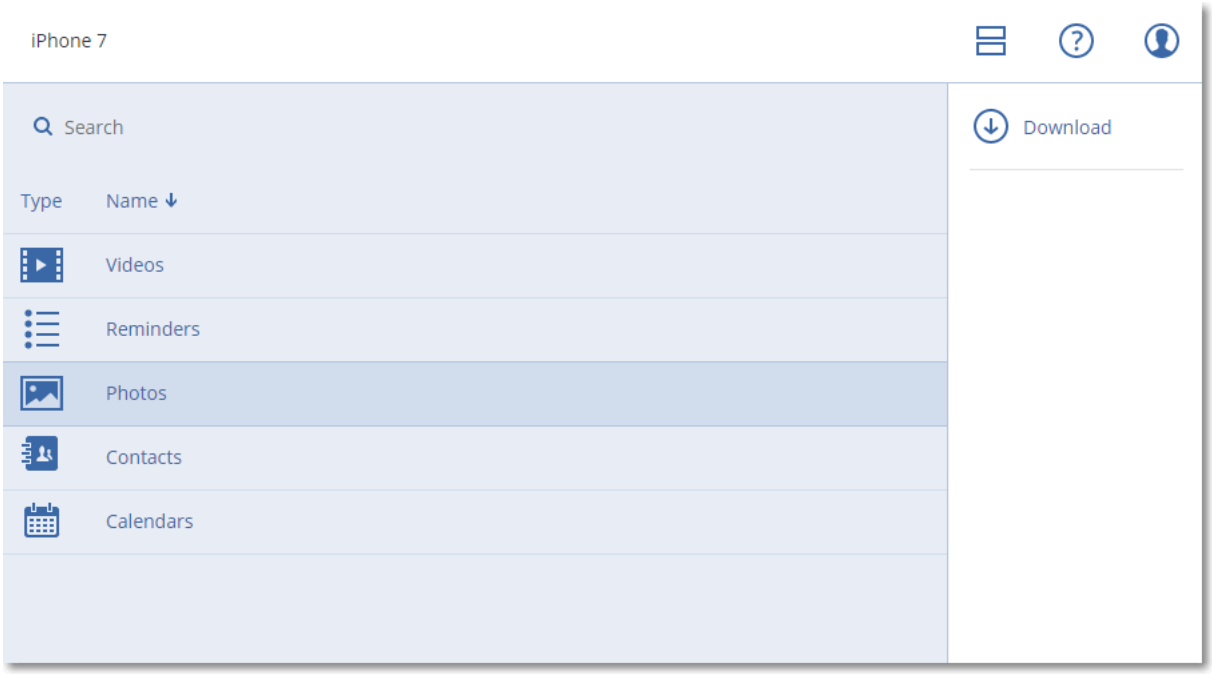
Obnovení dat do mobilního zařízení

1. Otevřete zálohovací aplikaci.
2. Klepněte na tlačítko **Procházet**.
3. Klepněte na název zařízení.
4. Proveďte jeden z následujících úkonů:
   - Chcete-li obnovit všechna zálohovaná data, klepněte na tlačítko **Obnovit vše**. Žádné další akce již nejsou třeba.
   - Chcete-li obnovit jednu nebo více kategorií dat, klepněte na možnost **Vybrat** a potom zaškrtněte políčka u požadovaných kategorií. Klepněte na tlačítko **Obnovit**. Žádné další akce již nejsou třeba.
   - Chcete-li obnovit jednu nebo více datových položek náležících do stejné kategorie dat, klepněte na požadovanou kategorii. Postupujte podle následujících kroků.
5. Proveďte jeden z následujících úkonů:
   - Jestliže chcete obnovit jedinou datovou položku, klepněte na ni.
   - Chcete-li obnovit více datových položek, klepněte na možnost **Vybrat** a potom zaškrtněte políčka u požadovaných datových položek.
6. Klepněte na tlačítko **Obnovit**.

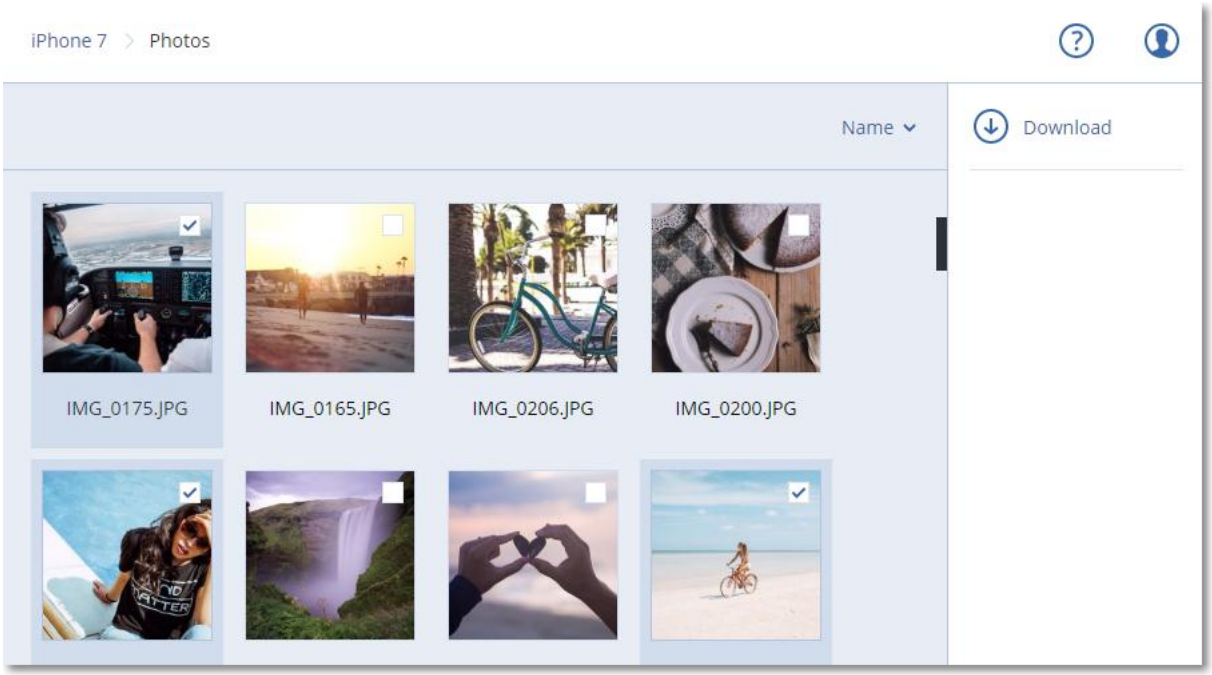
Kontrola dat pomocí webové konzole Cyber Protect

1. Na počítači otevřete prohlížeč a zadejte adresu URL webové konzole Cyber Protect.
2. Přihlaste se pomocí svého účtu.
3. V části **Všechna zařízení** klikněte pod názvem svého mobilního zařízení na položku **Obnova**.
4. Proveďte jeden z následujících úkonů:

- Chcete-li stáhnout všechny fotografie, videa, kalendáře nebo připomínky, vyberte odpovídající kategorii dat. Klikněte na tlačítko **Stáhnout**.



- Chcete-li stáhnout jednotlivé fotografie, videa, kontakty, kalendáře nebo připomínky, klikněte na název odpovídající kategorie dat a zaškrtněte políčka u požadovaných datových položek. Klikněte na tlačítko **Stáhnout**.



- Chcete-li zobrazit náhled fotografie nebo kontaktu, klikněte na název odpovídající kategorie dat a na požadovanou datovou položku.

14 Ochrana aplikací Microsoft

Důležité *Některé z funkcí popsané v této části jsou k dispozici pouze u místního nasazení.*

Ochrana aplikací Microsoft SQL Server a Microsoft Exchange Server

Tyto aplikace lze chránit dvěma způsoby:

- **Zálohování databází**

  Toto je zálohování databází a přidružených metadat na úrovni souborů. Databáze je možné obnovit do aktivní aplikace nebo jako soubory.

- **Zálohování s podporou aplikací**

  Toto je zálohování na úrovni disků, které také shromažďuje metadata aplikací. Tato metadata umožňují prohledávání a obnovu dat aplikací bez obnovení celého disku nebo svazku. Disk nebo svazek lze také obnovit jako celek. To znamená, že pro účely obnovy po havárii a ochrany dat lze použít jedno řešení s jediným plánem ochrany.

Pro Microsoft Exchange Server můžete zvolit **zálohu poštovní schránky**. Toto je zálohování jednotlivých poštovních schránek přes protokol Webové služby systému Exchange. Poštovní schránky nebo položky poštovních schránek je možné obnovit na aktivní server Exchange nebo do služby Microsoft Office 365. Záloha poštovní schránky je podporována pro Microsoft Exchange Server 2010 Service Pack 1 (SP1) nebo novější.

Ochrana služby Microsoft SharePoint

Farma Microsoft SharePoint se skládá ze serverů front-end, na kterých běží služby SharePoint, z databázových serverů, na kterých běží Microsoft SQL Server, a (volitelně) z aplikačních serverů, které přebírají některé služby SharePoint od serverů front-end. Některé front-end a aplikační servery mohou být shodné.

Jak chránit celou farmu SharePoint:

- Zálohujte všechny databázové servery pomocí zálohy s podporou aplikací.
- Zálohujte všechny jedinečné front-end a aplikační servery pomocí obvyklé zálohy na úrovni disku.

Zálohy všech serverů je třeba provádět podle stejného plánu.

Chcete-li chránit pouze obsah, můžete obsahové databáze zálohovat samostatně.

Ochrana řadiče domény

Počítač, na kterém běží doménové služby Active Directory, je možné zálohovat pomocí zálohy s podporou aplikací. Pokud doména obsahuje více řadičů a obnovíte jeden z nich, provede se neautoritativní obnova a po obnovení nedojde k vrácení čísla USN zpět.

Obnova aplikací

V následující tabulce jsou shrnuty dostupné možnosti obnovy aplikací.

	Ze zálohy databáze	Ze zálohy s podporou aplikací	Ze zálohy disku
Microsoft SQL Server	Databáze na aktivní instanci SQL Serveru (str. 310) Databáze jako soubory (str. 310)	Celý počítač (str. 198) Databáze na aktivní instanci SQL Serveru (str. 310) Databáze jako soubory (str. 310)	Celý počítač (str. 198)

Aplikace Microsoft Exchange Server	Databáze na aktivní server Exchange (str. 313) Databáze jako soubory (str. 313) Granulární obnova na aktivní server Exchange nebo do Office 365 (str. 316)*	Celý počítač (str. 198) Databáze na aktivní server Exchange (str. 313) Databáze jako soubory (str. 313) Granulární obnova na aktivní server Exchange nebo do Office 365 (str. 316)*	Celý počítač (str. 198)
Databázové servery Microsoft SharePoint	Databáze na aktivní instanci SQL Serveru (str. 310) Databáze jako soubory (str. 310) Granulární obnova pomocí služby SharePoint Explorer	Celý počítač (str. 198) Databáze na aktivní instanci SQL Serveru (str. 310) Databáze jako soubory (str. 310) Granulární obnova pomocí služby SharePoint Explorer	Celý počítač (str. 198)
Front-end webové servery Microsoft SharePoint	-	-	Celý počítač (str. 198)
Doménové služby Active Directory	-	Celý počítač (str. 198)	-

* Granulární obnova je k dispozici rovněž ze zálohy poštovní schránky.

14.1 Předpoklady

Před konfigurací zálohy aplikací zkontrolujte, zda jsou splněny níže uvedené požadavky.

Stav zapisovačů VSS zkontrolujete pomocí příkazu **`vssadmin list writers`**.

Společné požadavky

U serveru Microsoft SQL Server zkontrolujte, zda:

- Je spuštěna alespoň jedna instance serveru Microsoft SQL Server.
- Zapisovač SQL pro VSS je zapnutý.

U serveru Microsoft Exchange Server zkontrolujte, zda:

- Je spuštěna služba úložiště informací aplikace Microsoft Exchange.
- Je nainstalováno prostředí Windows PowerShell. U verze Exchange 2010 nebo novější musí být verze Windows PowerShell alespoň 2.0.
- Je nainstalováno rozhraní Microsoft .NET Framework.

  U verze Exchange 2007 musí být verze rozhraní Microsoft .NET Framework alespoň 2.0.

  U verze Exchange 2010 nebo novější musí být verze rozhraní Microsoft .NET Framework alespoň 3.5.
- Zapisovač Exchange pro VSS je zapnutý.

Poznámka *Pro správnou funkci Agenta pro Exchange je potřeba dočasné úložiště. Ve výchozím nastavení jsou dočasné soubory umístěny v adresáři* ***`%ProgramData%\Acronis\Temp`****. Přesvědčte se, že jste na svazku, na kterém se nachází složka* `%ProgramData%`*, ponechali alespoň tolik volného místa, kolik činí 15 % velikosti databáze Exchange. Také je možné změnit umístění dočasných souborů před vytvořením záloh serveru Exchange podle postupu popsaného v článku na adrese https://kb.acronis.com/content/40040..*

U řadiče domény zkontrolujte, zda:

- Je zapnutý zapisovač Active Directory pro VSS.

Při tvorbě plánu zálohování zkontrolujte, zda:

- U fyzických počítačů je zapnuta možnost zálohování Služba Stínová kopie svazku (VSS) (str. 194).
- U virtuálních počítačů je zapnuta možnost zálohování Služba Stínová kopie svazku (VSS) pro virtuální počítače (str. 195).

Další požadavky pro zálohy s podporou aplikací

Při tvorbě plánu zálohování zkontrolujte, že je vybrána možnost **Celý počítač**. Možnost obnovení dat **Sektor po sektoru** je nutné v plánu zálohování zakázat. V opačném případě nebude možné z těchto záloh provést obnovení dat aplikací. Pokud je plán spuštěn v režimu **Sektor po sektoru** z důvodu automatického přechodu do tohoto režimu, nebude obnovení dat aplikace možné ani v tomto případě.

Pokud aplikace běží na virtuálním počítači, který je zálohován Agentem pro VMware, zkontrolujte, že:

Zálohovaný virtuální počítač splňuje požadavky pro aplikačně konzistentní zálohu a obnovení uvedené v článku „Implementace záloh Windows“ v dokumentaci VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html

- V počítači je nainstalována nejnovější verze sady VMware Tools.
- V počítači je zakázáno řízení uživatelských účtů (UAC). Pokud UAC vypnout nechcete, je nutné při zapnutí zálohování aplikací zadat pověření vestavěného účtu správce domény (DOMAIN\Administrator).

14.2 Zálohování databáze

Před zálohováním databází zkontrolujte, že jsou splněny požadavky uvedené v části Předpoklady (str. 302).

Vyberte databáze podle níže uvedených pokynů a podle potřeby (str. 125) zadejte další nastavení plánu ochrany.

14.2.1 Výběr databází SQL

Záloha databáze SQL obsahuje databázové (.mdf, .ndf) a protokolové soubory (.ldf) a další související soubory. Soubory se zálohují pomocí služby SQL Writer. Služba musí být spuštěna ve chvíli, kdy služba stínové kopie svazku (VSS) požádá o zálohování nebo obnovu.

Soubory transakčních protokolů SQL se po každém úspěšném zálohování zkrátí. Zkrácení protokolů SQL je možné zakázat v možnostech plánu ochrany (str. 181).

Jak vybrat databáze SQL

1. Klikněte na možnost **Zařízení** > **Microsoft SQL**.

   Software zobrazí strom skupin AAG (Always On Availability Groups) na SQL Serverech, počítače, kde běží Microsoft SQL Server, instance SQL Serveru a databáze.
2. Vyhledejte data, která chcete zálohovat.

   Rozbalte uzly stromu nebo klikněte dvakrát na položky v seznamu napravo od stromu.
3. Vyberte data, která chcete zálohovat. Můžete vybrat skupiny AAG, počítače, kde běží SQL Server, instance SQL Serveru nebo jednotlivé databáze.

- Vyberete-li určitou skupinu AAG, budou zálohovány všechny databáze v ní zahrnuté. Další informace o zálohování skupin AAG nebo jednotlivých databází skupin AAG najdete v části Ochrana skupin dostupnosti AAG (Always On Availability Groups) (str. 305).
- Vyberete-li počítač, kde běží SQL Server, budou zálohovány všechny databáze připojené ke všem instancím SQL Serveru, které běží na vybraném počítači.
- Vyberete-li instanci SQL Serveru, budou zálohovány všechny databáze připojené k této instanci.
- Pokud vyberete přímo databáze, budou se zálohovat jenom tyto.

4. Klikněte na možnost **Zálohovat**. Pokud se zobrazí výzva, zadejte pověření k přístupu k serveru SQL. Účet musí být členem skupiny **Backup Operators** nebo **Administrators** na počítači a členem role **sysadmin** v každé instanci, kterou chcete zálohovat.

14.2.2 Výběr dat serveru Exchange

Následující tabulka shrnuje data serveru Microsoft Exchange, která lze vybrat pro zálohování, a minimální uživatelská oprávnění, která jsou k zálohování potřeba.

Verze Exchange	Datové položky	Uživatelská oprávnění
2007	Skupiny úložišť	Členství ve skupině role **Správci organizace Exchange**
2010/2013/2016/2019	Databáze, Skupina dostupnosti databáze (DAG)	Členství ve skupině role **Správa serveru**

Plná záloha obsahuje veškerá data vybraného serveru Exchange.

Přírůstková záloha obsahuje změněné bloky databázových souborů, soubory s kontrolními body a malé množství souborů protokolů, které jsou novější než odpovídající kontrolní bod databáze. Protože změny databázových souborů jsou zahrnuty do zálohy, není nutné zálohovat všechny záznamy transakčních protokolů od poslední zálohy. Po obnově je nutné přehrát pouze protokol, který je novější než kontrolní bod. Tímto se proces obnovy zrychluje a je zajištěno úspěšné zálohování databáze i se zapnutým cyklickým protokolováním.

Soubory transakčních protokolů se po každém úspěšném zálohování zkrátí.

Jak vybrat data serveru Exchange

1. Klikněte na **Zařízení** > **Microsoft Exchange**.

   Software zobrazí strom skupin dostupnosti databáze (DAG) serveru Exchange Server, počítače, kde běží server Microsoft Exchange Server a databáze serveru Exchange Server. Pokud jste nakonfigurovali Agenta pro Exchange podle pokynů v části Zálohování schránky (str. 309), zobrazí se v tomto stromu také poštovní schránky.
2. Vyhledejte data, která chcete zálohovat.

   Rozbalte uzly stromu nebo klikněte dvakrát na položky v seznamu napravo od stromu.
3. Vyberte data, která chcete zálohovat.
   - Vyberete-li určitou skupinu DAG, bude zálohována jedna kopie každé clusterované databáze. Další informace o zálohování skupin DAG najdete v části Ochrana skupin dostupnosti databáze (DAG) (str. 306).
   - Vyberete-li počítač, kde běží Microsoft Exchange Server, budou zálohovány všechny databáze připojené k danému Exchange Serveru, který běží na vybraném počítači.
   - Pokud vyberete přímo databáze, budou se zálohovat jenom tyto.

- Pokud jste nakonfigurovali Agenta pro Exchange podle pokynů v části Zálohování schránky (str. 309), můžete vybrat poštovní schránky k zálohování (str. 310).

4. Pokud se zobrazí výzva, zadejte pověření k přístupu k datům.
5. Klikněte na tlačítko **Chránit**.

14.2.3 Ochrana skupin dostupnosti AAG (Always On Availability Groups)

Přehled řešení vysoce dostupného SQL Serveru

Funkce WSFC (Windows Server Failover Clustering) umožňuje konfigurovat vysoce dostupný SQL Server pomocí redundance na úrovni instance (instance clusteru s podporou převzetí služeb při selhání, FCI) nebo na úrovni databáze (skupina dostupnosti AlwaysOn (AAG – AlwaysOn Availability Group)). Obě metody můžete kombinovat.

V instanci clusteru s podporou převzetí služeb při selhání jsou databáze SQL umístěny ve sdíleném úložišti. Přístup k tomuto úložišti lze získat pouze z aktivního uzlu clusteru. Jestliže se v aktivním uzlu vyskytne chyba, nastane převzetí služeb a aktivuje se jiný uzel.

Ve skupině dostupnosti se každá replika databáze nachází v jiném uzlu. Pokud bude primární replika nedostupná, primární role se přiřadí sekundární replice nacházející se v jiném uzlu.

Clustery tak samy slouží jako řešení pro obnovu po havárii. Mohou však nastat případy, kdy clustery nemohou poskytovat ochranu dat: například v případě poškození logické databáze nebo pokud se zhroutí celý cluster. Clustery také vzhledem k jejich okamžité replikaci do všech uzlů clusteru neochrání před škodlivými změnami obsahu.

Podporované konfigurace clusteru

Tento zálohovací software podporuje *pouze* skupinu dostupnosti AAG (Always On Availability Group) pro SQL Server 2012 nebo novější. Jiné konfigurace clusteru, například instance clusteru s podporou převzetí služeb při selhání, zrcadlení databáze a přesouvání protokolu, *nejsou* podporované.

Kolik agentů je potřeba k zálohování a obnově dat clusteru?

K úspěšnému zálohování a obnově clusteru je nutné nainstalovat Agenta pro SQL do každého uzlu clusteru WSFC.

Zálohování databází obsažených v AAG

1. Nainstalujte Agenta pro SQL do každého uzlu clusteru WSFC.

   Tip: *Po instalaci agenta do jednoho z uzlů zobrazuje software skupinu AAG a její uzly pod položkou* ***Zařízení*** *>* ***Microsoft SQL*** *>* ***Databáze****. K instalaci Agentů pro SQL do zbývajících uzlů vyberte skupinu AAG, klikněte na možnost* ***Podrobnosti*** *a pak u každého z těchto uzlů klikněte na* ***Instalovat agenta****.*

2. Vyberte skupinu AAG nebo sadu databází k zálohování podle popisu v části Výběr databází SQL (str. 303).

   Pokud chcete zálohovat všechny databáze skupin AAG, musíte také vybrat skupinu AAG. Chcete-li zálohovat sadu databází, definujte tuto sadu databází ve všech uzlech skupiny AAG.

   Upozornění *Sada databází musí být ve všech uzlech stejná. Pokud se jedna sada liší nebo není definovaná na všech uzlech, záloha clusteru nebude fungovat správně.*

3. Nakonfigurujte možnost zálohy Režim zálohování clusteru (str. 169).

Obnova databází obsažených v AAG

1. Vyberte databáze, které chcete obnovit, a pak vyberte bod obnovy, ze kterého chcete tyto databáze obnovit.

   Pokud vyberete clusterovanou databázi pod položkou **Zařízení** > **Microsoft SQL** > **Databáze** a pak kliknete na možnost **Obnovit**, zobrazí software pouze body obnovy, které odpovídají časům, kdy byla vybraná kopie databáze zálohována.

   Nejsnadnější způsob, jak zobrazit všechny body obnovení clusterované databáze, je vybrat zálohu celé AAG na kartě Úložiště záloh (str. 220). Názvy záloh AAG jsou založené na šabloně `<název AAG> – <název plánu ochrany` a mají zvláštní ikonu.

2. Pokud chcete nakonfigurovat obnovu, proveďte postup uvedený v části Obnovení databází SQL (str. 310) od kroku 5.

   Software automaticky definuje uzel clusteru, do kterého se data obnoví. Název uzlu se zobrazí v poli **Obnovit do**. Cílový uzel je možné ručně změnit.

Důležité: *Databázi obsaženou ve skupině dostupnosti Always On nelze během obnovení přepsat, protože to Microsoft SQL Server zakazuje. Před obnovením je nutné vyloučit cílovou databázi z AAG. Také je možné databázi obnovit jako novou databázi bez AAG. Po dokončení obnovy můžete znovu vytvořit původní konfiguraci AAG.*

14.2.4 Ochrana skupin dostupnosti databáze (DAG)

Přehled clusterů Exchange Serveru

Hlavní koncepcí clusterů Exchange je poskytování databáze s vysokou dostupností a rychlým převzetím služeb při selhání bez ztráty dat. Toho je obvykle dosaženo jednou nebo více kopiemi databází nebo skupin úložišť ve členech clusteru (uzlech clusteru). Pokud uzel clusteru hostující aktivní kopii databáze nebo jeho vlastní aktivní kopii selže, jiný uzel hostující pasivní kopii automaticky převezme jeho operace a s minimálním výpadkem poskytne přístup ke službám Exchange. Clustery tak samy slouží jako řešení pro obnovu po havárii.

Mohou však nastat případy, kdy řešení clusteru s podporou převzetí služeb při selhání nemohou poskytovat ochranu dat: například v případě poškození logické databáze nebo v případě, že určitá databáze v clusteru nemá kopii (repliku), nebo pokud se zhroutí celý cluster. Clustery také vzhledem k jejich okamžité replikaci do všech uzlů clusteru neochrání před škodlivými změnami obsahu.

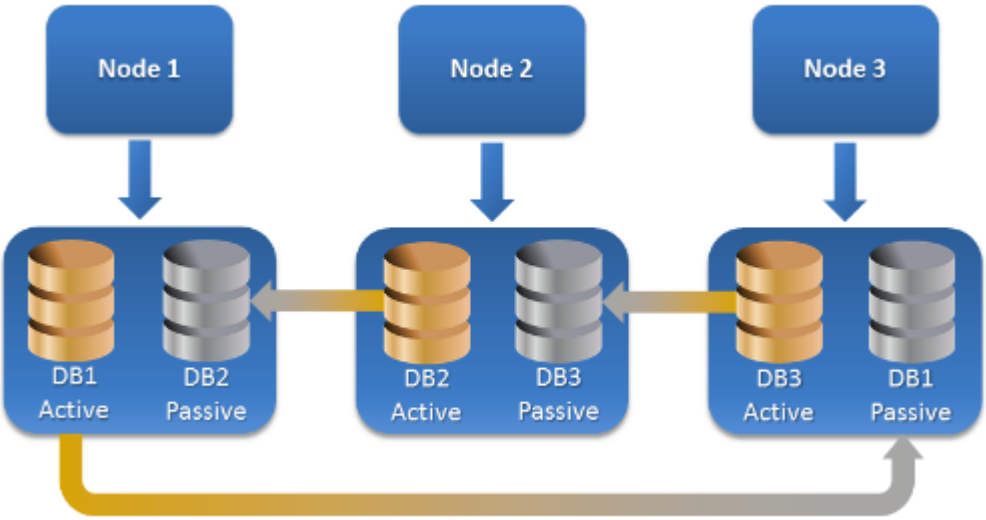
Zálohování s podporou clusteru

Při zálohování s podporou clusteru zálohujete pouze jednu kopii dat v clusteru. Pokud data změní umístění uvnitř clusteru (například přepnutí nebo převzetí dat při selhání), aplikace vyhledá všechna přemístění těchto dat a bezpečně je zálohuje.

Podporované konfigurace clusteru

Zálohování s podporou clusteru je podporováno *pouze* pro skupinu dostupnosti databáze (DAG) pro Exchange Server 2010 nebo novější. Jiné konfigurace clusteru, například cluster se sdíleným úložištěm (SCC) a průběžná replikace clusteru (CCR) pro Exchange 2007, *nejsou* podporované.

Skupina DAG je skupina až 16 serverů aplikace Exchange Mailbox. Libovolný uzel může hostovat kopii databáze schránek z libovolného jiného uzlu. Každý uzel může hostovat pasivní i aktivní kopie databáze. Je možné vytvořit až 16 kopií každé databáze.



Kolik agentů je potřeba k zálohování a obnovení s podporou clusteru?

K úspěšnému zálohování a obnovení databáze v clusteru je nutné nainstalovat Agenta pro Exchange do každého uzlu clusteru Exchange.

Tip *Po instalaci agenta do jednoho z uzlů zobrazuje webová konzole Cyber Protect skupinu DAG a její uzly v nabídce* ***Zařízení*** *>* ***Microsoft Exchange*** *>* ***Databáze****. K instalaci Agentů pro Exchange do zbývajících uzlů vyberte skupinu DAG, klikněte na možnost* ***Podrobnosti*** *a pak u každého z těchto uzlů klikněte na* ***Instalovat agenta****.*

Zálohování dat clusteru Exchange

1. Při vytváření plánu ochrany vyberte skupinu DAG způsobem popsaným v části Výběr dat serveru Exchange (str. 304).
2. Nakonfigurujte možnost zálohy Režim zálohování clusteru (str. 169).
3. Podle potřeby (str. 125) určete další nastavení plánu ochrany.

Důležité *Při zálohování s podporou cloudu se ujistěte, že jste vybrali skupinu DAG jako celek. Pokud vyberete jednotlivé uzly nebo databáze ve skupině DAG, budou zálohovány pouze vybrané položky a možnost* ***Režim zálohování clusteru*** *bude ignorována.*

Obnova dat clusteru Exchange

1. Vyberte bod obnovy databáze, kterou chcete obnovit. Pro obnovení není možné vybrat celý cluster.

   Pokud vyberete kopii clusterované databáze pod položkou **Zařízení** > **Microsoft Exchange** > **Databáze** > `<název clusteru>` > `<název uzlu>` a kliknete na možnost **Obnovit**, zobrazí software pouze body obnovy, které odpovídají časům, kdy byla tato kopie zálohována.

   Nejsnadnější způsob, jak zobrazit všechny body obnovení databáze v clusteru, je vybrat její zálohu na kartě Úložiště záloh (str. 220).
2. Použijte postup uvedený v části Obnovení databází Exchange od kroku 5.

   Software automaticky definuje uzel clusteru, do kterého se data obnoví. Název uzlu se zobrazí v poli **Obnovit do**. Cílový uzel je možné ručně změnit.

14.3 Zálohování s podporou aplikací

Zálohování na úrovni disku s podporou aplikací je dostupné pro fyzické počítače, virtuální počítače ESXi a virtuální počítače Hyper-V.

Při zálohování počítače, kde je spuštěn Microsoft SQL Server, Microsoft Exchange Server nebo doménové služby Active Directory, zapněte možnost **Záloha aplikací** pro dodatečnou ochranu dat těchto aplikací.

Proč používat zálohy s podporou aplikací?

Pokud použijete zálohu s podporou aplikací, zajistíte, že:

1. Aplikace se budou zálohovat v konzistentním stavu a budou dostupné okamžitě po obnově počítače.
2. Můžete obnovovat databáze SQL a Exchange, poštovní schránky a položky schránek bez obnovení celého počítače.
3. Soubory transakčních protokolů SQL se po každém úspěšném zálohování zkrátí. Zkrácení protokolů SQL je možné zakázat v možnostech plánu ochrany (str. 181). Soubory transakčních protokolů Exchange se zkracují pouze ve virtuálních počítačích. Pokud chcete zkracovat transakční protokoly Exchange ve fyzických počítačích, můžete použít možnost plné zálohy VSS (str. 194).
4. Pokud doména obsahuje více řadičů a obnovíte jeden z nich, provede se neautoritativní obnova a po obnovení nedojde k vrácení čísla USN zpět.

Co je třeba k tvorbě zálohy s podporou aplikací?

Na fyzickém počítači musí být kromě Agenta pro Windows nainstalován Agent pro SQL a/nebo Agent pro Exchange.

Na virtuálních počítačích není instalace agenta nutná; předpokládá se, že počítač zálohuje Agent pro VMware (ve Windows) nebo Agent pro Hyper-V.

Agent pro VMware (Virtual Appliance) a Agent pro VMware (Windows) mohou vytvořit zálohy s podporou aplikací, ale nemohou z nich obnovit data aplikací. K obnovení dat aplikací ze záloh vytvořených těmito agenty potřebujte Agenta pro VMware (Windows), Agenta pro SQL nebo Agenta pro Exchange v počítači, který má přístup do umístění s uloženými zálohami. Při konfiguraci obnovení dat aplikací vyberte bod obnovy na kartě **Úložiště záloh** a potom v okně **Počítač k procházení** vyberte tento počítač.

Ostatní požadavky jsou uvedeny v částech Předpoklady (str. 302) a Požadovaná uživatelská oprávnění (str. 308).

14.3.1 Požadovaná uživatelská oprávnění

Záloha s podporou aplikace obsahuje metadata aplikací s podporou služby VSS, která se nacházejí na disku. Pokud chce agent přistoupit k těmto metadatům, potřebuje k tomu účet s příslušnými oprávněními, která jsou uvedena níže. Při povolování zálohy aplikace budete vyzváni k určení tohoto účtu.

- U serveru SQL:

  Účet musí být členem skupiny **Backup Operators** nebo **Administrators** na počítači a členem role **sysadmin** v každé instanci, kterou chcete zálohovat.
- U serveru Exchange:

  Exchange 2007: Účet musí být členem skupiny **Správci** na zařízení a členem skupiny role **Správci organizace Exchange**.

  Exchange 2010 a novější: Účet musí být členem skupiny **Správci** na zařízení a členem skupiny role **Správa organizace**.
- U služby Active Directory:

  Účet musí být správce domény.

Další požadavky pro zálohy virtuální počítače

Pokud aplikace běží na virtuálním počítači, který je zálohován Agentem pro VMware nebo Agentem pro Hyper-V, zkontrolujte, že je v daném počítači zakázáno řízení uživatelských účtů (UAC). Pokud UAC vypnout nechcete, je nutné při zapnutí zálohování aplikací zadat pověření vestavěného účtu správce domény (DOMAIN\Administrator).

14.4 Záloha schránky

Záloha poštovní schránky je podporována pro Microsoft Exchange Server 2010 Service Pack 1 (SP1) nebo novější.

Záloha poštovní schránky je dostupná, pokud je na serveru pro správu zaregistrovaný alespoň jeden Agent pro Exchange. Agent musí být nainstalovaný na počítači, který patří do stejné stromové struktury Active Directory jako Microsoft Exchange Server.

Před zálohováním poštovních schránek musíte Agenta pro Exchange připojit k serveru s rolí **klientského přístupu** (CAS) serveru Microsoft Exchange. Ve verzi Exchange 2016 a novější není role CAS k dispozici jako samostatná možnost instalace. Instaluje se automaticky jako součást role Serveru poštovních schránek. Agenta tak můžete připojit k jakémukoli serveru se spuštěnou **rolí poštovních schránek**.

Připojení Agenta pro Exchange k CAS

1. Klikněte na **Zařízení** > **Přidat**.
2. Klikněte na **Microsoft Exchange Server**.
3. Klikněte na **Poštovní schránky Exchange**.

   Pokud na serveru pro správu není zaregistrován žádný Agent pro Exchange, software vás vyzve, abyste agenta nainstalovali. Po instalaci opakujte tento postup od kroku 1.
4. [Volitelné] Pokud je na serveru pro správu zaregistrováno více Agentů pro Exchange, klikněte na **Agent** a potom změňte agenta, který provede zálohování.
5. V možnosti **Server pro klientský přístup** zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** serveru Microsoft Exchange.

   Ve verzi Exchange 2016 a novější se služba klientského přístupu instaluje automaticky jako součást role Serveru poštovních schránek. Můžete tak zadat jakýkoli server se spuštěnou **rolí poštovních schránek**. Dále v této části označujeme tento server jako CAS.
6. V možnosti **Typ ověření** vyberte typ ověření, který CAS používá. Můžete vybrat ověření **Kerberos** (výchozí nastavení) nebo **Základní**.
7. [Pouze pro základní ověřování] Zvolte, který protokol se použije. Můžete vybrat **HTTP** (výchozí nastavení) nebo **HTTPS**.

8. [Pouze pro základní ověření pomocí protokolu HTTPS] Pokud CAS používá certifikát SSL, který byl získán od certifikační autority, a chcete, aby software při připojení k CAS zkontroloval tento certifikát, zaškrtněte políčko **Zkontrolovat certifikát SSL**. Jinak tento krok přeskočte.
9. Zadejte pověření účtu, který se bude používat pro přístup k CAS. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 310).
10. Klikněte na tlačítko **Přidat**.

Poštovní schránky se pak zobrazí v umístění **Zařízení** > **Microsoft Exchange** > **Poštovní schránky**.

14.4.1 Výběr poštovních schránek Exchange Serveru

Vyberte poštovní schránky podle níže uvedených pokynů a podle potřeby (str. 125) zadejte další nastavení plánu ochrany.

Jak vybrat poštovní schránky Exchange

1. Klikněte na **Zařízení** > **Microsoft Exchange**.

   Software zobrazí strom databází a poštovních schránek serveru Exchange.
2. Klikněte na **Poštovní schránky** a potom vyberte poštovní schránky, které chcete zálohovat.
3. Klikněte na možnost **Zálohovat**.

14.4.2 Požadovaná uživatelská oprávnění

Pokud chce Agent pro Exchange přistupovat k poštovním schránkám, potřebuje k tomu účet s příslušnými oprávněními. Při konfiguraci různých operací s poštovními schránkami budete vyzváni k určení tohoto účtu.

Členství daného účtu ve skupině role **Správa organizace** umožňuje přístup k libovolné poštovní schránce, včetně těch, které budou vytvořeny v budoucnosti.

Minimální požadovaná uživatelská oprávnění jsou následující:

- Účet musí být členem skupin rolí **Správa serveru** a **Správa příjemců**.
- Účet musí mít povolenou roli správy **ApplicationImpersonation** pro všechny uživatele a skupiny uživatelů, k jejichž poštovním schránkám má agent mít přístup.

  Informace o konfiguraci role správy **ApplicationImpersonation** najdete v následujícím článku znalostní databáze Microsoft Knowledge Base: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

14.5 Obnovení databází SQL

Tato část popisuje obnovu ze záloh databází i záloh podporujících aplikace.

Databáze SQL je možné obnovit do instance serveru SQL Server, pokud je v počítači, kde je instance spuštěna, nainstalován Agent pro SQL. Bude nutné zadat pověření pro účet, který je členem skupiny **Backup Operators** nebo **Administrators** v počítači a členem role **sysadmin** v cílové instanci.

Databáze můžete také obnovit jako soubory. To může být užitečné v případě, že potřebujete extrahovat data pro dolování dat, audit nebo další zpracování nástroji od externích dodavatelů. Soubory databáze SQL můžete připojit k instanci serveru SQL Server; postup je popsán v tématu Připojení databází SQL serveru (str. 313).

Pokud používáte jenom Agenta pro VMware (Windows), je obnovení databází do souborů jedinou dostupnou metodou obnovení. Obnovení databází pomocí Agenta pro VMware (virtuální zařízení) není možné.

Systémové databáze se v podstatě obnovují stejným způsobem jako uživatelské databáze. Zvláštnosti obnovy systémových databází jsou popsány v tématu Obnovení systémových databází (str. 312).

Obnovení databází SQL na instanci serveru SQL Server

1. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft SQL** a vyberte databáze, které chcete obnovit.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro SQL, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu databází SQL.
4. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací klikněte na možnost **Obnovit** > **Databáze SQL**, vyberte databáze, které chcete obnovit, a pak klikněte na **Obnovit**.
   - Při obnově ze zálohy databáze klikněte na možnost **Obnovit** > **Databáze na instanci**.
5. Ve výchozím nastavení se databáze obnoví do původních. Pokud původní databáze neexistuje, bude vytvořena. Můžete vybrat jinou instanci serveru SQL Server (spuštěnou na stejném počítači), kam se databáze obnoví.

   Jak obnovit databázi jako jinou do stejné instance:
   a. Klikněte na název databáze.
   b. V části **Obnovit do** vyberte možnost **Nová databáze**.
   c. Zadejte název nové databáze.
   d. Zadejte cestu k nové databázi a k protokolu. Zadaná složka nesmí obsahovat původní soubory databáze a protokolu.
6. [Volitelné] [Není k dispozici pro databázi obnovenou do původní instance jako nová databáze] Chcete-li změnit stav databáze po obnově, klikněte na její název a vyberte jednu z následujících možností:
   - **Připraveno k použití (RESTORE WITH RECOVERY)** (výchozí)

     Po dokončení obnovy bude databáze připravena k použití. Uživatelé k ní budou mít plný přístup. Software vrátí všechny neprovedené transakce obnovené databáze, které jsou uloženy v souboru transakčního protokolu. Z nativních záloh Microsoft SQL nebude možné obnovit další soubory transakčních protokolů.
   - **Nefunkční (RESTORE WITH NORECOVERY)**

     Po dokončení obnovy nebude databáze funkční. Uživatelé k ní nebudou mít přístup. Software zachová všechny neprovedené transakce obnovené databáze. Bude možné obnovit další

soubory transakčních protokolů z nativních záloh Microsoft SQL a získat tak potřebný bod obnovení.

- **Pouze ke čtení (RESTORE WITH STANDBY)**

  Po dokončení obnovy budou mít uživatelé k databázi přístup pouze ke čtení. Software vrátí všechny neprovedené transakce. Tyto akce však uloží do dočasného souboru, aby bylo možné dopady obnovení vrátit zpět.

  Pomocí této hodnoty se primárně detekuje bod v čase, kdy nastala chyba serveru SQL.

7. Klikněte na možnost **Spustit obnovu**.

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

Obnovení databází SQL jako souborů

1. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft SQL** a vyberte databáze, které chcete obnovit.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro SQL nebo Agent pro VMware, a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu databází SQL.
4. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací klikněte na možnost **Obnovit** > **Databáze SQL**, vyberte databáze, které chcete obnovit, a pak klikněte na **Obnovit jako soubory**.
   - Při obnově ze zálohy databáze klikněte na **Obnovit** > **Databáze jako soubory**.
5. Klikněte na **Procházet** a vyberte místní nebo síťovou složku, do které se soubory uloží.
6. Klikněte na možnost **Spustit obnovu**.

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

14.5.1 Obnova systémových databází

Všechny systémové databáze jedné instance se obnoví najednou. Při obnově systémových databází software automaticky restartuje cílovou instanci v jednouživatelském režimu. Po dokončení obnovy software restartuje instanci a obnoví ostatní databáze (pokud nějaké jsou).

Další důležité informace týkající se obnovy systémových databází:

- Systémové databáze je možné obnovit pouze na instanci stejné verze jako původní instance.
- Systémové databáze se vždy obnoví ve stavu "připraveno k použití".

Obnova hlavní databáze

Systémové databáze zahrnují i **hlavní** databázi. **Hlavní** databáze zaznamenává informace o všech databázích instance. Proto **hlavní** databáze (master) v záloze obsahuje informace o databázích, které existovaly v instanci v době zálohy. Po obnovení **hlavní** databáze bude možná nutné provést následující kroky:

- Databáze, které se zobrazily v instanci po provedení databáze, nejsou instancí viditelné. Chcete-li tyto databáze obnovit, připojte je k instanci ručně pomocí sady SQL Server Management Studio.
- Databáze, které byly odstraněny po provedení zálohy, se v instanci zobrazují jako offline. Odstraňte tyto databáze pomocí sady SQL Server Management Studio.

14.5.2 Připojení databází serveru SQL

V tomto tématu je popsán postup připojení databáze v serveru SQL pomocí aplikace SQL Server Management Studio. V libovolném okamžiku může být připojena pouze jedna databáze.

Připojení databáze vyžaduje libovolné z následujících oprávnění: **CREATE DATABASE** (tvorba databáze), **CREATE ANY DATABASE** (tvorba libovolné databáze) nebo **ALTER ANY DATABASE** (změna libovolné databáze). Tato oprávnění jsou obvykle udělována roli **sysadmin** v instanci.

Jak připojit databázi

1. Spusťte aplikaci Microsoft SQL Server Management Studio.
2. Připojte se k požadované instanci serveru SQL a rozbalte ji.
3. Klikněte pravým tlačítkem na možnost **Databases** (Databáze) a klikněte na možnost **Attach** (Připojit).
4. Klikněte na tlačítko **Add** (Přidat).
5. V dialogovém okně **Locate Database Files** (Vyhledat soubory databáze) najděte a vyberte soubor MDF databáze.
6. V části **Database Details** (Podrobnosti databáze) zkontrolujte, zda byly nalezeny ostatní soubory databáze (NDF a LDF).

   Podrobnosti. Soubory databáze serveru SQL nemusí být nalezeny automaticky, pokud:

   - Nejsou ve výchozím umístění nebo nejsou ve stejné složce jako primární soubor databáze (MDF). Řešení: Zadejte cestu k požadovaným souborům ručně do sloupce **Current File Path** (Aktuální cesta souboru).
   - Obnovili jste neúplnou sadu souborů tvořících databázi. Řešení: Obnovte chybějící soubory databáze serveru SQL ze zálohy.
7. Jakmile budou všechny soubory nalezeny, klikněte na tlačítko **OK**.

14.6 Obnova databází Exchange

Tato část popisuje obnovu ze záloh databází i záloh podporujících aplikace.

Data serveru Exchange můžete obnovit na aktivní server Exchange. Může jít o původní server Exchange nebo server se stejnou verzí spuštěný na počítači se stejným plně kvalifikovaným názvem domény (FQDN). V cílovém počítači musí být nainstalován Agent pro Exchange.

Následující tabulka shrnuje data serveru Exchange, která lze vybrat pro obnovu, a minimální uživatelská oprávnění, která jsou k obnově potřeba.

Verze Exchange	Datové položky	Uživatelská oprávnění
2007	Skupiny úložišť	Členství ve skupině role **Správci organizace Exchange**.
2010/2013/2016/2019	Databáze	Členství ve skupině role **Správa serveru**

Databáze (skupiny úložišť) můžete také obnovit jako soubory. Databázové soubory spolu s transakčními protokoly se extrahují ze zálohy do zadané složky. To může být užitečné, pokud potřebujete rozbalit data a zkontrolovat je či dále zpracovat pomocí nástrojů od externích dodavatelů nebo pokud se obnova z nějakého důvodu nezdaří a vy chcete databázi připojit ručně (str. 315).

Pokud používáte jenom Agenta pro VMware (Windows), je obnovení databází do souborů jedinou dostupnou metodou obnovení. Obnovení databází pomocí Agenta pro VMware (virtuální zařízení) není možné.

Databáze i skupiny úložišť budeme v rámci níže uvedených procedur označovat jako „databáze“.

Obnovení databází Exchange na aktivní Exchange Server

1. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft Exchange** > **Databáze** a vyberte databáze, které chcete obnovit.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na možnost **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro Exchange, a poté vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu dat Exchange.
4. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací klikněte na možnost **Obnovit** > **Databáze Exchange**, vyberte databáze, které chcete obnovit, a pak klikněte na **Obnovit**.
   - Při obnově ze zálohy databáze klikněte na možnost **Obnovit** > **Databáze na server Exchange**.
5. Ve výchozím nastavení se databáze obnoví do původních. Pokud původní databáze neexistuje, bude vytvořena.

   Jak obnovit databázi jako jinou:
   a. Klikněte na název databáze.
   b. V části **Obnovit do** vyberte možnost **Nová databáze**.
   c. Zadejte název nové databáze.
   d. Zadejte cestu k nové databázi a k protokolu. Zadaná složka nesmí obsahovat původní soubory databáze a protokolu.
6. Klikněte na možnost **Spustit obnovu**.

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

Obnovení databází Exchange jako souborů

1. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft Exchange** > **Databáze** a vyberte databáze, které chcete obnovit.
2. Klikněte na možnost **Obnova**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Proveďte jeden z následujících úkonů:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro Exchange nebo Agent pro VMware, a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

   Počítač vybraný při výše uvedených úkonech se stane cílovým počítačem pro obnovu dat Exchange.
4. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací klikněte na možnost **Obnovit** > **Databáze Exchange**, vyberte databáze, které chcete obnovit, a pak klikněte na **Obnovit jako soubory**.
   - Při obnově ze zálohy databáze klikněte na **Obnovit** > **Databáze jako soubory**.
5. Klikněte na **Procházet** a vyberte místní nebo síťovou složku, do které se soubory uloží.
6. Klikněte na možnost **Spustit obnovu**.

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

14.6.1 Připojení databází aplikace Exchange Server

Po obnovení souborů databází je možné databáze aktivovat jejich připojením. Připojení se provádí pomocí Konzoly pro správu serveru Exchange, Správce systému Exchange nebo prostředí Exchange Management Shell.

Obnovené databáze budou ve stavu nesprávného vypnutí. Databázi, která je ve stavu nesprávného vypnutí, je možné připojit systémem, pokud je obnovena do svého původního umístění (tzn. informace o původní databázi se nacházejí ve službě Active Directory). Při obnově databáze do alternativního umístění (například nová databáze nebo databáze obnovy) není možné databázi připojit, dokud ji nedostanete do stavu správného vypnutí pomocí příkazu **`Eseutil /r <Enn>`**. **`<Enn>`** určuje předponu protokolového souboru pro databázi (nebo skupinu úložišť obsahující databázi), do které je třeba aplikovat protokolové soubory transakcí.

Účet, který použijete k připojení databáze, musí mít přidělenu roli Exchange Server Administrator a musí být členem místní skupiny Administrators cílového serveru.

Podrobnosti o připojování databází naleznete v následujících článcích:

- Pro Exchange 2010 nebo novější: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

14.7 Obnovení poštovních schránek a položek schránek aplikace Exchange

Tato část popisuje postup pro obnovu poštovních schránek a položek schránek Exchange z databázových záloh, ze záloh s podporou aplikací a ze záloh poštovních schránek. Poštovní schránky nebo položky poštovních schránek je možné obnovit na aktivní server Exchange nebo do služby Microsoft Office 365.

Je možné obnovit následující položky:

- Poštovní schránky (kromě archivačních poštovních schránek)
- Veřejné složky
- Položky veřejné složky
- E-mailové složky
- E-mailové zprávy
- Události kalendáře
- Úlohy
- Kontakty
- Položky žurnálu
- Poznámky

Položky můžete najít pomocí vyhledávání.

Obnovení na server Exchange

Granulární obnovu lze provést jen v systému Microsoft Exchange Server 2010 Service Pack 1 (SP1) nebo novějším. Zdrojová záloha může obsahovat databáze nebo poštovní schránky z jakékoli podporované verze Exchange.

Granulární obnovu může provádět Agent pro Exchange nebo Agent pro VMware (ve Windows). Cílový server Exchange a počítač, na kterém je agent spuštěný, musí patřit do stejné stromové struktury Active Directory.

Když obnovíte poštovní schránku do už existující schránky, přepíší se existující položky se shodnými identifikátory.

Při obnově položek poštovních schránek se nic nepřepisuje. Místo toho je v cílové složce znovu vytvořena úplná cesta k položce poštovní schránky.

Požadavky na uživatelské účty

K poštovní schránce obnovené ze zálohy musí být přidružený uživatelský účet ve službě Active Directory.

Poštovní schránky uživatelů a jejich obsah lze obnovit pouze v případě, že jejich přidružené uživatelské účty jsou *povolené*. Sdílené poštovní schránky, schránky místností a schránky vybavení se dají obnovit pouze v případě, že jsou jejich přidružené uživatelské účty *zakázané*.

Poštovní schránka, která nesplňuje výše uvedené podmínky, bude během obnovy vynechána.

Jestliže byly některé schránky vynechány, obnova bude úspěšná s upozorněními. Pokud budou vynechány všechny schránky, obnova bude neúspěšná.

Obnovení do Office 365

Obnovení lze provést ze záloh serveru Microsoft Exchange Server 2010 nebo novějších.

Když obnovíte poštovní schránku do už existující poštovní schránky Office 365, budou existující položky zachovány beze změny a obnovené položky se umístí vedle nich.

Při obnovení jedné poštovní schránky musíte vybrat cílovou poštovní schránku Office 365. Při obnovení několika poštovních schránek v jedné operaci obnovení se software pokusí obnovit každou poštovní schránku do poštovní schránky uživatele se stejným jménem. Pokud daný uživatel není nalezen, příslušná poštovní schránka se přeskočí. Jestliže byly některé schránky vynechány, obnova bude úspěšná s upozorněními. Pokud budou vynechány všechny schránky, obnova bude neúspěšná.

Další informace o obnovení do služby Office 365 naleznete v tématu Ochrana poštovních schránek Office 365 (str. 321).

14.7.1 Obnova schránek

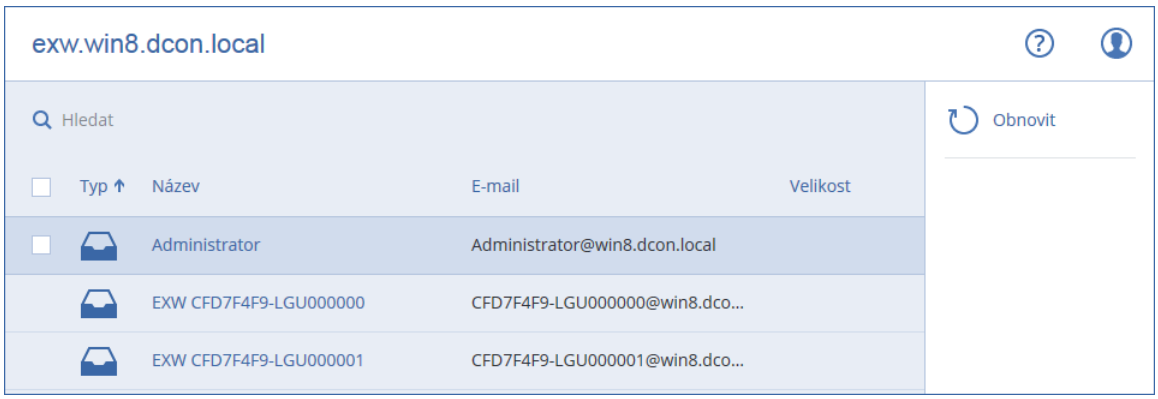
Obnovení poštovních schránek ze zálohy s podporou aplikací nebo zálohy databáze

1. [Pouze při obnově ze zálohy databáze do služby Office 365] Pokud v počítači se spuštěným Exchange Serverem, který byl zálohován, není nainstalován Agent pro Office 365, proveďte jednu z následujících akcí:
   - Není-li ve vaší organizaci Agent pro Office 365, nainstalujte jej do počítače, který byl zálohován (nebo do jiného počítače se stejnou verzí serveru Microsoft Exchange Server).
   - Pokud již máte ve vaší organizaci Agenta pro Office 365, zkopírujte knihovny z počítače, který byl zálohován (nebo z jiného počítače se stejnou verzí serveru Microsoft Exchange Server), do počítače s Agentem pro Office 365, jak je popsáno v článku Kopírování knihoven Microsoft Exchange (str. 321).
2. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft Exchange** > **Databáze** a vyberte databázi původně obsahující data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Použijte jiné způsoby obnovy:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro Exchange nebo Agent pro VMware, a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

   Místo původního počítače, který je offline, teď obnovu provede počítač, který jste v některém z předchozích kroků zvolili pro procházení.
5. Klikněte na možnost **Obnovit**>**Schránky Exchange**.
6. Vyberte schránky, které chcete obnovit.

Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.



7. Klikněte na příkaz **Obnovit**.
8. [Pouze při obnovení do Office 365]:
   a. V části **Obnovit na** vyberte **Microsoft Office 365**.
   b. [Pokud jste v kroku 6 vybrali pouze jednu poštovní schránku] V poli **Cílová poštovní schránka** určete cílovou poštovní schránku.
   c. Klikněte na možnost **Spustit obnovu**.

   Další kroky tohoto postupu nejsou nutné.
9. Kliknutím na **Cílový počítač se systémem Microsoft Exchange Server** vyberete nebo změníte cílový počítač. Tento krok umožňuje obnovu na počítač, kde není spuštěn Agent pro Exchange.

   Zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** (na serveru Microsoft Exchange Server 2010/2013) nebo **role poštovních schránek** (na serveru Microsoft Exchange Server 2016 nebo novějším). Počítač musí patřit ke stejnému stromu Active Directory jako počítač, který provádí obnovu.

   Pokud budete vyzváni, zadejte pověření účtu, který se bude používat pro přístup k počítači. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 310).
10. [Volitelné] Kliknutím na možnost **Databáze pro nové vytvoření všech chybějících poštovních schránek** změňte automaticky vybranou databázi.
11. Klikněte na možnost **Spustit obnovu**.

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

Obnovení poštovní schránky ze zálohy poštovních schránek

1. Klikněte na **Zařízení** > **Microsoft Exchange** > **Poštovní schránky**.
2. Klikněte na poštovní schránku, kterou chcete obnovit, a potom klikněte na možnost **Obnova**.

   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

   Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Úložiště záloh (str. 220) a klikněte na možnost **Zobrazit zálohy**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
4. Klikněte na **Obnovit** > **Poštovní schránka**.
5. Proveďte kroky 8–11 výše uvedeného postupu.

14.7.2 Obnovení položek poštovní schránky

Obnovení položek poštovní schránky ze zálohy s podporou aplikací nebo zálohy databáze

1. [Pouze při obnově ze zálohy databáze do služby Office 365] Pokud v počítači se spuštěným Exchange Serverem, který byl zálohován, není nainstalován Agent pro Office 365, proveďte jednu z následujících akcí:

- Není-li ve vaší organizaci Agent pro Office 365, nainstalujte jej do počítače, který byl zálohován (nebo do jiného počítače se stejnou verzí serveru Microsoft Exchange Server).
- Pokud již máte ve vaší organizaci Agenta pro Office 365, zkopírujte knihovny z počítače, který byl zálohován (nebo z jiného počítače se stejnou verzí serveru Microsoft Exchange Server), do počítače s Agentem pro Office 365, jak je popsáno v článku Kopírování knihoven Microsoft Exchange (str. 321).

2. Proveďte jeden z následujících úkonů:
   - Při obnově ze zálohy s podporou aplikací vyberte pod položkou **Zařízení** počítač původně obsahující data, která chcete obnovit.
   - Při obnově ze zálohy databáze klikněte na **Zařízení** > **Microsoft Exchange** > **Databáze** a vyberte databázi původně obsahující data, která chcete obnovit.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.

   Pokud je počítač offline, body obnovy se nezobrazí. Použijte jiné způsoby obnovy:
   - [Pouze při obnově ze zálohy s podporou aplikací] Jestliže se umístění zálohy nachází v cloudu nebo ve sdíleném úložišti (takže k němu mohou přistupovat také jiní agenti), klikněte na **Vybrat počítač**, vyberte počítač ve stavu online, na kterém je nainstalován Agent pro Exchange nebo Agent pro VMware, a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).

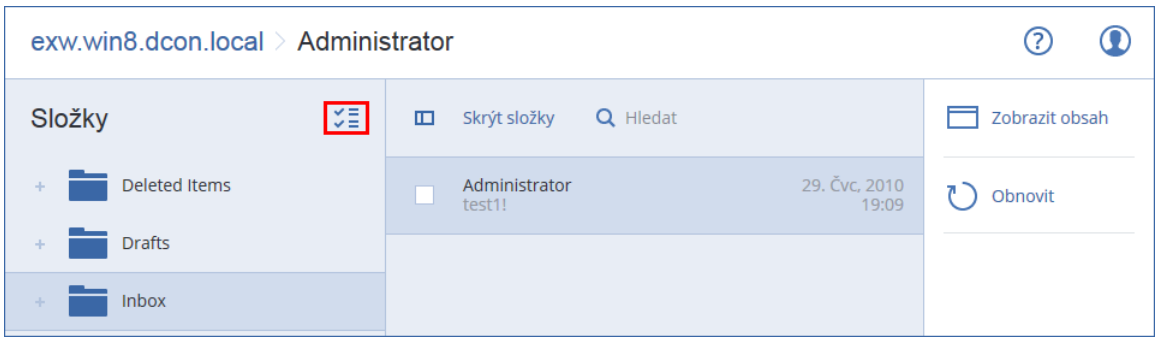
   Místo původního počítače, který je offline, teď obnovu provede počítač, který jste v některém z předchozích kroků zvolili pro procházení.
5. Klikněte na možnost **Obnovit**>**Schránky Exchange**.
6. Klikněte na poštovní schránku, která původně obsahovala položky, jež chcete obnovit.
7. Vyberte položky, které chcete obnovit.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.
   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.
   - U úkolů: vyhledávání podle předmětu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Zobrazit obsah** a zobrazit její obsah včetně příloh.

   Tip *Kliknutím na název přiloženého souboru jej stáhnete.*

   Chcete-li vybírat složky, klikněte na ikonu obnovy složek.



8. Klikněte na příkaz **Obnovit**.
9. Chcete-li obnovení provést do Office 365, vyberte **Microsoft Office 365** v části **Obnovit na**.

Chcete-li obnovu provést na server Exchange, vyberte možnost **Microsoft Exchange** v části **Obnovit na**.

10. [Pouze při obnově na server Exchange Server] Klikněte na **Cílový počítač se systémem Microsoft Exchange Server** a vyberte nebo změňte cílový počítač. Tento krok umožňuje obnovu na počítač, kde není spuštěn Agent pro Exchange.

    Zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** (na serveru Microsoft Exchange Server 2010/2013) nebo **role poštovních schránek** (na serveru Microsoft Exchange Server 2016 nebo novějším). Počítač musí patřit ke stejnému stromu Active Directory jako počítač, který provádí obnovu.

    Pokud budete vyzváni, zadejte pověření účtu, který se bude používat pro přístup k počítači. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 310).

11. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

    Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje nebo je vybrán jiný než původní cílový počítač, je nutné cílovou schránku zadat.

12. [Pouze při obnově e-mailových zpráv] V části **Cílová složka** si můžete prohlédnout nebo změnit cílovou složku v cílové poštovní schránce. Ve výchozím nastavení se vybere složka **Obnovené položky**. Z důvodu omezení služby Microsoft Exchange jsou události, úkoly, poznámky a kontakty obnoveny do původního umístění bez ohledu na jinou zadanou **cílovou složku**.
13. Klikněte na možnost **Spustit obnovu**.

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

Obnovení položky poštovní schránky ze zálohy poštovních schránek

1. Klikněte na **Zařízení** > **Microsoft Exchange** > **Poštovní schránky**.
2. Klikněte na poštovní schránku, která původně obsahovala položky, jež chcete obnovit, a potom klikněte na možnost **Obnova**.

   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

   Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Úložiště záloh (str. 220) a klikněte na možnost **Zobrazit zálohy**.
3. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
4. Klikněte na **Obnovit** > **E-mailové zprávy**.
5. Vyberte položky, které chcete obnovit.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.

   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.
   - U úkolů: vyhledávání podle předmětu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Zobrazit obsah** a zobrazit její obsah včetně příloh.

   Tip *Kliknutím na název přiloženého souboru jej stáhnete.*

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Odeslat jako e-mail** a odeslat zprávu na e-mailovou adresu. Zpráva bude odeslána z e-mailové adresy vašeho účtu správce.

   Chcete-li vybírat složky, klikněte na ikonu obnovy složek: 
6. Klikněte na příkaz **Obnovit**.
7. Proveďte kroky 9-13 výše uvedeného postupu.

14.7.3 Kopírování knihoven serveru Microsoft Exchange Server

Při obnovování poštovních schránek nebo položek pošty aplikace Exchange do Office 365 (str. 316) bude pravděpodobně třeba zkopírovat následující knihovny z počítače, který byl zálohován (nebo z jiného počítače se stejnou verzí serveru Microsoft Exchange Server), do počítače s Agentem pro Office 365.

Zkopírujte následující soubory podle verze serveru Microsoft Exchange Server, která byla zálohována.

Verze serveru Microsoft Exchange	Knihovny	Výchozí umístění
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Knihovny je třeba umístit do složky **%ProgramData%\Acronis\ese**. Pokud tato složka neexistuje, vytvořte ji ručně.

14.8 Změna pověření k přístupu pro SQL Server nebo Exchange Server

Pověření k přístupu pro SQL Server můžete změnit bez přeinstalování agenta.

Změna pověření k přístupu pro SQL Server nebo Exchange Server

1. Klikněte na **Zařízení** a potom klikněte na **Microsoft SQL** nebo **Microsoft Exchange**.
2. Vyberte skupinu dostupnosti Always On, skupinu dostupnosti databáze, instanci serveru SQL Server nebo server Exchange, pro který chcete pověření k přístupu změnit.
3. Klikněte na **Zadejte přihlašovací údaje**.
4. Zadejte nová pověření k přístupu a klikněte na **OK**.

Změna pověření k přístupu pro Exchange Server pro zálohu poštovní schránky

1. Klikněte na **Zařízení** > **Microsoft Exchange** a potom rozbalte **Poštovní schránky**.
2. Vyberte Exchange Server, pro který chcete pověření k přístupu změnit.
3. Klikněte na **Nastavení**.
4. V části **Účet správce Exchange** zadejte nová pověření k přístupu a potom klikněte na **Uložit**.

15 Ochrana poštovních schránek Office 365

Důležité *Tento oddíl platí pro místní nasazení aplikace Acronis Cyber Protect. Pokud používáte cloudové nasazení, prostudujte si dokument Argentina/support/documentation/BackupService/index.html#37287.html.*

Proč zálohovat poštovní schránky Office 365?

I když je Microsoft Office 365 cloudová služba, pravidelné zálohy poskytují další vrstvu ochrany před chybami uživatelů a záměrnými škodlivými útoky. Zálohy vám navíc umožní obnovit odstraněné položky i poté, co vyprší období uchovávání ve službě Office 365. Můžete si takto také archivovat místní kopii poštovních schránek Office 365, pokud tak vyžadují právní předpisy.

Co je třeba k zálohování poštovních schránek?

Chcete-li zálohovat a obnovovat poštovní schránky Office 365, musíte mít ve službě Microsoft Office 365 přiřazenou roli globálního správce.

Přidání organizace Microsoft Office 365

1. Nainstalujte Agenta pro Office 365 (str. 48) do počítače se systémem Windows, který je připojen k internetu. V organizaci lze využívat pouze jednoho Agenta pro Office 365.
2. Ve webové konzoli Cyber Protect klikněte na položku **Microsoft Office 365**.
3. V okně, které se otevře, zadejte ID aplikace, tajný kód aplikace a ID tenanta Microsoft 365. Další pokyny k tomu, jak tyto informace najít, najdete v tématu Získání ID aplikace a tajného kódu aplikace (p. 325).
4. Klikněte na možnost **Přihlásit se**.

Výsledkem bude, že se položky dat vaší organizace zobrazí ve webové konzoli Cyber Protect na stránce **Microsoft Office 365**.

Obnova

Ze zálohy poštovní schránky lze obnovit následující položky:

- Poštovní schránky
- E-mailové složky
- E-mailové zprávy
- Události kalendáře
- Úlohy
- Kontakty
- Položky žurnálu
- Poznámky

Položky můžete najít pomocí vyhledávání.

Obnovu lze provést ve službě Microsoft Office 365 nebo na aktivní server Exchange.

Když obnovíte poštovní schránku do už existující poštovní schránky Office 365, přepíší se existující položky se shodnými identifikátory. Když obnovíte poštovní schránku do už existující poštovní schránky na serveru Exchange, existující položky budou zachovány beze změny. Obnovené položky jsou umístěny vedle nich.

Při obnově položek poštovních schránek se nic nepřepisuje. Místo toho je v cílové složce znovu vytvořena úplná cesta k položce poštovní schránky.

Omezení

- Použití plánu ochrany u více než 500 poštovních schránek může způsobit snížení výkonu zálohování. Chcete-li chránit velký počet poštovních schránek, vytvořte několik plánů ochrany a naplánujte spuštění každého z nich na jiný čas.
- Archivační poštovní schránky (**Místní archiv**) nelze zálohovat.

- Záloha poštovní schránky zahrnuje pouze složky, které se zobrazují uživatelům. Složka **Obnovitelné položky** a její dílčí složky (**Odstraněné položky**, **Verze**, **Vyčištěné položky**, **Audity**, **DiscoveryHold**, **Protokolování kalendáře**) nejsou do zálohy poštovní schránky zahrnuty.
- Obnovení do nové poštovní schránky Office 365 není možné. Nejprve musíte ručně vytvořit nového uživatele služby Office 365 a poté můžete obnovit položky do poštovní schránky tohoto uiživatele.
- Obnovení do jiné organizace služby Microsoft Office 365 není podporováno.
- Některé typy položek nebo vlastnosti podporované službou Office 365 nemusí být podporovány serverem Exchange. Při obnově na server Exchange Server budou přeskočeny.

15.1 Výběr poštovních schránek

Vyberte poštovní schránky podle níže uvedených pokynů a podle potřeby (str. 125) zadejte další nastavení plánu ochrany.

Výběr poštovních schránek

1. Klikněte na **Microsoft Office 365**.
2. Pokud se zobrazí výzva, přihlaste se do služby Microsoft Office 365 jako globální správce.
3. Vyberte poštovní schránky, které chcete zálohovat.
4. Klikněte na možnost **Zálohovat**.

15.2 Obnovení poštovních schránek a jejich položek

15.2.1 Obnova schránek

1. [Pouze při obnovení na Exchange Server] Ujistěte se, zda existuje uživatel serveru Exchange se stejným přihlašovacím jménem, jako je uživatelské jméno k obnovované poštovní schránce. Pokud takový uživatel neexistuje, vytvořte ho. Další požadavky na tohoto uživatele jsou popsané v tématu Obnovení poštovních schránek a položek schránek aplikace Exchange (str. 316) v části Požadavky na uživatelské účty.
2. Klikněte na **Zařízení** > **Microsoft Office 365**.
3. Klikněte na poštovní schránku, kterou chcete obnovit, a potom klikněte na možnost **Obnova**.

   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

   Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Úložiště záloh (str. 220) a klikněte na možnost **Zobrazit zálohy**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
5. Klikněte na **Obnovit** > **Poštovní schránka**.
6. Chcete-li obnovení provést na server Exchange, vyberte možnost **Microsoft Exchange** v části **Obnovit na**. Pokračujte v obnovování podle pokynů v tématu Obnova schránek (str. 317) počínaje krokem 9. Další kroky tohoto postupu nejsou nutné.

   Obnovení do Office 365 zajistíte ponecháním výchozí hodnoty **Microsoft Office 365** v části **Obnovit na**.
7. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

   Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje, je nutné zadat cílovou schránku.
8. Klikněte na možnost **Spustit obnovu**.

15.2.2 Obnovení položek poštovní schránky

1. [Pouze při obnovení na Exchange Server] Ujistěte se, zda existuje uživatel serveru Exchange se stejným přihlašovacím jménem, jako je uživatelské jméno uživatele, jehož položky poštovní schránky chcete obnovit. Pokud takový uživatel neexistuje, vytvořte ho. Další požadavky na tohoto uživatele jsou popsané v tématu Obnovení poštovních schránek a položek schránek aplikace Exchange (str. 316) v části Požadavky na uživatelské účty.
2. Klikněte na **Zařízení** > **Microsoft Office 365**.
3. Klikněte na poštovní schránku, která původně obsahovala položky, jež chcete obnovit, a potom klikněte na možnost **Obnova**.

   Můžete je vyhledávat podle názvu. Zástupné znaky nejsou podporovány.

   Jestliže byla poštovní schránka odstraněna, vyberte ji na kartě Úložiště záloh (str. 220) a klikněte na možnost **Zobrazit zálohy**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
5. Klikněte na **Obnovit** > **E-mailové zprávy**.
6. Vyberte položky, které chcete obnovit.

   Dostupné jsou následující možnosti vyhledávání. Zástupné znaky nejsou podporovány.

   - U e-mailových zpráv: vyhledávání podle předmětu, odesílatele, příjemce a data.
   - U událostí: vyhledávání podle názvu a data.
   - U úkolů: vyhledávání podle předmětu a data.
   - U kontaktů: vyhledávání podle jména, e-mailové adresy a telefonního čísla.

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Zobrazit obsah** a zobrazit její obsah včetně příloh.

   Tip *Kliknutím na název přiloženého souboru jej stáhnete.*

   Když je vybraná e-mailová zpráva, můžete kliknout na možnost **Odeslat jako e-mail** a odeslat zprávu na e-mailovou adresu. Zpráva bude odeslána z e-mailové adresy vašeho účtu správce.

   Chcete-li vybírat složky, klikněte na ikonu obnovy složek. 
7. Klikněte na příkaz **Obnovit**.
8. Chcete-li obnovení provést na server Exchange, vyberte možnost **Microsoft Exchange** v části **Obnovit na**.

   Obnovení do Office 365 zajistíte ponecháním výchozí hodnoty **Microsoft Office 365** v části **Obnovit na**.
9. [Pouze při obnově na server Exchange Server] Klikněte na **Cílový počítač se systémem Microsoft Exchange Server** a vyberte nebo změňte cílový počítač. Tento krok umožňuje obnovu na počítač, kde není spuštěn Agent pro Exchange.

   Zadejte plně kvalifikovaný název domény (FQDN) počítače, kde je zapnutá role pro **klientský přístup** serveru Microsoft Exchange Server. Počítač musí patřit ke stejnému stromu Active Directory jako počítač, který provádí obnovu.

   Pokud budete vyzváni, zadejte pověření účtu, který se bude používat pro přístup k počítači. Požadavky na tento účet jsou uvedené v části Požadovaná uživatelská oprávnění (str. 310).
10. V části **Cílová poštovní schránka** si můžete prohlédnout, zadat nebo změnit cílovou schránku.

    Ve výchozím nastavení je vybrána původní poštovní schránka. Pokud tato poštovní schránka neexistuje, je nutné zadat cílovou schránku.

11. [Pouze při obnově e-mailových zpráv] V části **Cílová složka** si můžete prohlédnout nebo změnit cílovou složku v cílové poštovní schránce. Ve výchozím nastavení se vybere složka **Obnovené položky**.
12. Klikněte na možnost **Spustit obnovu**.

15.3 Změna pověření k přístupu pro Office 365

Pověření k přístupu pro Office 365 můžete změnit bez přeinstalování agenta.

Změna pověření k přístupu pro Office 365

1. Klikněte na **Zařízení** > **Microsoft Office 365**.
2. Vyberte organizaci Office 365.
3. Klikněte na **Zadejte přihlašovací údaje**.
4. Zadejte ID aplikace, tajný kód aplikace a ID tenanta Microsoft 365. Další pokyny k tomu, jak tyto informace najít, najdete v tématu Získání ID aplikace a tajného kódu aplikace (p. 325).
5. Klikněte na možnost **Přihlásit se**.

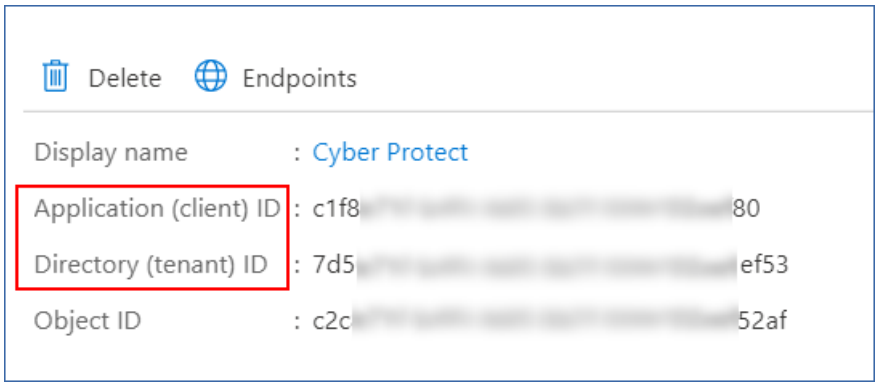
15.4 Získání ID a tajného kódu aplikace

Chcete-li použít moderní ověřování pro Office 365, musíte vytvořit vlastní aplikaci v Azure Active Directory a udělit jí konkrétní oprávnění k rozhraní API. Získáte tak **ID aplikace**, **tajný kód aplikace** a **ID adresáře (tenanta)**, které je třeba zadat do webové konzole Cyber Protect (p. 325).

Vytvoření aplikace v Azure Active Directory

1. Přihlaste se na portál Azure jako správce.
2. Přejděte do nabídky **Azure Active Directory** > **Registrace aplikací** a klikněte na položku **Nová registrace**.
3. Zadejte název vlastní aplikace, například Cyber Protect.
4. V části **Podporované typy účtů** vyberte možnost **Pouze účty v organizačním adresáři**.
5. Klikněte na **Registrovat**.

Aplikace je nyní vytvořená. Na portálu Azure přejděte na stránku **Přehled** aplikace a zkontrolujte ID aplikace (klienta) a adresář (ID tenanta).



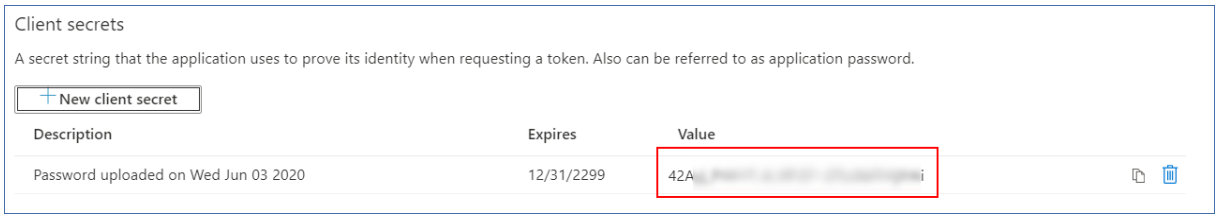
Další informace o vytvoření aplikace na portálu Azure najdete v dokumentaci společnosti Microsoft.

Udělení nezbytných oprávnění rozhraní API pro aplikaci

1. Na portálu Azure přejděte do části **oprávnění rozhraní API** a klikněte na položku **Přidat oprávnění**.
2. Vyberte možnost **Exchange**.
3. Vyberte **Oprávnění aplikace**.
4. Zaškrtněte políčko **full_access_as_app** a klikněte na položku **Přidat oprávnění**.
5. V části **Oprávnění rozhraní API** klikněte na položku **Přidat oprávnění**.
6. Vyberte **Microsoft Graph**.
7. Vyberte **Oprávnění aplikace**.
8. Rozbalte kartu **Adresář** a zaškrtněte políčko **Directory.Read.All**. Klikněte na tlačítko **Přidat oprávnění**.
9. Zkontrolujte všechna oprávnění a klikněte na položku **Udělit souhlas správce pro <název vaší aplikace>**.
10. Potvrďte volbu kliknutím na tlačítko **Ano**.

Vytvoření tajného kódu aplikace

1. Na portálu Azure přejděte do části **Certifikáty a tajné kódy** > **Nový tajný kód klienta**.
2. V dialogovém okně, které se otevře, vyberte Konec platnosti: **Nikdy** a klikněte na tlačítko **Přidat**.
3. V poli **Hodnota** zkontrolujte tajný kód aplikace a zapamatujte si ho.



Další informace o tajném kódu aplikace naleznete v dokumentaci společnosti Microsoft.

16 Ochrana dat v G Suite

Tato funkce je dostupná pouze v cloudových nasazeních aplikace Acronis Cyber Protect. Podrobný popis této funkce viz Argentina/support/documentation/BackupService/index.html#33827.html.

17 Ochrana databáze Oracle

Ochrana databáze Oracle je popsaná v samostatném dokumentu na adrese https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf.

18 Speciální operace s virtuálními počítači

18.1 Spuštění virtuálního počítače ze zálohy (funkce okamžitého obnovení)

Ze zálohy na úrovni disku, která obsahuje operační systém, můžete spustit virtuální počítač. Tato operace se nazývá okamžité obnovení a umožňuje spuštění virtuálního serveru během několika

sekund. Virtuální disky se emulují přímo ze zálohy a nespotřebovávají tedy místo v datovém úložišti. Prostor úložiště je nutný pouze pro záznam změn virtuálních disků.

Doporučujeme, aby takový dočasný virtuální počítač byl spuštěn maximálně tři dny. Potom jej můžete úplně odstranit nebo převést na běžný virtuální počítač (finalizovat) bez jakékoliv odstávky.

Dokud dočasný virtuální počítač existuje, nelze na zálohu, kterou používá, použít pravidla zachování. Zálohy původního počítače mohou běžet dál.

Příklady použití

- **Obnovení po havárii**

  Je možné okamžitě zprovoznit kopii havarovaného počítače.
- **Testování zálohy**

  Počítač můžete spustit ze zálohy a zkontrolovat, zda hostovaný OS a aplikace správně fungují.
- **Přístup k datům aplikací**

  Když je počítač spuštěn, můžete pomocí nativních nástrojů aplikace pro správu získat přístup k požadovaným datům a extrahovat je.

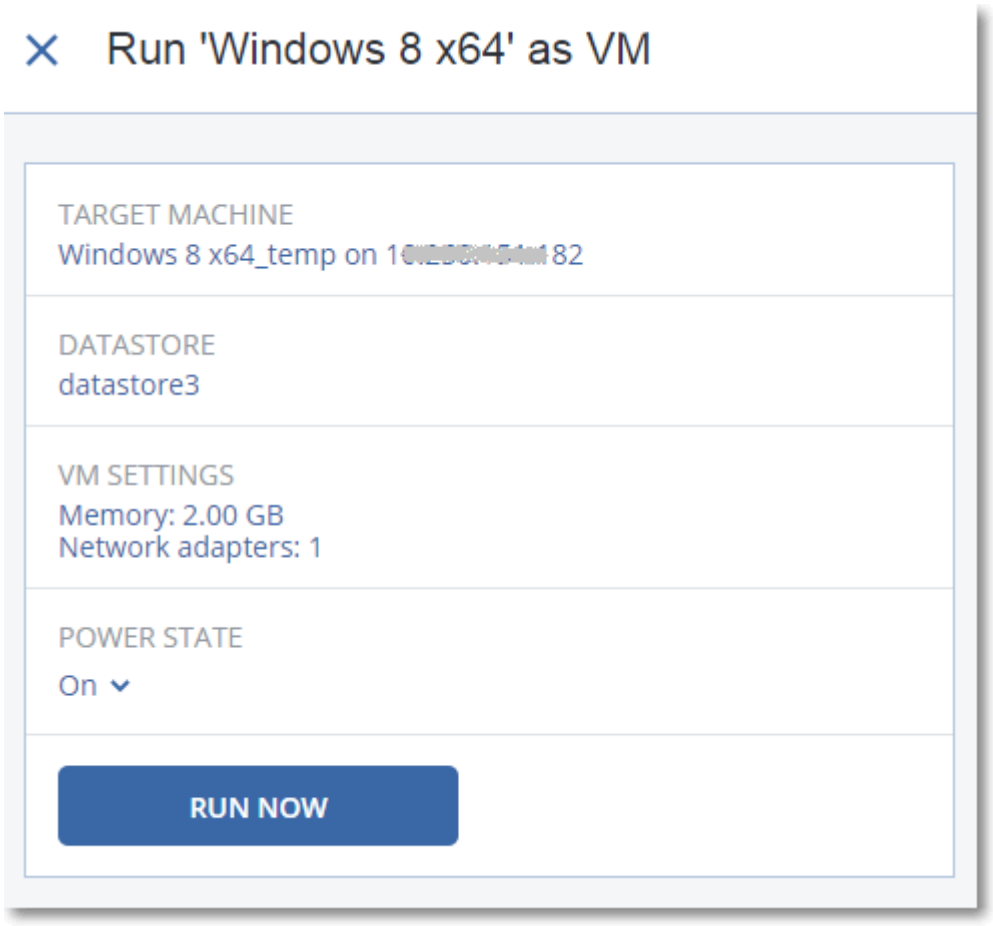
Předpoklady

- Ve službě kybernetické ochrany musí být zaregistrován alespoň jeden Agent pro VMware nebo Agent pro Hyper-V.
- Záloha může být uložena v síťové složce, uzlu úložišť nebo místní složce na počítači, kde je Agent pro VMware nebo Agent pro Hyper-V nainstalován. Pokud vyberete síťovou složku, musí být z tohoto počítače přístupná. Virtuální počítač lze spustit také ze zálohy uložené v cloudovém úložišti, tato operace je však pomalejší, protože vyžaduje velmi náročné čtení ze zálohy s náhodným přístupem. Virtuální počítač nelze spustit ze zálohy uložené na serveru SFTP, páskovém zařízení ani v Secure Zone.
- Záloha musí obsahovat celý počítač nebo všechny svazky, které jsou ke spuštění operačního systému potřeba.
- Je možné použít zálohy fyzických i virtuálních počítačů. Zálohy *kontejnerů* Virtuozzo nelze použít.
- Zálohy, které obsahují logické svazky systému Linux (LVM), musí být vytvořeny Agentem pro VMware nebo Agentem pro Hyper-V. Virtuální počítač musí být stejného typu jako původní počítač (ESXi nebo Hyper-V).

18.1.1 Spouštění počítače

1. Proveďte jeden z následujících úkonů:
   - Vyberte zálohovaný počítač, klikněte na možnost **Obnova** a pak vyberte bod obnovy.
   - Vyberte bod obnovy na kartě Úložiště záloh (str. 220).
2. Klikněte na možnost **Spustit jako virtuální počítač**.

Software automaticky vybere hostitele a další požadované parametry.



3. [Volitelné] Klikněte na možnost **Cílový počítač** a poté změňte typ virtuálního počítače (ESXi nebo Hyper-V), hostitele nebo název virtuálního počítače.
4. [Volitelné] Klikněte na možnost **Datové úložiště** u ESXi nebo na možnost **Cesta** u Hyper-V a poté vyberte datové úložiště virtuálního počítače.

   Změny na virtuálních discích se za běhu počítače shromažďují. Zajistěte, že vybrané na datovém úložišti bude dostatek volného místa. Pokud plánujete tyto změny zachovat tím, že virtuální počítač učiníte trvalým (str. 329), vyberte datové úložiště, které je vhodné pro provoz počítače v produkčním prostředí.
5. [Volitelné] Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti a síťová připojení virtuálního počítače.
6. [Volitelné] Vyberte stav napájení virtuálního počítače (**Zapnuto**/**Vypnuto**).
7. Klikněte na možnost **Spustit**.

Ve výsledku se počítač zobrazí ve webovém rozhraní s jednou z následujících ikon:  nebo 

. Tyto virtuální počítače není možné vybrat k zálohování.

18.1.2 Odstranění počítače

Nedoporučujeme odstraňovat dočasný virtuální počítač přímo ve vSphere/Hyper-V. Toto může vést k artefaktům ve webovém rozhraní. Taktéž záloha, ze které počítač běžel, by mohla na chvíli zůstat zamknutá (nemůže být odstraněna pravidly zachování).

Jak odstranit virtuální počítač, který běží ze zálohy

1. Na kartě **Všechna zařízení** vyberte počítač, který běží ze zálohy.
2. Klikněte na možnost **Odstranit**.

Počítač bude odebrán z webového rozhraní. Odebere se také z inventáře a datového úložiště vSphere nebo Hyper-V. Veškeré změny dat provedené za běhu počítače budou ztraceny.

18.1.3 Dokončení počítače

Pokud virtuální počítač běží ze zálohy, obsah virtuálních disků je získáván přímo z příslušné zálohy. Proto pokud je ztraceno spojení s umístěním zálohy nebo s agentem pro ochranu, počítač přestane být dostupný nebo dokonce dojde k jeho poškození.

Počítač můžete nastavit jako trvalý, jinými slovy obnovit všechny jeho virtuální disky společně se změnami, které se provedly za běhu počítače, do datového úložiště, které uchovává tyto změny. Tento proces se nazývá dokončení.

Dokončení se provede bez výpadku. Virtuální počítač *nebude* během dokončení vypnut.

Umístění konečných virtuálních disků je definováno v parametrech operace **Spustit jako virtuální počítač** (str. 327) (**datové úložiště** pro ESXi nebo **cesta** pro Hyper-V). Před zahájením dokončení se ujistěte, že v datovém úložišti je dostatek volného místa a že jeho možnosti sdílení a výkon jsou vhodné pro spuštění počítače v produkčním prostředí.

Poznámka: *Dokončení není podporováno pro Hyper-V v systému Windows Server 2008/2008 R2 a pro Microsoft Hyper-V Server 2008/2008 R2, protože v těchto verzích Hyper-V chybí potřebné rozhraní API.*

Jak dokončit počítač, který běží ze zálohy

1. Na kartě **Všechna zařízení** vyberte počítač, který běží ze zálohy.
2. Klikněte na možnost **Dokončit**.
3. [Volitelné] Určete nový název počítače.
4. [Volitelné] Změňte režim poskytování disku. Ve výchozím nastavení je nastaven režim **Tenký**.
5. Klikněte na možnost **Dokončit**.

Název počítače se okamžitě změní. Postup obnovy se zobrazuje na kartě **Aktivity**. Jakmile se obnova dokončí, ikona počítače se změní na ikonu běžného virtuálního počítače.

Co potřebujete vědět o dokončení

Dokončení vs. běžné obnovení

Proces dokončení je pomalejší než běžné obnovení, a to z následujících důvodů:

- Během dokončení agent provádí náhodný přístup k různým částem zálohy. Při obnovení celého počítače agent načítá data ze zálohy postupně.
- Pokud je během dokončení spuštěn virtuální počítač, agent načítá data ze zálohy častěji, aby udržoval oba procesy současně. Během běžného obnovení je virtuální počítač nečinný.

Dokončení počítačů spuštěných z cloudových záloh

Kvůli intenzivnímu přístupu k zálohovaným datům rychlost dokončení velmi závisí na šířce pásma připojení mezi umístěním zálohy a agentem. Dokončení bude pomalejší u záloh umístěných v cloudu ve srovnání s místními zálohami. Pokud je internetové připojení velmi pomalé nebo nestabilní, může dokončení počítače spuštěného z cloudové zálohy selhat. Doporučujeme spouštět virtuální počítače z místních záloh, pokud plánujete provést dokončení a máte na výběr.

18.2 Práce ve VMware vSphere

Tato část popisuje operace, které jsou specifické pro prostředí VMware vSphere.

18.2.1 Replikace virtuálních počítačů

Replikace je k dispozici pouze u virtuálních počítačů VMware ESXi.

Replikace je proces, při kterém se vytvoří přesná kopie (repliky) virtuálního počítače a replika se poté udržuje v synchronizaci s původním počítačem. Pokud replikujete důležitý virtuální počítač, budete mít vždy kopii tohoto počítače připravenou ke spuštění.

Replikaci je možné spustit ručně nebo ji naplánovat. První replikace je plná (kopie celého počítače). Všechny následující replikace jsou přírůstkové a provádějí se s možností Sledování změněných bloků (str. 333), pokud tato možnost není zakázána.

Replikace vs. zálohování

Na rozdíl od plánovaných záloh replika zachovává pouze nejnovější stav virtuálního počítače. Replika zabírá místo v datovém úložišti, zatímco záloha může být uchovávána v levnějším úložišti.

Spouštění repliky je však mnohem rychlejší, než obnova a spouštění virtuálního počítače ze zálohy. Zapnutá replika pracuje rychleji než virtuální počítač spuštěný ze zálohy a nenačítá agenta pro VMware.

Příklady použití

- **Replikace virtuálního počítače na vzdáleném serveru.**

  Replikace vám umožní odolávat částečným nebo úplným selháním datového centra pomocí klonování virtuálních počítačů z primárního serveru na sekundární server. Sekundární soubor se obvykle nachází na vzdáleném místě, u nějž je nepravděpodobné, že by byl ovlivněn faktory prostředí, infrastruktury a dalšími faktory, které mohly způsobit selhání primárního serveru.
- **Replikace virtuálního počítače v rámci jednoho serveru (z jednoho hostitele/datového úložiště do jiného).**

  Replikaci v rámci jednoho serveru je možné použít u scénářů vysoké dostupnosti a obnovy po havárii.

Jaké činnosti je možné provést s replikou

- **Testování repliky** (str. 332)

  Replika bude zapnuta k otestování. Pomocí aplikace vSphere Client nebo jiných nástrojů zkontrolujte, zda replika pracuje správně. Replikace je během procesu testování pozastavena.
- **Převzetí služeb při selhání replikou** (str. 332)

  Převzetí služeb při selhání je převod pracovního zatížení z původního virtuálního počítače na jeho repliku. Replikace je během procesu převzetí služeb při selhání pozastavena.
- **Zálohování repliky**

Jak zálohování, tak replikace vyžadují přístup k virtuálním diskům a proto ovlivňují výkon hostitele, na kterém běží virtuální počítač. Pokud chcete mít repliku i zálohy virtuálního počítače, ale nechcete dále zvyšovat zátěž produkčního hostitele, replikujte počítač na jiného hostitele a nastavte zálohy repliky.

Omezení

Následující typy virtuálních počítačů není možné replikovat:

- Počítače odolné vůči chybám běžící na ESXi 5.5 a nižší.
- Počítače běžící se záloh.
- Repliky virtuálních počítačů

18.2.1.1 Tvorba plánu replikace

Plány replikace je nutné vytvářet pro každý počítač jednotlivě. Již existující plán není možné použít pro jiné počítače.

Jak vytvořit plán replikace

1. Vyberte virtuální počítač, který chcete replikovat.
2. Klikněte na možnost **Replikace**.

   Software zobrazí šablonu nového plánu replikace.
3. [Volitelné] Pokud chcete upravit název plánu replikace, klikněte na výchozí název.
4. Klikněte na možnost **Cílový počítač** a proveďte toto:
   a. Vyberte, zda chcete vytvořit novou repliku nebo použít existující repliku původního počítače.
   b. Vyberte hostitele ESXi a zadejte název nové repliky nebo vyberte existující.

      Výchozí název nové repliky je **[název původního počítače]_replica**.
   c. Klikněte na tlačítko **OK**.
5. [Pouze při replikaci na nový počítač] Klikněte na možnost **Datové úložiště** a vyberte datové úložiště pro virtuální počítač.
6. [Volitelné] Klikněte na možnost **Plán** a změňte plán replikace.

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

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

   Můžete také provést toto:
   - Nastavte období, pro které plán platí. Zaškrtněte políčko **Spustit plán v časovém rozsahu** a zadejte období.
   - Vypněte použití plánu. V tomto případě je možné replikaci spustit ručně.
7. [Volitelné] Klikněte na ikonu ozubeného kola a upravte možnosti replikace (str. 333).
8. Klikněte na tlačítko **Použít**.
9. [Volitelné] Chcete-li plán spustit ručně, klikněte na panelu plánu na tlačítko **Spustit**.

Po spuštění plánu replikace se replika virtuálního počítače zobrazí v seznamu **Všechna zařízení** s touto ikonou: 

18.2.1.2 Testování repliky

Jak připravit repliku pro testování

1. Vyberte repliku, kterou chcete testovat.
2. Klikněte na možnost **Testovat repliku**.
3. Klikněte na možnost **Spustit testování**.
4. Vyberte, zda se má zapnutá replika připojit k síti. Ve výchozím nastavení nebude replika připojena k síti.
5. [Volitelné] Pokud chcete připojit repliku k síti, zaškrtněte políčko **Zastavit původní virtuální počítač**, aby se původní počítač před zapnutím repliky vypnul.
6. Klikněte na možnost **Spustit**.

Jak zastavit testování repliky

1. Vyberte repliku, jejíž testování probíhá.
2. Klikněte na možnost **Testovat repliku**.
3. Klikněte na možnost **Zastavit testování**.
4. Potvrďte své rozhodnutí.

18.2.1.3 Převzetí služeb při selhání replikou

Jak převzít služby počítače při selhání replikou

1. Vyberte repliku, která má služby převzít.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Podpora převzetí služeb při selhání**.
4. Vyberte, zda se má zapnutá replika připojit k síti. Ve výchozím nastavení bude replika připojena ke stejné síti jako původní počítač.
5. [Volitelné] Pokud chcete repliku připojit k síti, zrušte zaškrtnutí políčka **Zastavit původní virtuální počítač**, aby původní počítač zůstal online.
6. Klikněte na možnost **Spustit**.

Když je replika ve stavu převzetí služeb, můžete si vybrat jednu z následujících akcí:

- **Zastavit převzetí služeb při selhání** (str. 332)

  Zastaví převzetí služeb, pokud bude původní počítač opraven. Replika se vypne. Replikace bude obnovena.
- **Trvalé převzetí služeb replikou** (str. 333)

  Tato okamžitá operace odstraní z virtuálního počítače označení repliky; replikace na něj tedy již nebude možná. Pokud chcete obnovit replikaci, upravte plán replikace a vyberte tento počítač jako zdroj.
- **Navrácení služeb po obnovení** (str. 333)

  Provede navrácení služeb po obnovení, pokud došlo k převzetí služeb počítačem, který není určen pro nepřetržitý provoz. Replika bude obnovena na původní nebo nový virtuální počítač. Až bude obnova na původní počítač dokončena, počítač se zapne a replikace se obnoví. Pokud vyberete obnovu na nový počítač, upravte plán replikace a vyberte tento počítač jako zdroj.

Zastavení převzetí služeb při selhání

Jak zastavit převzetí služeb při selhání

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.
2. Klikněte na možnost **Akce repliky**.

3. Klikněte na možnost **Zastavit převzetí služeb při selhání**.
4. Potvrďte své rozhodnutí.

Provedení trvalého převzetí služeb při selhání

Jak provést trvalé převzetí služeb při selhání

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Trvalé převzetí služeb při selhání**.
4. [Volitelné] Změňte název virtuálního počítače.
5. [Volitelné] Zaškrtněte políčko **Zastavit původní virtuální počítač**.
6. Klikněte na možnost **Spustit**.

Navrácení služeb po obnovení

Jak provést navrácení služeb po obnovení z repliky

1. Vyberte repliku, která je ve stavu převzetí služeb při selhání.
2. Klikněte na možnost **Akce repliky**.
3. Klikněte na možnost **Navrácení služeb po obnovení z repliky**.
   Software automaticky vybere původní počítač jako cílový.
4. [Volitelné] Klikněte na možnost **Cílový počítač** a proveďte toto:
   a. Vyberte, zda se navrácení služeb provede na nový nebo existující počítač.
   b. Vyberte hostitele ESXi a zadejte název nového počítače nebo vyberte existující.
   c. Klikněte na tlačítko **OK**.
5. [Volitelné] Při navrácení služeb na nový počítač můžete udělat i toto:
   - Klikněte na možnost **Datové úložiště** a vyberte datové úložiště pro virtuální počítač.
   - Pomocí možnosti **Nastavení virtuálního počítače** změňte velikost paměti, počet procesorů a síťová připojení virtuálního počítače.
6. [Volitelné] Klikněte na možnost **Možnosti obnovy** a upravte možnosti navrácení služeb (str. 334).
7. Klikněte na možnost **Spustit obnovu**.
8. Potvrďte své rozhodnutí.

18.2.1.4 Možnosti replikace

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

Sledování změněných bloků (CBT)

Tato možnost je podobná jako možnost zálohování Sledování změněných bloků (CBT) (str. 169).

Poskytování disku

Tato možnost definuje nastavení poskytování disku u repliky.

Výchozí nastavení: **Tenké poskytování**.

Jsou k dispozici následující hodnoty: **Tenké poskytování**, **Tlusté poskytování**, **Ponechat původní nastavení**.

Zpracování chyb

Tato možnost je podobná možnosti zálohování Zpracování chyb (str. 171).

Příkazy před-po

Tato možnost je podobná možnosti zálohování Příkazy před-po (str. 186).

Služba VSS pro virtuální počítače

Tato možnost je podobná možnosti zálohování Služba VSS pro virtuální počítače (str. 195).

18.2.1.5 Možnosti navrácení služeb po obnovení

Možnosti navrácení služeb po obnovení změníte kliknutím na odkaz **Možnosti obnovy** při konfiguraci.

Zpracování chyb

Tato možnost je podobná jako možnost Zpracování chyb (str. 215) při obnově.

Výkon

Tato možnost je podobná jako možnost Výkon (str. 217) při obnově.

Příkazy před-po

Tato možnost je podobná jako možnost Příkazy před-po (str. 217) při obnově.

Správa napájení virtuálního počítače

Tato možnost je podobná jako možnost Správa napájení virtuálního počítače (str. 219) při obnově.

18.2.1.6 Naplnění počáteční repliky

Abyste urychlili replikaci do vzdáleného umístění a ušetřili šířku pásma sítě, můžete provést naplnění repliky.

Důležité *Aby bylo možné provést naplnění repliky, musí být na cílovém hostiteli ESXi spuštěný Agent pro VMware (Virtual Appliance).*

Postup naplnění počáteční repliky

1. Proveďte jeden z následujících úkonů:
   - Pokud lze původní virtuální počítač vypnout, vypněte ho a přejděte ke kroku 4.
   - Pokud původní virtuální počítač vypnout nejde, pokračujte dalším krokem.
2. Vytvoření plánu replikace (str. 331).

   Při vytváření plánu vyberte v části **Cílový počítač** možnost **Nová replika** a hostitele ESXi původního počítače.
3. Plán jednou spusťte.

   V původním hostiteli ESXi se vytvoří replika.
4. Vyexportujte soubory virtuálního počítače (nebo repliky) na externí pevný disk.
   a. Připojte externí pevný disk k počítači se spuštěným klientem vSphere.
   b. Připojte klienta vSphere k původnímu serveru vCenter nebo hostiteli ESXi.
   c. Vyberte nově vytvořenou repliku v inventáři.
   d. Klikněte na **Soubor** > **Exportovat** > **Exportovat šablonu OVF**.

e. V poli **Adresář** zadejte složku na externím pevném disku.

f. Klikněte na tlačítko **OK**.

5. Přeneste pevný disk do vzdáleného umístění.
6. Naimportujte repliku do cílového hostitele ESXi.
   a. Připojte externí pevný disk k počítači se spuštěným klientem vSphere.
   b. Připojte klienta vSphere k cílovému serveru vCenter nebo hostiteli ESXi.
   c. Klikněte na **Soubor** > **Nasadit šablonu OVF**.
   d. V poli **Nasadit ze souboru nebo URL** zadejte šablonu, kterou jste exportovali v kroku 4.
   e. Dokončete proces importu.
7. Upravte plán replikace vytvořený v kroku 2. V poli **Cílový počítač** vyberte možnost **Existující replika** a poté vyberte naimportovanou repliku.

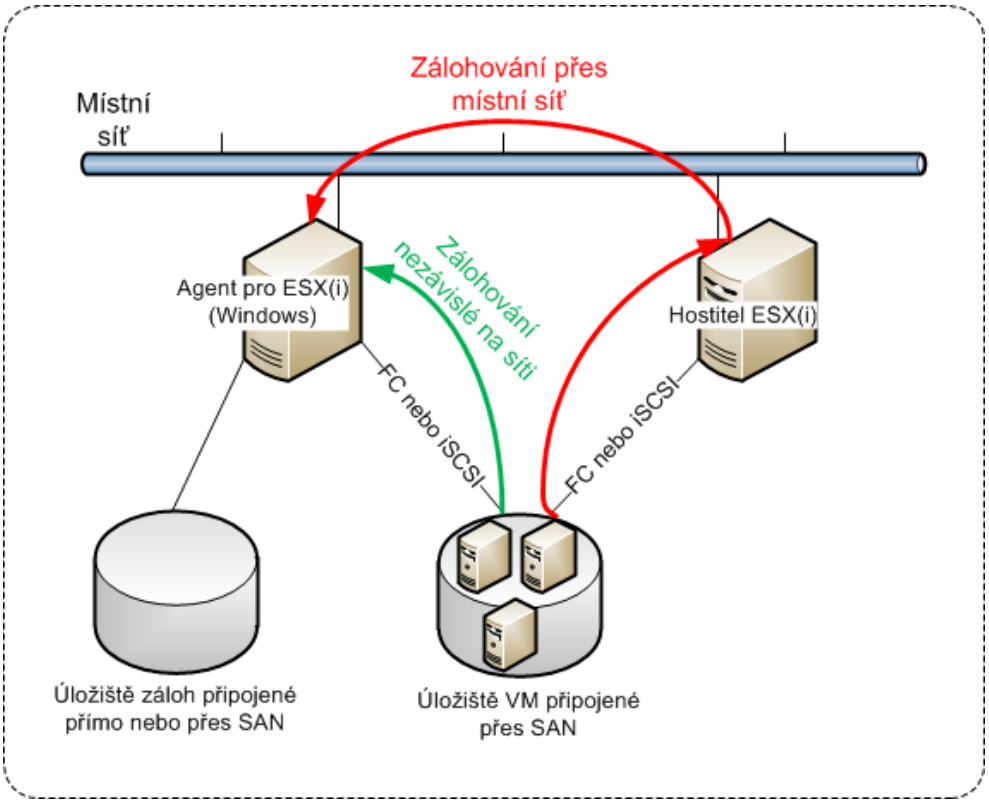
Software bude poté pokračovat v aktualizaci repliky. Všechny replikace budou přírůstkové.

18.2.2 Zálohování nezávislé na LAN

Pokud jsou produkční hostitelé ESXi tak silně zatíženi, že není vhodné spouštět virtuální zařízení, zvažte instalaci Agenta pro VMware (Windows) do fyzického počítače mimo infrastrukturu ESXi.

Pokud ESXi používá úložiště připojené pomocí sítě SAN, nainstalujte agenta do počítače připojeného ke stejné síti SAN. Agent bude zálohovat virtuální počítače přímo z úložiště a ne pomocí hostitele ESXi a LAN. Tato funkce se nazývá zálohování nezávislé na LAN.

Na následujícím obrázku je zálohování založené na LAN a zálohování bez LAN. Přístup na virtuální počítače bez LAN je dostupný, pokud máte síť SAN se standardem Fibre Channel nebo iSCSI. Chcete-li zcela odstranit přenos zálohovaných dat prostřednictvím LAN, uložte zálohy na místní disk počítače agenta nebo na úložiště připojené pomocí SAN.



Jak agentovi povolit přímý přístup k datovému úložišti

1. Nainstalujte Agenta pro VMware do počítače se systémem Windows, který má síťový přístup k serveru vCenter.
2. Připojte k počítači číslo logické jednotky (LUN), které hostí datové úložiště. Zvažte následující:
   - Použijte stejný protokol, (tj. iSCSI nebo FC), který je použitý pro připojení datového úložiště k ESXi.
   - LUN *nesmí* být inicializováno a ve **Správci disků** se musí zobrazit jako vypnutý (offline) disk. Pokud systém Windows inicializuje LUN, může se poškodit a stát se pro VMware vSphere nečitelným.

     Aby se zabránilo inicializaci LUN, parametr **SAN Policy** se při instalaci Agenta pro VMware (Windows) automaticky nastaví na **Offline All**.

Agent tak pro přístup k virtuálním diskům použije transportní režim SAN, tj. přečte sektory LUN prostřednictvím protokolu iSCSI/FC bez rozpoznání systému souborů VMFS (na což systém Windows není upozorněn).

Omezení

- V systému vSphere 6.0 a novějším agent nemůže použít transportní režim SAN, pokud některé disky virtuálního počítače jsou umístěny na virtuálním svazku VMware (VVol) a jiné nikoli. Zálohování takových virtuálních počítačů se nezdaří.
- Šifrované virtuální počítače, zavedené ve verzi VMware vSphere 6.5, budou zálohovány prostřednictvím sítě LAN, a to i v případě, že pro agenta nakonfigurujete transportní režim SAN. Agent se vrátí do transportního režimu NBD, protože VMware nepodporuje transportní režim SAN k zálohování šifrovaných virtuálních disků.

Příklad

Používáte-li úložiště iSCSI SAN, nakonfigurujte spouštěč iSCSI na počítači se systémem Windows, na kterém je nainstalován Agent pro VMware.

Postup konfigurace zásad SAN

1. Přihlaste se jako správce, otevřete příkazový řádek, zadejte **`diskpart`** a poté stiskněte klávesu **Enter**.
2. Zadejte **`san`** a poté stiskněte klávesu **Enter**. Ověřte, že se zobrazí následující údaje: **SAN Policy : Offline All**.
3. Pokud je pro zásady SAN nastavena jiná hodnota:
   a. Zadejte příkaz **`san policy=offlineall`**.
   b. Stiskněte klávesu **Enter**.
   c. Chcete-li ověřit, zda bylo nastavení správně uloženo, proveďte znovu druhý krok.
   d. Restartujte počítač.

Postup konfigurace spouštěče iSCSI

1. Přejděte na **Ovládací panely** > **Nástroje pro správu** > **Iniciátor iSCSI**.

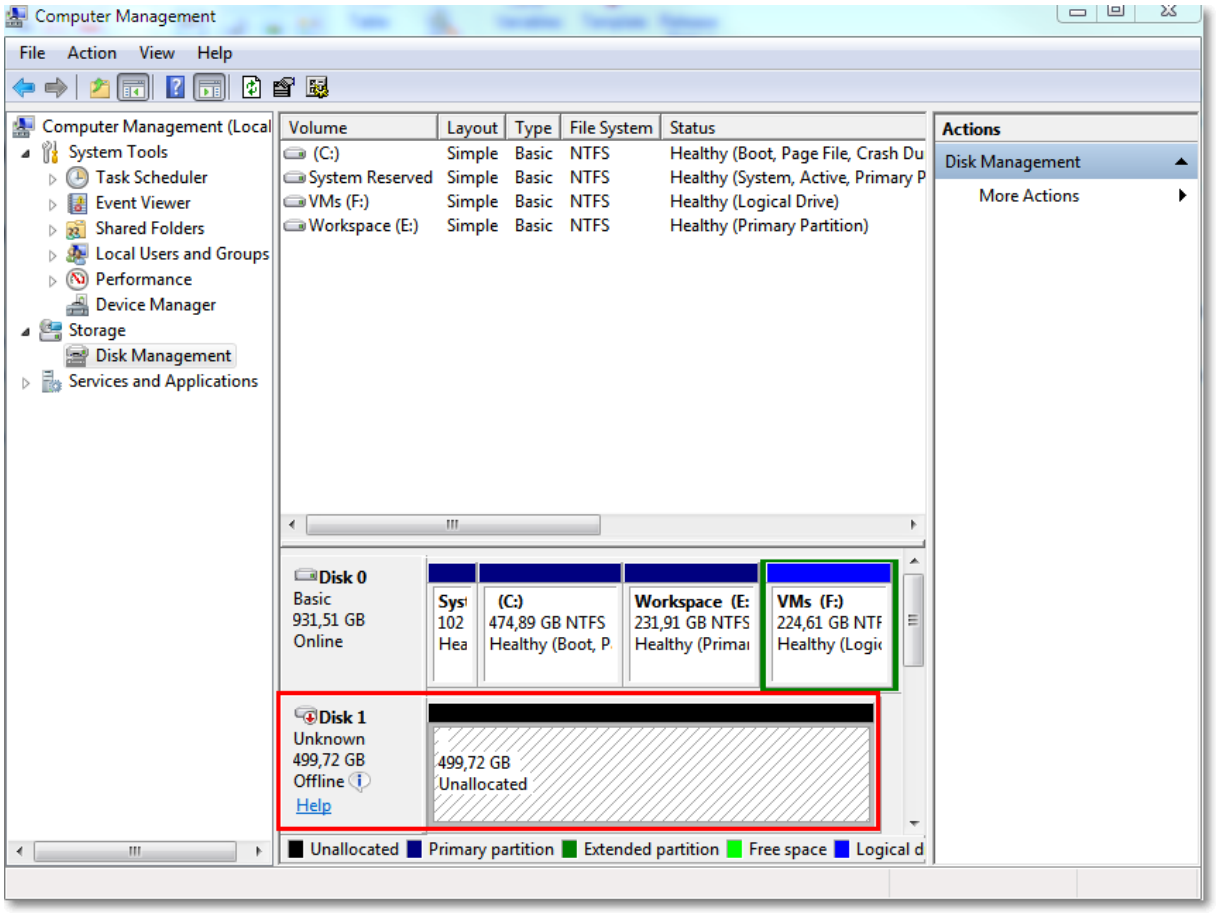
   ***Tip**: Pokud applet **Nástroje pro správu** nevidíte, bude pravděpodobně potřeba použít jiné zobrazení **Ovládacích panelů** než **Domů** nebo **Kategorie**, případně použijte hledání.*

2. Pokud Iniciátor iSCSI společnosti Microsoft spouštíte poprvé, potvrďte, že chcete spustit Službu iniciátoru iSCSI společnosti Microsoft.
3. Na kartě **Cíle** zadejte plně kvalifikovaný název domény nebo IP adresu zařízení SAN a poté klikněte na tlačítko **Rychlé připojení**.
4. Vyberte LUN, které hostí datové úložiště, a klikněte na tlačítko **Připojit**.

Není-li zobrazeno žádné LUN, přesvědčte se, zda nastavení zón na cíli iSCSI povolujte počítačům se spuštěnými agenty přístup k LUN. Příslušný počítač musí být na cíli přidán k povoleným spouštěčům iSCSI.

5. Klikněte na tlačítko **OK**.

Připravené zařízení SAN LUN by se mělo objevit v okně **Správa disků**, jak je zobrazeno na snímku obrazovky níže.



18.2.3 Použití snímků hardwaru SAN

Používá-li váš VMware vSphere jako datové úložiště systém úložiště SAN (Storage Area Network), můžete v agentovi pro VMware (Windows) povolit při vytváření zálohy použití snímků hardwaru SAN.

Důležité: *Podporováno je pouze úložiště NetApp SAN.*

Proč snímky hardwaru SAN používat?

Agent pro VMWare snímek virtuálního počítače potřebuje k vytvoření konzistentní zálohy. Jelikož agent z tohoto snímku čte obsah virtuálního disku, je nutné ho zachovat po celou dobu zálohování.

Ve výchozím nastavení, používá agent nativní snímky WMware vytvořené hostitelem ESXi. V době, kdy je snímek zachován, jsou soubory virtuálního disku ve stavu jen pro čtení a hostitel zapisuje všechny změny provedené na discích do samostatných rozdílových souborů. Jakmile se zálohování dokončí, hostitel snímek smaže, čímž sloučí rozdílové soubory se soubory virtuálního disku.

Zachování i odstranění snímku ovlivňuje výkon virtuálního počítače. U velkých virtuálních disků a rychlých změn dat tyto operace trvají dlouhou dobu, během které se může výkon zhoršit. V krajních

případech při zálohování několika počítačů najednou mohou narůstající rozdílové soubory téměř zaplnit datové úložiště a způsobit vypnutí všech virtuálních počítačů.

Využití prostředku hypervisor můžete snížit, když snímky přebere síť SAN. V tomto případě bude pořadí operací následující:

1. Hostitel ESXi vytvoří na začátku zálohování snímek VMWare, aby zajistil konzistentní stav virtuálních disků.
2. Síť SAN vytvoří snímek hardwaru svazku nebo LUN, který obsahuje virtuální počítač a jeho snímek WMware. Tato operace běžně zabere pár vteřin.
3. Hostitel ESXi snímek VMware odstraní. Agent pro VMware přečte obsah virtuálního disku ze snímku hardwaru SAN.

Jelikož je snímek WMware zachován pouze na několik vteřin, pokles výkonu virtuálního počítače je minimalizován.

Co je potřeba k vytvoření snímků hardwaru SAN?

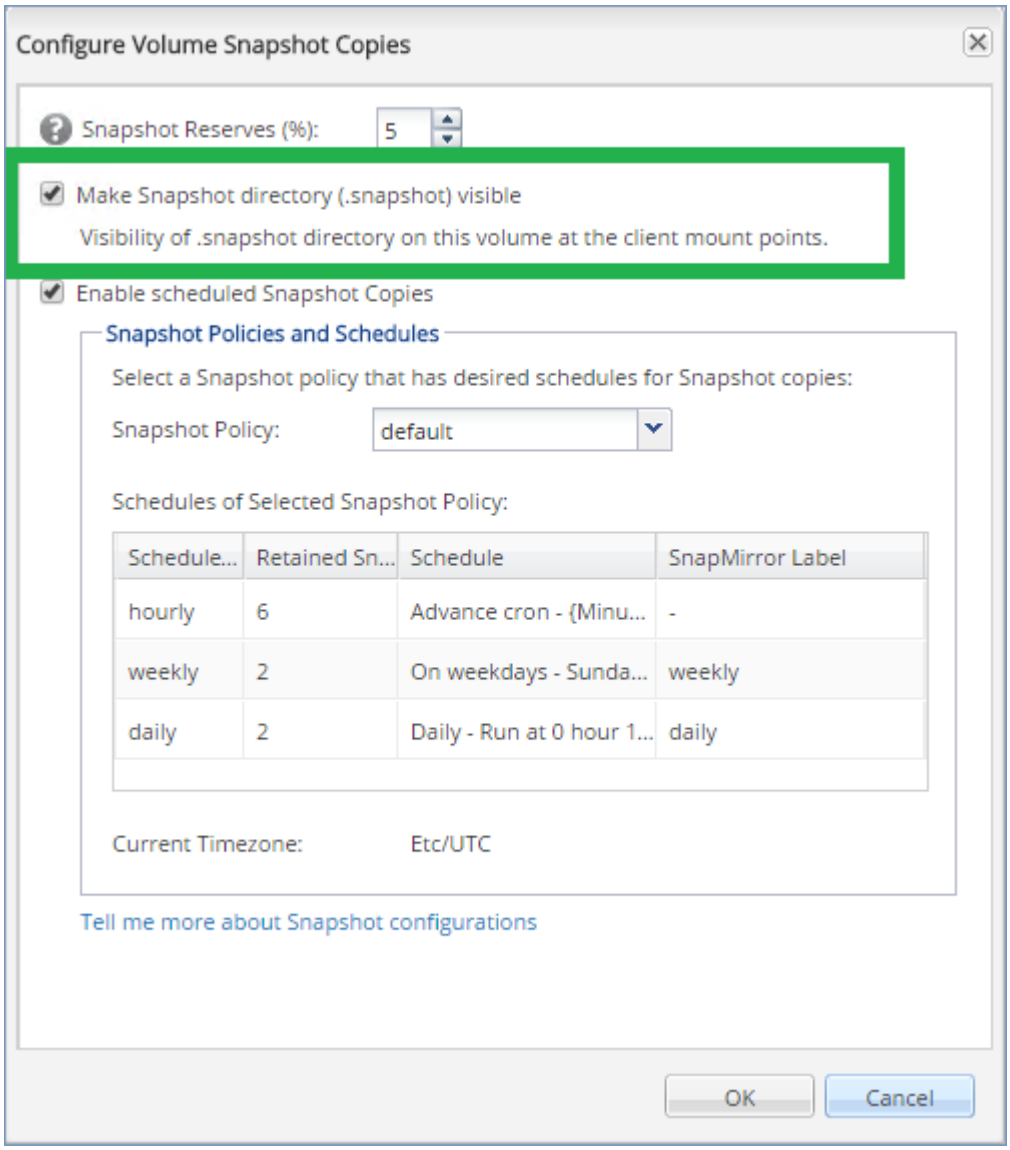
Jestliže chcete při zálohování virtuálních počítačů používat snímky hardwaru SAN, musíte splňovat následující podmínky:

- Úložiště NetApp SAN splňuje požadavky popsané v části Požadavky úložiště NetApp SAN (str. 338).
- Počítač, na kterém běží agent pro VMware (Windows), je nakonfigurován podle popisu v části Konfigurace počítače, na kterém běží agent pro WMware (str. 340).
- Úložiště SAN je registrováno na serveru pro správu (str. 341).
- [Existují-li agenti pro VMware, kteří nejsou zaregistrovaní podle výše uvedené registrace] Virtuální počítače umístěné v úložišti SAN jsou přiřazeny agentům podporujícím úložiště SAN, jak je popsáno v části Navázání virtuálního počítače (str. 342).
- Možnost zálohy Snímky hardwaru SAN (str. 189) je v možnostech plánu ochrany povolena.

18.2.3.1 Požadavky úložiště NetApp SAN

- Úložiště SAN musí být použito jako datové úložiště NFS nebo iSCSI.
- SAN musí používat Data ONTAP 8.1 nebo novější v režimu **Clustered Data ONTAP (cDOT)**. Režim **7-mode** není podporovaný.

- Ve správci NetApp OnCommand System Manager musí být zaškrtnuté políčko **Snapshot copies (Kopie snímků)** > **Configure (Konfigurovat)** > **Make Snapshot directory (.snapshot) visible (Nastavit adresář snímků (.snapshot) jako viditelný)** pro svazek, kde se datové úložiště nachází.

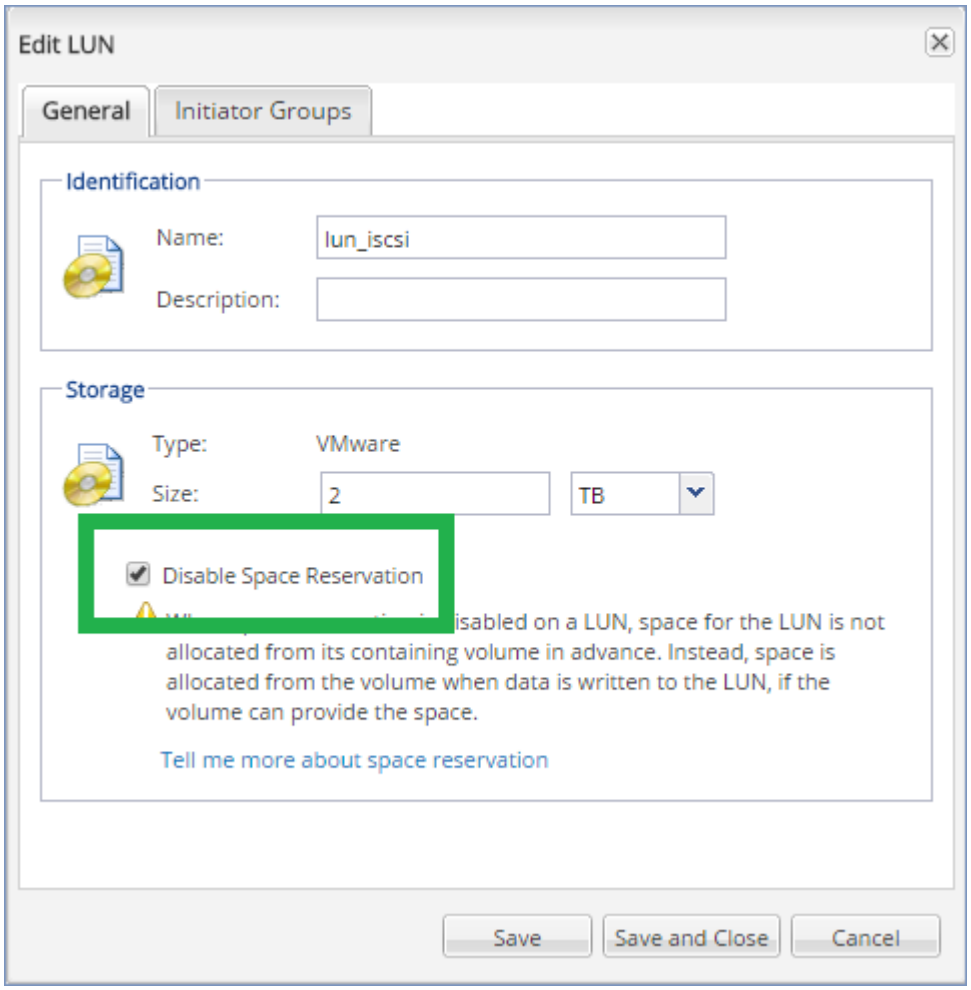


- [Pro datová úložiště NFS] Na virtuálním počítači úložiště (SVM: Storage Virtual Machine), který byl zadán při vytvoření datového úložiště, musí být povolen přístup ke sdíleným složkám systému souborů NFS z klientů NFSv3 ve Windows. Přístup lze povolit následujícím příkazem:

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

Další informace najdete v dokumentu NetApp Best Practices (Osvědčené postupy pro NetApp): https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices

- [Pro datová úložiště iSCSI] Ve správci NetApp OnCommand System Manager musí být zaškrtnuté políčko **Disable Space Reservation (Zakázat rezervaci prostoru)** pro logickou jednotku (LUN) iSCSI, kde se datové úložiště nachází.



18.2.3.2 Nakonfigurování počítače, na kterém běží Agent pro VMware

V závislosti na tom, jestli se úložiště SAN používá jako datové úložiště NFS nebo iSCSI, si níže projděte informace v odpovídající části.

Nakonfigurování Iniciátoru iSCSI

Musí být splněny následující podmínky:

- Je nainstalovaný Iniciátor iSCSI společnosti Microsoft.
- Typ spouštění služby Iniciátor iSCSI společnosti Microsoft je nastavený na **Automaticky** nebo **Ručně**. To lze provést v modul snap-in **Služby**.
- Iniciátor iSCSI konfigurujete podle postupu popsaného v tématu Zálohování nezávislé na LAN (str. 335) v části s příkladem.

Nakonfigurování klienta systému souborů NFS

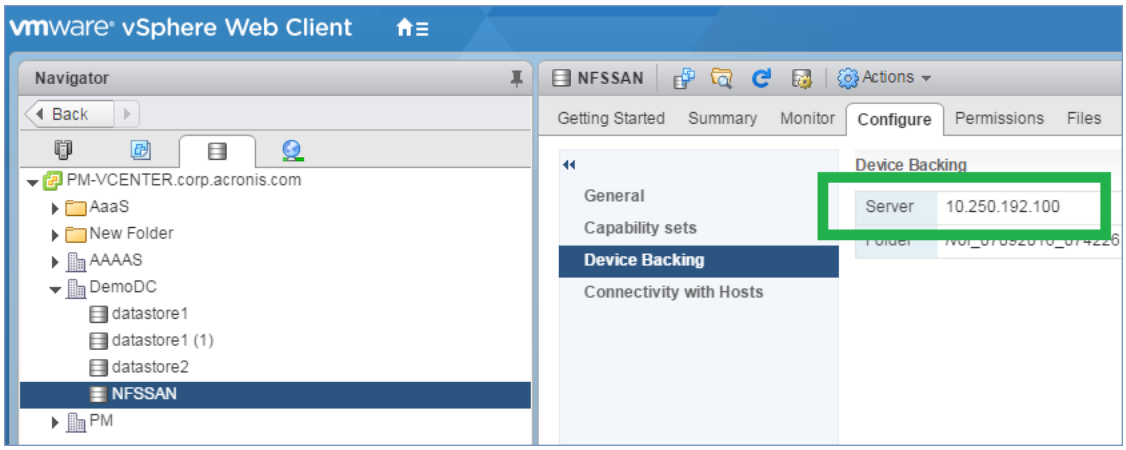
Musí být splněny následující podmínky:

- Je nainstalována součást **Služby pro systém souborů NFS** společnosti Microsoft (v systému Windows Server 2008) nebo **Klient pro systém souborů NFS** společnosti Microsoft (v systému Windows Server 2012 a novějším).

- Pro součást Klient pro systém souborů NFS je nakonfigurován anonymní přístup. To lze provést následujícím způsobem:
  a. Otevřete Editor registru.
  b. Vyhledejte následující klíč registru:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default
  c. V tomto klíči vytvořte novou hodnotu **DWORD** s názvem **AnonymousUID** a nastavte pro ni údaj hodnoty 0.
  d. Ve stejném klíči vytvořte novou hodnotu **DWORD** s názvem **AnonymousGID** a nastavte pro ni údaj hodnoty 0.
  e. Restartujte počítač.

18.2.3.3 Registrace úložiště SAN na serveru pro správu

1. Klikněte na **Nastavení** > **Úložiště SAN**.
2. Klikněte na možnost **Přidat úložiště**.
3. [Volitelné] V poli **Název** změňte název úložiště.
   Tento název se zobrazí na kartě **Úložiště SAN**.
4. Do pole **Název hostitele nebo IP adresa** zadejte virtuální počítač NetApp Storage Virtual Machine (SVM, označuje se také jako filtr), který byl zadán při vytváření datového úložiště.
   Pokud chcete vyhledat požadované informace ve webovém klientu VMware vSphere, vyberte datové úložiště a klikněte na možnost **Configure (Konfigurovat)** > **Device backing (Záloha zařízení)**. Název hostitele nebo IP adresa se zobrazí v poli **Server**.



5. Do polí **User name (Uživatelské jméno)** a **Password (Heslo)** zadejte pověření správce SVM.

Důležité *Zadaný účet musí být místní správce ve virtuálním počítači SVM a nikoliv správce celého systému NetApp.*

Můžete zadat existujícího uživatele nebo vytvořit nového. Nového uživatele vytvoříte tak, že ve správci NetApp OnCommand System Manager přejdete do oddílu **Configuration (Konfigurace)** > **Security (Zabezpečení)** > **Users (Uživatelé)** a pak vytvoříte nového uživatele.

6. Vyberte jednoho nebo víc agentů pro VMware (Windows), kterým bude uděleno oprávnění ke čtení pro dané zařízení SAN.
7. Klikněte na tlačítko **Přidat**.

18.2.4 Použití místně připojeného úložiště

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

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

Použití místně připojeného úložiště předpokládá, že agent vždy zálohuje stejné počítače. Pracuje-li ve vSphere více agentů a jeden nebo více z nich využívá místně připojené úložiště, je třeba ručně spojit (str. 342) každého agenta se všemi počítači, které agent musí zálohovat. Jinak, pokud budou počítače znovu distribuovány mezi agenty serverem pro správu, zálohy jednoho počítače mohou být rozprostřeny na více úložišť.

Úložiště můžete přidat již fungujícímu agentovi nebo při nasazení agenta ze šablony OVF (str. 94).

Jak připojit úložiště k již fungujícímu agentu

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

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

Jak vybrat místně připojené úložiště jako cíl zálohování

Při vytváření plánu ochrany (str. 122) v dialogovém okně **Kam se má zálohovat** vyberte položku **Místní složky** a zadejte písmeno odpovídající místně připojenému úložišti, například **D:**.

18.2.5 Navázání virtuálního počítače

Toto téma obsahuje přehled uspořádání operací více agentů v rámci VMware vCenter na serveru.

Níže popsaný distribuční algoritmus funguje pro virtuální zařízení i agenty instalované ve Windows.

Distribuční algoritmus

Virtuální počítače jsou automaticky rovnoměrně rozložené mezi agenty pro VMware. Rovnoměrně znamená, že každý agent má stejný počet počítačů. Množství místa na disku zabraného virtuálním počítačem se nepočítá.

Při výběru agenta pro počítač se však software snaží optimalizovat celkový výkon systému. V potaz se bere hlavně umístění agenta a virtuálního počítače. Upřednostňuje se agent na stejném hostiteli. Pokud není na stejném hostiteli žádný agent, preferuje se agent ze stejného clusteru.

Jakmile je virtuální počítač přiřazen k agentovi, všechny zálohy počítače budou prováděny tímto agentem.

Redistribuce

Redistribuce se provádí pokaždé, když je rovnováha porušena, nebo přesněji, pokud nerovnováha mezi agenty dosáhne 20 procent. To se může stát po přidání nebo odebrání počítače nebo agenta, nebo se počítač přesune do jiného hostitele nebo clusteru nebo ručně přiřadíte počítač agentovi. Pokud se to stane, server pro správu přerozdělí počítače pomocí stejného algoritmu.

Například si uvědomíte, že potřebujete více agentů za účelem zlepšení propustnosti a umístíte do clusteru další virtuální počítač. Server pro správu přiřadí novému agentovi nejvhodnější počítače. Zatížení předchozích agentů se sníží.

Pokud agenta ze serveru pro správu odeberete, počítače přiřazené tomuto agentovi budou rozmístěny mezi zbývající agenty. To se však nestane, pokud se agent poškodí nebo je ručně odstraněn z klienta vSphere. Redistribuce se spustí pouze tehdy, až takového agenta odstraníte z webového rozhraní.

Zobrazení výsledků redistribuce

Výsledek automatického rozdělení je možné zobrazit:

- ve sloupci **Agent**, který je dostupný pro každý virtuální počítač v části **Všechna zařízení**, nebo
- v části **Přiřazené virtuální počítače** na panelu **Podrobnosti**, která se zobrazí při výběru možnosti **Nastavení** v části **Agenti**.

Ruční navázání

Navázání Agenta pro VMware umožňuje vyloučit virtuální počítač z procesu rozdělení tak, že určí agenta, který vždy musí tento počítač zálohovat. Celková rovnováha bude zachována, ale tento konkrétní počítač může být předán jinému agentovi pouze v případě, že je původní agent odebrán.

Jak navázat počítač k agentovi

1. Vyberte požadovaný počítač.
2. Klikněte na možnost **Podrobnosti**.
   V části **Přiřazený agent** software zobrazí agenta, který momentálně spravuje vybraný počítač.
3. Klikněte na **Změnit**.
4. Zvolte **Ručně**.
5. Vyberte agenta, ke kterému chcete navázat počítač.
6. Klikněte na tlačítko **Uložit**.

Jak odpojit počítač od agenta

1. Vyberte požadovaný počítač.
2. Klikněte na možnost **Podrobnosti**.
   V části **Přiřazený agent** software zobrazí agenta, který momentálně spravuje vybraný počítač.
3. Klikněte na **Změnit**.
4. Zvolte **Automaticky**.
5. Klikněte na tlačítko **Uložit**.

Vypnutí automatického přiřazení k agentovi

Chcete-li vyloučit automatické přiřazení k agentovi pro VMware z procesu rozdělení, můžete ho vypnout určením seznamu počítačů, které tento agent musí zálohovat. Celková rovnováha bude mezi ostatními agenty zachována.

Automatické přiřazení k agentovi nelze vypnout, pokud neexistují další registrovaní agenti nebo u všech ostatních agentů není vypnuto automatické přiřazení.

Jak vypnout automatické přiřazení k agentovi

1. Klikněte na možnost **Nastavení** > **Agenti**.
2. Vyberte agenta pro VMware, u kterého chcete automatické přiřazení vypnout.
3. Klikněte na možnost **Podrobnosti**.
4. Vypněte přepínač **Automatické přiřazení**.

Příklady použití

- Ruční navázání je vhodné, pokud chcete, aby byl konkrétní (velmi objemný) počítač zálohován agentem pro VMware (Windows) pomocí standardu Fibre Channel, zatímco ostatní počítače budou zálohovány pomocí virtuálních zařízení.
- Používáte-li snímky hardwaru SAN (str. 337), je ruční navázání nezbytné. Agenta pro VMware (Windows), pro kterého jsou snímky hardwaru SAN nakonfigurované, svažte s počítači nacházejícími se na datovém úložišti SAN.
- Má-li agent místně připojené úložiště (str. 342), pak je svázání virtuálních počítačů s agentem nutné.
- Vypnutí automatického přiřazení vám umožní zajistit, že se konkrétní počítač bude předvídatelně zálohovat podle vámi určeného plánu. Agent, který zálohuje pouze jeden virtuální počítač, nemůže být v určeném čase zaneprázdněn zálohováním dalších virtuálních počítačů.
- Vypnutí automatického přiřazení je užitečné, když máte několik hostitelů ESXi, kteří jsou geograficky oddělení. Vypnete-li automatické přiřazení a potom navážete virtuální počítače běžící na jednotlivých hostitelích k agentům běžícím na stejných hostitelích, zajistíte tak, že žádný agent nebude zálohovat počítače běžící na vzdálených hostitelích ESXi, čímž snížíte zatížení sítě.

18.2.6 Podpora migrace VM

Tato část poskytuje informace o tom, co lze očekávat při migraci virtuálních počítačů v prostředí vSphere, včetně migrace mezi hostiteli ESXi, kteří jsou součástí clusteru vSphere.

vMotion

vMotion přesune stav a konfiguraci virtuálního počítače do jiného hostitelského počítače, zatímco disky počítače zůstanou ve stejném umístění na sdíleném úložišti.

- Funkce vMotion Agenta pro VMware (Virtual Appliance) není podporována a je vypnuta.
- Funkce vMotion virtuálního počítače je při zálohování vypnutá. Zálohy budou po dokončení migrace opět pokračovat.

Funkce Storage vMotion

Storage vMotion přesune disky virtuálního počítače z jednoho datového úložiště do druhého.

- Funkce Storage vMotion Agenta pro VMware (Virtual Appliance) není podporována a je vypnuta.
- Funkce Storage vMotion virtuálního počítače je při zálohování vypnutá. Zálohy budou po migraci opět pokračovat.

18.2.7 Správa prostředí pro virtualizaci

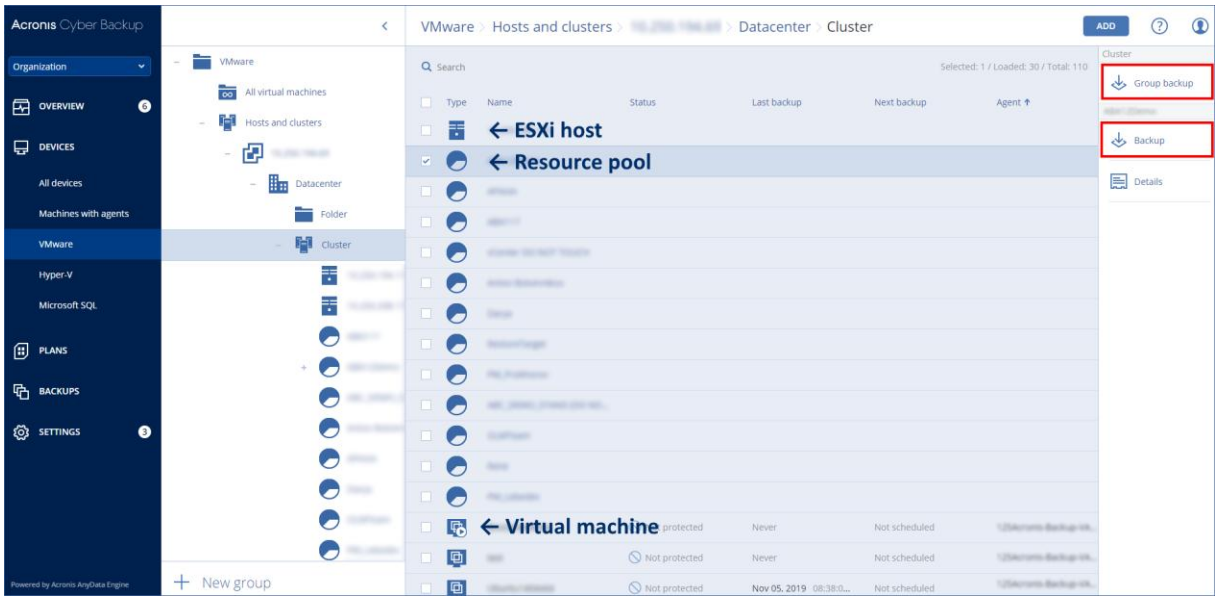
Prostředí vSphere, Hyper-V a Virtuozzo si můžete prohlédnout v nativním zobrazení. Po instalaci a registraci odpovídajícího agenta se karta **VMware**, **Hyper-V** nebo **Virtuozzo** zobrazí v části **Zařízení**.

Na kartě **VMware** můžete zálohovat následující objekty infrastruktury vSphere:

- Datové centrum
- Složka
- Cluster
- Hostitel ESXi
- Fond prostředků

Každý z těchto objektů infrastruktury pracuje jako skupinový objekt virtuálních počítačů. Když na některý z těchto skupinových objektů použijete plán ochrany, budou zálohovány všechny virtuální počítače, které jsou součástí skupiny. Kliknutím na tlačítko **Zálohovat** můžete zálohovat vybranou skupinu počítačů, nebo kliknutím na tlačítko **Skupina zálohování** můžete zálohovat nadřazenou skupinu počítačů, které je vybraná skupina součástí.

Vybrali jste například cluster a pak jste vybrali fond prostředků, který je jeho součástí. Pokud kliknete na tlačítko **Zálohovat**, budou zálohovány všechny virtuální počítače zahrnuté ve vybraném fondu prostředků. Pokud kliknete na tlačítko **Skupina zálohování**, budou zálohovány všechny virtuální počítače zahrnuté v daném clusteru.



Můžete změnit pověření k přístupu pro vCenter Server nebo samostatného hostitele ESXi bez opětovné instalace agenta.

Jak změnit přístupová pověření serveru vCenter nebo hostitele ESXi

1. V části **Zařízení** klikněte na **VMware**.
2. Klikněte na **Hostitelé a clustery**.
3. V seznamu **Hostitelé a clustery** (vpravo od stromu **Hostitelé a clustery**), vyberte server vCenter nebo samostatného hostitele ESXi, kterého jste určili při instalaci Agenta pro VMware.
4. Klikněte na **Podrobnosti**.
5. V části **Pověření** klikněte na uživatelské jméno.
6. Zadejte nová pověření k přístupu a klikněte na **OK**.

18.2.8 Zobrazení stavu zálohy v klientovi vSphere Client

V klientovi vSphere Client můžete zobrazit stav zálohy a čas posledního zálohování virtuálního počítače.

Tyto informace se zobrazí ve shrnutí virtuálního počítače (**Shrnutí** > **Vlastní atributy**/**Anotace**/**Poznámky** v závislosti na typu klienta a verzi vSphere). Můžete také povolit sloupce **Poslední záloha** a **Stav zálohy** na kartě **Virtuální počítače** pro jakéhokoli hostitele, datové centrum, složku, fond zdrojů nebo celý vCenter Server.

Aby bylo možné použít tyto atributy, musí mít Agent pro VMware následující oprávnění nad rámec oprávnění popsaných v tématu Agent pro VMware – potřebná oprávnění (str. 346):

- **Globální** > **Spravovat vlastní atributy**
- **Globální** > **Nastavit vlastní atribut**

18.2.9 Agent pro VMware – potřebná oprávnění

Tato část popisuje oprávnění vyžadovaná k operacím s virtuálními počítači ESXi a k nasazování virtuálních zařízení.

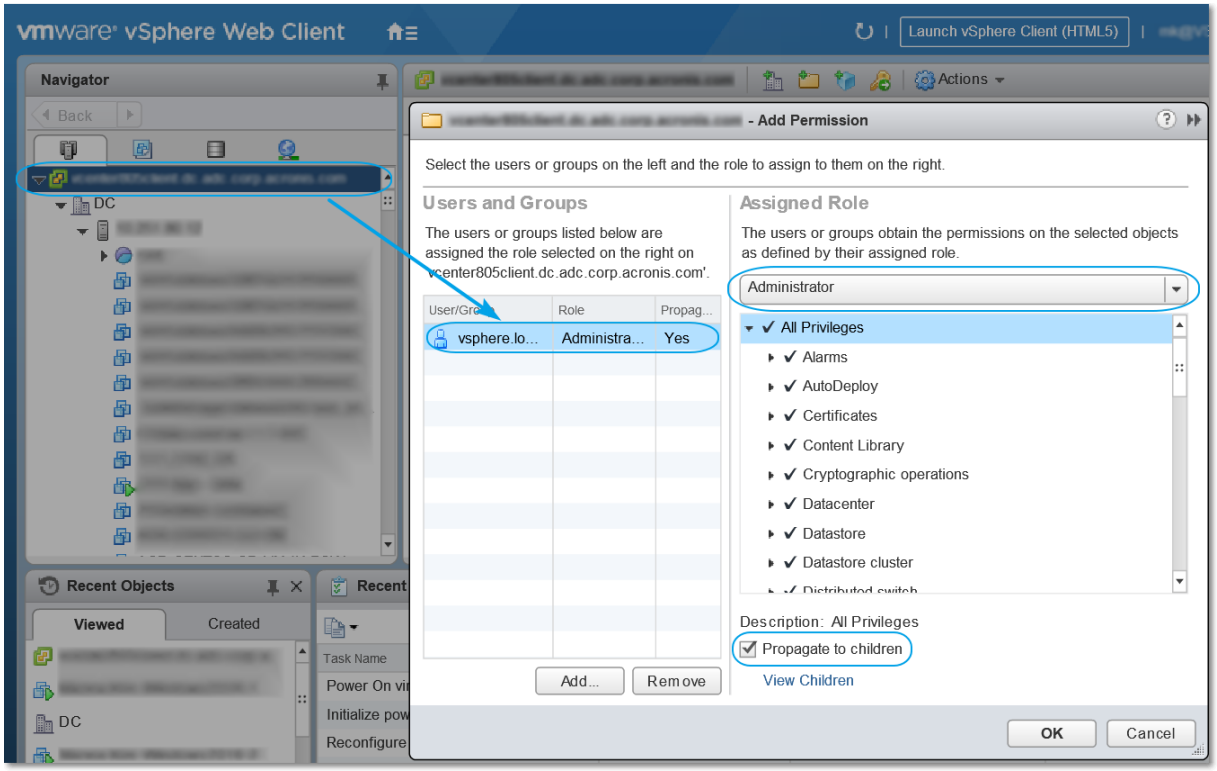
Za účelem provedení operací s objekty vCenter, například s virtuálními počítači, hostiteli ESXi, clustery, vCenter a dalšími objekty, provede Agent pro VMware ověření v centru vCenter nebo na hostiteli ESXi pomocí pověření vSphere zadaných uživatelem. Účet vSphere používaný Agentem pro VMware pro připojení k vSphere musí mít na všech úrovních infrastruktury vSphere počínaje úrovní vCenter požadovaná oprávnění.

Účet vSphere s potřebnými oprávněními můžete určit během instalace nebo konfigurace Agenta pro VMware. Budete-li účet chtít později změnit, přečtěte si část Správa virtualizačních prostředí (str. 344).

Postup přiřazení oprávnění uživateli vSphere na úrovni vCenter je následující:

1. Přihlaste se k webovému klientovi vSphere.
2. Pravým tlačítkem myši klikněte na položku vCenter a na možnost **Přidat oprávnění**.
3. Vyberte nebo přidejte nového uživatele s požadovanou rolí (role musí zahrnovat všechna požadovaná oprávnění z tabulky níže).

4. Vyberte možnost **Přenést na podřízené položky**.



		Operace				
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**	**Nasazení virtuálního zařízení**
Kryptografické operace (počínaje vSphere 6.5)	**Přidání disku**	+*				
	Přímý přístup	+*				
Datové úložiště	**Přidělit prostor**		+	+	+	+
	Procházet datové úložiště				+	+
	Konfigurovat datové úložiště	+	+	+	+	+
	Operace se soubory na nízké úrovni				+	+
Globální	**Licence**	+	+	+	+	
	Zakázat metody	+	+	+		
	Povolit metody	+	+	+		

		Operace				
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**	**Nasazení virtuálního zařízení**
	Spravovat vlastní atributy	+	+	+		
	Nastavit vlastní atributy	+	+	+		
Konfigurace > hostitele	**Konfigurace automatického spuštění virtuálního počítače**					+
	Konfigurace oddílu úložiště				+	
Inventář > hostitele	**Upravit cluster**					+
Místní operace > hostitele	**Vytvořit virtuální počítač**				+	+
	Odstranit virtuální počítač				+	+
	Změnit konfiguraci virtuálního počítače				+	+
Síť	**Přiřadit síť**		+	+	+	+
Zdroj	**Přiřadit virtuální počítač k fondu zdrojů**		+	+	+	+
Virtuální zařízení vApp	**Přidat virtuální počítač**				+	
	Import					+
Konfigurace > virtuálního počítače	**Přidat existující disk**	+	+		+	
	Přidat nový disk		+	+	+	+
	Přidat nebo odebrat zařízení		+		+	+
	Pokročilé	+	+	+		+
	Změnit počet CPU		+			
	Sledován změn disku	+		+		
	Zapůjčení disku	+		+		
	Paměť		+			
	Odebrat disk	+	+	+	+	
	Přejmenovat		+			
	Nastavit poznámku				+	

		Operace				
Objekt	**Oprávnění**	**Zálohování virtuálního počítače**	**Obnovení do nového virtuálního počítače**	**Obnovení do existujícího virtuálního počítače**	**Spuštění VM ze zálohy**	**Nasazení virtuálního zařízení**
	Nastavení		+	+	+	
Hostované operace >virtuálního počítače	**Spuštění programu hostovaných operací**	+**				+
	Dotazování hostovaných operací	+**				+
	Změny hostovaných operací	+**				
Interakce > virtuálního počítače	**Získat kontrolní lístek pro hosty** (vSphere 4.1 a 5.0)				+	+
	Konfigurovat disky CD		+	+		
	Interakce konzole					+
	Správa hostovaného operačního systému prostřednictvím rozhraní API VIX (vSphere 5.1 a novější)				+	+
	Vypnout			+	+	+
	Zapnout		+	+	+	+
Inventář > virtuálního počítače	**Vytvořit z existujícího**		+	+	+	
	Vytvořit nový		+	+	+	+
	Přesunout					+
	Registrovat				+	
	Odebrat		+	+	+	+
	Zrušit registraci				+	
Poskytování > virtuálního počítače	**Povolit přístup k disku**		+	+	+	
	Povolit přístup k disku v režimu jen pro čtení	+		+		
	Povolit stažení virtuálního počítače	+	+	+	+	
Stav > virtuálního počítače	**Vytvořit snímek**	+		+	+	+
	Odebrat snímek	+		+	+	+

* Toto oprávnění je vyžadováno pouze pro zálohování šifrovaných počítačů.

** Toto oprávnění je vyžadováno pouze pro zálohování s podporou aplikací.

18.3 Zálohování počítačů Hyper-V v clusteru

V clusteru Hyper-V mohou být virtuální počítače převáděny mezi uzly clusteru. Pomocí následujících doporučení vytvoříte správnou zálohu počítačů Hyper-V v clusteru:

1. Počítač musí být dostupný pro zálohování bez ohledu na uzel, ke kterému se přenese. Chcete-li zajistit, aby měl Agent pro Hyper-V přístup k počítači v libovolném uzlu, musí být služba agenta (str. 69) spuštěna pod účtem uživatele domény, který má oprávnění správce na každém z uzlů v clusteru.

   Doporučujeme určit takový účet pro službu agenta během instalace Agenta pro Hyper-V.
2. Nainstalujte Agenta pro Hyper-V na každý uzel clusteru.
3. Všechny agenty zaregistrujte na serveru pro správu.

Vysoká dostupnost obnoveného počítače

Při obnovení zálohovaných disků do *existujícího* virtuálního počítače Hyper-V zůstane jeho vysoké dostupnost nezměněna.

Pokud obnovíte zálohované disky na *nový* virtuální počítač Hyper-V nebo provedete konverzi na virtuální počítač Hyper-V v rámci plánu ochrany (str. 157), výsledný počítač nebude poskytovat vysokou dostupnost. Považuje se za náhradní počítač a normálně se vypne. Pokud tento počítač potřebujete použít v produkčním prostředí, můžete jej konfigurovat pro vysokou dostupnost pomocí modulu snap-in pro **správu clusterů s podporou převzetí služeb při selhání**.

18.4 Omezení celkového počtu současně zálohovaných virtuálních počítačů

Možnost zálohování **Plánování** (str. 189) určuje, kolik virtuálních počítačů může agent při provádění daného plánu ochrany zálohovat současně.

Pokud se více plánů ochrany překrývá v čase, sčítají se čísla uvedená v jejich možnostech zálohování. Přestože je výsledné celkové číslo programově omezeno na 10, překrývající se plány mohou ovlivnit výkon zálohování a přetížit hostitele i úložiště virtuálního počítače.

Můžete proto dále omezit celkový počet virtuálních počítačů, které může agent pro VMware nebo agent pro Hyper-V současně zálohovat.

Omezení celkového počtu virtuálních počítačů, které může agent pro VMware (Windows) nebo agent pro Hyper-V zálohovat

1. V počítači, ve kterém je spuštěný agent, vytvořte nový textový dokument a otevřete jej v textovém editoru, jako je Poznámkový blok.
2. Zkopírujte a vložte do souboru následující řádky:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Nahraďte hodnotu `00000001` hexadecimální hodnotou omezení, které chcete nastavit. Například `00000001` je 1 a `0000000A` je 10.

4. Uložte soubor pod názvem **limit.reg**.
5. Spusťte soubor jako správce.
6. Potvrďte, že chcete upravit registr systému Windows.
7. Restartujte agenta následujícím postupem:
   a. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
   b. Klikněte na tlačítko **OK**.
   c. Spusťte následující příkazy:

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

Omezení celkového počtu virtuálních počítačů, které může agent pro VMware (Virtual Appliance) nebo agent pro VMware (Linux) zálohovat

1. V počítači, ve kterém je spuštěný agent, spusťte příkazové prostředí:
   - **Agent pro VMware (Virtual Appliance)**: V uživatelském rozhraní virtuálního zařízení stiskněte klávesy CTRL+SHIFT+F2.
   - **Agent pro VMware (Linux)**: Přihlaste se jako uživatel root k počítači, ve kterém je spuštěno zařízení Acronis Cyber Protect. Heslo je stejné jako pro webovou konzoli Cyber Protect.
2. Otevřete soubor **/etc/Acronis/MMS.config** v textovém editoru, jako je **vi**.
3. Vyhledejte následující oddíl:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Nahraďte hodnotu `10` desítkovou hodnotou omezení, které chcete nastavit.
5. Uložte soubor.
6. Restartujte agenta:.
   - **Agent pro VMware (Virtual Appliance)**: Spusťte příkaz **`reboot`**.
   - **Agent pro VMware (Linux)**: Spusťte následující příkaz:

```
sudo service acronis_mms restart
```

18.5 Migrace počítače

Migraci počítače je možné provést pomocí obnovy jeho zálohy na jiný počítač než původní.

Následující tabulka shrnuje dostupné možnosti migrace.

Typ zálohovaného počítače	**Dostupná umístění obnovy**			
	Fyzický počítač	Virtuální počítač ESXi	Virtuální počítač Hyper-V	Virtuální počítač Scale Computing HC3
Fyzický počítač	+	+	+	-
Virtuální počítač VMware ESXi	+	+	+	-
Virtuální počítač Hyper-V	+	+	+	-
Virtuální počítač Scale Computing HC3	+	+	+	+

Pokyny k provedení migrace naleznete v následujících tématech:

- Migrace z fyzického počítače na virtuální (P2V) – Fyzický počítač na virtuální (str. 200)
- Migrace z virtuálního počítače na virtuální (V2V) – Virtuální počítač (str. 202)
- Migrace z virtuálního počítače na fyzický (V2P) – Virtuální počítač (str. 202) nebo Obnova disků pomocí spouštěcího média (str. 203)

Přestože je možné provést migraci V2P ve webovém rozhraní, doporučujeme ve specifických případech použití spouštěcího média. Někdy je užitečné použít médium u migrací na ESXi nebo Hyper-V.

Médium vám umožní provést následující úkony:

- Provést migraci P2V a V2P u počítače se systémem Linux obsahujícího logické svazky (LVM). Použití Agenta pro Linux nebo spouštěcího média k vytvoření zálohy a spouštěcího média pro obnovení.
- Zprostředkovat ovladače pro určitý hardware, který je důležitý pro spouštění systému.

18.6 Virtuální počítače Windows Azure a Amazon EC2

Chcete-li zálohovat virtuální počítače Windows Azure nebo Amazon EC2, nainstalujte si na ně agenta pro ochranu. Operace zálohování a obnovy jsou stejné jako u fyzického počítače. Když ale budete nastavovat limit počtu počítačů v cloudovém nasazení, bude tento počítač stále považován za virtuální.

Rozdíl od fyzického počítače spočívá v tom, že virtuální počítače Windows Azure a Amazon EC2 se nedají spustit ze spouštěcích médií. Potřebujete-li obnovit virtuální počítač Windows Azure nebo Amazon EC2, řiďte se následujícím postupem.

Obnovení počítače jako virtuálního počítače Windows Azure nebo Amazon EC2

1. Vytvořte nový virtuální počítač z obrazu nebo šablony uložené ve Windows Azure nebo Amazon EC2. Nový počítač musí mít stejnou konfiguraci disku jako počítač, který chcete obnovit.
2. Na nový počítač nainstalujte aplikaci Agent pro Windows nebo Agent pro Linux.
3. Obnovte zálohovaný počítač podle postupu popsaného v části Fyzický počítač (str. 198). Při konfiguraci obnovy vyberte jako cílový počítač právě tento nový počítač.

Síťové požadavky

Agenti nainstalovaní na zálohovaných počítačích musí být schopní komunikovat se serverem pro správu přes síť.

Místní nasazení

- Pokud jsou agenti i server pro správu nainstalované v cloudu Azure/EC2, všechny počítače jsou už umístěné ve stejné síti. Žádné další akce již nejsou třeba.
- Pokud je server pro správu umístěný v cloudu Azure/EC2, počítače v cloudu nebudou mít přístup k místní síti, kde je server pro správu nainstalovaný. Aby agenti nainstalovaní v takových počítačích mohli komunikovat se serverem pro správu, musí být vytvořeno připojení VPN mezi místní (interní) a cloudovou (Azure/EC2) sítí. Informace, jak vytvořit VPN připojení, naleznete v následujících článcích:

  Amazon EC2:
  http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure:
  https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Cloudové nasazení

V cloudovém nasazení je server pro správu umístěný v jednom z datových center Acronis a je tak přístupný pro agenty. Žádné další akce již nejsou třeba.

19 Ochrana platformy SAP HANA

Ochrana platformy SAP HANA je popsána v samostatném dokumentu na adrese https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper.pdf.

20 Ochrana proti malwaru a ochrana webu

Ochrana proti malwaru ve službě Cyber Protect přináší následující výhody:

- Špičková ochrana ve všech fázích: proaktivní, aktivní a reaktivní.
- Zahrnuje čtyři odlišné technologie ochrany proti malwaru, které poskytují tu nejlepší ochranu ve více vrstvách.
- Správa Microsoft Security Essentials a antivirové ochrany v programu Windows Defender.

20.1 Antivirová ochrana a ochrana proti malwaru

Modul Antivirová ochrana a ochrana proti malwaru umožňuje chránit počítače se systémem Windows a macOS před nejnovějším malwarem. Upozorňujeme, že funkce Active Protection, která je součástí ochrany proti malwaru, není podporována na počítačích macOS. Úplný seznam podporovaných funkcí ochrany proti malwaru: Podporované funkce podle operačního systému (p. 9).

Služba Acronis Cyber Protect je podporována a zaregistrována v Centru zabezpečení systému Windows.

Pokud je váš počítač v okamžiku použití modulu Antivirová ochrana a ochrana proti malwaru již chráněn antivirovým řešením jiného výrobce, systém vygeneruje výstrahu a zastaví ochranu při přístupu, aby nedošlo k potenciálním problémům s kompatibilitou a výkonem. Pokud budete chtít povolit všechny funkce antivirové ochrany a ochrany proti malwaru Acronis Cyber Protect, bude nutné antivirový program třetí strany buď zakázat, nebo odinstalovat.

K dispozici máte následující funkce ochrany proti malwaru:

- Detekce malwaru v souborech v režimech v reálném čase a na vyžádání (pro Windows, macOS)
- Detekce škodlivého chování v procesech (pro Windows)
- Blokování přístupu na škodlivé adresy URL (pro Windows)
- Přesunutí nebezpečných souborů do karantény
- Přidání důvěryhodných podnikových aplikací na seznam povolených aplikací

Modul Antivirová ochrana a ochrana proti malwaru poskytuje dva typy kontroly:

- Kontrola ochrany v reálném čase
- Kontrola malwaru na vyžádání

Kontrola ochrany v reálném čase

Ochrana v reálném čase zkontroluje všechny soubory, které jsou spouštěny nebo otevírány na počítači, a předchází tak malwarovým hrozbám.

Vybrat si můžete jeden z následujících typů kontroly:

- Detekce při přístupu znamená, že program ochrany proti malwaru běží na pozadí a aktivně a nepřetržitě vyhledává v počítačovém systému viry a další škodlivé hrozby, a to po celou dobu, kdy je systém spuštěný. Malware bude v obou případech zjištěn, když je soubor spouštěn, a během různých operací se souborem, například při otevření ke čtení nebo úpravám.
- Detekce při spuštění znamená, že v okamžiku spuštění budou zkontrolovány pouze spustitelné soubory k zajištění, že jsou čisté a že nepoškodí počítač a data. Zkopírování infikovaného souboru nebude zjištěno.

Kontrola malwaru na vyžádání

Antimalwarová kontrola se provádí na základě harmonogramu.

Výsledky antimalwarové kontroly můžete sledovat v ovládacím prvku v nabídce **Kontrolní panel** > **Přehled** > Nedávno ovlivněno (p. 412).

20.1.1 Nastavení antivirové ochrany a ochrany proti malwaru

Návod k vytvoření plánu ochrany s modulem Antivirová ochrana a ochrana proti malwaru naleznete v tématu Vytvoření plánu ochrany.

Pro modul Antivirová ochrana a ochrana proti malwaru je možné zadat následující nastavení.

Active Protection

Active Protection chrání systém před ransomwarem a malwarem zaměřeným na těžbu kryptoměn. Ransomware šifruje soubory a za šifrovací klíč požaduje výkupné. Malware pro těžbu kryptoměn provádí matematické výpočty na pozadí, což má za následek snížení výpočetního výkonu a vyšší zatížení sítě.

Active Protection je dostupná u počítačů se systémem Windows 7 nebo novějším a Windows Server 2008 R2 nebo novějším. Na počítači musí být nainstalovaný Agent pro Windows.

Jak to funguje

Active Protection sleduje procesy běžící na chráněném počítači. Když se proces třetích stran pokusí zašifrovat soubory nebo těžit kryptoměny, Active Protection vygeneruje výstrahu a provede další akce (pokud jsou určeny v konfiguraci).

Kromě toho Active Protection brání před neoprávněnými změnami vlastních procesů zálohovacího softwaru, záznamů v registru, spustitelných a konfiguračních souborů a záloh uložených v místních složkách.

K identifikaci škodlivých procesů používá Active Protection behaviorální heuristiku. Srovnává řetězec akcí provedený procesem s řetězci událostí zaznamenanými v databázi vzorců škodlivého chování. Tento přístup umožňuje Active Protection rozpoznávat nový malware na základě jeho typického chování.

Výchozí nastavení: **Povoleno**.

Nastavení Active Protection

U možnosti **Akce při detekování** vyberte akci, kterou software provede při zjištění aktivity typu ransomware, a potom klikněte na **Hotovo**.

Je možné vybrat jednu z následujících možností:

- **Pouze upozornit**

  Software o tomto procesu vygeneruje výstrahu.
- **Zastavit proces**

  Software o tomto procesu vygeneruje výstrahu a zastaví ho.
- **Vrátit pomocí mezipaměti**

  Software vygeneruje výstrahu, zastaví proces a vrátí změny souboru pomocí služby mezipaměti.

Výchozí nastavení: **Vrátit pomocí mezipaměti**.

Detekce chování

Acronis Cyber Protect chrání váš systém pomocí behaviorální heuristiky za účelem identifikace škodlivých procesů: porovnává řetězec akcí provedený procesem s řetězci akcí zaznamenanými v databázi vzorců škodlivého chování. Nový malware je tak detekován podle svého typického chování.

Detekce chování

Výchozí nastavení: **Povoleno**.

Nastavení detekce chování

U možnosti **Akce při detekování** vyberte akci, kterou software provede při zjištění aktivity typu malware, a potom klikněte na **Hotovo**.

Je možné vybrat jednu z následujících možností:

- **Pouze upozornit**
  Software o procesu podezřelém z aktivit typu malware vygeneruje výstrahu.
- **Zastavit proces**
  Software vygeneruje výstrahu a zastaví proces podezřelý z aktivit typu malware.
- **Karanténa**
  Software vygeneruje výstrahu, zastaví proces a přesune spustitelný soubor do složky karantény.

Výchozí nastavení: **Karanténa**.

Vlastní ochrana

Vlastní ochrana brání před neoprávněnými změnami softwarových vlastních procesů, záznamů v registru, spustitelných a konfiguračních souborů a záloh uložených v místních složkách. Tuto funkci doporučujeme nevypínat.

Výchozí nastavení: **Povoleno**.

Povolení procesům měnit zálohy

Možnost **Povolit konkrétní procesy, které mohou měnit zálohy** funguje, pokud je povolena možnost **Vlastní ochrana**.

Platí pro soubory s příponami .tibx, .tib, .tia, které jsou v místních složkách.

U této možnosti můžete vybrat, jaké procesy smí měnit soubory zálohy, i když tyto soubory mají vlastní ochranu. Je to praktické, například když jste použili skript, kterým soubory zálohy odstraníte nebo je přesunete jinam.

Pokud je tato možnost zakázána, mohou soubory záloh měnit jen procesy podepsané dodavatelem zálohovacího softwaru. Software tak může používat pravidla zachování a odstraňovat zálohy, jen když o to požádá uživatel ve webovém rozhraní. Jiné procesy zálohy měnit nemohou – bez ohledu na to, jestli jsou nebo nejsou podezřelé.

Pokud je tato možnost povolena, můžete ostatním procesům povolit upravovat zálohy. Zadejte úplnou cestu ke spustitelnému souboru procesu, počínaje písmenem jednotky.

Výchozí nastavení: **Zakázáno**.

Ochrana síťové složky

Možnost **Chránit síťové složky mapované jako místní jednotky** definuje, jestli modul Antivirová ochrana a ochrana proti malwaru chrání před místními škodlivými procesy síťové složky mapované jako místní jednotky.

Tato možnost platí pro složky sdílené prostřednictvím protokolů SMB i NFS.

Pokud se soubor původně nacházel na mapované jednotce, nemůžete ho při extrakci z mezipaměti akcí **Vrátit pomocí mezipaměti** uložit na původní místo. Místo toho se uloží do složky, kterou určíte v nastavení této možnosti. Výchozí složka je **C:\ProgramData\Acronis\Restored Network Files**. Pokud tato složka neexistuje, bude vytvořena. Pokud ji chcete změnit, nezapomeňte zadat místní složku. Síťové složky včetně složek na mapovaných jednotkách nejsou podporovány.

Výchozí nastavení: **Povoleno**.

Ochrana na straně serveru

Tato možnost definuje, jestli modul Antivirová ochrana a ochrana proti malwaru chrání síťové složky sdílené z externích příchozích připojení z jiných serverů v síti, které mohou být potenciálním zdrojem hrozeb.

Výchozí nastavení: **Zakázáno**.

Nastavení důvěryhodných a blokovaných připojení

Na kartě **Důvěryhodné** můžete zadat připojení, která mohou měnit data. Musíte definovat uživatelské jméno a IP adresu.

Na kartě **Blokované** můžete zadat připojení, která nebudou moct měnit data. Musíte definovat uživatelské jméno a IP adresu.

Detekce procesu těžby kryptoměn

Tato možnost definuje, zda modul Antivirová ochrana a ochrana proti malwaru detekuje potenciální malware pro těžbu kryptoměn.

Malware pro těžbu kryptoměn degraduje výkon užitečných aplikací, zvyšuje účty za elektřinu, může způsobit selhání systému a dokonce poškodit hardware v důsledku zneužití. Malware pro těžbu kryptoměn doporučujeme přidat do seznamu **Škodlivé procesy**, aby nedošlo k jeho spuštění.

Výchozí nastavení: **Povoleno**.

Nastavení detekce procesu těžby kryptoměn

Vyberte akci, kterou software provede při zjištění aktivity těžby kryptoměn, a potom klikněte na tlačítko **Hotovo**. Je možné vybrat jednu z následujících možností:

- **Pouze upozornit**

  Software vygeneruje výstrahu o procesu podezřelém z aktivit dolování kryptoměn.
- **Zastavit proces**

  Software vygeneruje výstrahu a zastaví proces podezřelý z aktivit dolování kryptoměn.

Výchozí nastavení: **Zastavit proces**.

Ochrana v reálném čase

Ochrana v reálném čase neustále kontroluje, zda počítačový systém neobsahuje viry a další hrozby, a to po celou dobu, kdy je systém spuštěný.

Výchozí nastavení: **Povoleno**.

Konfigurace akce při detekování pro ochranu v reálném čase

V části **Akce při detekování** vyberte akci, kterou software provede při zjištění viru nebo jiné hrozby, a potom klikněte na **Hotovo**.

Je možné vybrat jednu z následujících možností:

- **Blokovat a upozornit**

  Software proces podezřelý z aktivit typu malware zablokuje a vygeneruje výstrahu.
- **Karanténa**

  Software vygeneruje výstrahu, zastaví proces a přesune spustitelný soubor do složky karantény.

Výchozí nastavení: **Karanténa**.

Konfigurace režimu kontroly pro ochranu v reálném čase

V části **Režim kontroly** vyberte akci, kterou software provede při zjištění viru nebo jiné hrozby, a potom klikněte na **Hotovo**.

Je možné vybrat jednu z následujících možností:

- **Inteligentní při přístupu** – sleduje všechny systémové aktivity a automaticky prohledává soubory při přístupu ke čtení nebo zápisu nebo vždy při spuštění programu.
- **Při spuštění** – automaticky kontroluje pouze spustitelné soubory při spuštění k ověření, zda jsou čisté a nepoškodí váš počítač nebo data.

Výchozí nastavení: **Inteligentní při přístupu**.

Naplánovat kontrolu

Můžete definovat harmonogram, podle kterého bude ve vašem počítačovém systému vyhledáván malware. Povolte možnost **Naplánovat kontrolu**.

Výchozí nastavení: **Povoleno**.

Akce při detekování:

- **Karanténa**

  Software vygeneruje výstrahu a přesune spustitelný soubor do složky karantény.
- **Pouze upozornit**

  Software vygeneruje výstrahu o procesu s podezřením na malware.

Výchozí nastavení: **Karanténa**.

Typ kontroly:

- **Plná**

  Dokončení plné kontroly trvá v porovnání s rychlou kontrolou mnohem déle, protože bude zkontrolován každý soubor.
- **Rychlá**

Rychlá kontrola kontroluje pouze běžné oblasti, ve kterých se malware v počítači obvykle nachází.

Výchozí nastavení: **Rychlá**.

Naplánujte spuštění úlohy pomocí následujících událostí:

- **Naplánovat podle času** – úloha se spustí podle zadaného času.
- **Když se uživatel přihlásí do systému** – ve výchozím nastavení zahájí spuštění úlohy přihlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.
- **Když se uživatel odhlásí ze systému** – ve výchozím nastavení zahájí spuštění úlohy odhlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.

Poznámka *Úloha nebude spuštěna při vypnutí systému. Vypnutí a odhlášení jsou dvě různé akce.*

- **Při spuštění systému** – úloha se spustí při spuštění operačního systému.
- **Při vypnutí systému** – úloha se spustí při vypnutí operačního systému.

Výchozí nastavení: **Naplánovat podle času**.

Typ harmonogramu:

- **Měsíčně** – vyberte měsíce a týdny nebo dny v měsíci, kdy se úloha spustí.
- **Denně** – vyberte dny v týdnu, kdy se úloha spustí.
- **Po hodině**– vyberte dny v týdnu, počet opakování a časový interval, během kterého se úloha spustí.

Výchozí nastavení: **Denně**.

Spustit v – vyberte přesný čas, kdy se úloha spustí.

Výchozí nastavení: **14:00** (v počítači, ve kterém je software nainstalován).

Spustit v časovém rozsahu – nastavte časový rozsah, ve kterém bude nakonfigurovaný harmonogram platný.

Podmínky spuštění – definujte všechny podmínky, které musí být současně splněny před spuštěním úlohy. Podobají se podmínkám spuštění pro modul zálohy popsaným v tématu Podmínky spuštění.

Definovat lze například následující dodatečné podmínky spuštění:

- **Rozložit časy spuštění úlohy do časového rámce**– tato možnost umožňuje definovat časový rámec, během kterého musí být úloha spuštěna, a rozložit úlohy, aby nedošlo k přetížení sítě, protože mnoho počítačů může mít malou šířku pásma pro hostitele, kde se nacházejí služby Windows Server Update Services (WSUS) nebo server pro správu. Můžete zadat prodlevu v hodinách, minutách nebo sekundách. Pokud je například výchozí čas spuštění 10:00 a prodleva je 60 minut, bude úloha spuštěna mezi 10:00 a 11:00.
- **Pokud je počítač vypnutý, vynechané úlohy se spustí při spuštění počítače**
- **Zabránit režimu spánku nebo hibernace při spuštění úlohy** – tato možnost platí pouze v počítačích se systémem Windows.
- **Pokud podmínky spuštění nejsou splněny, spustit úlohu za** – zadejte dobu v hodinách, za kterou bude úloha spuštěna bez ohledu na jiné podmínky spuštění.

Kontrolovat archivní soubory

Výchozí nastavení: **Povoleno**.

- **Max. hloubka rekurze**

Kolik úrovní vložených archivů lze skenovat. Například dokument MIME > archiv ZIP > archiv Office > obsah dokumentu.

Výchozí nastavení: **16**.

- **Max. velikost**

  Maximální velikost souboru archivu, který bude kontrolován.

  Výchozí nastavení: **Neomezená**.

Kontrolovat vyměnitelné jednotky

Výchozí nastavení: **Zakázáno**.

- **Namapované (vzdálené) síťové jednotky**
- **Paměťová zařízení USB** (jednotky flash a externí pevné disky)
- **CD/DVD**

Kontrolovat pouze nové a změněné soubory – zkontrolovány budou pouze nově vytvořené a změněné soubory.

Výchozí nastavení: **Povoleno**.

Karanténa

Karanténa je složka sloužící k izolaci podezřelých (pravděpodobně napadených) nebo potenciálně nebezpečných souborů.

Odebrat soubory v karanténě po – definuje období ve dnech, po kterém budou soubory v karanténě odstraněny.

Výchozí nastavení: **30 dní**.

Výjimky

Chcete-li omezit prostředky využívané heuristickou analýzou a vyloučit takzvané falešně pozitivní výsledky, kdy je důvěryhodný program považován za ransomware, můžete definovat následující nastavení:

Na kartě **Důvěryhodné** můžete určit:

- Procesy, které nebudou nikdy považovány za malware. Procesy podepsané společností Microsoft jsou vždy důvěryhodné.
- Složky, ve kterých nebudou změny souborů sledovány.
- Soubory a složky, ve kterých nebude provedena naplánovaná kontrola.

Na kartě **Blokované** můžete určit:

- Procesy, které budou vždy zablokovány. Tyto procesy nebudou moci být spuštěny, dokud je v počítači povolena Active Protection.
- Složky, ve kterých budou všechny procesy zablokovány.

Zadejte úplnou cestu ke spustitelnému souboru procesu, počínaje písmenem jednotky. Například: `C:\Windows\Temp\er76s7sdkh.exe`.

K zadání složky můžete použít zástupné znaky * a ?: Znak hvězdičky (*) nahrazuje nula nebo více znaků. Znak otazníku (?) nahrazuje přesně jeden znak. Proměnné prostředí, jako `%AppData%`, nelze použít.

Výchozí nastavení: Ve výchozím nastavení nejsou definovány žádné výjimky.

20.2 Active Protection

Ve verzích Cyber Backup služby Acronis Cyber Protect je Active Protection samostatný modul v plánu ochrany (p. 118). Tento modul má následující nastavení:

- Akce při detekování
- Vlastní ochrana
- Ochrana síťové složky
- Ochrana na straně serveru
- Detekce procesu těžby kryptoměn
- Výjimky

Ve verzích Protect služby Acronis Cyber Protect je Active Protection součástí modulu Antivirová ochrana a ochrana proti malwaru.

Další informace o službě Active Protection a jejím nastavení naleznete v tématu Nastavení antivirové ochrany a ochrany proti malwaru (p. 354).

20.3 Antivirová ochrana v programu Windows Defender

Antivirová ochrana v programu Windows Defender je zabudovaná antimalwarová komponenta systému Microsoft Windows, která je poskytována počínaje systémem Windows 8.

Modul antivirové ochrany v programu Windows Defender umožňuje nakonfigurovat zásady zabezpečení antivirové ochrany v programu Windows Defender a sledovat jejich stav pomocí webové konzole Cyber Protect.

Tento modul lze použít na počítačích, ve kterých je nainstalována antivirová ochrana v programu Windows Defender.

Naplánovat kontrolu

Určete harmonogram naplánované kontroly.

Režim kontroly:

- **Úplná** – úplná kontrola všech souborů a složek nad rámec položek kontrolovaných během rychlé kontroly. Ve srovnání s rychlou kontrolou vyžaduje více prostředků počítače.
- **Rychlá** – rychlá kontrola procesů a složek v paměti, kde se obvykle nachází malware. Vyžaduje méně prostředků počítače.

Definujte čas a den v týdnu, kdy bude kontrola provedena.

Každodenní rychlá kontrola – definujte čas každodenní rychlé kontroly.

V závislosti na svých potřebách můžete nastavit následující možnosti:

Spustit naplánovanou kontrolu, když je počítač zapnutý, ale nepoužívá se

Před spuštěním naplánované kontroly vyhledat nejnovější definice virů a spywaru

Omezit využití CPU během kontroly na

Další informace o nastavení harmonogramu modulu antivirové ochrany v programu Windows Defender naleznete na adrese

https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Výchozí akce

Definujte výchozí akce, které se provedou pro zjištěné hrozby různých úrovní závažnosti:

- **Smazat** – odstranit zjištěný malware na počítači.
- **Umístit do karantény** – umístit zjištěný malware do složky karantény, ale neodstranit ho.
- **Odstranit** – odstranit zjištěný malware z počítače.
- **Povolit** – neodebírat zjištěný malware ani ho neumisťovat do karantény.
- **Definováno uživatelem** – uživatel bude vyzván k určení akce, která se pro zjištění malware provede.
- **Žádná akce** – nebude provedena žádná akce.
- **Blokovat** – blokovat zjištěný malware.

Další informace o nastavení výchozích akcí modulu antivirové ochrany v programu Windows Defender naleznete na adrese https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-setting.

Ochrana v reálném čase

Možnost **Ochrana v reálném čase** povolte, pokud chcete zastavit instalaci nebo spuštění malwaru na počítačích.

Kontrola všech stažených souborů – je-li tato možnost vybrána, budou zkontrolovány všechny stažené soubory a přílohy.

Povolit sledování chování – je-li tato možnost vybrána, bude aktivní sledování chování.

Kontrolovat soubory v síti – je-li tato možnost vybrána, budou zkontrolovány soubory v síti.

Povolit úplnou kontrolu namapovaných síťových jednotek – je-li tato možnost vybrána, provede se úplná kontrola síťových jednotek.

Povolit kontrolu pošty – je-li tato možnost povolena, modul analyzuje poštovní schránku a soubory pošty na základě jejich specifického formátu s cílem zkontrolovat texty e-mailů a přílohy.

Další informace o nastavení ochrany v reálném čase modulu antivirové ochrany v programu Windows Defender naleznete na adrese https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Pokročilé

Zadejte nastavení rozšířené kontroly:

- **Kontrolovat archivní soubory** – zahrnout do kontroly archivované soubory, například soubory .zip nebo .rar.
- **Kontrolovat vyměnitelné jednotky** – během úplných kontrol kontrolovat vyměnitelné jednotky.
- **Vytvořit bod obnovení systému** – v některých případech by mohlo dojít k odstranění důležitého souboru nebo záznamu v registru jako „falešně pozitivní“ položky. Pokud k tomu dojde, můžete provést obnovení z bodu obnovení.

- **Odebrat soubory v karanténě po** – definujte období, po kterém budou soubory v karanténě odstraněny.
- **Automaticky odeslat vzorky souborů, pokud je vyžadována další analýza:**
  - **Vždycky se zeptat** – před odesláním souboru budete požádáni o potvrzení.
  - **Automaticky odeslat bezpečné vzorky** – většina vzorků bude odeslána automaticky, s výjimkou souborů, které mohou obsahovat osobní údaje. Takové soubory budou vyžadovat dodatečné potvrzení.
  - **Automaticky odeslat všechny vzorky** – všechny vzorky budou odeslány automaticky.
- **Zakázat grafické rozhraní antivirové ochrany v programu Windows Defender** – je-li tato možnost vybrána, uživatel nebude moct používat uživatelské rozhraní modulu antivirové ochrany v programu Windows Defender. Zásady modulu antivirové ochrany v programu Windows Defender můžete spravovat prostřednictvím webové konzole Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** – online komunita, která vám pomůže se rozhodnout, jak reagovat na potenciální hrozby.
  - **Nechci se připojit k MAPS** – společnosti Microsoft nebudou odeslány žádné informace o softwaru, který byl detekován.
  - **Základní členství** – společnosti Microsoft budou odeslány základní informace o softwaru, který byl detekován.
  - **Rozšířené členství** – společnosti Microsoft budou odeslány podrobné informace o softwaru, který byl detekován.

  Další informace naleznete na adrese https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise

Další informace o pokročilém nastavení modulu antivirové ochrany v programu Windows Defender naleznete na adrese https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Výjimky

Můžete definovat následující soubory a složky, které se mají vyčlenit z kontroly:

- **Procesy** – každý soubor, ze kterého definovaný proces čte nebo do kterého zapisuje, bude vyloučen z kontroly. Musíte definovat celou cestu ke spustitelnému souboru procesu.
- **Soubory a složky** – zadané soubory a složky budou vyloučeny z kontroly. Musíte definovat celou cestu ke složce nebo souboru nebo musíte definovat příponu souboru.

Další informace o nastavení vyloučení modulu antivirové ochrany v programu Windows Defender naleznete na adrese https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

20.4 Microsoft Security Essentials

Microsoft Security Essentials je zabudovaná antimalwarová komponenta systému Microsoft Windows, která je poskytována v systémech Windows předcházejících verzi 8.

Modul Microsoft Security Essentials umožňuje nakonfigurovat zásady zabezpečení programu Microsoft Security Essentials a sledovat jejich stav pomocí webové konzole Cyber Protect.

Tento modul lze použít na počítačích, ve kterých je nainstalován program Microsoft Security Essentials.

Nastavení programu Microsoft Security Essentials je téměř stejné jako u antivirové ochrany v programu Windows Defender (p. 363), s výjimkou absence nastavení ochrany v reálném čase a nemožnosti definovat výjimky prostřednictvím webové konzole Cyber Protect.

20.5 Filtrování adres URL

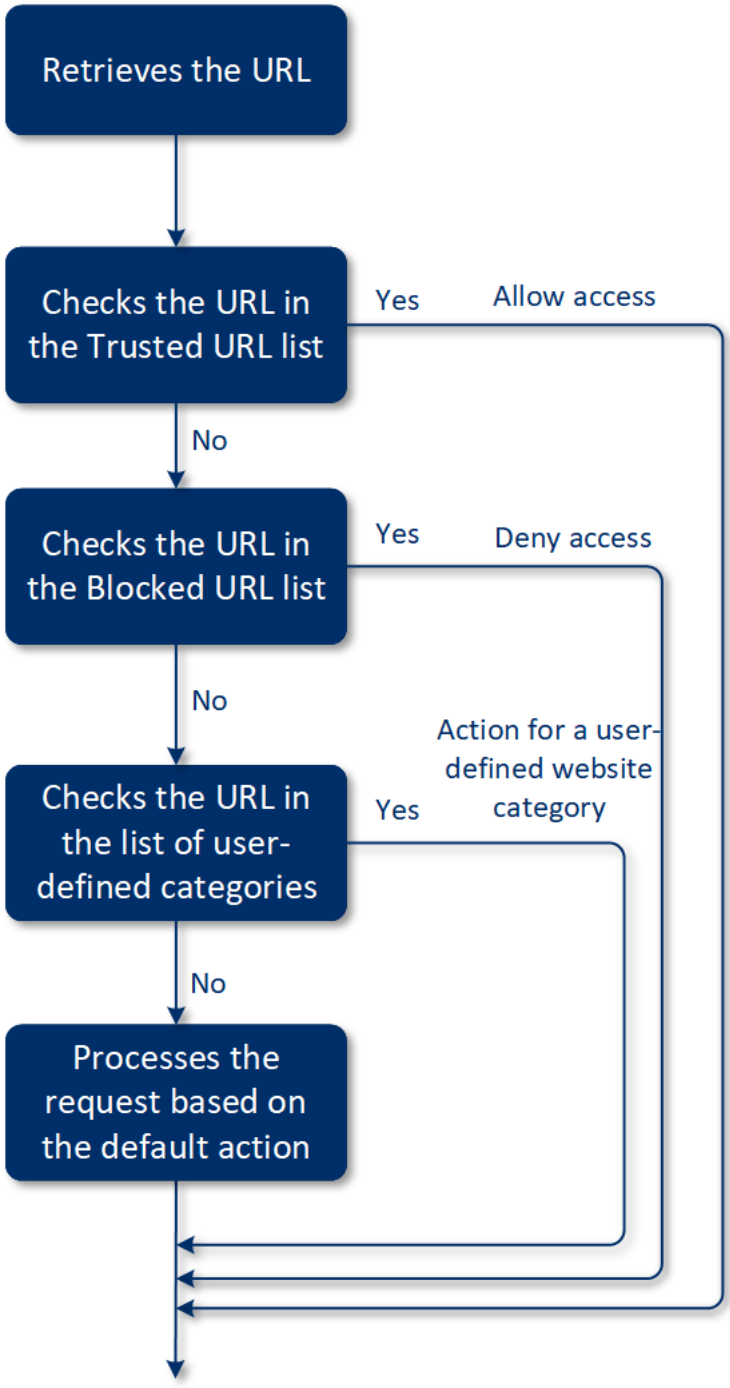
Malware je často distribuován škodlivými nebo infikovanými weby a využívá metodu neúmyslného stažení z webové stránky. Filtrování adres URL umožňuje chránit počítače před hrozbami přicházejícími z internetu, jako je malware a phishing. Můžete zablokovat přístup k webovým stránkám, které mají škodlivý obsah. Databáze filtrování adres URL zahrnuje také data o webech se spornými informacemi o onemocnění COVID-19, podvodech a phishingových adresách URL. Systém tyto webové stránky automaticky zablokuje, když se je uživatel pokusí otevřít.

Pomocí filtrování adres URL můžete také řídit používání webu, a zajistit tak dodržování externích předpisů a interních podnikových zásad. Můžete nakonfigurovat různé zásady přístupu pro více než 40 kategorií webů.

Připojení přes HTTP/HTTPS na počítačích se systémem Windows jsou momentálně zkontrolována agentem pro ochranu.

Jak to funguje

Uživatel klikne na odkaz nebo zadá adresu URL na adresním řádku prohlížeče. Interceptor adresu URL zachytí a odešle ji agentovi pro ochranu. Agent pro ochranu adresu URL analyzuje, zkontroluje databázi a vrátí výsledek interceptoru. Pokud je adresa URL zakázaná, interceptor k ní zablokuje přístup a upozorní uživatele, že tento obsah nelze zobrazit.



Konfigurace filtrování adres URL

1. Vytvořte plán ochrany s povoleným modulem filtrování adres URL.
2. Nakonfigurujte nastavení filtrování adres URL (viz níže).
3. Přiřaďte plán ochrany k požadovaným počítačům.

Adresy URL, které byly blokovány, naleznete v nabídce **Kontrolní panel** > **Výstrahy**.

Nastavení filtrování adres URL

Pro modul filtrování adres URL je možné nakonfigurovat následující nastavení:

Přístup škodlivého webu

Určete, která akce bude provedena, když se uživatel pokusí otevřít škodlivý web.

- **Zablokovat** – přístup na škodlivý web bude zablokován a vygeneruje se výstraha.
- **Vždy se zeptat uživatele** – uživateli se zobrazí dotaz, zda přesto na web přejít, nebo zda se vrátit.

Kategorie, které lze filtrovat

K dispozici máte 44 kategorií webů, pro které můžete nakonfigurovat zásady přístupu. Ve výchozím nastavení je přístup na weby všech kategorií povolen.

	Kategorie webu	Popis
1	**Reklama**	Tato kategorie zahrnuje domény, jejichž hlavním účelem je zobrazovat reklamy.
2	**Vývěsky zpráv**	Tato kategorie zahrnuje fóra, diskusní skupiny a typy webů obsahující otázky a odpovědi. Tato kategorie nezahrnuje konkrétní části podnikových webů, kde mohou zákazníci pokládat dotazy.
3	**Osobní webové stránky**	Tato kategorie zahrnuje osobní weby a všechny typy blogů: individuální, skupinová a dokonce i firemní. Blog je deník zveřejněný na internetu. Zahrnuje příspěvky, které jsou obvykle zobrazeny v chronologickém pořadí tak, že jako první jsou uvedeny nejnovější příspěvky.
4	**Podnikové/obchodní webové stránky**	Toto je obsáhlá kategorie zahrnující firemní weby, které obvykle nespadají do žádné jiné kategorie.
5	**Počítačový software**	Tato kategorie zahrnuje weby nabízející počítačový software, obvykle buď open source, freeware, nebo shareware. Může zahrnovat také některé internetové obchody se softwarem.
6	**Léčiva**	Tato kategorie zahrnuje weby týkající se léků, alkoholu a cigaret, které obsahují diskuse ohledně používání nebo prodeje (povolených) léčivých přípravků nebo vybavení, alkoholu a tabákových výrobků. Upozorňujeme, že ilegální léčiva jsou zahrnuta v kategorii Drogy.
7	**Vzdělávání**	Tato kategorie zahrnuje weby patřící oficiálním vzdělávacím institucím, včetně těch mimo doménu .edu. Zahrnuje také vzdělávací weby, například encyklopedie.
8	**Zábava**	Tato kategorie zahrnuje weby poskytující informace týkající se uměleckých aktivit a muzeí a weby, které recenzují nebo hodnotí obsah jako filmy, hubu a umění.
9	**Sdílení souborů**	Tato kategorie zahrnuje weby pro sdílení souborů, kde může uživatel nahrávat soubory a sdílet je s ostatními. Zahrnuje také weby pro sdílení torrentů a sledování torrentů.
10	**Finance**	Tato kategorie zahrnuje weby patřící všem bankám po celém světě, které poskytují online přístup. Zahrnuty jsou také některé úvěrové společnosti a další finanční instituce. Zahrnuty ale nemusí být některé místní banky.

11	**Hazard**	Tato kategorie zahrnuje weby zaměřené na hazard. Jedná se o weby typu online kasina nebo online loterie, které obvykle vyžadují platbu před tím, než může uživatel začít hrát v online ruletě, pokeru, blackjacku nebo podobných hrách. Některé z těchto webů jsou legitimní, což znamená, že zde existuje šance vyhrát. Některé jsou podvodné, což znamená, že zde vyhrát nelze. Detekuje také weby nabízející tipy a podvody k získání výhry popisující způsoby, jak vydělat peníze na hazardních webech a v online loteriích.
12	**Hry**	Tato kategorie zahrnuje weby poskytující online hry, obvykle využívající Adobe Flash nebo applety Java. Pro účely detekce není důležité, zda je hra zdarma, nebo vyžaduje předplatné. Weby typu kasina jsou detekovány v kategorii Hazard. Tato kategorie nezahrnuje: ▪ Oficiální webové stránky společností, které vyvíjejí videohry (pokud neprodukují online hry) ▪ Diskuzní weby, kde probíhají diskuze o hrách ▪ Weby, kde lze stáhnout hry ke hraní offline (některé z nich spadají do kategorie Nezákonné) ▪ Hry vyžadující stažení a spuštění spustitelného souboru, jako je World of Warcraft; těmto lze zabránit jinými prostředky, například branou firewall
13	**Státní správa**	Tato kategorie zahrnuje weby státní správy, včetně státních institucí, ambasád a webů úřadů.
14	**Hackerské útoky**	Tato kategorie zahrnuje weby poskytující nástroje pro hackování, články a diskusí platformy pro hackery. Zahrnuje také weby nabízející prostředky zneužití pro oblíbené platformy, které umožňují napadení účtu Facebook nebo Gmail.
15	**Nezákonné aktivity**	Toto je obsáhlá kategorie týkající se nenávisti, násilí a rasismu a jejím cílem je zablokovat následující kategorie webů: ▪ Weby patřící teroristickým organizacím ▪ Weby s rasistickým nebo xenofobním obsahem ▪ Weby s diskusemi o agresivních sportech nebo propagující násilí
16	**Zdraví a fitness**	Tato kategorie zahrnuje weby spojené s léčebnými ústavy, weby týkající se prevence a léčby nemocí, weby nabízející informace nebo produkty zaměřené na hubnutí, diety, steroidy, anabolika nebo produkty HGH a weby poskytující informace o plastických operacích.
17	**Koníčky**	Tato kategorie zahrnuje weby obsahující zdroje týkající se činností obvykle vykonávaných ve volném čase, jako je sběratelství, umění a řemesla a cyklistika.
18	**Webhosting**	Tato kategorie zahrnuje bezplatné a komerční webhostingové služby, které umožňují soukromým uživatelům i organizacím vytvářet a publikovat webové stránky.

19	**Ilegální stahování**	Tato kategorie zahrnuje weby týkající se softwarového pirátství, včetně následujících: ▪ Weby Peer-to-peer (BitTorrent, emule, DC++), o kterých je známo, že pomáhají distribuovat obsah chráněný autorskými právy bez souhlasu vlastníka práva. ▪ Warezové (padělaný komerční software) weby a diskusní weby ▪ Weby poskytující uživatelům crackové kódy, generátory klíčů a sériová čísla k nezákonnému použití. Některé z těchto webů mohou být také detekovány jako weby z kategorie pornografie nebo alkoholu a cigaret, protože za účelem výdělku často používají reklamu na pornografii a cigarety.
20	**Rychlé zasílání zpráv**	Tato kategorie zahrnuje weby pro rychlé zasílání zpráv a chaty, na kterých mohou uživatelé komunikovat v reálném čase. Detekovány budou také weby yahoo.com a gmail.com , protože obsahují integrovanou službu pro rychlé zasílání zpráv.
21	**Pracovní pozice / zaměstnání**	Tato kategorie zahrnuje weby obsahující nabídky pracovních pozic, reklamy týkající se práce a kariérní příležitosti, i agregátory takových služeb. Nezahrnuje weby personálních agentur nebo stránky s volnými pracovními pozicemi společností.
22	**Obsah pro dospělé**	Tato kategorie zahrnuje obsah, který autor webu určit pro dospělé publikum. Zahrnuje širokou škálu webů od Kámasútry a webů zaměřených na sexuální výchovu po tvrdé porno.
23	**Drogy**	Tato kategorie zahrnuje weby sdílející informace o rekreačních a ilegálních drogách. Tato kategorie zahrnuje také weby zaměřené na vývoj nebo pěstování drog.
24	**Zprávy**	Tato kategorie zahrnuje zpravodajské weby, které poskytují zprávy v podobě textu a videí. Cílem je zahrnout globální i místní zpravodajské servery. Některé malé místní zpravodajské servery ale zahrnuty být nemusí.
25	**Online seznamka**	Tato kategorie zahrnuje weby pro online seznamování (placené i zdarma), kde mohou uživatelé vyhledávat další lidi na základě určitých kritérií. Lidé mohou také zveřejnit své profily, aby je ostatní našli. Tato kategorie zahrnuje bezplatné i placené online seznamky. Vzhledem k tomu, že některé oblíbené sociální sítě lze také použít jako seznamku, jsou v této kategorii detekovány také oblíbené weby jako Facebook. Tuto kategorii doporučujeme použít s kategorií Sociální sítě.
26	**Online platby**	Tato kategorie zahrnuje weby nabízející online platby nebo převody peněz. Detekuje populární platební weby jako je PayPal nebo Moneybookers. Heuristicky také detekuje stránky na běžných webech, které vyžadují informace o kreditních kartách, a umožňuje detekci skrytých, neznámých nebo ilegálních internetových obchodů.
27	**Sdílení fotografií**	Tato kategorie zahrnuje weby pro sdílení fotografií, jejichž primárním účelem je umožnit uživatelům nahrávat a sdílet fotografie.
28	**Internetové obchody**	Tato kategorie zahrnuje známé internetové obchody. Web je považován za internetový obchod, pokud prodává zboží nebo služby online.
29	**Pornografie**	Tato kategorie zahrnuje weby obsahující erotický obsah a pornografii. Zahrnuje placené weby i neplacené weby. Zahrnuje weby poskytující obrázky, příběhy a videa a detekuje také pornografický obsah na webech se smíšeným obsahem.

30	**Portály**	Tato kategorie zahrnuje weby, které shromažďují informace z více zdrojů a různých domén a které obvykle nabízejí funkce jako vyhledávače, e-mail, zprávy a zábavné informace.
31	**Rádio**	Tato kategorie zahrnuje weby nabízející služby pro streamování hudby od stanic online rádia po weby poskytující audio obsah na vyžádání (zdarma nebo za poplatek).
32	**Víra**	Tato kategorie zahrnuje weby propagující víru nebo sektu. Zahrnuje diskuzní fóra týkající se jedné nebo více věr.
33	**Vyhledávače**	Tato kategorie zahrnuje vyhledávací weby jako je Google, Yahoo nebo Bing.
34	**Sociální sítě**	Tato kategorie zahrnuje weby sociálních sítí. Zahrnuje MySpace.com, Facebook.com, Bebo.com atd. Specializované sociální sítě, jako je YouTube.com, budou uvedeny v kategorii Video/Fotografie.
35	**Sport**	Tato kategorie zahrnuje weby, které nabízejí sportovní informace, zpravodajství a návody.
36	**Sebevražda**	Tato kategorie zahrnuje weby propagující, nabízející nebo podporující sebevraždu. Nezahrnuje kliniky zaměřené na prevenci sebevražd.
37	**Bulvár**	Tato kategorie je určena hlavně pro soft porno a weby s novinkami ze života celebrit. Mnoho zpravodajských webů ve stylu bulváru může mít různé podkategorie. Detekce pro tuto kategorii je také založena na heuristice.
38	**Ztráta času**	Tato kategorie zahrnuje weby, na kterých lidé většinou tráví hodně času. Jedná se o weby z jiných kategorií, jako jsou sociální sítě nebo zábava.
39	**Cestování**	Tato kategorie zahrnuje weby obsahující nabídky cestování a vybavení na cesty i recenze a hodnocení destinací.
40	**Videa**	Tato kategorie zahrnuje weby, které hostují různá videa nebo fotografie nahraná uživateli nebo poskytnutá různými poskytovateli obsahu. Patří sem weby jako YouTube, Metacafe, Google Video a weby určené pro fotografie jako Picasa nebo Flickr. Detekovány budou také videa vložená na jiných webech nebo blozích.
41	**Animované filmy o násilí**	Tato kategorie zahrnuje weby pro diskusi, sdílení a nabízení animovaných videí s obsahem násilí nebo manga, která mohou být nevhodná pro nezletilé osoby kvůli násilí, nevhodnému jazyku nebo sexuálnímu obsahu. Tato kategorie nezahrnuje weby, které nabízejí oblíbené animované seriály, jako je Tom a Jerry.
42	**Zbraně**	Tato kategorie zahrnuje weby nabízející zbraně k prodeji nebo jejich výměnu, výrobu či použití. Zahrnuje také vybavení pro lov a využití vzduchových a BB zbraní i osobních zbraní.
43	**E-mail**	Tato kategorie zahrnuje weby poskytující funkce e-mailu ve formě webové aplikace.

44	**Webový proxy server**	Tato kategorie zahrnuje weby poskytující služby webového proxy serveru. Jedná se o typ webu zahrnující prohlížeč v prohlížeči, kdy uživatel otevře webovou stránku, zadá do formuláře požadovanou adresu URL a klikne na tlačítko Odeslat. Web s webovým proxy serverem stáhne aktuální stránku a zobrazí ji uvnitř uživatelského prohlížeče. Tento typ je detekován z následujících důvodů (a proto je vhodné ho zablokovat): ▪ Pro anonymní procházení. Vzhledem k tomu, že jsou požadavky na cílový webový server prováděny z webového proxy serveru, je viditelná pouze jeho IP adresa, a pokud správci serveru sledují uživatele, sledování skončí na proxy serveru – který může a nemusí uchovávat protokoly potřebné k vyhledání původního uživatele. ▪ Pro falšování polohy. IP adresy uživatele jsou často používány pro profilování služby podle zdrojové polohy (některé weby státní správy mohou být dostupné pouze z místních IP adres) a pomocí těchto služeb může uživatel falšovat svoji skutečnou polohu. ▪ Pro přístup k zakázanému obsahu. Pokud se používá jednoduchý filtr adres URL, uvidí pouze adresy URL webového serveru proxy a ne skutečných serverů, které uživatel navštíví. ▪ Pro předejití sledování ze strany firmy. Firemní zásady mohou vyžadovat sledování využívání internetu zaměstnanci. Pokud uživatel bude na všechny stránky přistupovat prostřednictvím webového proxy serveru, sledování nemusí poskytnout správné informace. Vzhledem k tomu, že sada SDK analyzuje stránku HTML (je-li poskytnuta) a nikoli jen adresy URL, bude v případě některých kategorií sada SDK přesto schopna obsah detekovat. Jiným důvodům se však nelze vyhnout pouhým použitím sady SDK.

Pokud zaškrtnete políčko **Zobrazit všechna upozornění pro zablokované adresy URL podle kategorií**, zobrazí se na liště upozornění pro zablokované adresy URL podle kategorií. Pokud má web několik dílčích domén, vygenerují se upozornění i pro tyto domény, takže počet upozornění může být vysoký.

Výjimky

Adresy URL, o kterých je známo, že jsou bezpečné, lze přidat na seznam důvěryhodných adres URL. Adresy URL, které představují hrozbu, lze přidat na seznam blokovaných adres URL.

Přidání adresy URL na seznam

1. V modulu filtrování adres URL plánu ochrany klikněte na položku **Výjimky**.
2. Vyberte požadovaný seznam: **Důvěryhodné** nebo **Zablokované**.
3. Klikněte na tlačítko **Přidat**.
4. Zadejte adresu URL nebo IP adresu a klikněte na zatržítko.

Důležité *Všechny adresy ze zadané domény budou považovány za důvěryhodné nebo blokované. Pokud například zadáte* `https://www.xyz.com/en-us/my/beta/2020/page.html` *jako důvěryhodnou adresu URL, budou za důvěryhodné považovány všechny adresy v doméně* `xyz.com`*.*

20.6 Karanténa

Karanténa je speciální izolovaná složka na pevném disku počítače, kam jsou umístěny podezřelé soubory detekované modulem Antivirová ochrana a ochrana proti malwaru s cílem zabránit dalšímu šíření hrozeb.

Karanténa umožňuje zkontrolovat podezřelé a potenciálně nebezpečné soubory ze všech počítačů a rozhodnout se, zda by měly být odebrány, nebo obnoveny. Soubory v karanténě jsou automaticky odebrány, pokud je počítač odebrán ze systému.

Jak se soubory dostanou do složky karantény?

1. Nakonfigurujete plán ochrany a definujete výchozí akci pro infikované soubory – umístění do karantény.
2. Systém během naplánované kontroly nebo kontroly při přístupu detekuje škodlivé soubory a umístí je do bezpečné složky – karantény.
3. Systém aktualizuje seznam karantény na počítačích.
4. Soubory jsou z karantény automaticky odstraněny po uplynutí období definovaného v nastavení **Odebrat soubory v karanténě po** v plánu ochrany.

Správa souborů v karanténě

Soubory v karanténě můžete spravovat v nabídce **Ochrana proti malwaru** > **Karanténa**. Zobrazí se seznam souborů umístěných do karantény ze všech počítačů.

Název	Popis
Soubor	Název souboru.
Datum umístění do karantény	Datum a čas, kdy byl soubor umístěn do karantény.
Zařízení	Zařízení, na kterém byl infikovaný soubor nalezen.
Název hrozby	Název hrozby.
Plán ochrany	Plán ochrany, na základě kterého byl podezřelý soubor umístěn do karantény.

Se soubory v karanténě můžete provést dvě akce:

- **Odstranit** – trvale odebrat soubor umístěný do karantény ze všech počítačů.
- **Obnovit** – obnovit soubor umístěný do karantény do původního umístění bez změn. Pokud v původním umístění momentálně existuje soubor se stejným názvem, bude přepsán obnoveným souborem. Upozorňujeme, že obnovený soubor bude přidán na seznam povolených souborů a během příštích antimalwarových kontrol bude přeskočen.

Umístění karantény na počítačích

Výchozí umístění souborů umístěných do karantény je:

Pro počítač se systémem Windows: **`%ProgramData%\%product_name%\Quarantine`**

Pro počítač se systémem Mac/Linux: **`/usr/local/share/%product_name%/quarantine`**

20.7 Seznam povolených podnikových aplikací

Tato funkce je k dispozici, pouze pokud je služba vyhledávání nainstalována na serveru pro správu.

Firmy obvykle využívají své vlastní podnikové aplikace, které mohou antivirová řešení rozpoznat a detekovat jako falešně pozitivní. Ruční přidávání důvěryhodných aplikací na seznam povolených aplikací je navíc časově náročné.

Cyber Protect může proces přidání takových aplikací na seznam povolených aplikací automatizovat. Zálohy jsou zkontrolovány modulem Antivirová ochrana a ochrana proti malwaru a zkontrolovaná

data jsou analyzována s cílem takové aplikace přidat na seznam povolených aplikací a předejít falešně pozitivním detekcím.

Přidání důvěryhodných aplikací na seznam povolených aplikací na celopodnikové úrovni umožňuje ještě zvýšit výkon kontroly.

Automatické přidání na seznam povolených položek

1. Nejprve byste měli alespoň na dvou počítačích spustit cloudovou kontrolu záloh. To lze provést pomocí plánů kontroly zálohy.
2. Následně byste měli v nastavení seznamu povolených položek aktivovat možnost **Automatické vygenerování seznamu povolených položek**.

Ruční přidání na seznam povolených položek

Ruční přidání aplikací na seznam povolených položek je k dispozici, pouze pokud je aktivována možnost **Automatické vygenerování seznamu povolených položek**.

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Ochrana proti malwaru** > **Seznam povolených položek**.
2. Klikněte na tlačítko **Přidat soubor**.
3. Určete cestu k souboru a klikněte na tlačítko **Přidat**.

Nastavení seznamu povolených položek

Můžete aktivovat možnost **Automatické vygenerování seznamu povolených položek**.

Následně můžete určit jednu ze tří úrovní důvěryhodných pravidel, které definují úroveň útoku heuristiky:

- **Nízká** – podnikové aplikace budou přidány na seznam povolených položek pouze po dlouhém časovém období a po provedení kontrol. Tyto aplikace jsou důvěryhodnější. Tento přístup však zvyšuje pravděpodobnost falešně pozitivních detekcí. Kritéria, na základě kterých bude soubor považován za čistý a důvěryhodný, jsou vysoká.
- **Výchozí** – podnikové aplikace budou přidány na seznam povolených položek podle doporučené úrovně ochrany, aby se omezily falešně pozitivní detekce. Kritéria, na základě kterých bude soubor považován za čistý a důvěryhodný, jsou střední.
- **Vysoká** – podnikové aplikace budou přidány na seznam povolených položek, aby se omezily falešně pozitivní detekce. To však nezaručuje, že software je čistý. Později může být potvrzen jako podezřelý nebo malware. Kritéria, na základě kterých bude soubor považován za čistý a důvěryhodný, jsou nízká.

20.8 Antimalwarová kontrola záloh

Chcete-li zabránit obnovení infikovaných souborů ze záloh, můžete v zálohách vyhledat případný malware. Kontrola záloh je podporována pouze v operačních systémech Windows. Funkce je k dispozici, pouze pokud je služba vyhledávání nainstalována na serveru pro správu Cyber Protect.

Chcete-li v zálohách vyhledat malware, vytvořte plán kontroly zálohy (str. 224).

Poznámka *Z důvodu zabezpečení a výkonu doporučujeme pro účely vyhledávání použít vyhrazený počítač. Tento počítač bude mít přístup ke všem kontrolovaným zálohám.*

Výsledky kontroly naleznete na kontrolním panelu v ovládacím prvku Podrobnosti kontroly záloh (str. 412). Stav zálohy si můžete také zobrazit v nabídce **Úložiště záloh** > **Umístění** > **<název zálohy>**.

Pokud kontrola záloh nebyla provedena, mají zálohy dále stav **Nekontrolováno**. Po provedení kontroly mají zálohy jeden z následujících aktualizovaných stavů:

- **Žádný malware**
- **Zjištěn malware**

Omezení

- Malware lze vyhledat pouze v zálohách typu **Celý počítač** a **Disky/svazky**.
- Zkontrolovány budou pouze svazky se systémem souborů NTFS s oddíly GPT a MBR.
- Podporovaná umístění záloh: **Cloudové úložiště**, **místní složka** a **síťová složka**.
- Zálohy, které mají body obnovení souvislé ochrany dat (str. 133), lze vybrat ke kontrole, ale tyto body obnovení nebudou zkontrolovány. Zkontrolovány budou pouze běžné body obnovení.
- Pokud byla záloha souvislé ochrany dat vybrána pro bezpečné obnovení celého počítače, bude počítač bezpečně obnoven bez dat v bodě obnovení souvislé ochrany dat. Chcete-li obnovit data souvislé ochrany dat, spusťte obnovení **souborů/složek**.

21 Ochrana aplikací pro spolupráci a komunikaci

Aplikace Zoom, Cisco Webex Meetings a Microsoft Teams jsou nyní běžně používány pro video a webové konference a komunikace. Se službou Cyber Protect můžete své nástroje pro spolupráci chránit.

Konfigurace ochrany pro aplikace Zoom, Cisco Webex Meetings a Microsoft Teams je podobná. V příkladu níže je uvedena konfigurace pro aplikaci Zoom.

Nastavení ochrany aplikace Zoom

1. Nainstalujte agenta pro ochranu na počítači, kde je nainstalovaná aplikace pro spolupráci.
2. Přihlaste se do webové konzole Cyber Protect a použijte plán ochrany (p. 120), který má povolen jeden z následujících modulů:
   - **Antivirová ochrana a ochrana proti malwaru** (p. 354) (s povoleným nastavením **Self-Protection** a **Active Protection**) – pokud máte jednu z verzí Cyber Protect.
   - **Active Protection** (p. 361) (s povoleným nastavením **Self-Protection**) – pokud máte jednu z verzí Cyber Backup.
3. [Volitelné] Pro automatickou instalaci aktualizace nakonfigurujte modul **Správa oprav** (p. 378) v plánu ochrany.

Ochrana aplikace Zoom se pak bude vztahovat na následující aktivity:

- Automatická instalace aktualizací klienta aplikace Zoom
- Ochrana procesů aplikace Zoom před injektážemi kódu
- Bránění podezřelým operacím aplikace Zoom
- Ochrana souboru Hostitelé před přidáním domén souvisejících s aplikací Zoom

22 Posouzení ohrožení zabezpečení a správa oprav

22.1 Podporované produkty společnosti Microsoft a produkty třetích stran

Podporované produkty Microsoft

Windows OS

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Windows Server OS

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012.
- Windows Server 2008 R2

Microsoft Office a související komponenty

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Komponenty související s OS Windows

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio a aplikace
- Komponenty operačního systému

Serverové aplikace

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016

- Microsoft Sharepoint Server 2016

Podporované produkty třetích stran pro operační systém Windows

Služba Kybernetická ochrana podporuje posouzení ohrožení zabezpečení a opravy pro širokou škálu aplikací třetích stran, včetně nástrojů pro správu a klientů VPN, které jsou důležité při práci vzdáleně.

Úplný seznam podporovaných produktů třetích stran pro systém Windows naleznete v tématu https://kb.acronis.com/content/62853.

22.2 Posouzení ohrožení zabezpečení

Posouzení ohrožení zabezpečení je proces identifikace, kvantifikace a prioretizace zjištěných ohrožení zabezpečení v systému. Modul Posouzení ohrožení zabezpečení umožňuje vyhledávat v počítačích ohrožení zabezpečení a zajistit, že všechny nainstalované aplikace a operační systémy jsou aktuální a pracují správně.

Pro kontrolu posouzení ohrožení zabezpečení jsou momentálně podporovány pouze systémy Windows a Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastucture). Další informace o konfiguracích pro počítače se systémem Linux naleznete v tématu Posouzení ohrožení zabezpečení pro počítače se systémem Linux (p. 378).

Jak to funguje

1. Vytvoříte plán ochrany s povoleným modulem posouzení ohrožení zabezpečení, zadáte nastavení posouzení ohrožení zabezpečení (p. 375) a přiřadíte plán k počítačům.
2. Systém podle harmonogramu nebo na vyžádání odešle příkaz ke spuštění kontroly posouzení zabezpečení agentům pro ochranu nainstalovaným na počítačích.
3. Agenti obdrží příkaz, spustí vyhledávání ohrožení zabezpečení na počítačích a vygenerují aktivitu kontroly.
4. Po dokončení kontroly ohrožení zabezpečení agenti vygenerují výsledky a odešlou je sledovací službě.
5. Sledovací služba zpracuje data od agentů a zobrazí výsledky v ovládacích prvcích posouzení ohrožení zabezpečení (p. 411) a v seznamu zjištěných ohrožení zabezpečení.
6. Zobrazí se seznam nalezených ohrožení zabezpečení (p. 377). Můžete ho pracovat a rozhodnout, která ze zjištěných ohrožení je třeba opravit.

Výsledky kontroly posouzení ohrožení zabezpečení můžete sledovat v ovládacích prvcích v nabídce **Kontrolní panel** > **Přehled** > **Ohrožení zabezpečení / Existující ohrožení zabezpečení**.

22.2.1 Nastavení posouzení ohrožení zabezpečení

Návod k vytvoření plánu ochrany s modulem Posouzení ohrožení zabezpečení naleznete v tématu „Vytvoření plánu ochrany“. Kontrola posouzení ohrožení zabezpečení může být provedena podle harmonogramu nebo na vyžádání (kliknutím na příkaz **Spustit nyní** v plánu ochrany).

Pro posouzení ohrožení zabezpečení je možné zadat následující nastavení:

Co kontrolovat

Vyberte softwarové produkty, u kterých chcete zkontrolovat ohrožení zabezpečení:

- Počítače se systémem Windows:
  - **Produkty Microsoft**

    - **Produkty Windows třetích stran** (Další informace o podporovaných produktech třetích stran pro systém Windows naleznete v tématu https://kb.acronis.com/content/62853.
- Počítače se systémem Linux:
    - **Kontrola linuxových balíků**

Plán

Definujte harmonogram, na základě kterého bude na vybraných počítačích provedena kontrola posouzení ohrožení zabezpečení:

Naplánujte spuštění úlohy pomocí následujících událostí:

- **Naplánovat podle času** – úloha se spustí podle zadaného času.
- **Když se uživatel přihlásí do systému** – ve výchozím nastavení zahájí spuštění úlohy přihlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.
- **Když se uživatel odhlásí ze systému** – ve výchozím nastavení zahájí spuštění úlohy odhlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.

  Poznámka *Úloha nebude spuštěna při vypnutí systému. Vypnutí a odhlášení jsou dvě různé akce.*
- **Při spuštění systému** – úloha se spustí při spuštění operačního systému.
- **Při vypnutí systému** – úloha se spustí při vypnutí operačního systému.

Výchozí nastavení: **Naplánovat podle času**.

Typ harmonogramu:

- **Měsíčně** – vyberte měsíce a týdny nebo dny v měsíci, kdy se úloha spustí.
- **Denně** – vyberte dny v týdnu, kdy se úloha spustí.
- **Po hodině**– vyberte dny v týdnu, počet opakování a časový interval, během kterého se úloha spustí.

Výchozí nastavení: **Denně**.

Spustit v – vyberte přesný čas, kdy se úloha spustí.

Výchozí nastavení: **14:00** (v počítači, ve kterém je software nainstalován).

Spustit v časovém rozsahu – nastavte časový rozsah, ve kterém bude nakonfigurovaný harmonogram platný.

Podmínky spuštění – definujte všechny podmínky, které musí být současně splněny před spuštěním úlohy. Podobají se podmínkám spuštění pro modul zálohy popsaným v tématu Podmínky spuštění.

Definovat lze například následující dodatečné podmínky spuštění:

- **Rozložit časy spuštění úlohy do časového rámce**– tato možnost umožňuje definovat časový rámec, během kterého musí být úloha spuštěna, a rozložit úlohy, aby nedošlo k přetížení sítě, protože mnoho počítačů může mít malou šířku pásma pro hostitele, kde se nacházejí služby Windows Server Update Services (WSUS) nebo server pro správu. Můžete zadat prodlevu v hodinách, minutách nebo sekundách. Pokud je například výchozí čas spuštění 10:00 a prodleva je 60 minut, bude úloha spuštěna mezi 10:00 a 11:00.
- **Pokud je počítač vypnutý, vynechané úlohy se spustí při spuštění počítače**
- **Zabránit režimu spánku nebo hibernace při spuštění úlohy** – tato možnost platí pouze v počítačích se systémem Windows.

- **Pokud podmínky spuštění nejsou splněny, spustit úlohu za** – zadejte dobu v hodinách, za kterou bude úloha spuštěna bez ohledu na jiné podmínky spuštění.

22.2.2 Správa zjištěných ohrožení zabezpečení

Pokud bylo posouzení ohrožení zabezpečení provedeno alespoň jednou a byla nalezena nějaká ohrožení zabezpečení, zobrazí se v nabídce **Správa softwaru** > **Ohrožení zabezpečení**. V seznamu ohrožení zabezpečení jsou uvedena ohrožení zabezpečení, pro která lze nainstalovat opravy, i ohrožení, která nemají navržené opravy. Pomocí filtru můžete zobrazit pouze ohrožení zabezpečení s opravami.

Název	Popis
Název	Název ohrožení zabezpečení.
Postižené produkty	Softwarové produkty, pro které byla ohrožení zabezpečení zjištěna.
Počítače	Počet postižených počítačů.
Závažnost	Závažnost zjištěného ohrožení zabezpečení. Přiřadit lze následující úrovně podle rámce CVSS (Common Vulnerability Scoring System): ▪ **Kritická**: 9–10 CVSS ▪ **Vysoká**: 7–9 CVSS ▪ **Střední**: 3–7 CVSS ▪ **Nízká**: 0–3 CVSS ▪ **Žádné**
Opravy	Počet odpovídajících oprav.
Publikováno	Datum a čas, kdy bylo ohrožení zabezpečení publikováno v seznamu Common Vulnerabilities and Exposures (CVE).
Detekováno	První datum, kdy bylo existující ohrožení zabezpečení na počítačích zjištěno.

Popis nalezeného ohrožení zabezpečení zobrazíte kliknutím na jeho název v seznamu.

Zahájení procesu opravy ohrožení zabezpečení

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Správa softwaru** > **Ohrožení zabezpečení**.
2. V seznamu vyberte ohrožení zabezpečení a klikněte na tlačítko **Instalovat opravy**. Otevře se průvodce opravou ohrožení zabezpečení.
3. Vyberte opravy k instalaci. Klikněte na tlačítko **Další**.
4. Vyberte počítače, pro které chcete nainstalovat opravy.
5. Zvolte, zda má být počítač po instalaci opravy restartován:
   - **Ne** – po instalaci aktualizace nebude nikdy proveden restart.
   - **Je-li vyžadováno** – restart bude proveden, pokud je vyžadován k použití aktualizací.
   - **Vždy** – restart bude po nainstalování aktualizací proveden vždy. Vždy můžete zadat prodlení restartu.

   Restartovat až po dokončení zálohy – pokud běží proces zálohování, bude restart zařízení odložen, dokud nebude záloha dokončena.

   Jakmile budete připraveni, klikněte na položku **Instalovat opravy**.

Vybrané opravy se nainstalují na vybraných počítačích.

22.2.3 Posouzení ohrožení zabezpečení pro počítače se systémem Linux

Posouzení ohrožení zabezpečení je podporováno také pro počítače se systémem Linux. V počítačích se systémem Linux můžete vyhledat ohrožení zabezpečení na úrovni aplikace a na úrovni jádra.

Podporovány jsou následující distribuce a verze systému Linux:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

Konfigurace posouzení ohrožení zabezpečení pro počítače se systémem Linux

1. Nainstalujte agenta pro Linux na hostiteli Acronis Cyber Infrastructure (nebo Virtuozzo) nebo na virtuálním počítači se systémem CentOS.
2. Ve webové konzoli Cyber Protect vytvořte plán ochrany a povolte modul **Posouzení ohrožení zabezpečení**.
3. Zadejte nastavení posouzení ohrožení zabezpečení:
   - **Co kontrolovat** – vyberte možnost **Kontrola linuxových balíků**.
   - **Harmonogram** – definujte harmonogram posouzení ohrožení zabezpečení.
4. Přiřaďte plán k počítačům.

Po provedení posouzení ohrožení zabezpečení se zobrazí seznam nalezených ohrožení (p. 377). Můžete ho zpracovat a rozhodnout se, která ze zjištěných ohrožení je třeba opravit.

Výsledky posouzení ohrožení zabezpečení můžete sledovat v ovládacích prvcích v nabídce **Kontrolní panel** > **Přehled** > **Ohrožení zabezpečení / Existující ohrožení zabezpečení**.

22.3 Správa oprav

Správa oprav (PM) přináší funkce správy oprav a aktualizací pro aplikace a operační systémy nainstalované na vašich počítačích a umožňuje udržovat systémy v aktuálním stavu. Modul správy oprav umožňuje automaticky nebo ručně schvalovat instalaci oprav na počítačích. Funkce správy oprav je momentálně podporována pouze na počítačích se systémem Windows.

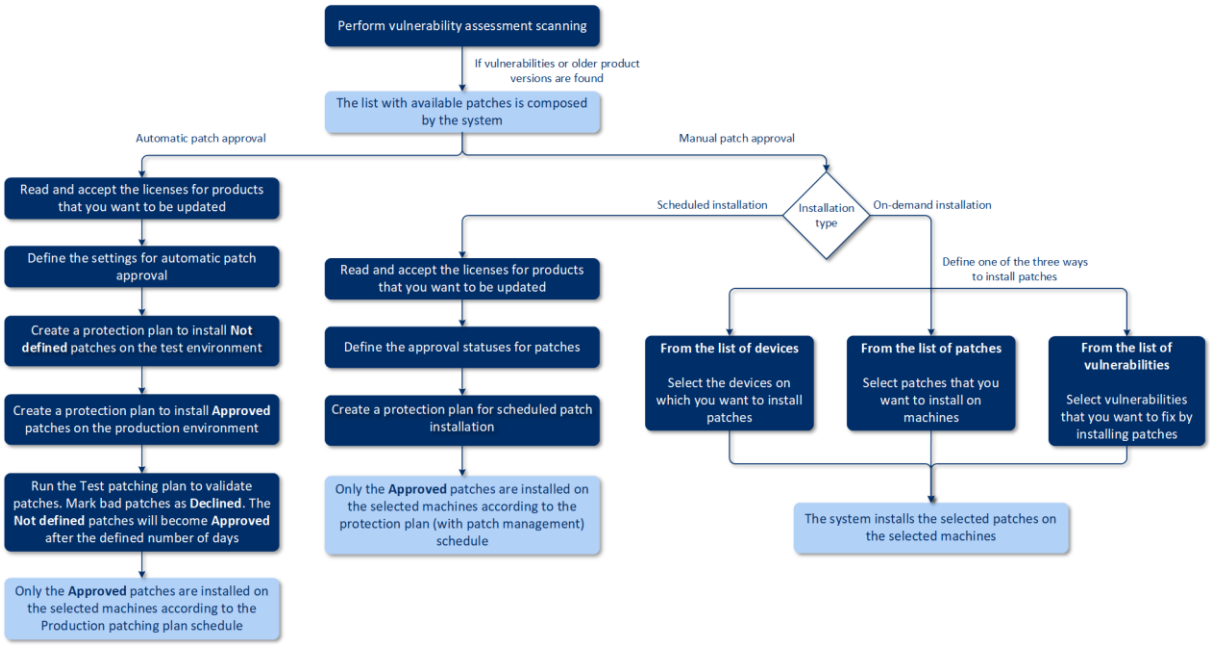
Funkce správy oprav umožňuje:

- Instalovat aktualizace na úrovni operačního systému a aplikací
- Schvalovat opravy ručně nebo automaticky
- Instalovat opravy na vyžádání a podle harmonogramu
- Přesně definovat, které opravy se mají použít, podle různých kritérií: závažnost, kategorie a stav schválení
- Provádět zálohy před aktualizací k zabránění možným neúspěšným aktualizacím
- Definovat možnost restartu po instalaci opravy

Služba Cyber Protect používá peer-to-peer technologii, aby minimalizovala provoz v síti. Můžete si vybrat jednoho a více vyhrazených agentů, kteří stáhnou aktualizace z internetu a distribuují je mezi další agenty v síti. Všichni agenti budou také aktualizace sdílet navzájem jako peer-to-peer agenti.

Jak to funguje

Nakonfigurovat můžete buď automatické, nebo ruční schvalování oprav. Ve schématu níže vidíte postup automatického i ručního schvalování oprav.



1. Nejprve musíte provést alespoň jednu kontrolu ohrožení zabezpečení (p. 375) pomocí plánu ochrany s povoleným modulem **Posouzení ohrožení zabezpečení**. Po provedení kontroly vytvoří systém seznam nalezených ohrožení zabezpečení (p. 377) a dostupných oprav (p. 382).
2. Pak můžete nakonfigurovat automatické schválení opravy (p. 384) nebo použít ruční schválení opravy (p. 386).
3. Definujte, jak chcete opravy nainstalovat – podle harmonogramu nebo na vyžádání. Instalaci oprav na vyžádání lze provést třemi způsoby, podle vašich preferencí:
   - Přejděte na seznam oprav (**Správa softwaru** > **Opravy**) a nainstalujte potřebné opravy.
   - Přejděte na seznam ohrožení zabezpečení (**Správa softwaru** > **Ohrožení zabezpečení**) a zahajte proces řešení, který také zahrnuje instalaci opravy.
   - Přejděte na seznam všech zařízení (**Zařízení** > **Všechna zařízení**), vyberte konkrétní počítače, které chcete aktualizovat, a nainstalujte na ně opravy.

Výsledky instalace oprav můžete sledovat v ovládacím prvku v nabídce **Kontrolní panel** > **Přehled** > **Historie instalace oprav**.

22.3.1 Nastavení správy oprav

Návod k vytvoření plánu ochrany s modulem správy oprav naleznete v tématu „Vytvoření plánu ochrany“. Pomocí plánu ochrany můžete určit, jaké aktualizace určené pro produkty společnosti Microsoft a ostatní produkty třetích stran pro operační systém Windows se mají automaticky nainstalovat na definovaných počítačích.

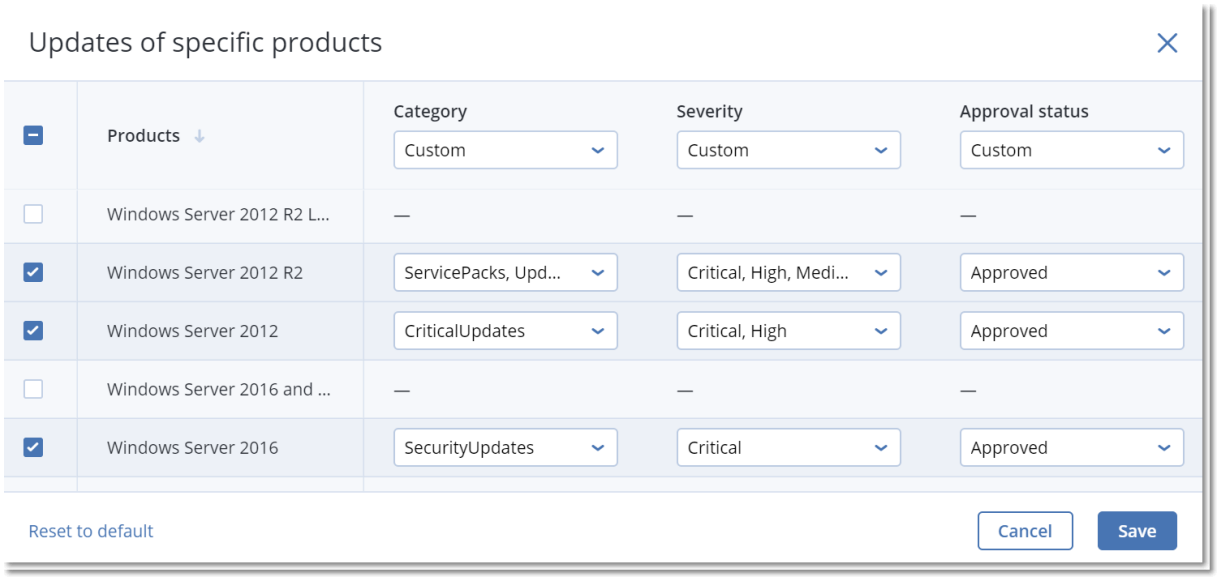
Pro modul správy oprav je možné zadat následující nastavení.

Produkty Microsoft

Chcete-li na vybraných počítačích nainstalovat aktualizace společnosti Microsoft, povolte možnost **Aktualizovat produkty Microsoft**.

Vyberte, které aktualizace chcete nainstalovat:

- **Všechny aktualizace**
- **Pouze kritické aktualizace a aktualizace zabezpečení**
- **Aktualizace konkrétních produktů**: můžete definovat vlastní nastavení pro různé produkty. Pokud chcete aktualizovat konkrétní produkty, můžete pro každý produkt definovat, které aktualizace se mají nainstalovat na základě kategorie, závažnosti nebo stavu schválení (p. 382).



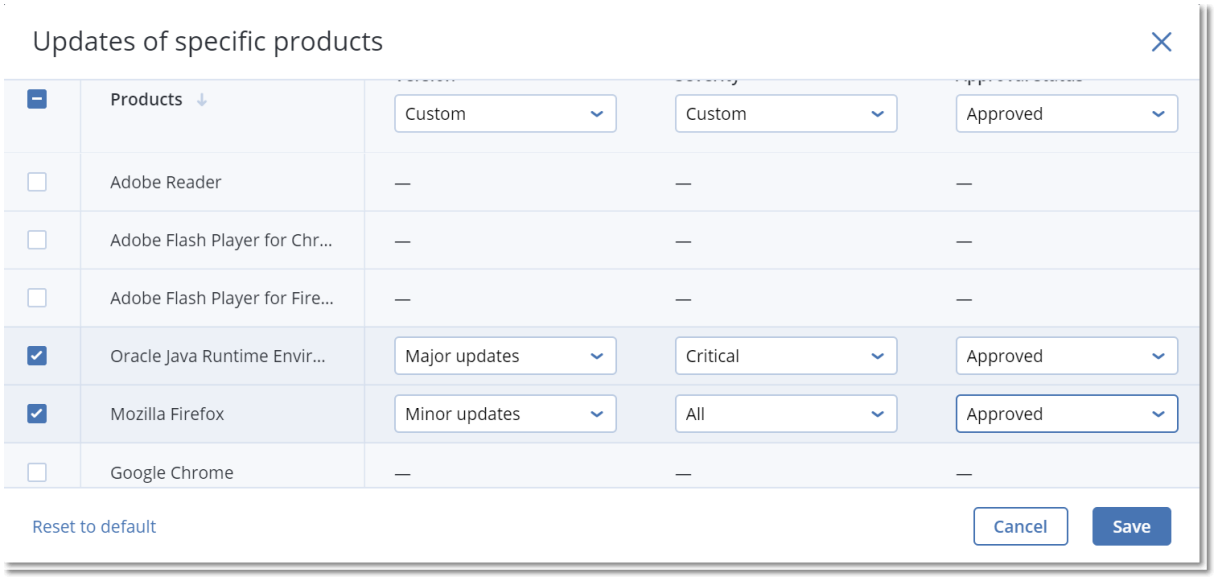
Produkty Windows třetích stran

Chcete-li na vybraných počítačích nainstalovat aktualizace třetích stran pro operační systém Windows, povolte možnost **Produkty Windows třetích stran**.

Vyberte, které aktualizace chcete nainstalovat:

- Volba **Pouze hlavní aktualizace** umožňuje nainstalovat pouze nejnovější dostupnou verzi aktualizace.
- Volba **Pouze vedlejší aktualizace** umožňuje nainstalovat podverzi aktualizace.

- **Aktualizace konkrétních produktů**: můžete definovat vlastní nastavení pro různé produkty. Pokud chcete aktualizovat konkrétní produkty, můžete pro každý produkt definovat, které aktualizace se mají nainstalovat na základě kategorie, závažnosti nebo stavu schválení (p. 382).



Plán

Definujte harmonogram, na základě kterého budou na vybraných počítačích nainstalovány aktualizace.

Naplánujte spuštění úlohy pomocí následujících událostí:

- **Naplánovat podle času** – úloha se spustí podle zadaného času.
- **Když se uživatel přihlásí do systému** – ve výchozím nastavení zahájí spuštění úlohy přihlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.
- **Když se uživatel odhlásí ze systému** – ve výchozím nastavení zahájí spuštění úlohy odhlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.

  Poznámka *Úloha nebude spuštěna při vypnutí systému. Vypnutí a odhlášení jsou dvě různé akce.*

- **Při spuštění systému** – úloha se spustí při spuštění operačního systému.
- **Při vypnutí systému** – úloha se spustí při vypnutí operačního systému.

Výchozí nastavení: **Naplánovat podle času**.

Typ harmonogramu:

- **Měsíčně** – vyberte měsíce a týdny nebo dny v měsíci, kdy se úloha spustí.
- **Denně** – vyberte dny v týdnu, kdy se úloha spustí.
- **Po hodině**– vyberte dny v týdnu, počet opakování a časový interval, během kterého se úloha spustí.

Výchozí nastavení: **Denně**.

Spustit v – vyberte přesný čas, kdy se úloha spustí.

Výchozí nastavení: **14:00** (v počítači, ve kterém je software nainstalován).

Spustit v časovém rozsahu – nastavte časový rozsah, ve kterém bude nakonfigurovaný harmonogram platný.

Podmínky spuštění – definujte všechny podmínky, které musí být současně splněny před spuštěním úlohy. Podobají se podmínkám spuštění pro modul zálohy popsaným v tématu Podmínky spuštění.

Definovat lze například následující dodatečné podmínky spuštění:

- **Rozložit časy spuštění úlohy do časového rámce**– tato možnost umožňuje definovat časový rámec, během kterého musí být úloha spuštěna, a rozložit úlohy, aby nedošlo k přetížení sítě, protože mnoho počítačů může mít malou šířku pásma pro hostitele, kde se nacházejí služby Windows Server Update Services (WSUS) nebo server pro správu. Můžete zadat prodlevu v hodinách, minutách nebo sekundách. Pokud je například výchozí čas spuštění 10:00 a prodleva je 60 minut, bude úloha spuštěna mezi 10:00 a 11:00.
- **Pokud je počítač vypnutý, vynechané úlohy se spustí při spuštění počítače**
- **Zabránit režimu spánku nebo hibernace při spuštění úlohy** – tato možnost platí pouze v počítačích se systémem Windows.

Pokud podmínky spuštění nejsou splněny, spustit úlohu za – zadejte dobu v hodinách, za kterou bude úloha spuštěna bez ohledu na jiné podmínky spuštění.

Záloha před aktualizací

Spustit zálohu před instalací aktualizací softwaru – systém před instalací aktualizací vytvoří přírůstkovou zálohu počítače. Pokud dříve nebyly vytvořeny žádné zálohy, bude vytvořena plná záloha počítače. V případě selhání instalace opravy se tak budete moct vrátit do původního stavu. Pokud chcete možnost **Záloha před aktualizací** použít, musí mít příslušné počítače v plánu ochrany povolený modul správy oprav a modul zálohování a musí být určeny položky, které chcete zálohovat – celý počítač nebo spouštěcí a systémový svazek. Pokud k zálohování vyberete nevhodné položky, systém neumožní povolení možnosti **Záloha před aktualizací**.

22.3.2 Správa seznamu oprav

Po provedení posouzení ohrožení zabezpečení naleznete dostupné opravy v nabídce **Správa softwaru** > **Opravy**.

Název	Popis
Název	Název opravy
Závažnost	Závažnost opravy: ▪ **Kritická** ▪ **Vysoká** ▪ **Střední** ▪ **Nízká** ▪ **Žádná**
Prodejce	Prodejce opravy
Produkt	Produkt, kterého se oprava týká
Nainstalované verze	Verze produktu, které jsou již nainstalované
Verze	Verze opravy

Kategorie	Kategorie, do které oprava náleží: ▪ **Důležitá aktualizace** – obecně vydávané opravy pro konkrétní problémy řešící kritické chyby nesouvisející se zabezpečením. ▪ **Aktualizace zabezpečení** – obecně vydávané opravy pro konkrétní produkty řešící problémy zabezpečení. ▪ **Aktualizace definic** – aktualizace souborů s definicemi virů nebo jiných souborů s definicemi. ▪ **Kumulativní aktualizace** – sada hotfixů, aktualizací zabezpečení, důležitých aktualizací a aktualizací, které jsou spojeny za účelem snadného nasazení. Kumulativní aktualizace je obecně zaměřena na konkrétní oblast, jako je zabezpečení, nebo na konkrétní komponentu, například na Internetové informační služby. ▪ **Aktualizace Service Pack** – sada všech hotfixů, aktualizací zabezpečení, kritických aktualizací a aktualizací vytvořených od vydání produktu. Aktualizace Service Pack mohou také obsahovat omezený počet změn designu či funkcí požadovaných zákazníkem. ▪ **Nástroj** – nástroje nebo funkce, které pomáhají provádět úlohy nebo sady úloh. ▪ **Balíček funkcí** – nová vydání funkcí, které budou obvykle implementovány v produktech při příštím vydání. ▪ **Aktualizace** – obecně vydávané opravy pro konkrétní problémy řešící chyby, které nejsou kritické a nesouvisejí se zabezpečením. ▪ **Aplikace** – opravy pro aplikaci.
Znalostní báze Microsoft	V případě opravy pro produkt Microsoft je uvedeno ID článku Znalostní báze.
Datum vydání	Datum vydání opravy
Počítače	Počet postižených počítačů
Stav schválení	Stav schválení je vyžadován hlavně pro scénář automatického schvalování a umožňuje v plánu ochrany podle stavu definovat, které aktualizace se mají nainstalovat. Definovat můžete jeden z následujících stavů opravy: ▪ **Schváleno** – oprava byla nainstalována alespoň na jednom počítači a bylo ověřeno, že je OK. ▪ **Zamítnuto** – oprava není bezpečná a může poškodit systém počítače. ▪ **Nedefinované** – stav opravy je nejasný a opravu je třeba ověřit.
Licenční ujednání	▪ Přečíst a přijmout ▪ Nesouhlasil(a). Pokud s licenčním ujednáním nesouhlasíte, bude stav opravy nastaven na **Zamítnuto** a oprava nebude nainstalována.
Ohrožení zabezpečení	Počet ohrožení zabezpečení. Pokud na položku kliknete, budete přesměrováni na seznam ohrožení zabezpečení.
Velikost	Průměrná velikost opravy.
Jazyk	Jazyk, který oprava podporuje.
Web prodejce	Oficiální webové stránky prodejce.

22.3.3 Automatické schválení opravy

Automatické schválení opravy usnadňuje proces instalace aktualizací na počítače. Podívejme se, jak to funguje.

Jak to funguje

Měli byste mít dvě prostředí: testovací a produkční Testovací prostředí se používá k testování instalace opravy a zajištění, že se nic nepoškodí. Po otestování instalace opravy v testovacím prostředí můžete tyto bezpečné opravy automaticky nainstalovat v produkčním prostředí.

Konfigurace automatického schválení opravy

Konfigurace automatického schválení opravy

1. Pro každého prodejce, jehož produkty plánujete aktualizovat, si musíte přečíst a přijmout licenční smlouvy. V opačném případě nebude automatická instalace opravy možná.
2. Nakonfigurujte nastavení automatického schválení.
3. Připravte plán ochrany (například „Testovací opravy“) s povoleným modulem **Správa oprav** a použijte ho na počítače v testovacím prostředí. Zadejte následující podmínku instalace opravy: stav schválení opravy musí být **Nedefinované**. Tento krok je potřeba k ověření oprav a kontrole, zda počítače po instalaci opravy fungují správně.
4. Připravte plán ochrany (například „Produkční opravy“) s povoleným modulem **Správa oprav** a použijte ho na počítače v produkčním prostředí. Zadejte následující podmínku instalace opravy: stav opravy musí být **Schváleno**.
5. Spusťte plán testovacích oprav a zkontrolujte výsledky. Stav schválení těchto počítačů, které nemají žádné problémy, lze zachovat jako **Nedefinované**. Stav počítačů, které nepracují správně, musí být nastaven na **Zamítnuto**.
6. Podle počtu dní nastavených v možnosti **Automatické schválení** se opravy se stavem **Nedefinované** změní na **Schváleno**.
7. Po spuštění plánu Produkční opravy budou na produkčních počítačích nainstalovány pouze opravy se stavem **Schváleno**.

Kroky manuálního postupu jsou uvedeny níže.

Krok 1. Přečtěte si a přijměte licenční smlouvy pro produkty, které chcete aktualizovat.

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Správa softwaru** > **Opravy**.
2. Vyberte opravu a přečtěte si a přijměte licenční smlouvy.

Krok 2. Nakonfigurujte nastavení automatického schválení.

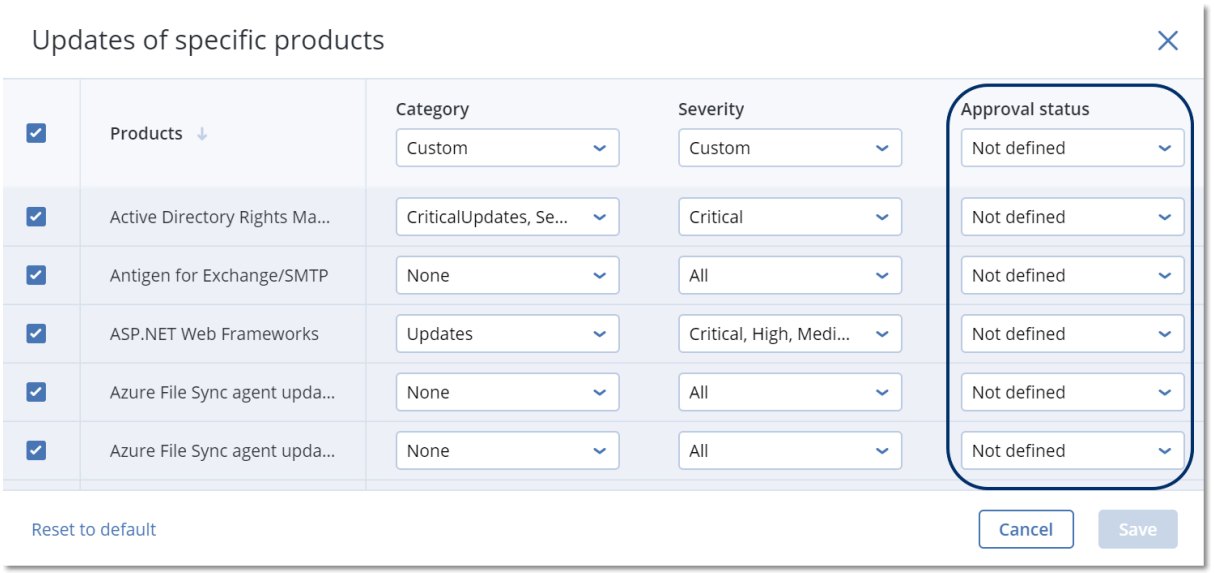
1. Ve webové konzoli Cyber Protect přejděte do nabídky **Správa softwaru** > **Opravy**.
2. Klikněte na **Nastavení**.
3. Povolte možnost **Automatické schválení** a zadejte počet dní. To znamená, že po uplynutí zadaného počtu dní od prvního pokusu o instalaci opravy se stav opravy **Nedefinované** automaticky změní na **Schváleno**.

   Zadali jste například 10 dní. Spustili jste plán testovacích oprav pro testovací počítače a nainstalovali opravy. Opravy, které počítače poškodily, jste označili jako **Zamítnuto**, zatímco u zbytku oprav zůstává stav **Nedefinované**. Po uplynutí 10 dní se opravy se stavem **Nedefinované** automaticky změní na stav **Schváleno**.
4. Povolte možnost **Automaticky přijmout licenční ujednání**. Je to nutné pro automatické přijetí licenčních ujednání během instalace oprav. Od uživatele není vyžadováno žádné potvrzení.

Krok 3. Připravte plán ochrany Testovací opravy.

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Plány** > **Ochrana**.
2. Klikněte na **Vytvořit plán**.
3. Povolte modul **Správa oprav**.
4. Definujte, které aktualizace budou nainstalovány pro produkty společnosti Microsoft a třetích stran, harmonogram a zálohu před aktualizací. Podrobnosti o těchto nastaveních naleznete v tématu „Nastavení správy oprav (p. 379)“.

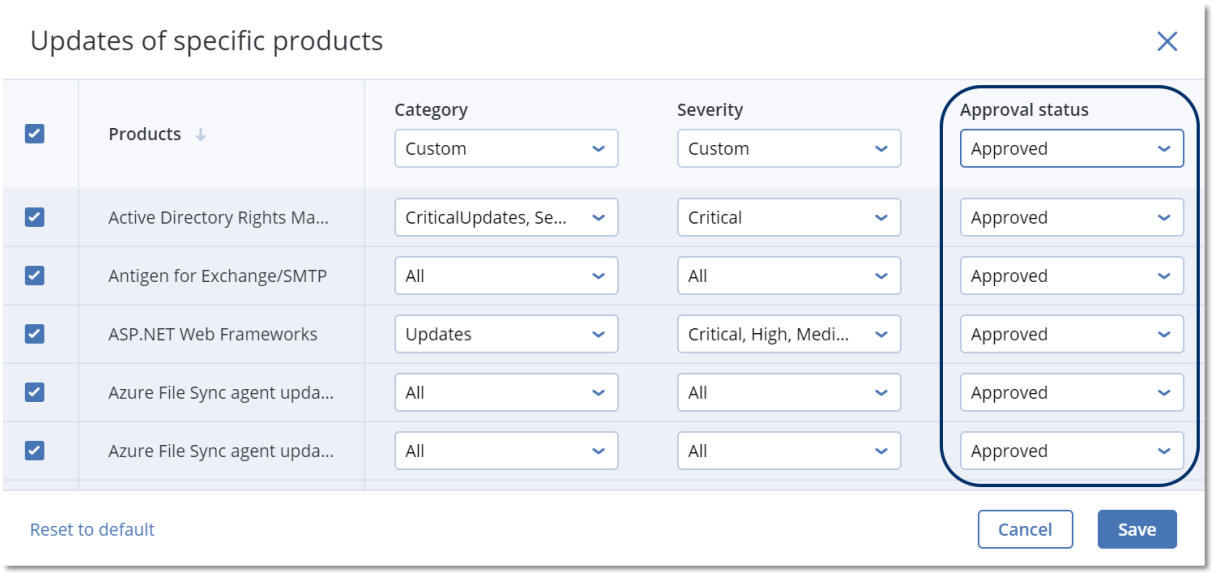
***Důležité**: Pro všechny produkty, které chcete aktualizovat, definujte **Stav schválení** jako **Nedefinované**. Když nastane čas aktualizace, agent nainstaluje pouze opravy se stavem **Nedefinované**, a to na vybraných počítačích v testovacím prostředí.*



Krok 4. Připravte plán ochrany Produkční opravy.

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Plány** > **Ochrana**.
2. Klikněte na **Vytvořit plán**.
3. Povolte modul **Správa oprav**.
4. Definujte, které aktualizace budou nainstalovány pro produkty společnosti Microsoft a třetích stran, harmonogram a zálohu před aktualizací. Podrobnosti o těchto nastaveních naleznete v tématu „Nastavení správy oprav (p. 379)“.

***Důležité**: Pro všechny produkty, které chcete aktualizovat, definujte **Stav schválení** jako **Schváleno**. Když nastane čas aktualizace, agent nainstaluje pouze opravy se stavem **Schváleno**, a to na vybraných počítačích v produkčním prostředí.*



Krok 5. Spusťte plán ochrany testovacích oprav a zkontrolujte výsledky.

1. Spusťte plán ochrany testovacích oprav (podle harmonogramu nebo na vyžádání).
2. Následně zkontrolujte, které z nainstalovaných oprav jsou bezpečné a které nikoli.
3. Přejděte do nabídky **Správa softwaru** > **Opravy** a u oprav, které nejsou bezpečné, nastavte **Stav schválení** na**Zamítnuto**.

22.3.4 Manuální schválení opravy

Proces manuálního schválení opravy je následující:

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Správa softwaru** > **Opravy**.
2. Vyberte opravy, které chcete nainstalovat, a přečtěte si a přijměte licenční ujednání.
3. U oprav, které jste schválili k instalaci, nastavte **Stav schválení** na **Schváleno**.
4. Vytvořte plán ochrany s povoleným modulem správy oprav (p. 379). Můžete buď nakonfigurovat harmonogram, nebo spustit plán na vyžádání kliknutím na tlačítko **Spustit nyní** v nastavení modulu správy oprav.

Na vybraných počítačích se tak nainstalují pouze schválené opravy.

22.3.5 Instalace oprav na vyžádání

Instalaci oprav na vyžádání lze provést třemi způsoby, podle vašich preferencí:

- Přejděte na seznam oprav (**Správa softwaru** > **Opravy**) a nainstalujte potřebné opravy.
- Přejděte na seznam ohrožení zabezpečení (**Správa softwaru** > **Ohrožení zabezpečení**) a zahajte proces řešení, který také zahrnuje instalaci opravy.
- Přejděte na seznam všech zařízení (**Zařízení** > **Všechna zařízení**), vyberte konkrétní počítače, které chcete aktualizovat, a nainstalujte na ně opravy.

Podívejme se na instalaci opravy ze seznamu oprav:

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Správa softwaru** > **Opravy**.
2. Přijměte licenční ujednání pro opravy, které chcete nainstalovat.
3. Vyberte opravy, které chcete nainstalovat, a klikněte na tlačítko **Instalovat**.
4. Vyberte počítače, ve kterých se mají nainstalovat opravy.

   Pokud chcete mít možnost vrácení instalace, když oprava poškodí systém, vyberte možnost **Spustit zálohu před instalací aktualizací softwaru**. Systém ihned zkontroluje, zda existuje plán ochrany s povoleným modulem zálohování (je vyžadována záloha celého počítače). Pokud k počítači plán ochrany přiřazen není, je takový počítač označen červenou ikonou. Výběr těchto počítačů můžete zrušit a pokračovat.
5. Definujte, zda bude po instalaci oprav proveden restart:
   - **Nikdy** – po instalaci oprav nebude nikdy proveden restart.
   - **Je-li vyžadováno** – restart bude proveden, pokud je vyžadován k použití oprav.
   - **Vždy** – restart bude po nainstalování oprav proveden vždy. Vždy můžete zadat prodlení restartu.

   Restartovat až po dokončení zálohy – pokud běží proces zálohování, bude restart zařízení odložen, dokud nebude záloha dokončena.
6. Klikněte na tlačítko **Instalovat opravy**.

Vybrané opravy se nainstalují na vybraných počítačích.

22.3.6 Životnost opravy v seznamu

Chcete-li seznam oprav udržovat aktuální, přejděte do nabídky **Správa softwaru** > **Opravy** > **Nastavení** a zadejte možnost **Životnost v seznamu**.

Možnost **Životnost v seznamu** definuje, jak dlouho bude zjištěná dostupná oprava v seznamu oprav uvedena. Oprava je obecně ze seznamu odebrána, pokud je úspěšně nainstalována na všech počítačích, kde byla zjištěna její absence, nebo pokud uplyne stanovená doba.

- **Navždy** – oprava zůstává na seznamu.
- **7 dní** – oprava je odebrána, pokud od první instalace uběhlo sedm dní.

  Máte například dva počítače, na kterých je potřeba nainstalovat opravy. Jeden z nich je online a druhý je offline. Oprava byla nainstalována na prvním počítači. Po sedmi dnech bude oprava ze seznamu oprav odebrána, přestože nebyla nainstalována na druhém počítači, který byl offline.
- **30 dní** – oprava je odebrána, pokud od první instalace uběhlo 30 dní.

23 Chytrá ochrana

23.1 Kanál hrozeb

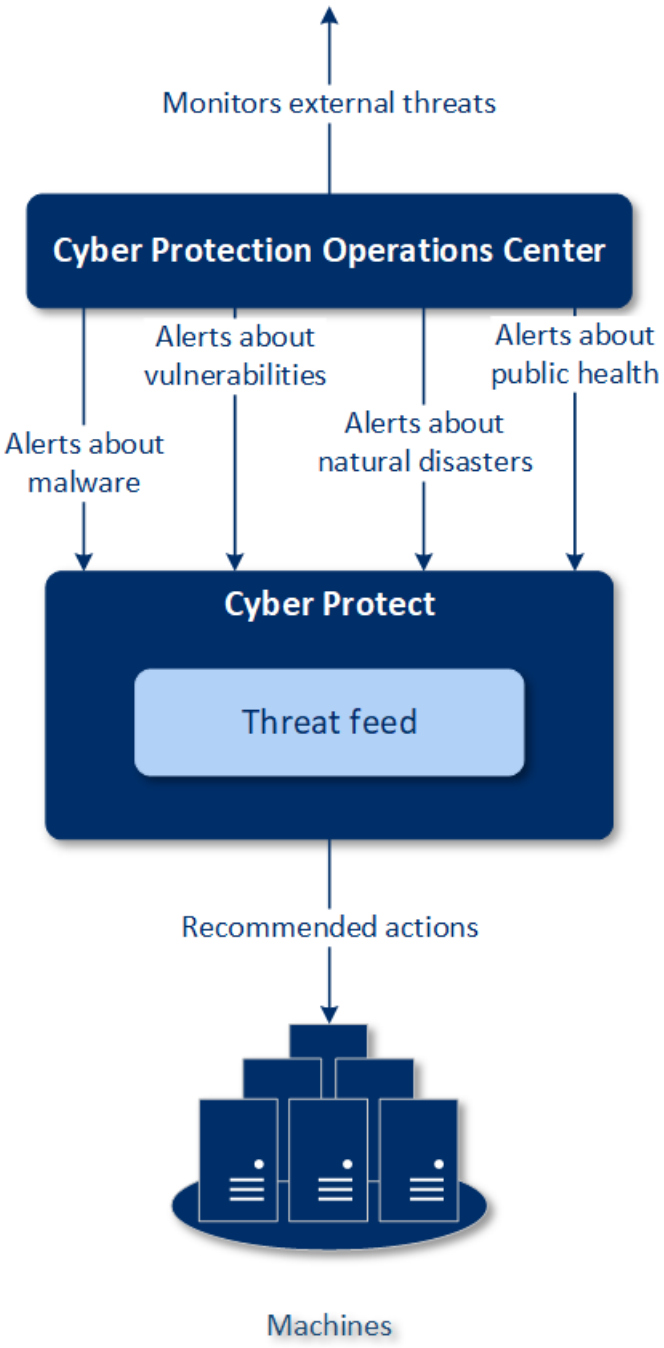
Centrum operací kybernetické ochrany Acronis generuje výstrahy zabezpečení, které jsou zasílány pouze do souvisejících geografických oblastí. Tyto výstrahy zabezpečení poskytují informace o malwaru, ohrožení zabezpečení, přírodních katastrofách, zdravotnictví a dalších typech globálních událostí, které mohou mít vliv na ochranu vašich dat. Kanál hrozeb vás informuje o všech potenciálních hrozbách a umožňuje vám jim předcházet.

Výstrahu zabezpečení lze vyřešit několika konkrétními kroky, které zajišťují odborníci na zabezpečení. Některé výstrahy vás pouze upozorňují na blížící se hrozby, ale k dispozici nejsou žádné doporučené kroky.

Jak to funguje

Centrum operací kybernetické ochrany Acronis monitoruje externí hrozby a generuje výstrahy ohledně malwaru, ohrožení zabezpečení, přírodních katastrof a zdravotnictví. Všechny tyto výstrahy si můžete zobrazit ve webové konzoli Cyber Protect v části **Kanál hrozeb**. V závislosti na typu výstrahy můžete provést příslušné doporučené kroky.

Hlavní postup kanálu hrozeb je popsán ve schématu níže.



Doporučené akce pro obdržené výstrahy z centra operací kybernetické ochrany Acronis zahájíte následovně:

1. Ve webové konzoli Cyber Protect v nabídce **Kontrolní panel** > **Kanál hrozeb** zkontrolujte, zda jsou zde uvedeny nějaké výstrahy zabezpečení.

2. V seznamu vyberte výstrahu a přečtěte si uvedené podrobnosti.

3. Kliknutím na položku **Spustit** spusťte průvodce.

4. Povolte akce, které chcete provést, a vyberte počítače, ve kterých je tyto akce třeba provést. Navrhnout lze následující kroky:

- **Posouzení ohrožení zabezpečení** – kontrola, zda u vybraných počítačů není ohroženo zabezpečení
- **Správa oprav** – instalace oprav na vybraných počítačích
- **Ochrana proti malwaru** – spuštění kompletní kontroly vybraných počítačů
- **Zálohování chráněných nebo nechráněných počítačů** – zálohování chráněných nebo nechráněných počítačů

5. Klikněte na **Spustit**.

6. Na stránce **Aktivity** ověřte, zda byla aktivita úspěšně provedena.

Odstranění všech výstrah

Výstrahy kanálu hrozeb jsou automaticky vymazány po uplynutí následujících lhůt:

- Přírodní katastrofa – 1 týden
- Ohrožení zabezpečení – 1 měsíc
- Malware – 1 měsíc
- Zdravotnictví – 1 týden

23.2 Mapa ochrany dat

Funkce Mapa ochrany dat umožňuje:

- Získat podrobné informace o datech uložených na počítačích (klasifikace, umístění, stav ochrany a další informace);
- Zjistit, zda jsou data chráněna, nebo ne. Data jsou považována za chráněná, pokud jsou chráněna pomocí zálohy (plán ochrany s povoleným modulem zálohování).
- provádět akce v rámci ochrany dat.

Jak to funguje

1. Nejprve vytvořte plán ochrany s povoleným modulem mapy ochrany dat (p. 391).
2. Po provedení plánu a zjištění a analýze vašich dat se zobrazí vizuální znázornění ochrany dat v ovládacím prvku Mapa ochrany dat (p. 410).
3. Můžete také přejít do nabídky **Zařízení** > **Mapa ochrany dat** a vyhledat zde informace o nechráněných souborech v jednotlivých zařízeních.
4. Můžete provést kroky k ochraně nechráněných souborů zjištěných na zařízeních.

Správa zjištěných nechráněných souborů

Důležité soubory, u kterých bylo zjištěno, že nejsou chráněné, můžete ochránit následovně:

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Mapa ochrany dat**.

   V seznamu zařízení naleznete obecné informace o počtu nechráněných souborů, velikosti těchto souborů v jednotlivých zařízeních a o posledním zjištění dat.

   Chcete-li chránit soubory na konkrétním počítači, klikněte na ikonu tří teček (...) a na položku **Chránit všechny soubory**. Budete přesměrováni na seznam plánů, kde můžete vytvořit plán ochrany s povoleným modulem zálohování.

   Chcete-li odstranit konkrétní zařízení s nechráněnými soubory ze seznamu, klikněte na položku **Skrýt do dalšího zjišťování dat**.
2. Chcete-li si zobrazit podrobnější informace o nechráněných souborech na konkrétním zařízení, klikněte na název daného zařízení.

Zobrazí se seznam nechráněných souborů na příponu a umístění. Tento seznam můžete filtrovat podle přípony souboru.

3. Chcete-li chránit všechny nechráněné soubory, klikněte na položku **Chránit všechny soubory**. Budete přesměrováni na seznam plánů, kde můžete vytvořit plán ochrany s povoleným modulem zálohování.

Chcete-li získat informace o nechráněných souborech ve formě zprávy, klikněte na položku **Stáhnout podrobnou zprávu ve formátu CSV**.

23.2.1 Nastavení mapy ochrany dat

Návod k vytvoření plánu ochrany s modulem mapy ochrany dat naleznete v tématu „Vytvoření plánu ochrany“.

Pro modul mapy ochrany dat je možné zadat následující nastavení:

Plán

Můžete definovat různá nastavení a vytvořit harmonogram podle toho, jaká úloha mapy ochrany dat bude provedena.

Naplánujte spuštění úlohy pomocí následujících událostí:

- **Naplánovat podle času** – úloha se spustí podle zadaného času.
- **Když se uživatel přihlásí do systému** – ve výchozím nastavení zahájí spuštění úlohy přihlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.
- **Když se uživatel odhlásí ze systému** – ve výchozím nastavení zahájí spuštění úlohy odhlášení libovolného uživatele. Libovolného uživatele můžete změnit na účet konkrétního uživatele.

  Poznámka *Úloha nebude spuštěna při vypnutí systému. Vypnutí a odhlášení jsou dvě různé akce.*

- **Při spuštění systému** – úloha se spustí při spuštění operačního systému.
- **Při vypnutí systému** – úloha se spustí při vypnutí operačního systému.

Výchozí nastavení: **Naplánovat podle času**.

Typ harmonogramu:

- **Měsíčně** – vyberte měsíce a týdny nebo dny v měsíci, kdy se úloha spustí.
- **Denně** – vyberte dny v týdnu, kdy se úloha spustí.
- **Po hodině**– vyberte dny v týdnu, počet opakování a časový interval, během kterého se úloha spustí.

Výchozí nastavení: **Denně**.

Spustit v – vyberte přesný čas, kdy se úloha spustí.

Výchozí nastavení: **14:00** (v počítači, ve kterém je software nainstalován).

Spustit v časovém rozsahu – nastavte časový rozsah, ve kterém bude nakonfigurovaný harmonogram platný.

Podmínky spuštění – definujte všechny podmínky, které musí být současně splněny před spuštěním úlohy. Podobají se podmínkám spuštění pro modul zálohy popsaným v tématu Podmínky spuštění.

Definovat lze například následující dodatečné podmínky spuštění:

- **Rozložit časy spuštění úlohy do časového rámce**– tato možnost umožňuje definovat časový rámec, během kterého musí být úloha spuštěna, a rozložit úlohy, aby nedošlo k přetížení sítě, protože mnoho počítačů může mít malou šířku pásma pro hostitele, kde se nacházejí služby Windows Server Update Services (WSUS) nebo server pro správu. Můžete zadat prodlevu v hodinách, minutách nebo sekundách. Pokud je například výchozí čas spuštění 10:00 a prodleva je 60 minut, bude úloha spuštěna mezi 10:00 a 11:00.
- **Pokud je počítač vypnutý, vynechané úlohy se spustí při spuštění počítače**
- **Zabránit režimu spánku nebo hibernace při spuštění úlohy** – tato možnost platí pouze v počítačích se systémem Windows.
- **Pokud podmínky spuštění nejsou splněny, spustit úlohu za** – zadejte dobu v hodinách, za kterou bude úloha spuštěna bez ohledu na jiné podmínky spuštění.

Výjimky a pravidla výjimek

Na kartě **Výjimky** můžete definovat seznam přípon souborů, které budou během zjišťování dat považovány za důležité a bude u nich zkontrolováno, zda jsou chráněné. K definici přípon použijte následující formáty:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Na kartě **Pravidla výjimky** můžete definovat, u kterých souborů a složek nemá být během zjišťování dat ověřen stav ochrany.

- **Skryté soubory a složky** – pokud tuto možnost vyberete, budou během kontroly vynechány skryté soubory a složky.
- **Systémové soubory a složky** – pokud tuto možnost vyberete, budou během kontroly vynechány systémové soubory a složky.

24 Přístup ke vzdálené ploše

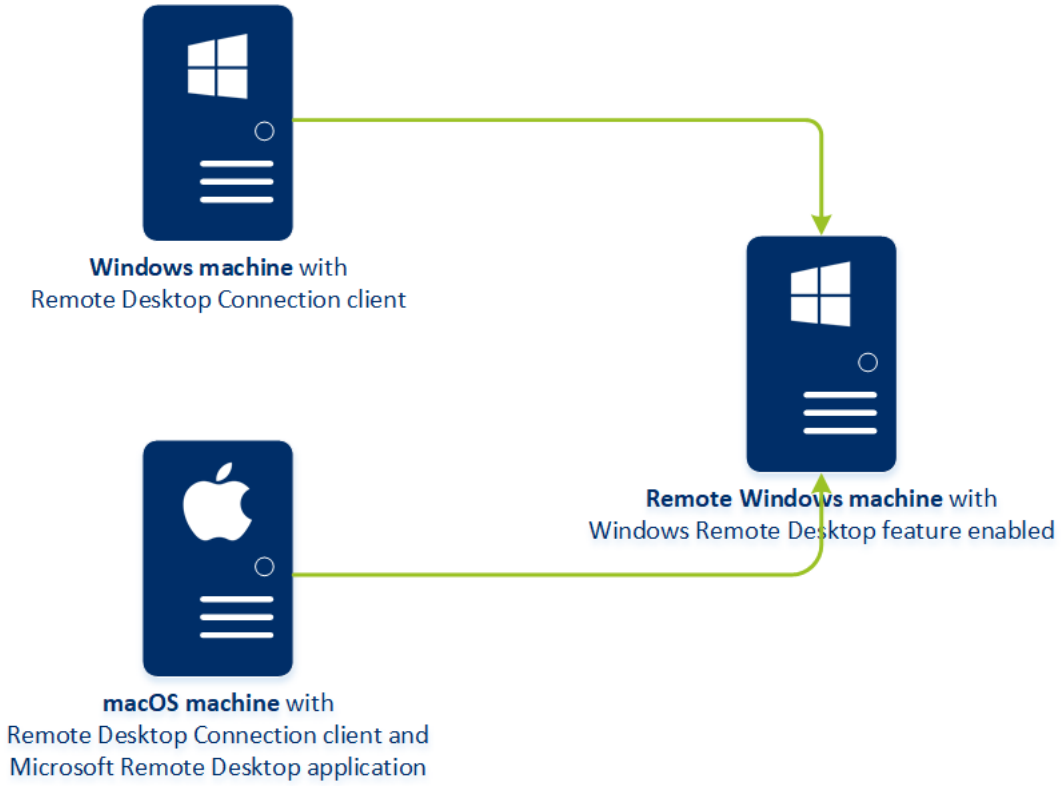
24.1 Vzdálený přístup (klienti RDP a HTML5)

Cyber Protect přináší funkce vzdáleného přístupu. K počítačům svých koncových uživatelů se můžete vzdáleně připojit a spravovat je přímo z webové konzole. Můžete jim tak snadno pomáhat při řešení problémů s počítači.

Předpoklady:

- Agent pro ochranu je nainstalován na vzdáleném počítači a je zaregistrován na serveru pro správu.
- K počítači je přiřazena příslušná licence Cyber Protect.
- Na počítači, ze kterého bude připojení iniciováno, je nainstalován klient Připojení ke vzdálené ploše.
- Počítač, ze kterého bude připojení ke vzdálené ploše inicializováno, musí být schopen připojit se k serveru pro správu podle svého názvu hostitele. Nastavení DNS musí být nakonfigurováno správně nebo musí být název hostitele serveru pro správu vložen do souboru hostitele.

Vzdálené připojení lze navázat z počítače se systémem Windows i macOS.



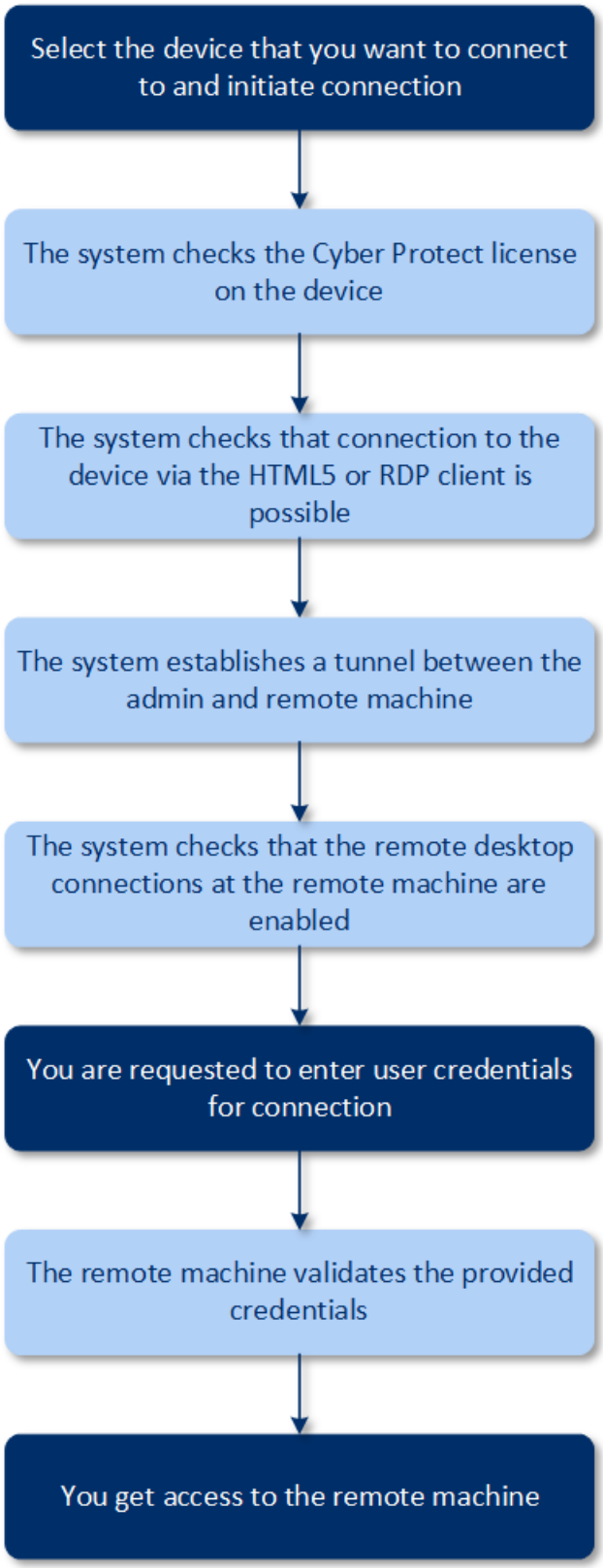
Funkci vzdáleného přístupu lze použít pro připojení k počítačům se systémem Windows s dostupnou funkcí Windows Remote Desktop. Proto není možný vzdálený přístup, například do systémů Windows 10 Home a macOS.

Chcete-li z počítače se systémem macOS navázat připojení ke vzdálenému počítači, zkontrolujte, zda jsou na počítači s macOS nainstalovány následující aplikace:

- Klient Připojení ke vzdálené ploše
- Aplikace Vzdálená plocha Microsoft

Jak to funguje

Když se pokusíte připojit ke vzdálenému počítači, systém nejprve zkontroluje, zda má tento počítač licenci Cyber Protect. Následně zkontroluje, zda je možné připojení prostřednictvím klienta HTML5 nebo RDP. Zahájíte připojení prostřednictvím klienta RDP nebo HTML5. Systém vytvoří tunel do vzdáleného počítače a zkontroluje, zda je na vzdáleném počítači povoleno připojení ke vzdálené ploše. Pak zadáte pověření a po jejich ověření máte přístup ke vzdálenému počítači.



Připojení ke vzdálenému počítači

Postup připojení ke vzdálenému počítači je následující:

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Všechna zařízení**.
2. Klikněte na počítač, ke kterému se chcete vzdáleně připojit, a klikněte na položku **Cyber Protection Desktop** > **Připojit pomocí klienta RDP** nebo **Připojit pomocí klienta HTML5**.

   Poznámka *Připojení prostřednictvím klienta HTML5 je k dispozici, pouze pokud je server pro správu nainstalován na počítači se systémem Linux.*
3. [Volitelné, pouze pro připojení prostřednictvím klienta RDP] Stáhněte a nainstalujte klienta Připojení ke vzdálené ploše. Zahajte připojení ke vzdálenému počítači.
4. Zadejte přihlašovací jméno a heslo pro přístup ke vzdálenému počítači a klikněte na tlačítko **Připojit**.

Budete připojeni ke vzdálenému počítači a můžete ho spravovat.

24.2 Sdílení vzdáleného připojení

Zaměstnanci pracující z domu mohou vyžadovat přístup k pracovním počítačům, ale je možné, že vaše organizace pro vzdálené připojení nenakonfigurovala síť VPN nebo jiné nástroje. Cyber Protect poskytuje funkce pro sdílení odkazu RDP s uživateli, díky kterému získají vzdálený přístup ke svým počítačům.

Povolení funkce sdílení vzdáleného připojení

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Nastavení** > **Ochrana** > **Vzdálené připojení**.
2. Zaškrtněte políčko **Sdílet připojení ke vzdálené ploše**.

Po výběru zařízení ve webové konzoli Cyber Protect se zobrazí nová možnost **Sdílet vzdálené připojení**.

Sdílení vzdáleného připojení s uživateli

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Všechna zařízení**.
2. Vyberte zařízení, ke kterému chcete zajistit vzdálené připojení.
3. Klikněte na možnost **Sdílet vzdálené připojení**.
4. Klikněte na možnost **Získat odkaz**. V otevřeném okně zkopírujte vygenerovaný odkaz. Tento odkaz můžete sdílet s uživatelem, který potřebuje vzdálený přístup k počítači. Platnost odkazu je deset hodin.

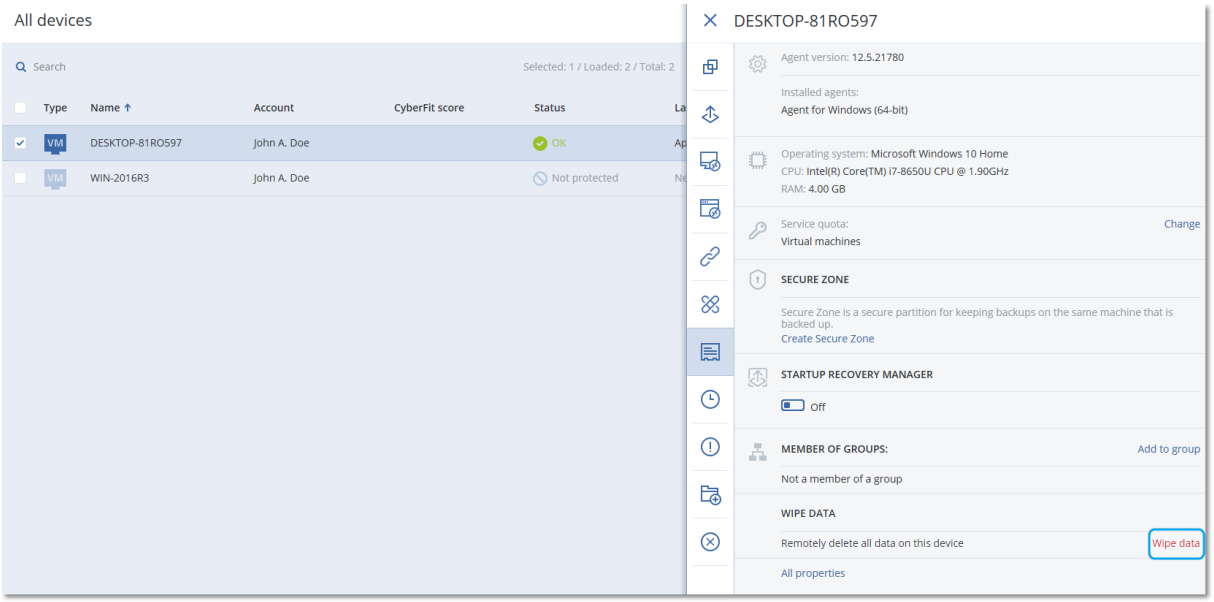
Po získání odkazu ho můžete sdílet e-mailem nebo jiným způsobem. Uživatel, se kterým byl odkaz sdílen, na něj musí kliknout a vybrat typ připojení:

- Připojit pomocí klienta RDP.
  Toto připojení vyzve ke stažení a instalaci klienta Připojení ke vzdálené ploše.
- Připojit pomocí klienta HTML5.
  Toto připojení nevyžaduje instalaci žádného klienta RDP na počítači uživatele. Uživatel bude přesměrován na přihlašovací obrazovku a musí zadat pověření pro přístup k počítači.

25 Vzdálené vymazání

Díky funkci vzdáleného vymazání může správce služby Cyber Protect a vlastník počítače vymazat data na spravovaném počítači – například v případě jeho ztráty nebo odcizení. Tím lze zabránit neoprávněnému přístupu k citlivým informacím.

Vzdálené vymazání je k dispozici pouze pro počítače se systémem Windows 10. Počítač musí být spuštěný a připojený k internetu, aby mohl obdržet příkaz k vymazání.



Vymazání dat z počítače

1. Ve webové konzoli Cyber Protect přejděte do nabídky **Zařízení** > **Všechna zařízení**.
2. Vyberte počítač, jehož data chcete vymazat.

   Poznámka *Vymazat data lze vždy jen z jednoho počítače.*

3. Klikněte na možnost **Podrobnosti** a na příkaz **Vymazat data**.

   Pokud je vybraný počítač offline, je možnost **Vymazat data** nedostupná.
4. Potvrďte výběr.
5. Zadejte pověření místního správce tohoto počítače a klikněte na příkaz **Vymazat data**.

   Tip *V nabídce* ***Kontrolní panel*** *>* ***Aktivity*** *naleznete podrobnosti o procesu mazání a o tom, kdo ho spustil.*

26 Skupiny zařízení

Skupiny zařízení slouží k pohodlné správě většího množství zaregistrovaných zařízení.

Plán ochrany můžete použít na skupinu. Když se ve skupině objeví nové zařízení, začne být plánem chráněné. Pokud je zařízení ze skupiny odebráno, nebude už plánem chráněno. Plán, který je použitý na skupinu, nelze odvolat pro člena skupiny, ale jen pro celou skupinu.

Do skupiny lze přidat jen zařízení stejného typu. Například pod **Hyper-V** můžete vytvořit skupinu virtuálních počítačů Hyper-V. Pod možností **Počítače s agenty** můžete vytvořit skupinu počítačů s nainstalovanými agenty. Pod možností **Všechna zařízení** skupinu vytvořit nelze.

Jedno zařízení může být členem více než jedné skupiny.

Vestavěné skupiny

Když je zařízení zaregistrováno, zobrazí se v jedné z vestavěných kořenových skupin na kartě **Zařízení**.

Kořenové skupiny *nelze* upravit ani odstranit. Na kořenové skupiny *nelze* použít plány.

Některé kořenové skupiny obsahují vestavěné dílčí kořenové skupiny. Tyto skupiny *nelze* upravit ani odstranit. Na dílčí kořenové vestavěné skupiny ale *můžete* použít plány.

Vlastní skupiny

Ochrana všech zařízení ve vestavěné skupině jediným plánem ochrany nemusí být dostačující kvůli odlišným rolím počítačů. Zálohovaná data jsou specifická pro každé oddělení, některá data je nutné zálohovat často, jiná dvakrát do roka. Proto tedy může být nutné vytvořit různé plány ochrany použitelné v různých počítačích. V takovém případě zvažte vytvoření vlastních skupin.

Vlastní skupina může obsahovat jednu nebo více vnořených skupin. Všechny vlastní skupiny lze upravit nebo odstranit. Existují tyto typy vlastních skupin:

- **Statické skupiny**

  Statické skupiny obsahují počítače, které do nich byly ručně přidány. Obsah statické skupiny se nikdy nemění, pokud explicitně nepřidáte nebo neodstraníte počítač.

  Příklad: Vytvoříte vlastní skupinu pro oddělení účtárny a ručně do ní přidáte počítače účetních. Jakmile na skupinu použijete plán ochrany, začnou být počítače účetních chráněné. Pokud je zaměstnán nový účetní, bude nutné nový počítač přidat do skupiny ručně.

- **Dynamické skupiny**

  Dynamické skupiny obsahují počítače přidané automaticky podle kritérií hledání zadaných při vytváření skupiny. Obsah dynamické skupiny se mění automaticky. Počítač zůstává ve skupině, dokud splňuje zadaná kritéria.

  Příklad 1: Názvy hostitelů počítačů patřících do oddělení účtárny obsahují slovo „účtárna“. Zadáte částečný název počítače jako kritérium členství ve skupině a použijete na ni plán ochrany. Pokud je přijat nový účetní, přidá se nový počítač do skupiny přidán ihned při registraci, a je tak automaticky chráněn.

  Příklad 2: Oddělení účtárny tvoří samostatnou organizační jednotku Active Directory. Zadáte organizační jednotku účtárny jako kritérium členství ve skupině a použijete na danou skupinu plán ochrany. Pokud je přijat nový účetní, přidá se nový počítač do skupiny přidán ihned při registraci a přidání do organizační jednotky (bez ohledu na pořadí akcí), a je tak automaticky chráněn.

26.1 Vytvoření statické skupiny

1. Klikněte na možnost **Zařízení** a vyberte vestavěnou skupinu obsahující zařízení, pro která chcete vytvořit statickou skupinu.
2. Klikněte na ikonu ozubeného kola nacházející se vedle skupiny, ve které chcete vytvořit skupinu.
3. Klikněte na **Nová skupina**.
4. Zadejte název skupiny a klikněte na **OK**.

   Nová skupina se zobrazí ve stromu skupin.

26.2 Přidání zařízení do statických skupin

1. Klikněte na možnost **Zařízení** a potom vyberte jedno nebo více zařízení, která chcete do skupiny přidat.
2. Klikněte na možnost **Přidat do skupiny**.

   Software zobrazí strom skupin, do kterých můžete vybrané zařízení přidat.
3. Pokud chcete vytvořit novou skupinu, postupujte následovně. Jinak tento krok přeskočte.
   a. Vyberte skupinu, ve které chcete vytvořit skupinu.

b. Klikněte na **Nová skupina**.

c. Zadejte název skupiny a potom klikněte na tlačítko **OK**.

4. Zvolte skupinu, ke které chcete zařízení přidat, a potom klikněte na **Hotovo**.

Další způsob, jak přidat zařízení do statické skupiny, je výběr skupiny a kliknutí na možnost **Přidat zařízení**.

26.3 Vytvoření dynamické skupiny

1. Klikněte na možnost **Zařízení** a vyberte skupinu obsahující zařízení, pro která chcete vytvořit dynamickou skupinu.
2. Zařízení vyhledejte pomocí vyhledávacího pole. Použít můžete několik kritérií hledání a operátorů popsaných níže.
3. Klikněte na tlačítko **Uložit jako** vedle vyhledávacího pole.

Poznámka *Některá kritéria nejsou pro vytvoření skupiny podporována. Prohlédněte si tabulku Kritéria hledání níže.*

4. Zadejte název skupiny a klikněte na **OK**.

Kritéria hledání

V následující tabulce jsou shrnuta dostupná kritéria hledání.

Kritérium	Význam	Příklady vyhledávacích dotazů	Podporováno pro vytvoření skupiny
`name`	▪ Název hostitele pro fyzické počítače ▪ Název pro virtuální počítače ▪ Název databáze ▪ E-mailové adresy poštovních schránek	`name = 'en-00'`	Ano
`comment`	Komentář pro zařízení. Výchozí hodnota: ▪ Pro fyzické počítače se systémem Windows je to popis počítače z vlastností počítače v systému Windows. ▪ Pro ostatní zařízení je výchozí hodnota prázdná. Chcete-li komentář zobrazit, v části **Zařízení** vyberte požadované zařízení, klikněte na **Podrobnosti** a vyhledejte část **Komentář**. Pokud chcete komentář přidat nebo změnit, klikněte na **Přidat** nebo **Upravit**.	`comment = 'important machine'` `comment = ''` (všechny počítače bez komentáře)	Ano
`ip`	IP adresa (pouze u fyzických počítačů)	`ip RANGE ('10.250.176.1','10.250.176.50')`	Ano
`memorySize`	Velikost paměti RAM v megabytech (MB)	`memorySize < 1024`	Ano

Kritérium	Význam	Příklady vyhledávacích dotazů	Podporováno pro vytvoření skupiny
insideVm	Virtuální počítač s agentem. Možné hodnoty: ▪ **true** ▪ **false**	**insideVm = true**	Ano
osName	Název operačního systému.	**osName LIKE '%Windows XP%'**	Ano
osType	Typ operačního systému. Možné hodnoty: ▪ **'windows'** ▪ **'linux'** ▪ **'macosx'**	**osType IN ('linux', 'macosx')**	Ano
osProductType	Typ produktu operačního systému. Možné hodnoty: ▪ **'dc'** Znamená řadič domény. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**	Ano
tenant	Název jednotky, ke které zařízení náleží.	**tenant = 'Unit 1'**	Ano
tenantId	Identifikátor jednotky, ke které zařízení náleží. ID jednotky najdete vybráním zařízení v části **Zařízení** a kliknutím na možnost **Podrobnosti** > **Všechny vlastnosti**. Požadované ID je zobrazeno v poli **ownerId**.	**tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'**	Ano

Kritérium	Význam	Příklady vyhledávacích dotazů	Podporováno pro vytvoření skupiny
state	Stav zařízení. Možné hodnoty: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replicate'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**	Ne
protectedByPlan	Zařízení chráněná plánem ochrany s přiděleným ID. Abyste získali ID plánu, klikněte na **Plány** > **Zálohování**, vyberte plán, klikněte na diagram ve sloupci **Stav** a pak klikněte na stav. Vytvoří se nové hledání s ID plánu.	**protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne
okByPlan	Zařízení chráněná plánem ochrany s přiděleným ID a stavem **OK**.	**okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne
errorByPlan	Zařízení chráněná plánem ochrany s přiděleným ID a stavem **Chyba**.	**errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne
warningByPlan	Zařízení chráněná plánem ochrany s přiděleným ID a stavem **Upozornění**.	**warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne
runningByPlan	Zařízení chráněná plánem ochrany s přiděleným ID a stavem **Probíhající**.	**runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne
interactionByPlan	Zařízení chráněná plánem ochrany s přiděleným ID a stavem **Je nutný zásah uživatele**.	**interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ne

Kritérium	Význam	Příklady vyhledávacích dotazů	Podporováno pro vytvoření skupiny
ou	Počítače patřící do zadané organizační jednotky v Active Directory	**ou IN ('RnD', 'Computers')**	Ano
id	ID zařízení. ID zařízení najdete vybráním zařízení v části **Zařízení** a kliknutím na možnost **Podrobnosti** > **Všechny vlastnosti**. Požadované ID je zobrazeno v poli **id**.	**id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ano
lastBackupTime	Datum a čas posledního úspěšného zálohování. Formát je 'RRRR-MM-DD HH:MM'.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**	Ne
lastBackupTryTime	Čas posledního pokusu o zálohování. Formát je 'RRRR-MM-DD HH:MM'.	**lastBackupTryTime >= '2016-03-11'**	Ne
nextBackupTime	Čas příštího pokusu o zálohování. Formát je 'RRRR-MM-DD HH:MM'.	**nextBackupTime >= '2016-03-11'**	Ne
agentVersion	Verze nainstalovaného agenta pro ochranu.	**agentVersion LIKE '12.0.*'**	Ano
hostId	Interní ID agenta pro ochranu. ID agenta pro ochranu najdete vybráním počítače v části **Zařízení** a kliknutím na možnost **Podrobnosti** > **Všechny vlastnosti**. Použijte hodnotu **"id"** vlastnosti **agent**.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**	Ano
resourceType	Typ zdroje. Možné hodnoty: ▪ **'machine'** ▪ **'virtual_machine.vmwesx'** ▪ **'virtual_machine.mshyperv'** ▪ **'virtual_machine.rhev'** ▪ **'virtual_machine.kvm'** ▪ **'virtual_machine.xen'**	**resourceType = 'machine'** **resourceType in ('mssql_aag_database', 'mssql_database')**	Ano

Poznámka *Pokud přeskočíte hodnotu pro hodiny a minuty, použije se jako počáteční čas RRRR-MM-DD 00:00 a jako koncový čas RRRR-MM-DD 23:59:59. Například lastBackupTime = 2020-02-20 znamená, že výsledky vyhledávání budou zahrnovat všechny zálohy z intervalu lastBackupTime >= 2020-02-20 00:00 a lastBackup time <= 2020-02-20 23:59:59*

Operátory

V následující tabulce jsou shrnuty dostupné operátory.

Operátor	Význam	Příklady
AND	Operátor logické konjunkce.	**name like 'en-00' AND tenant = 'Unit 1'**

Operátor	Význam	Příklady
OR	Operátor logické disjunkce.	`state = 'backup' OR state = 'interactionRequired'`
NOT	Operátor logické negace.	`NOT(osProductType = 'workstation')`

`LIKE 'vzorec zástupných znaků'`	Tento operátor se používá pro testování, zda se výraz shoduje se vzorcem zástupných znaků.
	U tohoto operátoru se nerozlišuje velikost písmen.
	Lze použít následující operátory zástupných znaků:
	▪ * nebo % Hvězdička a znak procent představují žádný, jeden nebo několik znaků
	▪ _ Podtržítko představuje jediný znak
		`name LIKE 'en-00'`
		`name LIKE '*en-00'`
		`name LIKE '*en-00*'`
		`name LIKE 'en-00_'`

IN (<hodnota1>,... <hodnotaN>)	Tento operátor se používá pro testování, zda se výraz shoduje s kteroukoli hodnotou uvedenou v seznamu hodnot. U tohoto operátoru se rozlišuje velikost písmen.	`osType IN ('windows', 'linux')`
RANGE(<počáteční_hodnota>, <koncová_hodnota>)	Tento operátor se používá pro testování, zda se výraz nachází v určitém rozsahu hodnot (včetně krajních hodnot).	`ip RANGE('10.250.176.1','10.250.176.50')`

26.4 Použití plánu ochrany na skupinu

1. Klikněte na možnost **Zařízení** a vyberte vestavěnou skupinu obsahující skupinu, na kterou chcete plán ochrany použít.

   Software zobrazí seznam podřízených skupin.
2. Vyberte skupinu, na kterou chcete plán ochrany použít.
3. Klikněte na možnost **Skupina zálohování**.

   Software zobrazí seznam plánů ochrany, které lze použít na danou skupinu.
4. Proveďte jeden z následujících úkonů:
   - Rozbalte existující plán ochrany a klikněte na tlačítko **Použít**.
   - Klikněte na možnost **Vytvořit nový** a potom vytvořte nový plán ochrany podle popisu v tématu Zálohování (str. 122).

27 Monitorování a zprávy

Na kontrolním panelu **Přehled** můžete monitorovat aktuální stav chráněné infrastruktury.

V sekci **Zprávy** můžete generovat zprávy na vyžádání a naplánované zprávy o chráněné infrastruktuře. Tato sekce je dostupná pouze s licencí Advanced.

27.1 Kontrolní panel Přehled

Kontrolní panel **Přehled** nabízí celou řadu přizpůsobitelných ovládacích prvků, které poskytují přehled o vaší chráněné infrastruktuře. Můžete vybírat z více než 20 ovládacích prvků v podobě výsečových grafů, tabulek, diagramů, pruhových grafů a seznamů. Ovládací prvky obsahují prokliknutelné prvky,

které vám umožní prozkoumat a řešit různé problémy. Uvedené informace se aktualizují každých pět minut.

Pokud máte licenci Advanced, můžete si také stáhnout stav kontrolního panelu nebo ho poslat e-mailem ve formátu .pdf nebo .xlsx. Pokud budete chtít kontrolní panel poslat e-mailem, ujistěte se, že jsou nakonfigurována nastavení **e-mailového serveru** (str. 441).

Dostupné ovládací prvky závisí na verzi Cyber Protect. Výchozí ovládací prvky jsou uvedeny níže:

Ovládací prvek	Dostupnost	Popis
Kybernetická ochrana (p. 406)	Není k dispozici ve verzích Cyber Backup	Zobrazuje souhrnné informace o velikosti záloh, zablokovaném malwaru, zablo URL, zjištěných ohrožení zabezpečení a nainstalovaných opravách.
Stav ochrany (p. 406)	K dispozici ve všech verzích	Zobrazuje aktuální stav ochrany všech počítačů.
Aktivity	K dispozici ve všech verzích	Zobrazuje souhrn aktivit, které byly provedeny během zadaného časového obd
Shrnutí aktivních výstrah	K dispozici ve všech verzích	Zobrazuje shrnutí aktivních výstrah podle typu výstrahy a závažnosti.
Stav instalace opravy (p. 411)	Není k dispozici ve verzích Cyber Backup	Zobrazuje počet počítačů seskupených podle stavu instalace opravy.
Chybějící aktualizace podle kategorie (p. 411)	Není k dispozici ve verzích Cyber Backup	Zobrazuje počet chybějících aktualizací podle kategorie.
Stav disku (p. 407)	Není k dispozici ve verzích Cyber Backup	Zobrazuje počet disků podle jejich stavu.
Zařízení	K dispozici ve všech verzích	Zobrazuje podrobné informace o zařízeních ve vašem prostředí.
Podrobnosti aktivních výstrah	K dispozici ve všech verzích	Zobrazuje podrobné informace o aktivních výstrahách.
Stávající zranitelnosti (p. 411)	K dispozici ve všech verzích	Zobrazuje existující ohrožení zabezpečení pro operační systémy a aplikace ve v dotčené počítače.
Historie instalace oprav (p. 411)	Není k dispozici ve verzích Cyber Backup	Zobrazuje podrobné informace o nainstalovaných opravách.
Nedávno napadeno (p. 412)	K dispozici ve všech verzích	Zobrazuje podrobné informace o nedávno napadených počítačích.
Shrnutí umístění	K dispozici ve všech verzích	Zobrazuje podrobné informace o umístěních záloh.

Jak přidat ovládací prvek

Klikněte na **Přidat ovládací prvek** a proveďte jeden z následujících úkonů:

- Klikněte na ovládací prvek, který chcete přidat. Ovládací prvek se přidá s výchozím nastavením.
- Chcete-li ovládací prvek před přidáním upravit, vyberte jej a klikněte na ikonu tužky. Po úpravě ovládacího prvku klikněte na tlačítko **Hotovo**.

Jak uspořádat ovládací prvky na kontrolním panelu

Ovládací prvky přesunete kliknutím na jejich název.

Jak upravit ovládací prvek

Klikněte na ikonu tužky vedle názvu ovládacího prvku. Úpravy umožňují ovládací prvek přejmenovat, změnit jeho časový rozsah, nastavit u něj filtry a seskupit řádky.

Jak odstranit ovládací prvek

Klikněte na znak X vedle názvu ovládacího prvku.

27.1.1 Kybernetická ochrana

Tento ovládací prvek zobrazuje souhrnné informace o velikosti záloh, zablokovaném malwaru, zablokovaných adresách URL, zjištěných ohroženích zabezpečení a nainstalovaných opravách.

Na horním řádku je uvedena aktuální statistika:

- **Zálohováno dnes** – celková velikost bodů obnovení za posledních 24 hodin
- **Zablokovaný malware** – počet aktuálních aktivních výstrah týkajících se zablokovaného malwaru
- **Zablokované adresy URL** – počet aktuálních aktivních výstrah týkajících se zablokovaných adres URL
- **Existující ohrožení zabezpečení** – počet aktuálních ohrožení zabezpečení
- **Opravy připravené k instalaci** – počet oprav aktuálně dostupných k instalaci

Na dolním řádku je uvedena celková statistika:

- Komprimovaná velikost všech záloh
- Celkový počet zablokovaných položek malwaru na všech počítačích
- Celkový počet zablokovaných adres URL na všech počítačích
- Celkový počet zjištěných ohrožení zabezpečení na všech počítačích
- Celkový počet nainstalovaných aktualizací/oprav na všech počítačích

27.1.2 Stav ochrany

Stav ochrany

Tento ovládací prvek ukazuje aktuální stav ochrany všech počítačů.

Počítač se může nacházet v jednom z následujících stavů:

- **Chráněno** – počítače s použitým plánem ochrany.
- **Nechráněno** – počítače bez použitého plánu ochrany. Zahrnují zjištěné i spravované počítače bez použitého plánu ochrany.
- **Spravováno** – počítače s nainstalovaným agentem pro ochranu.
- **Zjištěno** – počítače bez nainstalovaného agenta pro ochranu.

Pokud kliknete na stav počítače, budete přesměrováni na seznam počítačů s tímto stavem, kde si můžete přečíst další podrobnosti.

Zjištěné počítače

Tento ovládací prvek zobrazuje seznam zjištěných počítačů během zadaného období.

27.1.3 Předpověď stavu disku

Funkce řízení stavu disku umožňuje monitorovat aktuální stav disku a získat předpověď stavu. Díky těmto informacím můžete předejít problémům se ztrátou dat v souvislosti s pádem disku. Podporovány jsou disky HDD a SSD.

Omezení:
1. Předpověď stavu disku je podporována pouze u počítačů se systémem Windows.
2. Monitorovat lze pouze disky fyzických počítačů. Disky virtuálních počítačů nelze monitorovat ani zobrazit v ovládacím prvku.

Stav disku může mít jednu z následujících hodnot:

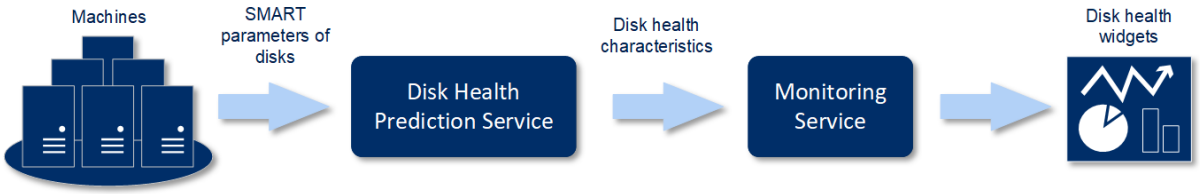
- **OK** – stav disku je 70–100 %
- **Upozornění** – stav disku je 30–70 %
- **Kritický** – stav disku je 0–30 %
- **Probíhá výpočet dat na disku** – probíhá výpočet aktuálního stavu disku a předpovědi

Jak to funguje

Služba předpovědi stavu disku využívá model předpovědí založený na umělé inteligenci.

1. Agent shromáždí parametry disků SMART a tyto údaje předá službě předpovědi stavu disku:
   - SMART 5 – počet přerozdělených sektorů
   - SMART 9 – hodiny zapnutí
   - SMART 187 – nahlášené neopravitelné chyby
   - SMART 188 – vypršel časový limit příkazu
   - SMART 197 – aktuální počet čekajících sektorů
   - SMART 198 – offline počet neopravitelných sektorů
   - SMART 200 – počet chyb zápisu
2. Služba předpovědi stavu disku zpracuje obdržené parametry SMART, vytvoří předpovědi a poskytne následující charakteristiky stavu disku:
   - Aktuální stav disku: Ok, Upozornění, Kritický
   - Prognóza stavu disku: negativní, stabilní, pozitivní
   - Pravděpodobnost předpovědi stavu disku v procentech

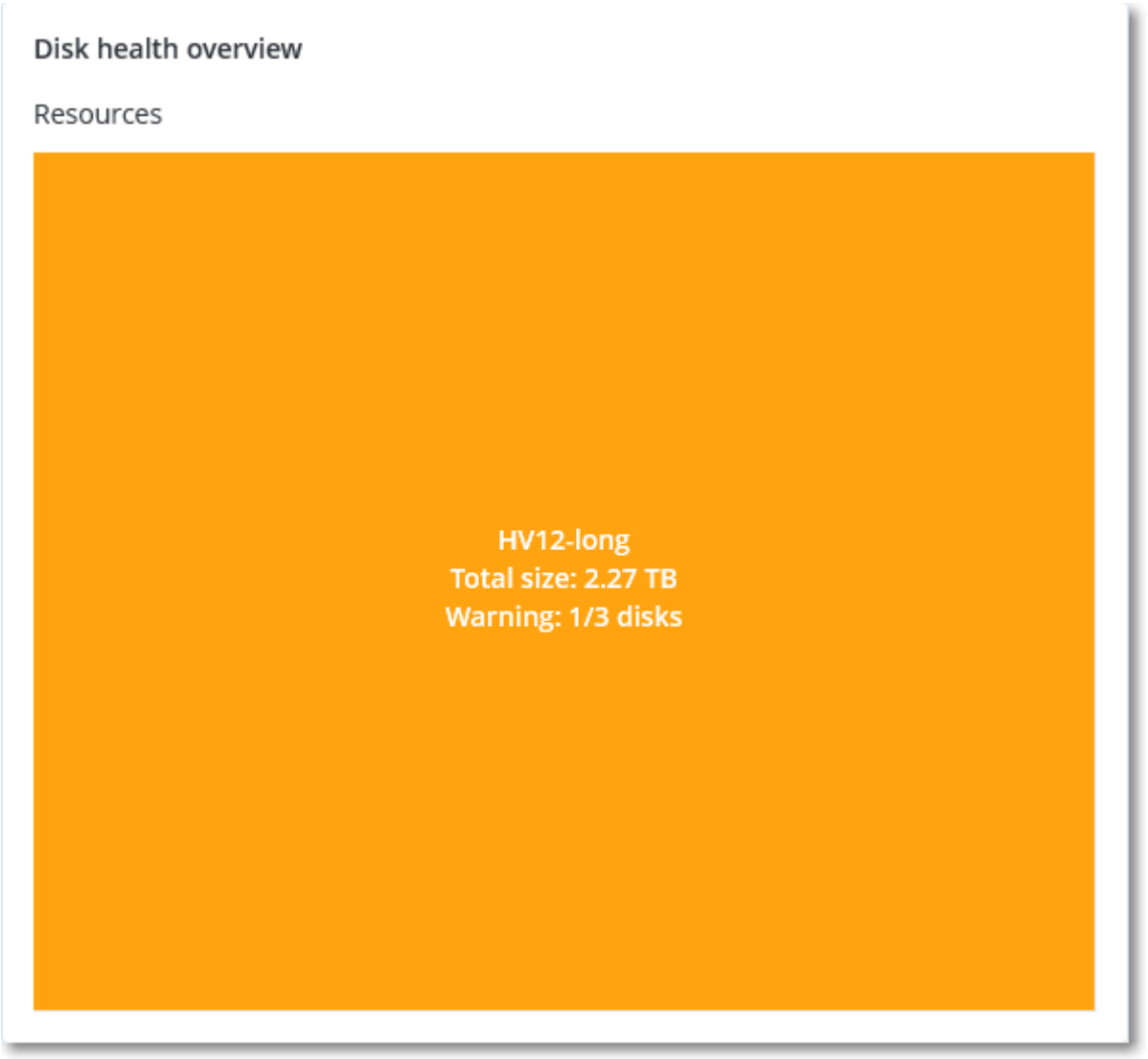
   Období předpovědi je vždy jeden měsíc.
3. Sledovací služba načte charakteristiky stavu disku a zobrazí je v ovládacích prvcích, které jsou k dispozici ve webové konzoli Cyber Protect.



Ovládací prvky stavu disku

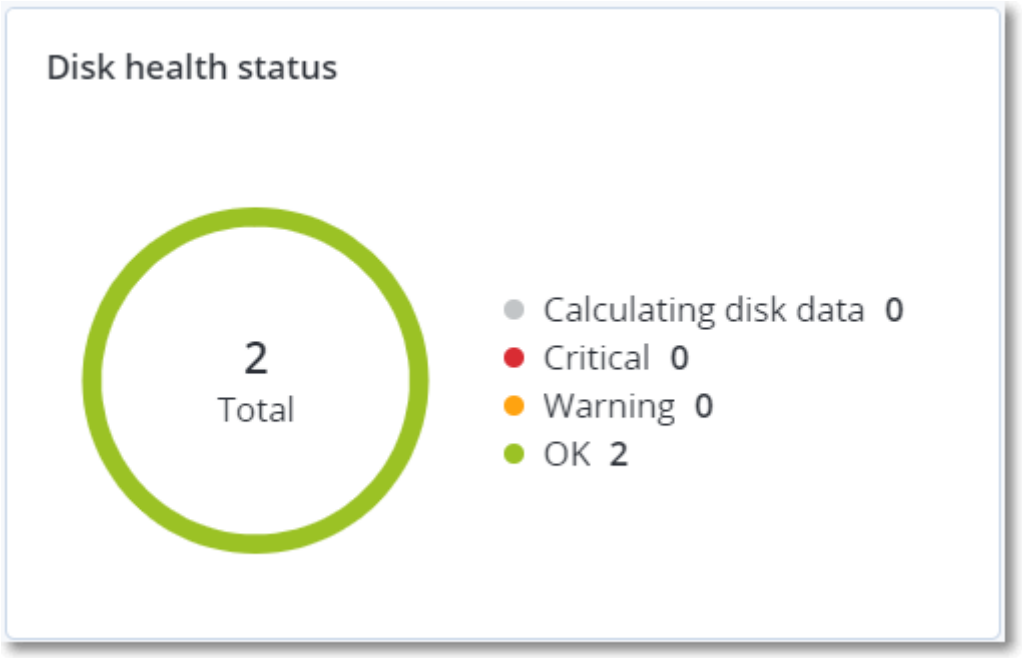
Výsledky sledování stavu disku naleznete na kontrolním panelu v ovládacích prvcích souvisejících se stavem disku:

- **Přehled stavu disku** – ovládací prvek stromové mapy se dvěma úrovněmi detailů, které lze přepínat procházením:
  - Úroveň počítače – zobrazuje souhrnné informace o stavu disku všech počítačů ve vybrané organizační jednotce. Ovládací prvek obsahuje údaje o nejkritičtějším stavu disku. Ostatní stavy se zobrazí v popisku po umístění kurzoru na konkrétní blok. Velikost bloku počítače závisí na celkové velikosti všech disků daného počítače. Barva bloku počítače závisí na zjištěném nejkritičtějším stavu disku.



- Úroveň disku – zobrazuje aktuální stav disku všech disků pro vybraný počítač. Každý blok disku zobrazuje předpověď změny stavu disku:
  - Zhorší se (pravděpodobnost předpovědi stavu disku v procentech)
  - Zůstane stabilní (pravděpodobnost předpovědi stavu disku v procentech)
  - Zlepší se (pravděpodobnost předpovědi stavu disku v procentech)

- **Stav disku** – ovládací prvek kruhového diagramu zobrazující počet disků pro každý stav.



Výstrahy stavu disku

Kontrola stavu disku probíhá každých 30 minut a odpovídající výstraha se generuje jednou denně. Když se stav disku změní z **Upozornění** na **Kritický**, zobrazí se také výstraha, i když se během dne již nějaká výstraha zobrazila.

Název výstrahy	Závažnost	Stav disku	Popis
Může dojít k selhání disku.	Upozornění	(30–70 %)	Disk [název_disku] na počítači [název_počítače] v budoucnu pravděpodobně selže. Co nejdříve spusťte plnou zálohu bitové kopie, nahraďte ji a pak ji obnovte na nový disk.
Brzy dojde k selhání disku.	Kritická	(0–30 %)	Disk [název_disku] na počítači [název_počítače] je v kritickém stavu a velmi pravděpodobně brzy selže. Záloha bitové kopie tohoto disku není momentálně doporučena, protože zátěž navíc může způsobit selhání disku. Zálohujte ihned všechny nejdůležitější soubory na tomto disku a disk vyměňte.

27.1.4 Mapa ochrany dat

Funkce mapy ochrany dat umožňuje prozkoumat všechna data, která jsou pro vás důležitá, a získat podrobné informace o počtu, velikosti, umístění a stavu ochrany všech důležitých souborů ve škálovatelném zobrazení stromové mapy.

Velikost každého bloku závisí na celkovém počtu/velikosti všech důležitých souborů, které náleží organizační jednotce/počítači.

Soubory mohou mít jeden z následujících stavů ochrany:

- **Kritický** – existuje 51–100 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.

- **Nízký** – existuje 21–50 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.
- **Střední** – existuje 1–20 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.
- **Vysoký** – všechny soubory se zadanými příponami jsou pro vybraný počítač/umístění chráněny (zálohovány).

Výsledky kontroly ochrany dat naleznete na kontrolním panelu v ovládacím prvku Mapa ochrany dat, což je prvek stromové mapy zobrazující podrobnosti na úrovni počítače.

Umístěním kurzoru na barevný blok zobrazíte další informace o počtu nechráněných souborů a jejich umístění. Chcete-li je chránit, klikněte na položku **Chránit všechny soubory**.

27.1.5 Ovládací prvky posouzení ohrožení zabezpečení

Ohrožené počítače

Tento ovládací prvek zobrazuje ohrožené počítače podle závažnosti ohrožení zabezpečení.

Zjištěné ohrožení zabezpečení může mít jednu z následujících úrovní závažnosti podle rámce Common Vulnerability Scoring System (CVSS) v3.0:

- Zabezpečeno: nebyla zjištěna žádná ohrožení zabezpečení
- Kritická: 9,0–10,0 CVSS
- Vysoká: 7,0–8,9 CVSS
- Střední: 4,0–6,9 CVSS
- Nízká: 0,1–3,9 CVSS
- Žádná: 0,0 CVSS

Stávající zranitelnosti

Tento ovládací prvek zobrazuje aktuální ohrožení zabezpečení na počítačích. V ovládacím prvku **Existující ohrožení zabezpečení** uvidíte dva sloupce s časovými razítky:

- **Zjištěno poprvé** – datum a čas, kdy bylo ohrožení zabezpečení na počítači zjištěno poprvé.
- **Zjištěno naposledy** – datum a čas, kdy bylo ohrožení zabezpečení na počítači zjištěno naposledy.

27.1.6 Ovládací prvky instalace oprav

Pro funkci správy oprav jsou k dispozici čtyři ovládací prvky.

Stav instalace opravy

Tento ovládací prvek zobrazuje počet počítačů seskupených podle stavu instalace opravy.

- **Nainstalováno** – všechny dostupné opravy jsou nainstalovány na počítači
- **Nutný restart** – po instalaci opravy je vyžadován restart počítače
- **Nezdařilo se** – instalace opravy se nezdařila

Souhrn instalace opravy

Tento ovládací prvek zobrazuje souhrn oprav podle stavu instalace.

Historie instalace oprav

Tento ovládací prvek zobrazuje podrobné informace o opravách, které byly nainstalovány na počítačích.

Chybějící aktualizace podle kategorie

Tento ovládací prvek zobrazuje počet chybějících oprav podle kategorie. Zobrazeny jsou následující kategorie:

- Aktualizace zabezpečení
- Kritické aktualizace
- Jiné

27.1.7 Podrobnosti kontroly zálohy

Tento ovládací prvek je k dispozici, pouze pokud je služba vyhledávání nainstalována na serveru pro správu. Zobrazuje podrobné informace o hrozbách, které byly zjištěny v zálohách.

27.1.8 Nedávno napadeno

Tento ovládací prvek zobrazuje podrobné informace o nedávno napadených počítačích. Naleznete zde informace o zjištěných hrozbách a o počtu infikovaných souborů.

27.2 Zprávy

Můžete použít předdefinované zprávy nebo vytvořit vlastní. Zpráva může obsahovat jakoukoli sadu ovládacích prvků kontrolního panelu (p. 404).

Zprávy můžete nakonfigurovat jen pro jednotky, které spravujete.

Zprávy lze posílat e-mailem nebo je stahovat podle plánu. Chcete-li posílat zprávy e-mailem, ujistěte se, že jsou nakonfigurována nastavení **e-mailového serveru** (str. 441). Pokud chcete zprávu zpracovat pomocí softwaru třetích stran, naplánujte uložení zprávy ve formátu .xlsx do konkrétní složky.

Dostupné zprávy závisí na verzi Cyber Protect. Výchozí zprávy jsou uvedeny níže:

Název zprávy	Dostupnost	Popis
Výstrahy	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje výstrahy, ke kterým došlo během zadaného časového období.
Podrobnosti kontroly zálohy	Cyber Protect Advanced	Zobrazuje podrobné informace o zjištěných hrozbách v zálohách.
Zálohy	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje podrobnosti o aktuálních zálohách a bodech obnovení.
Aktuální stav	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje aktuální stav vašeho prostředí.
Denní aktivity	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje souhrn aktivit, které byly provedeny během zadaného časového období.

Mapa ochrany dat	Cyber Protect Advanced	Zobrazuje podrobné informace o počtu, velikosti, umístění a stavu ochrany všech důležitých souborů na počítačích.
Zjištěné hrozby	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje podrobnosti dotčených počítačů podle počtu zablokovaných hrozeb a informace o zdravých a ohrožených počítačích.
Zjištěné počítače	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje všechny počítače nalezené v síti organizace.
Předpověď stavu disku	Cyber Protect Advanced	Zobrazuje předpovědi výpadku vašeho pevného disku nebo disku SSD a aktuální stav disku.
Stávající zranitelnosti	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje existující ohrožení zabezpečení pro operační systémy a aplikace ve vašem prostředí a dotčené počítače.
Licence	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje shrnutí dostupných licencí.
Umístění	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje statistiku využití umístění záloh pro zadané časové období.
Souhrn správy oprav	Cyber Protect Advanced	Zobrazuje počet chybějících oprav, nainstalovaných oprav a oprav, které jsou k dispozici. Ve zprávách si můžete zobrazit detaily chybějících a nainstalovaných oprav a detaily všech systémů.
Shrnutí	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje souhrnné informace o chráněných zařízeních pro zadané časové období.
Aktivity pásek	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje seznam pásek, které byly použity během posledních 24 hodin.
Týdenní aktivity	Cyber Backup Advanced Cyber Protect Advanced	Zobrazuje souhrn aktivit, které byly provedeny během zadaného časového období.

Základní operace se zprávami

- Zprávu zobrazíte kliknutím na její název.
- Chcete-li ze zprávy přejít na operace, klikněte na ikonu tří teček (...).

  Stejné operace jsou k dispozici uvnitř zprávy.

Přidání zprávy

1. Klikněte na **Přidat zprávu**.
2. Proveďte jeden z následujících úkonů:
   - Předdefinovanou zprávu přidáte kliknutím na její název.
   - Chcete-li přidat vlastní zprávu, klikněte na možnost **Vlastní**. Na seznam zpráv se přidá nová zpráva s názvem **Vlastní**. Otevřete tuto zprávu a přidejte do ní ovládací prvky.
3. [Volitelné] Ovládací prvky přesunete kliknutím a přetažením.
4. [Volitelné] Zprávu upravíte podle kroků popsaných níže.

Úprava zprávy

1. Klikněte na ikonu tří teček (...) vedle názvu zprávy a na tlačítko **Nastavení**.

2. Upravte zprávu. Můžete:
   - zprávu přejmenovat,
   - změnit časový rozsah pro všechny ovládací prvky obsažené ve zprávě,
   - naplánovat odesílání zprávy e-mailem ve formátu PDF nebo XLSX.
3. Klikněte na tlačítko **Uložit**.

Naplánování zprávy

1. Vyberte zprávu a pak klikněte na možnost **Plán**.
2. Zapněte přepínač **Odeslat naplánovanou zprávu**.
3. Zvolte, zda chcete poslat zprávu e-mailem, uložit ji do složky nebo obojí. Podle zvolené možnosti zadejte e-mailové adresy, cestu ke složce nebo obojí.
4. Vyberte formát zprávy: .pdf, .xlsx nebo oba.
5. Vyberte období vykazování: 1 den, 7 dní nebo 30 dní.
6. Zadejte dny a čas, kdy bude zpráva odeslána nebo uložena.
7. Klikněte na tlačítko **Uložit**.

Export a import struktury zprávy

Strukturu zprávy (sadu ovládacích prvků a nastavení plánu) můžete exportovat a importovat ze souboru .json. To se může hodit v případě reinstalace serveru pro správu nebo při kopírování struktury zprávy na jiný server pro správu.

Strukturu zprávy vyexportujete vybráním zprávy a kliknutím na možnost **Exportovat**.

Strukturu zprávy naimportujete kliknutím na možnost **Vytvořit zprávu** a potom na možnost **Importovat**.

Výpis dat ze zprávy

Výpis dat ze zprávy můžete uložit do souboru .csv. Výpis zahrnuje veškerá data ze zprávy (bez filtrování) pro vlastní časový rozsah.

Software generuje výpis dat průběžně. Pokud zadáte dlouhé časové období, může tato akce trvat poměrně dlouho.

Jak vytvořit výpis dat ze zprávy

1. Vyberte zprávu a pak klikněte na možnost **Otevřít**.
2. Klikněte na ikonu tří teček (...) v pravém horním rohu a na možnost **Vypsat data**.
3. Do pole **Umístění** zadejte cestu ke složce pro soubor .csv.
4. V části **Časový rozsah** zadejte časový rozsah.
5. Klikněte na tlačítko **Uložit**.

27.3 Nakonfigurování závažnosti výstrah

Výstraha je zpráva, která upozorňuje na aktuální nebo potenciální problémy. Výstrahy můžete používat různými způsoby:

- V části **Výstrahy** na kartě **Přehled** můžete rychle identifikovat a řešit problémy monitorováním aktuálních výstrah.
- V části **Zařízení** se z výstrah odvozuje stav zařízení. Ve sloupci **Stav** můžete filtrovat zařízení s problémy.

- Při konfigurování e-mailových upozornění (str. 440) můžete nastavit, které výstrahy budou aktivovat upozornění.

Výstrahy mohou mít jednu z následujících závažností:

- **Kritická**
- **Chyba**
- **Upozornění**

Podle potřeby můžete změnit závažnost výstrahy (nebo můžete také výstrahu zcela zakázat) pomocí konfiguračního souboru výstrah podle níže uvedeného popisu. Tato operace vyžaduje restartování serveru pro správu.

Změna závažnosti výstrahy nemá vliv na již vygenerované výstrahy.

Konfigurační soubor výstrah

Konfigurační soubor je uložený v počítači, na kterém běží server pro správu.

- Ve Windows: `<cesta_instalace>`**\AlertManager\alert_manager.yaml**
  `<Cesta_instalace>` je zde cestou instalace serveru pro správu. Ve výchozím nastavení je to umístění **%ProgramFiles%\Acronis**.
- V Linuxu: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

Soubor má strukturu dokumentu YAML. Každá výstraha je položkou na seznamu **`alertTypes`**.

Klíč **`name`** identifikuje výstrahu.

Závažnost výstrahy definuje klíč **`severity`**. Ten musí mít jednu z následujících hodnot: **`critical`**, **`error`** nebo **`warning`**.

To, jestli je výstraha povolená nebo zakázaná, definuje volitelný klíč **`enabled`**. Ten musí mít buď hodnotu **`true`**, nebo hodnotu **`false`**. Ve výchozím nastavení (bez tohoto klíče) jsou všechny výstrahy povoleny.

Změna závažnosti nebo zakázání výstrahy

1. Na počítači, na kterém je nainstalovaný server pro správu, otevřete soubor **alert_manager.yaml** v textovém editoru.
2. Vyhledejte výstrahu, kterou chcete změnit nebo zakázat.
3. Proveďte jeden z následujících úkonů:
   - Pokud chcete změnit závažnost výstrahy, změňte hodnotu klíče **`severity`**.
   - Jestliže chcete výstrahu zakázat, přidejte klíč **`enabled`** a jako jeho hodnotu nastavte **`false`**.
4. Uložte soubor.
5. Restartujte službu serveru pro správu podle postupu uvedeného níže.

Restartování služby serveru pro správu ve Windows

1. V nabídce **Start** klikněte na příkaz **Spustit** a zadejte **cmd**.
2. Klikněte na tlačítko **OK**.
3. Spusťte následující příkazy:

```
net stop acrmngsrv
net start acrmngsrv
```

Restartování služby serveru pro správu v Linuxu

1. Otevřete **Terminál**.
2. V jakémkoli adresáři spusťte následující příkaz:

```
sudo service acronis_ams restart
```

28 Pokročilé možnosti úložiště

28.1 Pásková zařízení

Následující část podrobně popisuje použití páskových zařízení k ukládání záloh.

28.1.1 Co je páskové zařízení?

Páskové zařízení je obecný pojem, který označuje knihovnu pásek nebo samostatnou páskovou jednotku.

Knihovna pásek (robotická knihovna) je vysokokapacitní úložné zařízení, které se skládá z následujících součástí:

- jedna nebo více páskových jednotek,
- několik (až několik tisíc) slotů, do kterých se ukládají pásky,
- jeden nebo více měničů (robotických mechanismů), které slouží k přesunu pásek mezi sloty a páskovými jednotkami.

Může také obsahovat další součásti, například čtečky a tiskárny čárových kódů.

Automatický zavaděč je speciálním případem knihoven pásek. Obsahuje jednu jednotku, několik slotů, měnič a čtečku čárových kódů (nepovinně).

Samostatná pásková jednotka (také označovaná jako **streamer**) obsahuje jeden slot a může v ní být uložena současně pouze jedna páska.

28.1.2 Přehled podpory páskových zařízení

Agenti pro ochranu mohou zálohovat data na páskové zařízení přímo nebo prostřednictvím uzlu úložišť. V každém případě je zajištěna plně automatická operace páskové jednotky. Pokud je k uzlu úložišť připojeno páskové zařízení s více jednotkami, může na pásky zálohovat současně více agentů.

28.1.2.1 Kompatibilita s RSM a softwarem jiných dodavatelů

Spolupráce se softwarem jiných dodavatelů

Není možné pracovat s páskami v počítači, ve kterém je nainstalován software třetích stran s vlastními nástroji pro správu pásek. Pokud chcete v takovém počítači používat pásky, je nutné odinstalovat nebo vypnout software pro správu pásek jiných dodavatelů.

Interakce se službou RMS (Removable Storage Manager) systému Windows

Agenti pro ochranu a uzly úložišť službu RMS nepoužívají. Při detekování páskového zařízení (str. 425) vyřadí zařízení ze služby RSM (pokud není používáno jiným softwarem). Pokud chcete, aby software pracoval s páskovým zařízením, ujistěte se, že uživatel ani software třetích stran nepovoluje zařízení v RSM. Jestliže bylo páskové zařízení v RSM povoleno, opakujte detekci páskového zařízení.

28.1.2.2 Podporovaný hardware

Aplikace Acronis Cyber Protect podporuje zařízení SCSI. Jedná se o zařízení připojené k Fibre Channel nebo pomocí rozhraní SCSI, iSCSI, Serial Attached SCSI (SAS). Aplikace Acronis Cyber Protect podporuje také pásková zařízení připojená přes USB.

V systému Windows může aplikace Acronis Cyber Protect zálohovat na páskové zařízení i v případě, že nejsou nainstalovány ovladače pro měnič zařízení. Takové páskové zařízení je ve **Správci zařízení** zobrazeno jako **Neznámý měnič médií**. Ovladače pro pásky však musejí být nainstalovány. V systému Linux a při použití spouštěcího média není zálohování na páskové zařízení bez ovladačů možné.

Rozpoznání připojených zařízení IDE nebo SATA není zaručeno. Závisí to na tom, zda byly do operačního systému instalovány příslušné ovladače.

Pokud chcete zjistit, jestli je podporováno vaše konkrétní zařízení, použijte nástroj pro určení kompatibility hardwaru, jak je popsáno v článku http://kb.acronis.com/content/57237. Zprávu s výsledky testů můžete poslat do společnosti Acronis. Podporovaný hardware je uveden na seznamu kompatibilního hardwaru: https://go.acronis.com/acronis-cyber-backup-advanced-tape-hcl.

28.1.2.3 Databáze správy pásek

Informace o všech páskových zařízeních připojených k počítači se ukládají do databáze správy pásek. Výchozí cesta k databázi je následující:

- V systému Windows XP/Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database**.
- V systému Windows Vista a novějších verzích systému Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database**.
- V Linuxu: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**.

Velikost databáze závisí na počtu záloh uložených na páskách, přičemž vychází přibližně 10 MB na 100 záloh.Pokud knihovna pásek obsahuje tisíce záloh, databáze může zabírat hodně místa. V tomto případě můžete databázi pásek uložit do jiného svazku.

Chcete-li databázi přemístit v systému Windows:

1. Zastavte službu Removable Storage Management Service.
2. Přesuňte všechny soubory z výchozího umístění do nového umístění.
3. Vyhledejte klíč registru HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings.
4. Zadejte novou cestu k umístění do hodnoty registru **ArsmDmlDbProtocol**. Tento řetězec může obsahovat až 32 765 znaků.
5. Spusťte službu Removable Storage Management Service.

Chcete-li databázi přemístit v systému Linux:

1. Zastavte službu **`acronis_rsm`**.
2. Přesuňte všechny soubory z výchozího umístění do nového umístění.
3. Otevřete konfigurační soubor **/etc/Acronis/ARSM.config** v textovém editoru.
4. Vyhledejte řádek **`<value name="ArsmDmlDbProtocol" type="TString">`**.
5. Změňte cestu na tomto řádku.
6. Uložte soubor.
7. Spusťte službu **`acronis_rsm`**.

28.1.2.4 Parametry pro zapisování na pásky

Parametry pro zapisování na pásky (velikost bloku a velikost mezipaměti) umožňují vyladit software pro maximální výkon. K zápisu na pásky jsou potřeba oba parametry, ale běžně je potřeba upravit pouze velikost bloku. Optimální hodnota závisí na typu páskové jednotky a na zálohovaných datech, jako například počet a velikost souborů.

Poznámka *Když zařízení čte z pásky, používá stejnou velikost bloku, která byla použitá při zápisu na pásku. Pokud pásková jednotka tuto velikost bloku nepodporuje, čtení selže.*

Tyto parametry se nastavují ve všech počítačích, které mají připojenou páskovou jednotku. Může se jednat o počítač, kde je nainstalovaný agent nebo uzel úložišť. V počítači se systémem Windows se konfigurace provádí v registru, v počítači se systémem Linus se provádí v konfiguračním souboru **/etc/Acronis/BackupAndRecovery.config**.

V systému Windows vytvořte odpovídající klíče registru a jejich hodnoty DWORD. V systému Linus přidejte na konec konfiguračního souboru, přímo před značku **</registry>**, následující text:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "hodnota"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "hodnota"
     </value>
</key>
```

DefaultBlockSize

Toto je velikost bloku (v bajtech) používaná při zápisu na pásky.

Možné hodnoty: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Pokud je hodnota 0 nebo pokud parametr chybí, velikost bloku se určuje následovně:

- V systému Windows je hodnota převzata z ovladače páskové jednotky.
- V systému Linux je hodnota **64 kB**.

Klíč registru (v počítači se systémem Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize

Řádek v souboru /etc/Acronis/BackupAndRecovery.config (v počítači se systémem Linux):

```
     <value name=DefaultBlockSize" type="Dword">
          "hodnota"
     </value>
```

Pokud není zadaná hodnota páskovou jednotkou akceptována, software ji dělí dvěma, dokud není dosažena použitelná hodnota nebo dokud hodnota není rovna 32 bajtům. Pokud není nalezena použitelná hodnota, software zadanou hodnotu násobí dvěma, dokud není dosažena použitelná hodnota nebo dokud hodnota není rovna 1 MB. Pokud jednotka neakceptuje žádnou hodnotu, záloha selže.

WriteCacheSize

Toto je velikost vyrovnávací paměti (v bajtech) používaná při zápisu na pásky.

Možné hodnoty: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, ale ne méně než hodnota parametru **DefaultBlockSize**.

Pokud je hodnota 0 nebo pokud parametr chybí, velikost vyrovnávací paměti je **1 MB**. Pokud operační systém tuto hodnotu nepodporuje, software ji dělí dvěma, dokud není nalezena použitelná hodnota nebo dokud není dosažena hodnota parametru **DefaultBlockSize**. Pokud není nalezena hodnota podporovaná operačním systémem, zálohování selže.

Klíč registru (v počítači se systémem Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Řádek v souboru /etc/Acronis/BackupAndRecovery.config (v počítači se systémem Linux):

```
    <value name="WriteCacheSize" type="Dword">
        "hodnota"
    </value>
```

Pokud zadáte nenulovou hodnotu, která není podporována operačním systémem, zálohování selže.

28.1.2.5 Možnosti zálohy související s páskami

Konfigurací možností zálohy **správy pásky** (str. 191) můžete určit:

- Zda povolit obnovu souborů z diskových záloh uložených na páskách
- Zda pásky po dokončení plánu ochrany vrátit zpět do jejich slotů
- Zda pásky vysunout po dokončení zálohy.
- Zda používat volnou pásku pro každou plnou zálohu.
- Zda se má páska přepsat při tvorbě plné zálohy (pouze pro samostatné páskové jednotky).
- Zda používat sady pásek k odlišení použitých pásek – například pro zálohy vytvořené v různých dnech v týdnu nebo pro zálohy jiných typů počítače.

28.1.2.6 Souběžné operace

Aplikace Acronis Cyber Protect může současně provádět operace s různými součástmi páskového zařízení. Během operace, která používá jednotku (zálohování, obnova, překontrolování (str. 430) nebo mazání (str. 431)), můžete spustit operaci, která používá měnič (přesun (str. 427) pásky do jiného slotu nebo vysouvání (str. 431) pásky) a naopak. Pokud vaše knihovna pásek má více než jednu jednotku, můžete také spustit operaci, která používá jednu z jednotek během operace s jinou jednotkou. Různé počítače mohou například zálohovat nebo obnovovat současně pomocí různých jednotek stejné knihovny pásek.

Operace detekce nových páskových zařízení (str. 425) může být provedena současně s jakoukoliv jinou operací. Během inventarizace (str. 428) není dostupná žádná jiná operace kromě detekce nových páskových zařízení.

Operace, které nelze provádět paralelně, se řadí do fronty.

28.1.2.7 Omezení

Omezení použití páskových zařízení jsou následující:

1. Pásková zařízení nejsou podporována, pokud se počítač spouští ze spouštěcího média založeného na 32bitovém systému Linux.

2. Následující typy dat na pásky zálohovat nelze: Poštovní schránky Microsoft Office 365, poštovní schránky Exchange.
3. Nelze vytvářet zálohy fyzických a virtuálních počítačů s podporou aplikací.
4. V systému macOS je podporována pouze záloha na úrovni souborů do spravovaného páskového umístění.
5. Sloučení záloh umístěných na páskách není možné. Výsledkem je to, že schéma zálohování **Vždy přírůstkový** není při zálohování na pásky dostupné.
6. Deduplikace záloh umístěných na páskách není možná.
7. Software nemůže automaticky přepsat pásku, pokud obsahuje alespoň jednu neodstraněnou zálohu nebo pokud na jiných páskách existují závislé zálohy.
8. Obnova v operačním systému ze zálohy umístěné na páskách není možná, pokud obnova vyžaduje restartování operačního systému. Takovou obnovu proveďte pomocí spouštěcího média.
9. Ověřit (str. 226) můžete libovolnou zálohu uloženou na páskách, ale nelze k ověření vybrat celé páskové umístění nebo páskové zařízení.
10. Spravované páskové umístění nelze chránit šifrováním. Zálohy můžete šifrovat.
11. Software nemůže současně zapisovat jednu zálohu na více pásek nebo více záloh pomocí jedné jednotky na jednu pásku.
12. Nejsou podporována zařízení používající protokol NDMP (Network Data Management Protocol).
13. Nejsou podporovány tiskárny čárových kódů.
14. Pásky formátované pomocí systému LTFS (Linear Tape File System) nejsou podporované.

28.1.2.8 Čtení pásek zapsaných staršími produkty Acronis

Následující tabulka shrnuje čitelnost pásek zapsaných rodinami produktu Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10 a Acronis Backup & Recovery 11 v aplikaci Acronis Cyber Protect. Tato tabulka také ukazuje kompatibilitu pásek zapsaných různými součástmi aplikace Acronis Cyber Protect.

Je možné připojit přírůstkové a rozdílové zálohy ke znovu prohledávaným zálohám vytvořeným aplikacemi Acronis Backup 11.5 a Acronis Backup 11.7.

			...je čitelná na páskovém zařízení připojeném k počítači s...			
			Spouštěcí média aplikace Acronis Cyber Protect	Acronis Cyber Protect Agent pro Windows	Acronis Cyber Protect Agent pro Linux	Uzel úložišť Acronis Cyber Protect
Páska zapsaná na místně připojeném páskovém zařízení (pásková jednotka nebo pásková knihovna) pomocí...	Spouštěcí médium	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		Záloha ABR11/ Acronis 11.5/11.7/12.5	+	+	+	-
	Agent pro Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+

		Záloha ABR11/ Acronis 11.5/11.7/12.5	+	+	+	-
	Agent pro Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		Záloha ABR11/ Acronis 11.5/11.7/12.5	+	+	+	-
Páska zapsaná na páskovém zařízení prostřednictvím...	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Uzel úložišť	ABR10	+	+	+	+
		Záloha ABR11/ Acronis 11.5/11.7/12.5	+	+	+	+

28.1.3 Začínáme s páskovým zařízením

28.1.3.1 Záloha počítače na místně připojené páskové zařízení

Předpoklady

- Páskové zařízení je připojeno k počítači podle instrukcí výrobce.
- V počítači je nainstalován agent pro ochranu.

Před zálohováním

1. Vložte pásky do zařízení.
2. Přihlaste se k webové konzoli Cyber Protect.
3. V **Nastavení** > **Správa pásek** rozbalte uzel počítače a potom klikněte na možnost **Pásková zařízení**.
4. Zkontrolujte, zda se připojené páskové zařízení zobrazuje. Pokud se nezobrazuje, klikněte na **Detekovat zařízení**.
5. Proveďte inventarizaci pásky:
   a. Klikněte na název páskového zařízení.
   b. Kliknutím na příkaz **Inventarizovat** detekujte načtené pásky. **Plnou inventarizaci** ponechte zapnutou. Možnost **Přesunout nerozpoznané nebo importované pásky do fondu Volné pásky** nezapínejte. Klikněte na **Spustit inventarizaci**.

      Výsledek. Načtené pásky byly přesunuty do správných fondů podle zadání v části Inventarizace (str. 428).

      Plná inventarizace celého páskového zařízení může trvat dlouho.

   c. Pokud byly načtené pásky odeslány do fondu **Nerozpoznané pásky** nebo **Importované pásky** a chcete je použít pro zálohování, přesuňte (str. 428) je ručně do fondu **Volné pásky**.

      *Pásky odeslané do fondu **Importované pásky** obsahují zálohy zapsané softwarem Acronis . Před přesunutím takových pásek do fondu **Volné pásky** zkontrolujte, že tyto zálohy nepotřebujete.*

Zálohování

Vytvořte plán ochrany podle popisu v části Zálohování (str. 122). Při určování umístění zálohy vyberte **Fond pásek Acronis**.

Výsledky

- Chcete-li získat přístup k umístění, kde budou vytvářeny zálohy, klikněte na **Úložiště záloh** > **Fond pásek Acronis**.
- Pásky se zálohami budou přesunuty do fondu **Acronis**.

28.1.3.2 Zálohování na páskové zařízení připojené k uzlu úložišť

Předpoklady

- Uzel úložišť je registrován na serveru pro správu.
- Páskové zařízení je připojeno k uzlu úložišť podle pokynů výrobce.

Před zálohováním

1. Vložte pásky do zařízení.
2. Přihlaste se k webové konzoli Cyber Protect.
3. Klikněte na **Nastavení** > **Správa pásek**, rozbalte uzel s názvem uzlu úložišť a potom klikněte na možnost **Páskové zařízení**.
4. Zkontrolujte, zda se připojené páskové zařízení zobrazuje. Pokud se nezobrazuje, klikněte na **Detekovat zařízení**.
5. Proveďte inventarizaci pásky:
   a. Klikněte na název páskového zařízení.
   b. Kliknutím na příkaz **Inventarizovat** detekujte načtené pásky. **Plnou inventarizaci** ponechte zapnutou. Možnost **Přesunout nerozpoznané nebo importované pásky do fondu Volné pásky** nezapínejte. Klikněte na **Spustit inventarizaci**.

      Výsledek. Načtené pásky byly přesunuty do správných fondů podle zadání v části Inventarizace (str. 428).

      Plná inventarizace celého páskového zařízení může trvat dlouho.

   c. Pokud byly načtené pásky odeslány do fondu **Nerozpoznané pásky** nebo **Importované pásky** a chcete je použít pro zálohování, přesuňte (str. 428) je ručně do fondu **Volné pásky**.

      *Pásky odeslané do fondu **Importované pásky** obsahují zálohy zapsané softwarem Acronis . Před přesunutím takových pásek do fondu **Volné pásky** zkontrolujte, že tyto zálohy nepotřebujete.*

   d. Rozhodněte, zda chcete zálohovat do fondu **(str. 425)Acronis** nebo vytvořit nový fond (str. 426).

      Podrobnosti. Více fondů umožňuje použít samostatnou sadu pásek pro každý počítač nebo pro každé oddělení společnosti. Použití více fondů zabraňuje promíchání záloh (vytvořených pomocí různých plánů ochrany) na pásce.
   e. Pokud může vybraný fond získávat pásky v případě potřeby z fondu **Volné pásky**, tento krok vynechejte.

      Jinak pásky z fondu **Volné pásky** přesuňte do vybraného fondu.

      Tip: Chcete-li zjistit, zda fond může získávat pásky z fondu **Volné pásky**, klikněte na něj a vyberte možnost **Informace**.

Zálohování

Vytvořte plán ochrany podle popisu v části Zálohování (str. 122). Při určování umístění zálohy vyberte vytvořený fond pásek.

Výsledky

- Chcete-li získat přístup k umístění, kde budou vytvářeny zálohy, klikněte na **Zálohy** a potom klikněte na název vytvořeného fondu pásek.
- Pásky se zálohami budou přesunuty do vybraného fondu.

Tipy pro další používání knihovny pásek

- Není nutné provádět plnou inventarizaci pokaždé, když načtete novou pásku. Chcete-li ušetřit čas, postupujte podle části Inventarizace (str. 428) v tématu „Kombinace rychlé a plné inventarizace“.
- Ve stejné knihovně pásek je možné vytvořit další fondy a kterýkoli z nich vybrat jako cíl pro zálohy.

28.1.3.3 Obnova pod operačním systémem z páskového zařízení

Jak provést obnovu pod operačním systémem z páskového zařízení

1. Přihlaste se k webové konzoli Backup & Recovery 11.
2. Klikněte na možnost **Zařízení** a vyberte zálohovaný počítač.
3. Klikněte na možnost **Obnova**.
4. Vyberte bod obnovy. Body obnovy se filtrují podle umístění.
5. Software zobrazí seznam pásek potřebných k obnově. Chybějící pásky jsou zašedlé. Pokud má páskové zařízení prázdné sloty, vložte tyto pásky do zařízení.
6. Konfigurujte (str. 198) jiná nastavení obnovy.
7. Kliknutím na možnost **Spustit obnovu** spusťte operaci obnovy.
8. Pokud z nějakého důvodu nejsou vloženy některé z požadovaných pásek, software zobrazí zprávu s identifikátorem potřebné pásky. Postupujte takto:
   a. Vložte pásku.
   b. Proveďte rychlou inventarizaci (str. 428).
   c. Klikněte na možnost **Přehled** > **Aktivity** a pak klikněte na aktivitu obnovy se stavem interakce **Je nutný zásah uživatele**.
   d. Klikněte na **Zobrazit podrobnosti** a pokračujte v obnově kliknutím na tlačítko **Zkusit znovu**.

Co když nevidím zálohy uložené na páskách?

Může to znamenat, že databáze s obsahem pásek byla ztracena nebo poškozena.

Chcete-li databázi obnovit, postupujte takto:

1. Proveďte rychlou inventarizaci (str. 428).

   Během inventarizace nezapínejte *možnost* ***Přesunout nerozpoznané a importované pásky do fondu Volné pásky****. Pokud by byla tato možnost zapnutá, mohli byste přijít o všechny zálohy.*

2. Překontrolujte (str. 430) fond **Nerozpoznané pásky**. Výsledkem bude obsah načtených pásek.
3. Pokud některá ze zjištěných záloh pokračuje na jiných páskách, které ještě nebyly překontrolovány, načtěte tyto pásky a překontrolujte je.

28.1.3.4 Obnova se spustitelným médiem z místně připojeného páskového zařízení

Chcete-li provést obnovu pomocí spouštěcího média z místně připojeného páskového zařízení:

1. Vložte pásky potřebné k obnově do páskového zařízení.
2. Spusťte počítač ze spouštěcího média.

3. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).
4. Pokud je páskové zařízení připojeno pomocí rozhraní iSCSI, nakonfigurujte jej podle popisu v tématu Konfigurace zařízení iSCSI a NDAS (str. 293).
5. Klikněte na **Správa pásek**.
6. Klikněte na **Inventarizovat**.
7. V části **Objekty k inventarizaci** vyberte páskové zařízení.
8. Kliknutím na příkaz **Start** spusťte inventarizaci.
9. Po dokončení inventarizace klikněte na **Zavřít**.
10. Klikněte na možnost **Akce** > **Obnovit**.
11. Klikněte na **Označit data** a poté klikněte na **Procházet**.
12. Rozbalte možnost **Pásková zařízení** a pak vyberte potřebné zařízení.Systém zobrazí výzvu k potvrzení překontrolování. Klikněte na tlačítko **Ano**.
13. Vyberte fond **Nerozpoznané pásky**.
14. Vyberte pásky, které budou překontrolovány. Chcete-li vybrat všechny dostupné pásky ve fondu, zaškrtněte políčko vedle záhlaví sloupce **Název pásky**.
15. Pokud pásky obsahují zálohu chráněnou heslem, zaškrtněte odpovídající políčko a zadejte heslo pro zálohu do pole **Heslo**. Pokud nezadáte heslo nebo heslo není správné, nebude záloha nalezena. Pamatujte na to v případě, že se po překontrolování nezobrazí žádné zálohy.

    Tip. Pokud pásky obsahují několik záloh chráněných různými hesly, je nutné překontrolování opakovat několikrát a pokaždé zadat heslo.
16. Kliknutím na **Start** spusťte kontrolu. Výsledkem bude obsah načtených pásek.
17. Pokud některá ze zjištěných záloh pokračuje na jiných páskách, které ještě nebyly překontrolovány, načtěte tyto pásky a překontrolujte je.
18. Po dokončení překontrolování klikněte na tlačítko **OK**.
19. V **zobrazení archivu** vyberte zálohu, jejíž data mají být obnovena, a poté vyberte data k obnově. Jakmile kliknete na **OK**, stránka **Obnovit data** zobrazí seznam pásek potřebných k obnově. Chybějící pásky jsou zašedlé. Pokud má páskové zařízení prázdné sloty, vložte tyto pásky do zařízení.
20. Konfigurujte jiná nastavení obnovy.
21. Kliknutím na tlačítko **OK** spusťte obnovu.
22. Pokud z nějakého důvodu nejsou vložené některé z požadovaných pásek, software zobrazí zprávu s identifikátorem potřebné pásky. Postupujte takto:
    a. Vložte pásku.
    b. Proveďte rychlou inventarizaci (str. 428).
    c. Klikněte na možnost **Přehled** > **Aktivity** a pak klikněte na aktivitu obnovy se stavem interakce **Je nutný zásah uživatele**.
    d. Klikněte na **Zobrazit podrobnosti** a pokračujte v obnově kliknutím na tlačítko **Zkusit znovu**.

28.1.3.5 Obnova pomocí spouštěcího média z páskového zařízení připojeného k uzlu úložišť

Obnova pomocí spouštěcího média z páskového zařízení připojeného k uzlu úložišť:

1. Vložte pásky potřebné k obnově do páskového zařízení.
2. Spusťte počítač ze spouštěcího média.

3. Klikněte na možnost **Místní správa tohoto počítače** nebo dvakrát klikněte na možnost **Spouštěcí záchranná média** (podle typu média, které používáte).
4. Klikněte na příkaz **Obnovit**.
5. Klikněte na **Označit data** a poté klikněte na **Procházet**.
6. V poli **Cesta** zadejte **bsp://**<adresa uzlu úložiště>**/**<název fondu>**/**, kde <adresa uzlu úložiště> je IP adresa uzlu úložiště, který obsahuje požadovanou zálohu, a <název fondu> je název fondu pásek. Klikněte na **OK** a zadejte pověření pro přístup k fondu.
7. Vyberte zálohu a poté vyberte data, která chcete obnovit. Jakmile kliknete na **OK**, stránka **Obnovit data** zobrazí seznam pásek potřebných k obnově. Chybějící pásky jsou zašedlé. Pokud má páskové zařízení prázdné sloty, vložte tyto pásky do zařízení.
8. Konfigurujte jiná nastavení obnovy.
9. Kliknutím na tlačítko **OK** spusťte obnovu.
10. Pokud z nějakého důvodu nejsou vložené některé z požadovaných pásek, software zobrazí zprávu s identifikátorem potřebné pásky. Postupujte takto:
    a. Vložte pásku.
    b. Proveďte rychlou inventarizaci (str. 428).
    c. Klikněte na možnost **Přehled** > **Aktivity** a pak klikněte na aktivitu obnovy se stavem interakce **Je nutný zásah uživatele**.
    d. Klikněte na **Zobrazit podrobnosti** a pokračujte v obnově kliknutím na tlačítko **Zkusit znovu**.

28.1.4 Správa pásek

28.1.4.1 Detekování páskových zařízení

Při detekování páskových zálohovací zařízení software hledá pásková zařízení připojená k počítači a vkládá informace o nich do databáze správy pásek. Detekovaná pásková zařízení jsou vyřazena z RSM.

Páskové zařízení je obvykle detekováno automaticky, jakmile je připojeno k počítači s nainstalovaným produktem. Je však možné, že budete muset pásková zařízení nechat detekovat ručně, a to v následujících případech:

- Po připojení nebo opětovném připojení páskové jednotky.
- Po instalaci nebo opětovné instalaci zálohovacího softwaru do počítače, ke kterému je pásková jednotka připojena.

Jak detekovat pásková zařízení

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač, ke kterému je páskové zařízení připojeno.
3. Klikněte na možnost **Detekovat zařízení**. Zobrazí se připojená pásková zařízení, jejich jednotky a sloty.

28.1.4.2 Fondy pásek

Zálohovací software používá fondy pásek, které jsou logickými skupinami pásek. Software obsahuje následující předdefinované fondy pásek: **Nerozpoznané pásky**, **Importované pásky**, **Volné pásky** a **Acronis**. Můžete také vytvořit vlastní fondy.

Fond **Acronis** a vlastní fondy se také používají jako umístění záloh.

Předdefinované skupiny

Nerozpoznané pásky

Skupina obsahuje pásky, které byly zapsány aplikacemi třetích stran. Chcete-li zapisovat na takovéto pásky, je nutné je přesunout (str. 428) do skupiny **Volné pásky**. Přesun pásek z této skupiny do jiné není možný s výjimkou skupiny **Volné pásky**.

Importované pásky

Fond obsahuje pásky, které byly zapsány aplikací Acronis Cyber Protect v páskovém zařízení připojeném k jinému uzlu úložiště nebo agentovi. Chcete-li zapisovat na takovéto pásky, je nutné je přesunout do skupiny **Volné pásky**. Přesun pásek z této skupiny do jiné není možný s výjimkou skupiny **Volné pásky**.

Volné pásky

Skupina obsahuje volné (prázdné) pásky. Do tohoto fondu můžete ručně přesunout pásky z jiných fondů.

Pokud přesunete pásku do skupiny **Volné pásky**, software ji označí jako prázdnou. Pokud páska obsahuje zálohy, jsou označeny ikonou  .Když software začne přepisovat pásku, data související se zálohami budou z databáze odebrána.

Acronis

Skupina se ve výchozím nastavení používá pro zálohování, když nechcete vytvářet vlastní skupiny. To platí obvykle pro jednu páskovou jednotku s malým počtem pásek.

Vlastní fondy

Pokud chcete mít samostatné zálohy různých dat, je nutné vytvořit několik fondů. Vlastní fondy můžete chtít vytvořit například v případě, kdy budete chtít oddělit:

- zálohy od různých oddělení společnosti,
- zálohy od různých počítačů,
- zálohy systémových svazků a uživatelská data.

28.1.4.3 Operace se skupinami

Vytvoření fondu

Jak vytvořit fond:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na **Vytvořit fond**.
4. Zadejte název fondu.
5. [Volitelné] Zrušte zaškrtnutí políčka **Automaticky brát pásky z fondu Volné pásky**. Pokud není toto políčko zaškrtnuto, použijí se pro zálohování pouze pásky, které jsou v daném okamžiku obsaženy v novém fondu.
6. Klikněte na tlačítko **Vytvořit**.

Úprava fondu

Je možné změnit parametry fondu **Acronis** nebo vlastního fondu.

Jak upravit fond:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Vyberte požadovaný fond a klikněte na **Upravit fond**.
4. Můžete změnit název fondu nebo nastavení. Další informace o nastavení fondu naleznete v tématu Vytvoření fondu (str. 426).
5. Kliknutím na **Uložit** změny uložíte.

Odstranění fondu

Odstranit můžete pouze vlastní fondy. Předdefinované fondy pásek (**Nerozpoznané pásky**, **Importované pásky**, **Volné pásky** a **Acronis**) není možné odstranit.

Poznámka: *Po odstranění fondu nezapomeňte upravit plány ochrany, které mají fond jako umístění zálohování. V opačném případě dojde k selhání těchto plánů ochrany.*

Chcete-li odstranit fond:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Vyberte požadovaný fond a klikněte na **Odstranit**.
4. Vyberte fond, do kterého budou po odstranění fondu přesunuty pásky.
5. Kliknutím na tlačítko **OK** fond odstraňte.

28.1.4.4 Operace s páskami

Přesunutí do jiného slotu

Tuto operaci použijte v následujících situacích:

- Potřebujete z páskového zařízení odebrat současně více pásek.
- Pokud páskové zařízení nemá emailový slot a pásky, které se mají vysunout, jsou umístěny ve slotech neodpojitelného zásobníku.

Pásky je nutné přesunout do slotů zásobníku s jedním slotem a vysunout zásobník ručně.

Jak přesunout pásku do jiného slotu:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadovanou pásku, a potom ji vyberte.
4. Klikněte na **Přesunout do slotu**.
5. Vyberte nový slot, do kterého bude přesunuta vybraná páska.
6. Kliknutím na **Přesunout** spusťte operaci.

Přesunutí do jiného fondu

Tato operace vám umožňuje přesunout jednu nebo více páskových jednotek z jednoho fondu do druhého.

Pokud přesunete pásku do skupiny **Volné pásky**, software ji označí jako prázdnou. Pokud páska obsahuje zálohy, jsou označeny ikonou  . Když software začne přepisovat pásku, data související se zálohami budou z databáze odebrána.

Poznámky ke konkrétním typům pásky

- Do fondu **Volné pásky** nelze přesouvat pásky chráněné proti zápisu a nepřepisovatelné pásky WORM (Write-Once-Read-Many).
- Vyčištěné pásky se vždy zobrazí ve fondu **Nerozpoznané pásky**; nelze je přesunout do jiného fondu.

Jak přesunout pásky do jiného fondu:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadované pásky, a vyberte je.
4. Klikněte na **Přesunout do fondu**.
5. [Volitelné] Pokud chcete vytvořit pro vybrané pásky další fond, klikněte na možnost **Vytvořit nový fond**. Proveďte akce popsané v části Vytvoření fondu (str. 426).
6. Vyberte fond, do kterého chcete pásky přesunout.
7. Kliknutím na **Přesunout** změny uložíte.

Inventarizace

Operace inventarizace vyhledává pásky načtené v páskovém zařízení a přiřazuje názvy těm, které žádné názvy nemají.

Metody inventarizace

Existují dva způsoby inventarizace.

Rychlá inventarizace

Agent nebo uzel úložišť vyhledá na páskách čárové kódy. Pomocí čárových kódů může aplikace rychle vrátit pásku do fondu, kde byla používána dříve.

Výběrem této metody rozpoznáte pásky použité stejným páskovým zařízením připojeným ke stejnému počítači. Ostatní pásky budou přesunuty do fondu **Nerozpoznané pásky**.

Pokud knihovna pásek neobsahuje čtečku čárových kódů, všechny pásky budou přesunuty do fondu **Nerozpoznané pásky**. Chcete-li své pásky rozpoznat, proveďte plnou inventarizaci nebo zkombinujte rychlou a plnou inventarizaci podle postupu dále v tomto tématu.

Plná inventarizace

Agent nebo uzel úložišť přečte dříve zapsané značky a analyzuje další informace o obsahu načtených pásek. Pomocí této metody lze rozpoznat prázdné pásky a pásky zapsané stejným softwarem na všech páskových zařízeních a v libovolném počítači.

V následující tabulce jsou zobrazeny fondy, do kterých jsou při plné inventarizaci přesunuty pásky.

Páska byla používána...	**Páska je čtena...**	**Páska je přesunuta do fondu...**
Agent	Stejným agentem	Kde byla páska dříve
	Jiným agentem	**Importované pásky**
	Uzel úložišť	**Importované pásky**
Uzel úložišť	Stejným uzlem úložišť	Kde byla páska dříve
	Jiným uzlem úložišť	**Importované pásky**
	Agent	**Importované pásky**
Zálohovací aplikace od jiných výrobců	Agentem nebo uzlem úložišť	**Nerozpoznané pásky**

Pásky určitých typů jsou přesunuty do zvláštních fondů:

Typ pásky	**Páska je přesunuta do fondu...**
Prázdná páska	**Volné pásky**
Prázdná páska chráněná proti zápisu	**Nerozpoznané pásky**
Čisticí páska	**Nerozpoznané pásky**

Rychlou inventarizaci lze použít na celá páskové zařízení. Plnou inventarizaci lze použít na celá páskové zařízení, samostatné jednotky nebo sloty. Pro samostatné páskové jednotky se však provede plná inventarizace i v případě, že je vybrána metoda rychlé inventarizace.

Kombinace rychlé a plné inventarizace

Plná inventarizace celého páskového zařízení může trvat dlouho. Pokud potřebujete provést inventarizaci pouze několika pásek, postupujte následovně:

1. Proveďte rychlou inventarizaci páskového zařízení.
2. Klikněte na fond **Nerozpoznané pásky**. Najděte pásky, u kterých chcete provést inventarizaci, a poznamenejte si sloty, ve kterých se nacházejí.
3. Proveďte plnou inventarizaci těchto slotů.

Co dělat po inventarizaci

Pokud chcete zálohovat na pásky, které byly vloženy do fondu **Nerozpoznané pásky** nebo **Importované pásky**, přesuňte (str. 428) je do fondu **Volné pásky** a potom do fondu **Acronis** nebo do vlastního fondu. Pokud je fond, do kterého chcete zálohovat, obnovitelný, můžete pásky nechat ve fondu **Volné pásky**.

Pokud chcete obnovovat z pásky, která byla umístěna do fondu **Nerozpoznané pásky** nebo **Importované pásky**, je nutné pásku překontrolovat (str. 430). Páska bude přesunuta do fondu vybraného během překontrolování a zálohy uložené na pásce se zobrazí v umístění.

Posloupnost akcí

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač, ke kterému je páskové zařízení připojené, a pak vyberte páskové zařízení, které chcete inventarizovat.
3. Klikněte na **Inventarizovat**.
4. [Volitelné] Pokud chcete zvolit rychlou inventarizaci, vypněte možnost **Plná inventarizace**.

5. [Volitelné] Zapněte možnost **Přesuňte nerozpoznané a importované pásky do fondu Volné pásky**.

   Upozornění: *Tento přepínač aktivujte jen tehdy, pokud jste si zcela jisti, že data uložená na páskách mohou být přepsána.*

6. Kliknutím na **Spustit inventarizaci** spusťte inventarizaci.

Překontrolování

Informace o obsahu pásek jsou uloženy ve vyhrazené databázi. Operace překontrolování čte obsah pásek a aktualizuje databázi, pokud informace v ní neodpovídají datům uloženým na páskách. Zálohy zjištěné během operace jsou umístěny do zvláštního fondu.

V rámci jedné operace lze překontrolovat pásky jednoho fondu. Pro operaci mohou být vybrány pouze připojené pásky.

Překontrolování spusťte v následujících případech:

- Pokud je databáze uzlu úložišť nebo spravovaného počítače ztracena nebo poškozena.
- Pokud jsou informace o pásce v databázi zastaralé (například jestliže byl obsah pásky změněn jiným uzlem úložišť nebo agentem).
- Chcete-li získat přístup k zálohám uloženým na pásky během práce ze spouštěcího média.
- Pokud jste omylem odstranili (str. 432) informace o pásce z databáze. Jestliže překontrolujete odstraněnou pásku, zálohy na ní uložené se znovu objeví v databázi a stanou se dostupné pro obnovu dat.
- Pokud byly zálohy odstraněny z pásky ručně nebo pomocí pravidel zachování, ale chcete je zpřístupnit k obnovení dat. Před překontrolováním takovou pásku vyjměte (str. 431), odstraňte (str. 432) informace o ní z databáze a poté pásku do zařízení znovu vložte.

Jak překontrolovat pásky:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Páskové zařízení** nacházející se pod tímto počítačem.
3. Vyberte páskové zařízení, do kterého jste vložili pásky.
4. Proveďte rychlou inventarizaci (str. 428).

   Poznámka: *Během inventarizace* nezapínejte *přepínač* ***Přesunout nerozpoznané a importované pásky do fondu Volné pásky***.

5. Vyberte fond **Nerozpoznané pásky**. Do tohoto fondu se přesunuje většina pásek jako výsledek rychlé inventarizace. Překontrolování jakéhokoli jiného fondu je také možné.
6. [Volitelné] Chcete-li překontrolovat pouze jednotlivé pásky, vyberte je.
7. Klikněte na **Překontrolovat**.
8. Vyberte fond, kam se umístí nově zjištěné zálohy.
9. V případě nutnosti zaškrtněte políčko **Povolit obnovu souborů z diskových záloh uložených na páskách**.

   Podrobnosti. Je-li toto políčko zaškrtnuto, aplikace vytvoří speciální dodatečné soubory na pevném disku počítače, ke kterému je připojeno páskové zařízení. Dokud budou tyto dodatečné soubory zachovány, je možné provést obnovení souborů z diskových záloh. Zkontrolujte, zda je políčko zaškrtnuto, pokud pásky obsahují zálohy s podporou aplikací. Jinak nebudete schopní z těchto záloh obnovit data aplikace.

10. Pokud pásky obsahují zálohy chráněné heslem, zaškrtněte odpovídající políčko a zadejte heslo pro dané zálohy. Pokud nezadáte heslo nebo heslo není správné, nebude záloha nalezena. Pamatujte na to v případě, že se po překontrolování nezobrazí žádné zálohy.

    Tip. Pokud pásky obsahují zálohy chráněné různými hesly, je nutné kontrolu opakovat několikrát a pokaždé zadat heslo.
11. Kliknutím na příkaz **Spustit překontrolování** spusťte kontrolu.

Výsledek. Vybrané pásky jsou přesunuty do vybraného fondu. Zálohy uložené na páskách naleznete v tomto fondu. Dokud nebudou překontrolovány všechny pásky, záloha rozložená na několik pásek se ve fondu nezobrazí.

Přejmenování

Pokud je softwarem zjištěna nová páska, je jí automaticky přiřazen název v následujícím formátu: **Páska XXX**, kde **XXX** je jedinečné číslo. Pásky jsou číslovány postupně. Operace přejmenování umožňuje ručně změnit název pásky.

Jak přejmenovat pásky:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadovanou pásku, a potom ji vyberte.
4. Klikněte na **Přejmenovat**.
5. Zadejte nový název vybrané pásky.
6. Kliknutím na tlačítko **Přejmenovat** uložte změny.

Vymazání

Vymazání pásky fyzicky odstraní všechny zálohy uložené na pásce a odstraní informace o těchto zálohách z databáze. Informace o pásce samotné však v databázi zůstávají.

Po vymazání se páska umístěná ve fondu **Nerozpoznané pásky** nebo **Importované pásky** přesune do fondu **Volné pásky**. Páska umístěná v jakémkoliv jiném fondu se nepřesouvá.

Jak vymazat pásky:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadované pásky, a vyberte je.
4. Klikněte na **Smazat**. Systém zobrazí výzvu pro potvrzení operace.
5. Vyberte metodu smazání: rychlé nebo plné.
6. Operaci zahájíte kliknutím na **Smazat**.

    Podrobnosti. Operaci mazání nelze zrušit.

Vysunutí

Pro úspěšné vysunutí pásky z knihovny pásek musí mít knihovna e-mailový slot a tento slot nesmí být uzamčen uživatelem nebo softwarem.

Jak vysunout pásky:

1. Klikněte na **Nastavení** > **Správa pásek**.

2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadované pásky, a vyberte je.
4. Klikněte na **Vysunout**. Aplikace zobrazí výzvu, abyste zadali popis pásky. Doporučujeme zadat popis fyzického umístění, kde budou pásky uloženy. Software během obnovy tento popis zobrazí, abyste mohli pásky snadno najít.
5. Kliknutím na **Vysunout** zahájíte operaci.

Po ručním nebo automatickém (str. 191) vysunutí pásky je doporučeno zapsat na pásku její název.

Odstranění

Operace odstranění odstraní informace o zálohách uložených na vybrané pásce a o pásce samotné z databáze.

Odstranit můžete pouze odpojenou (vysunutou (str. 431)) pásku.

Jak odstranit pásku:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadovanou pásku, a potom ji vyberte.
4. Klikněte na **Odebrat**. Systém zobrazí výzvu pro potvrzení operace.
5. Kliknutím na tlačítko **Odebrat** odstraňte pásku.

Co dělat, pokud odstraníte pásku omylem?

Na rozdíl od vymazané (str. 431) pásky nejsou data z odstraněné pásky fyzicky odstraněna. Je tedy možné zálohy uložené na takové pásce znovu obnovit. Postupujte následujícím způsobem:

1. Vložte pásku do páskového zařízení.
2. Provedením rychlé inventarizace (str. 428) detekujte pásku.

   Poznámka *Během inventarizace* nezapínejte *přepínač* ***Přesunout nerozpoznané a importované pásky do fondu Volné pásky***.
3. Překontrolováním (str. 430) porovnejte data uložená na páskách s databází.

Zadání sady pásek

Tato operace vám umožní pro pásky zadat sadu pásek.

Sada pásek je skupina pásek v rámci jednoho fondu.

Na rozdíl od sad pásek v možnostech zálohy (str. 191), kde lze používat proměnné, můžete zde zadat pouze hodnotu řetězce.

Tuto operaci proveďte, pokud chcete, aby software zálohoval na*konkrétní* pásky podle určitého pravidla (například chcete-li uložit pondělní zálohy na pásku 1, úterní na pásku 2 atd.). Zadejte sadu pásek pro každou požadovanou pásku a potom zadejte stejnou sadu pásek v možnostech zálohy nebo použijte vhodné proměnné.

V rámci uvedeného příkladu zadejte sadu pásek **`Monday`** pro pásku 1, **`Tuesday`** pro pásku 2 atd. V možnostech zálohování zadejte **`[Weekday]`**. V tomto případě se v příslušný den v týdnu použije správná páska.

Jak zadat sadu pásek pro jednu nebo několik pásek:

1. Klikněte na **Nastavení** > **Správa pásek**.
2. Vyberte počítač nebo uzel úložišť, ke kterému je připojeno páskové zařízení, a klikněte na možnost **Fondy pásek** nacházející se pod tímto počítačem.
3. Klikněte na fond, který obsahuje požadované pásky, a vyberte je.
4. Klikněte na možnost **Sada pásek**.
5. Zadejte název sady pásek. Pokud je pro vybrané pásky již zadaná jiná sada pásek, nahradí se. Chcete-li vyloučit pásky ze sady pásek bez zadání jiné sady, odstraňte název existující sady pásek.
6. Kliknutím na **Uložit** změny uložíte.

28.2 Uzly úložišť

Uzel úložišť je server určený k optimalizaci použití různých prostředků (například firemní kapacity úložišť, zatížení sítě a vytížení procesoru produkčních serverů) potřebných k zabezpečení podnikových dat. Tohoto cíle lze dosáhnout uspořádáním a správou umístění, která slouží jako vyhrazená úložiště podnikových záloh (spravovaná umístění).

28.2.1 Instalace uzlu úložišť a katalogové služby

Před instalací uzlu úložišť zkontrolujte, zda počítač splňuje systémové požadavky (str. 32).

Katalogovou službu a uzel úložišť doporučujeme nainstalovat na odlišné počítače. Systémové požadavky na počítač s katalogovou službu jsou popsány v části Osvědčené postupy katalogizace (str. 439).

Instalace uzlu úložišť a/nebo katalogové služby

1. Přihlaste se jako správce a spusťte instalační program aplikace Acronis Cyber Protect.
2. [Volitelné] Pokud chcete změnit jazyk instalačního programu, klikněte na **Jazyk instalace**.
3. Vyjádřete souhlas s licenčními podmínkami a vyberte, jestli se počítač bude účastnit Programu zkušeností uživatelů Acronis (ACEP).
4. Klikněte na tlačítko **Instalovat agenta pro ochranu**.
5. Klikněte na **Přizpůsobit nastavení instalace**.
6. Vedle možnosti **Co je nutno nainstalovat** klikněte na **Změnit**.
7. Vyberte součásti k nainstalování:
   - Pokud chcete nainstalovat uzel úložišť, zaškrtněte políčko**Uzel úložišť**. Políčko **Agent pro Windows** je zaškrtnuté automaticky.
   - Pokud chcete nainstalovat katalogovou službu, zaškrtněte políčko **Katalogová služba**.
   - Pokud do tohoto počítače nechcete instalovat žádné další součásti, zrušte zaškrtnutí příslušných políček.

   Pokračujte kliknutím na **Hotovo**.
8. Zadejte server pro správu, kde bude součást zaregistrována:
   a. Vedle možnosti **Server pro správu Acronis Cyber Protect** klikněte na **Zadat**.
   b. Zadejte název hostitele nebo IP adresu počítače, ve kterém je server pro správu nainstalován.
   c. Zadejte pověření správce serveru pro správu nebo registrační token.

      Další informace o vygenerování registračního tokenu naleznete v části Instalace agentů pomocí zásad skupiny (str. 101).

Pokud nejste správce serveru pro správu, můžete počítač zaregistrovat výběrem možnosti **Připojit bez ověřování**. To je možné v případě, že server pro správu umožňuje anonymní registraci, což může být zakázáno (str. 443).

d. Klikněte na tlačítko **Hotovo**.

9. Při zobrazení výzvy vyberte, zda se má počítač s uzlem úložišť a/nebo katalogovou službou přidat do organizace nebo do některé jednotky.

   Tato výzva se zobrazí, pokud spravujete více jednotek nebo organizaci s alespoň jednou jednotkou. Jinak se počítač bez výzev přidá do jednotky nebo organizace, kterou spravujete. Další informace najdete v části Správci a jednotky (str. 444).

10. [Volitelné] Změňte další nastavení instalace způsobem popsaným v části Přizpůsobit nastavení instalace (str. 37).
11. Kliknutím na **Instalovat** zahajte instalaci.
12. Po dokončení instalace klikněte na **Zavřít**.

28.2.2 Přidání spravovaného umístění

Spravované umístění lze uspořádat:

- V místní složce:
  - na místním pevném disku uzlu úložišť,
  - v úložišti SAN, které se operačnímu systému jeví jako místně připojené zařízení.
- V síťové složce:
  - ve sdílené složce SMB/CIFS,
  - v úložišti SAN, které se operačnímu systému jeví jako síťová složka,
  - v úložišti NAS,
- na páskovém zařízení místně připojeném k uzlu úložišť.

  Pásková umístění jsou vytvářena formou fondů pásek (str. 425). Ve výchozím nastavení je k dispozici jeden fond pásek. V případě potřeby lze vytvořit další fondy pásek, jak je popsáno níže v tomto oddílu.

Jak vytvořit spravované umístění v místní nebo síťové složce

1. Proveďte jeden z následujících úkonů:
   - Klikněte na **Úložiště záloh** > **Přidat umístění** a potom na možnost **Uzel úložiště**.
   - Při vytváření plánu ochrany klikněte na možnost **Kam zálohovat** > **Přidat umístění** a potom klikněte na **Uzel úložišť**.
   - Klikněte na **Nastavení** > **Uzly úložišť**, vyberte uzel úložišť, který bude provádět správu tohoto umístění, a potom klikněte na možnost **Přidat umístění**.
2. V části **Název** zadejte jedinečný název úložiště. Jedinečný název znamená, že nesmí existovat jiné umístění se stejným názvem spravované ve stejném uzlu úložišť.
3. [Volitelné] Vyberte uzel úložišť, který bude provádět správu tohoto umístění. Pokud jste v prvním kroku vybrali poslední možnost, nebudete moci změnit uzel úložišť.
4. Vyberte název uzlu úložišť nebo IP adresu, které agenti použijí pro přístup k serveru.

   Ve výchozím nastavení se vybere název uzlu úložišť. Toto nastavení změňte, pokud server DNS nedokáže přeložit název na IP adresu, což vede k selhání přístupu. Toto nastavení můžete později změnit kliknutím na **Úložiště záloh** > dané umístění > **Upravit** a změnou hodnoty pole **Adresa**.
5. Zadejte cestu ke složce nebo procházením složku najděte.
6. Klikněte na tlačítko **Hotovo**. Software zkontroluje přístup k zadané složce.

7. [Volitelné] Zapněte v umístění deduplikaci záloh.

   Deduplikace minimalizuje zatížení zálohováním a omezuje velikost záloh uložených v umístění vyloučením duplicitních bloků disku.

   Další informace o omezeních deduplikace naleznete v části Omezení deduplikace (str. 435).
8. [Pouze pokud je deduplikace povolena] Určete nebo změňte hodnotu pole **Cesta k deduplikační databázi**.

   Musí se jednat o složku na místním pevném disku uzlu úložišť. Chcete-li zlepšit výkon systému, doporučujeme vytvořit deduplikační databázi a spravované umístění na různých discích.

   Další informace o deduplikační databázi naleznete v části Osvědčené postupy při deduplikaci (str. 436).
9. [Volitelné] Vyberte, zda má být umístění chráněno šifrováním. Vše, co bude zapisováno do tohoto umístění, bude šifrováno, a vše, co z něj bude čteno, bude transparentně dešifrováno pomocí šifrovacího klíče, který se váže ke konkrétnímu umístění a který je uložen v uzlu úložišť.

   Další informace o šifrování naleznete v části Šifrování umístění (str. 437).
10. [Volitelné] Vyberte, zda chcete katalogizovat zálohy uložené v umístění. Katalog dat umožňuje snadno nalézt požadovanou verzi dat a obnovit ji.

    Pokud je na serveru pro správu registrováno několik katalogových služeb, můžete vybrat službu, která bude katalogizovat zálohy uložené v umístění.

    Katalogizaci můžete povolit nebo zakázat později, jak je popsáno v části Povolení nebo zakázání katalogizace (str. 440).
11. Umístění vytvoříte kliknutím na **Hotovo**.

Jak vytvořit spravované umístění na páskovém zařízení

1. Klikněte na **Úložiště záloh** > **Přidat umístění** nebo, vytváříte-li plán ochrany, na možnost **Kam zálohovat** > **Přidat umístění**.
2. Klikněte na možnost **Pásky**.
3. [Volitelné] Vyberte uzel úložišť, který bude provádět správu tohoto umístění.
4. Postupujte podle pokynů v části Vytvoření fondu (str. 426) od kroku 4.

Poznámka *Ve výchozím nastavení slouží název uzlu úložišť agentům pro přístup ke spravovanému páskovému umístění. Kliknutím na* ***Úložiště záloh*** *>* *dané umístění* *>* ***Upravit*** *a změnou hodnoty pole* ***Adresa*** *zajistíte, aby agenti používali IP adresu uzlu úložiště.*

28.2.3 Deduplikace

28.2.3.1 Omezení deduplikace

Běžná omezení

Šifrované zálohy nelze deduplikovat. Pokud chcete současně používat deduplikaci a šifrování, nechte zálohy nešifrované a přesměrujte je do umístění, kde je povolena deduplikace i šifrování.

Záloha na úrovni disku

Deduplikace bloků disku se neprovádí, jestliže velikost alokační jednotky svazku – známé též jako velikost clusteru nebo bloku – není dělitelná 4 KB.

Tip: *Velikost alokační jednotky na většině NTFS a ext3 svazků je 4 KB. To umožňuje deduplikaci na úrovni bloků. Dalšími příklady velikostí alokační jednotky, které umožňují deduplikaci na úrovni bloku, jsou 8 kB, 16 kB a 64 kB.*

Zálohy na úrovni souborů

Deduplikace souboru se neprovádí, pokud je soubor zašifrován.

Deduplikace a datové proudy NTFS

V souborovém systému NTFS může mít soubor přiřazenu jednu nebo více sad dalších dat – často nazývanou *alternativní datový proud*.

Pokud je takový soubor zálohován, zálohují se rovněž všechny jeho datové proudy. Tyto proudy však nikdy nejsou deduplikovány – ani když je deduplikován samotný soubor.

28.2.3.2 Osvědčené postupy při deduplikaci

Deduplikace je složitý proces, který závisí na mnoha faktorech.

Nejdůležitější faktory, které ovlivňují rychlost deduplikace, jsou:

- rychlost přístupu k deduplikační databázi,
- kapacita paměti RAM v uzlu úložišť,
- Počet deduplikačních umístění vytvořených v uzlu úložišť.

Chcete-li zvýšit výkone deduplikace, dbejte následujících doporučení.

Umístěte deduplikační databázi a deduplikační umístění na samostatná fyzická zařízení.

Deduplikační databáze ukládá hodnoty hash všech položek uložených v umístění – kromě těch, které nelze deduplikovat, jako jsou šifrované soubory.

Chcete-li zvýšit rychlost přístupu k deduplikační databázi, musí se databázi a umístění nacházet na samostatných fyzických zařízeních.

Nejvhodnější je přidělit vyhrazená zařízení pro umístění a databázi. Pokud to není možné, neumisťujte aspoň umístění nebo databázi na jeden disk s operačním systémem. A to z důvodu, že operační systém provádí velké množství operací pro zápis/čtení z disku, které podstatně zpomalují deduplikaci.

Výběr disku pro deduplikační databázi

- Databáze se musí nacházet na pevném disku. Neumisťujte deduplikační databázi na externí jednotky.
- Pokud chcete co nejvíce zkrátit přístupové časy k databázi, uložte ji místo připojeného síťového svazku přímo na připojený disk. Výkon deduplikace může výrazně snížit latence sítě.
- Požadovaný diskový prostor pro deduplikační databázi lze odhadnout pomocí následujícího vzorce:

  $$V = U * 90 / 65536 + 10$$

  Kde,

  V je velikost disku v GB,

  U je plánované množství jedinečných dat v deduplikačním úložišti dat v GB,

  Pokud je například plánované množství jedinečných dat v deduplikačním úložišti dat U=5 TB, bude deduplikační databáze požadovat minimum volného prostoru, jak je ukázáno níže:

  $$V = 5000 * 90 / 65536 +10 = 17 GB$$

Výběr disku pro deduplikační umístění

Aby se předešlo ztrátě dat, doporučujeme používat RAID 10, 5 nebo 6. RAID 0 se nedoporučuje, protože není odolný vůči chybám. RAID 1 není doporučován, kvůli relativně nízké rychlosti. Řešení pomocí místních disků nebo SAN je rovnocenné, obě řešení jsou dobrá.

40 až 160 MB paměti RAM na 1 TB jedinečných dat

Po dosažení limitu se deduplikace zastaví, ale zálohování a obnovení budou i nadále fungovat. Pokud do uzlu úložišť přidáte více paměti RAM, bude po dalším zálohování deduplikace pokračovat. Obecně platí, že čím více máte paměti RAM, tím větší objem jedinečných dat můžete ukládat.

Pouze jedno deduplikační umístění ke každému uzlu úložišť

Doporučuje se vytvořit pouze jedno deduplikační umístění v uzlu úložišť. V opačném případě může být celý dostupný svazek paměti RAM rozdělen podle velikosti mezi více umístění.

Nepřítomnost aplikací soupeřících o prostředky

V počítači s uzlem úložiště by neměly běžet aplikace, které požadují mnoho systémových prostředků, například systém řízení báze dat (SŘBD) nebo systém ERP (Enterprise Resource Planning).

Procesor s více jádry a frekvencí procesoru alespoň 2,5 GHz

Doporučujeme použít procesor s nejméně čtyřmi jádry a taktem CPU minimálně 2,5 GHz.

Dostatek volného prostoru v umístění

Deduplikace u cíle vyžaduje tolik volného místa, kolik zabírají zálohovaná data ihned po uložení do umístění. Bez komprese nebo deduplikace ve zdroji je tato hodnota rovna velikosti původních dat zálohovaných během dané operace zálohování.

Vysokorychlostní LAN

Doporučuje se 1GB síť LAN. Ta povolí aplikaci provést 5 až 6 záloh zároveň s deduplikací a rychlost se výrazně nesníží.

Zálohujte obvyklý počítač před zálohováním více počítačů s podobným obsahem

Při zálohování více počítačů s podobným obsahem se doporučuje zálohovat nejdříve jeden z počítačů a počkat, dokud neskončí indexování zálohovaných dat. Poté budou ostatní počítače zálohovány rychleji díky efektivní deduplikaci. Většina dat je již v deduplikačním úložišti dat, protože záloha prvního počítače byla indexována.

Záloha různých počítačů v různém čase

Pokud zálohujete velký počet počítačů, rozložte operace zálohování v čase. K tomu je potřeba vytvořit více plánů ochrany s různým plánováním.

28.2.4 Šifrování umístění

Pokud umístění chráníte šifrováním, pak vše, co bude do tohoto umístění zapisováno, bude šifrováno, a vše, co z něj bude čteno, bude transparentně dešifrováno pomocí šifrovacího klíče, který se váže ke konkrétnímu umístění a je uložen na uzlu. V případě, že je paměťové médium odcizeno nebo k němu přistupuje neoprávněná osoba, pachatel nebude schopen obsah umístění bez přístupu k tomuto uzlu úložišť dešifrovat.

Toto šifrování nemá nic společného se šifrováním zálohy, které je určeno plánem ochrany a prováděno agentem. Pokud je již záloha šifrována, šifrování na straně uzlu úložišť je aplikováno šifrováním prováděným agentem.

Ochrana umístění šifrováním

1. Zadejte a potvrďte slovo (heslo), které se použije k vytvoření šifrovacího klíče.

   U hesla se rozlišuje velikost písmen. Při připojování umístění k jinému uzlu úložišť se zobrazí pouze výzva k zadání tohoto hesla (slova).
2. Vyberte jeden z následujících algoritmů šifrování:
   - **AES 128** – obsah umístění se šifruje pomocí algoritmu AES (Advanced Encryption Standard) se 128bitovým klíčem.
   - **AES 192** – obsah umístění se šifruje pomocí algoritmu AES se 192bitovým klíčem.
   - **AES 256** – obsah umístění se šifruje pomocí algoritmu AES s 256bitovým klíčem.
3. Klikněte na tlačítko **OK**.

Šifrovací algoritmus AES pracuje v režimu zřetězení číselných bloků (CBC) a používá náhodně generovaný klíč s uživatelem definovanou velikostí 128, 192 nebo 256 bitů. Čím delší je klíč, tím déle bude aplikaci trvat šifrování záloh uložených v umístění a tím více budou zálohy zabezpečené.

Šifrovací klíč je pak šifrován pomocí algoritmu AES-256 pomocí hodnoty hashovací funkce SHA-256 vybraného slova jako klíče. Samotné slovo není na disku uloženo; pro účely ověření je použita hodnota hash slova. S tímto dvojúrovňovým zabezpečením jsou zálohy chráněny před neautorizovaným přístupem, ale obnovení ztraceného slova (zapomenutého hesla) není možné.

28.2.5 Katalogizace

28.2.5.1 Katalog dat

Katalog dat umožňuje snadno nalézt požadovanou verzi dat a obnovit ji. Zobrazuje data uložená ve spravovaných umístěních, pro která byla nebo je povolena katalogizace.

Část **Katalog** se zobrazuje pod kartou **Úložiště záloh** pouze v případě, že je na serveru pro správu zaregistrována minimálně jedna katalogová služba. Informace o instalaci katalogové služby najdete v části Instalace uzlu úložišť a katalogové služby (str. 433).

Část **Katalog** je viditelná pouze pro správce organizace (str. 444).

Omezení

Katalogizace je podporována pouze pro zálohy fyzických počítačů na úrovni disku nebo souborů a pro zálohy virtuálních počítačů.

V katalogu nelze zobrazit následující data:

- Data z šifrovaných záloh
- Data zálohovaná na pásková zařízení
- Data zálohovaná do cloudového úložiště
- Data zálohovaná verzemi produktu staršími než Acronis Cyber Protect 12.5

Výběr zálohovaných dat k obnovení

1. Klikněte na **Úložiště záloh** > **Katalog**.

2. Pokud je na serveru pro správu registrováno několik katalogových služeb, vyberte službu, která bude katalogizovat zálohy uložené v umístění.

   Tip *Pokud chcete zjistit, která služba katalogizuje dané umístění, vyberte umístění v části* ***Úložiště záloh*** *>* ***Umístění*** *>* ***Umístění*** *a potom klikněte na* ***Podrobnosti****.*

3. Software zobrazí počítače, které byly zálohovány do spravovaných umístění katalogizovaných vybranou katalogovou službou.

   Procházením nebo hledáním vyberte data, která chcete obnovit.

   - **Procházení**

     Dvojím kliknutím na počítač zobrazíte zálohované disky, svazky, složky a soubory.

     Disk obnovíte vybráním disku označeného následující ikonou: 

     Svazek obnovíte dvojím kliknutím na disk obsahující svazek a potom vybráním svazku.

     Chcete-li obnovit soubory a složky, najděte jejich umístění procházením svazku. Můžete procházet svazky označené ikonou složky: 

   - **Hledat**

     Do pole pro hledání zadejte informace, které pomohou identifikovat požadované datové položky (může se jednat o název počítače, souboru nebo složky nebo jmenovku disku), a pak klikněte na tlačítko **Hledat**.

     Lze použít zástupné znaky hvězdička (*) a otazník (?).

     Ve výsledku hledání se zobrazí seznam zálohovaných datových položek, jejichž názvy zcela nebo částečně odpovídají zadaným hodnotám.

4. Ve výchozím nastavení se data vrátí do nejnovějšího možného stavu. Pokud jste vybrali jedinou položku, můžete pomocí tlačítka **Verze** vybrat bod obnovy.
5. Až budete mít vybraná požadovaná data, proveďte jednu z následujících akcí:
   - Klikněte na **Obnovit** a potom nakonfigurujte parametry operace obnovy tak, jak jsou popsány v části věnované obnově (str. 196).
   - [Pouze pro soubory/složky] Pokud chcete soubory uložit do souboru ZIP, klikněte na **Stáhnout**, vyberte umístění pro uložení dat a klikněte na **Uložit**.

28.2.5.2 Nejlepší postupy z hlediska katalogizace

Chcete-li zvýšit výkon katalogizace, dbejte následujících doporučení.

Instalace

Katalogovou službu a uzel úložišť doporučujeme nainstalovat na odlišné počítače. V opačném případě budou tyto součásti ve stejnou dobu využívat stejné prostředky procesoru a paměti RAM.

Pokud je na serveru pro správu zaregistrovaných více uzlů úložišť, bude stačit jedna katalogová služba, pokud nebude docházet ke zhoršení výkonu při indexování nebo vyhledávání. Pokud si například všimnete, že katalogizace probíhá nonstop (to znamená, že mezi aktivitami katalogizace nejsou žádné přestávky), nainstalujte na samostatný počítač další katalogovou službu. Pak odeberte některá spravovaná umístění a znovu je vytvořte s novou katalogovou službou. Zálohy uložené v těchto umístěních zůstanou beze změny.

Systémové požadavky

Parametr	Minimální hodnota	Doporučená hodnota
Počet jader procesoru	2	4 a více
PAMĚŤ RAM	8 GB	16 GB a více
Pevný disk	Pevný disk 7200 ot./min	SSD
Síťové připojení mezi počítačem s uzlem úložišť a počítačem s katalogovou službou	100 Mb/s	1 Gb/s

28.2.5.3 Povolení nebo zakázání katalogizace

Pokud je pro spravované umístění povolena katalogizace, obsah jednotlivých záloh směrovaných do daného umístění se přidá do katalogu dat, jakmile je vytvořena záloha.

Katalogizaci můžete povolit při přidávání spravovaného umístění polohy nebo později. Po povolení katalogizace budou všechny zálohy, které jsou uloženy v daném umístění a nebyly dříve katalogizovány, katalogizovány po příštím zálohování do daného umístění.

Proces katalogizace může být časově náročný, zvláště pokud je zálohováno velké množství počítačů do stejného umístění. Katalogizaci můžete kdykoli zakázat. Katalogizace záloh vytvořených před zákazem katalogizace bude dokončena. Nově vytvořené zálohy katalogizovány nebudou.

Konfigurace katalogizace pro existující umístění

1. Klikněte na **Úložiště záloh** > **Umístění**.
2. Klikněte na **Umístění** a potom vyberte spravované umístění, pro které chcete konfigurovat katalogizaci.
3. Klikněte na tlačítko **Upravit**.
4. Přepínačem **Katalogová služba** povolte nebo zakažte katalogizaci.
5. Klikněte na tlačítko **Hotovo**.

29 Nastavení systému

Tato nastavení jsou k dispozici jen pro místní nasazení.

K těmto nastavením se dostanete kliknutím na **Nastavení** > **Nastavení systému**.

Část **Nastavení systému** je viditelná pouze pro správce organizace (str. 444).

29.1 E-mailová upozornění

Můžete nakonfigurovat globální nastavení, která jsou společná pro všechna e-mailová upozornění posílaná ze serveru pro správu.

Ve výchozích možnostech zálohy (str. 443) lze tato nastavení přepsat výhradně pro události, které se vyskytnou při zálohování. V takovém případě budou mít tato globální nastavení účinek pro jiné operace než zálohování.

Při vytváření plánu ochrany (str. 170) si můžete zvolit, která nastavení budou použita: globální nastavení nebo nastavení zadaná ve výchozích možnostech zálohy. Můžete je také přepsat vlastními hodnotami, které budou platit jen pro tento plán.

Důležité: *Změna globálních nastavení e-mailových upozornění ovlivní všechny plány ochrany, které tato globální nastavení používají.*

Před konfigurací těchto nastavení se ujistěte, že jsou nakonfigurována nastavení **e-mailového serveru** (str. 441).

Konfigurace globálních nastavení e-mailových upozornění

1. Klikněte na **Nastavení** > **Nastavení systému** > **E-mailová upozornění**.
2. Do pole **E-mailové adresy příjemců** zadejte cílovou e-mailovou adresu. Je možné zadat více adres oddělených středníky.
3. [Volitelné] V poli **Předmět** změňte předmět e-mailového upozornění.

   Můžete použít následující proměnné:

   - **`[Alert]`** – shrnutí výstrah
   - **`[Device]`** – název zařízení
   - **`[Plan]`** – název plánu, který vygeneroval výstrahu
   - **`[ManagementServer]`** – název hostitele počítače, ve kterém je server pro správu nainstalován
   - **`[Unit]`** – název jednotky, do které počítač náleží

   Výchozí předmět je **`[Alert]`Zařízení: `[Device]` Plán: `[Plan]`**
4. [Volitelné] Zaškrtněte políčko **Denní shrnutí aktivních výstrah** a proveďte některou z následujících akcí:
   a. Zadejte čas odeslání shrnutí.
   b. [Volitelné] Zaškrtněte políčko **Neodesílat zprávy „Žádné aktivní výstrahy“**.
5. [Volitelné] Vyberte jazyk, který bude používán v e-mailových upozorněních.
6. Zaškrtněte políčka u událostí, na které chcete dostávat upozornění. Můžete vybírat ze seznamu možných výstrah seskupených podle závažnosti.
7. Klikněte na tlačítko **Uložit**.

29.2 E-mailový server

Můžete určit e-mailový server, který se bude používat k posílání e-mailových upozornění ze serveru pro správu.

Postup určení e-mailového serveru

1. Klikněte na **Nastavení** > **Nastavení systému** > **E-mailový server**.
2. V části **E-mailová služba** vyberte jednu z následujících možností:
   - **Vlastní**
   - **Gmail**

     Ve vašem účtu služby Gmail musí být zapnuto nastavení **Méně bezpečné aplikace**. Další informace naleznete na stránce https://support.google.com/accounts/answer/6010255.
   - **Yahoo Mail**
   - **Outlook.com**
3. [Pouze pro vlastní e-mailovou službu] Zadejte následující nastavení:
   - Do pole **Server SMTP** zadejte název serveru odchozí pošty (SMTP).
   - Do pole **Port SMTP** zadejte port serveru odchozí pošty. Implicitně je tento port nastaven na 25.

- Vyberte, jestli se má používat šifrování SSL nebo TLS. Výběrem možnosti **Žádné** šifrování zakážete.
- Jestliže server SMTP vyžaduje ověření, zaškrtněte políčko **Server SMTP vyžaduje ověření** a poté zadejte pověření účtu, který se bude používat pro odesílání zpráv. Pokud si nejste jisti, zda server SMTP vyžaduje ověření, kontaktujte správce sítě nebo poskytovatele e-mailových služeb.

4. [Pouze pro Gmail, Yahoo Mail a Outlook.com] Zadejte pověření účtu, který se bude používat pro odesílání zpráv.
5. [Pouze pro vlastní e-mailovou službu] Do pole **Odesílatel** zadejte jméno odesílatele. Toto jméno se bude zobrazovat v poli **Od** e-mailových upozornění. Necháte-li toto pole prázdné, budou zprávy obsahovat účet zadaný v kroku 3 nebo 4.
6. [Volitelné] Kliknutím na **Zaslat zkušební zprávu** zkontrolujte, jestli e-mailová upozornění se zadanými nastaveními správně fungují. Zadejte e-mailovou adresu, na kterou se má odeslat zkušební zpráva.

29.3 Zabezpečení

Tyto možnosti slouží ke zvýšení zabezpečení místního nasazení Acronis Cyber Protect.

Odhlásit neaktivní uživatele po

Tato možnost dovoluje určit časový limit automatického odhlášení z důvodu neaktivity uživatele. Když z nastaveného časového limitu zbývá jedna minuta, zobrazí software uživateli výzvu k zachování přihlášení. Po uplynutí časového limitu je uživatel odhlášen a všechny neuložené změny se ztratí.

Výchozí nastavení: **Povoleno. Časový limit: 10 minut.**

Zobrazit oznámení o posledním přihlášení aktuálního uživatele

Tato možnost povoluje zobrazení data a času posledního úspěšného přihlášení uživatele, počet nezdařených ověření od posledního úspěšného přihlášení a IP adresu posledního úspěšného přihlášení. Tyto informace se zobrazí v dolní části obrazovky po každém přihlášení uživatele.

Výchozí nastavení: **Zakázáno**.

Zobrazit upozornění o vypršení platnosti místního nebo doménového hesla

Tato možnost povoluje zobrazení času do vypršení hesla pro přístup uživatele k serveru pro správu Acronis Cyber Protect. Jde o doménové heslo, se kterým se uživatel přihlašuje do počítače, kde je nainstalován server pro správu. Čas do vypršení hesla se zobrazuje v dolní části obrazovky a v nabídce účtu v pravém horním rohu.

Výchozí nastavení: **Zakázáno**.

29.4 Aktualizace

Tato možnost určuje, zda při každém přihlášení správce organizace do webové konzole Cyber Protect proběhne v produktu Acronis Cyber Protect kontrola nové verze.

Výchozí nastavení: **Povoleno**.

Je-li tato možnost vypnutá, může správce kontrolovat aktualizace ručně, jak je popsáno v tématu Kontrola dostupných aktualizací (str. 64).

29.5 Výchozí možnosti zálohování

Výchozí hodnoty možností zálohy (str. 160) jsou společné pro všechny plány ochrany na serveru pro správu. Správce organizace může změnit výchozí hodnotu určité možnosti oproti předdefinované. Nová hodnota bude po provedení změny použita ve výchozím nastavení ve všech plánech ochrany.

Při vytváření plánu ochrany může uživatel výchozí hodnotu přepsat vlastní hodnotou, která bude platit jen pro tento plán.

Jak změnit výchozí hodnotu volby

1. Přihlaste se k webové konzoli Cyber Protect jako správce organizace.
2. Klikněte na **Nastavení** > **Nastavení systému**.
3. Rozbalte část **Výchozí možnosti zálohy**.
4. Vyberte možnost a proveďte potřebné změny.
5. Klikněte na tlačítko **Uložit**.

29.6 Konfigurace anonymní registrace

Během místní instalace agenta (str. 48) instalační program navrhne možnost anonymní registrace počítače na serveru pro správu. Jinými slovy možnost připojení bez ověřování. Anonymní registrace je použita také v případě, že jsou zadána nesprávná pověření pro server pro správu v rozhraní Agenta pro VMware (Virtual Appliance). Anonymní registrace umožňuje správci serveru pro správu delegovat instalaci agenta na uživatele.

Anonymní registraci je možné na serveru pro správu zakázat, aby při registraci zařízení bylo vždy požadováno platné uživatelské jméno a heslo správce serveru pro správu. Pokud se v takovém případě uživatel rozhodne pro anonymní registraci, registrace se nezdaří. Registrace spouštěcího média, které bylo předem nakonfigurováno s možností **Nepožadovat uživatelské jméno a heslo**, bude také zamítnuta. Během bezobslužné instalace budete muset zadat registrační token v souboru transformace (.mst) nebo jako parametr příkazu **`msiexec`**.

Zakázání anonymní registrace na serveru pro správu

1. Přihlaste se do počítače, kde je nainstalován server pro správu.
2. V textovém editoru otevřete následující konfigurační soubor:
   - Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**
3. Vyhledejte následující oddíl:

   ```
   "auth": {
     "anonymous_role": {
       "enabled": true
     }
   },
   ```

   Pokud jste aktualizovali server pro správu ze sestavení 11010 nebo staršího, tento oddíl není k dispozici. Vložte jej na začátek souboru hned za úvodní závorku **{**.
4. Změňte **`true`** na **`false`**.
5. Uložte soubor **api_gateway.json**.

   Důležité *Buďte opatrní, abyste nedopatřením neodstranili z konfiguračního souboru žádné čárky, závorky ani uvozovky.*
6. Restartujte službu serveru pro správu Acronis podle postupu popsaném v tématu Změna nastavení certifikátu SSL (str. 114).

30 Správa uživatelských účtů a organizačních jednotek

30.1 Místní nasazení

Funkce popsané v této části jsou k dispozici pouze správcům organizace (str. 444).

K těmto nastavením se dostanete kliknutím na položky **Nastavení** > **Účty**.

30.1.1 Správci a jednotky

Panel **Účty** zobrazuje skupinu **Organizace** se stromem jednotek (pokud nějaké existují) a seznam správců jednotky vybrané v tomto stromu.

Kdo jsou správci serveru pro správu?

Správcem serveru pro správu je jakýkoli účet, který se může přihlásit do webové konzole Cyber Protect.

Správci organizace jsou správci nejvyšší úrovně. *Správci jednotek* jsou správci podřízených skupin (jednotek).

Každý správce má ve webové konzoli Cyber Protect zobrazení zahrnující oblast, kterou může ovládat. Správce může zobrazit nebo spravovat cokoli na své nebo nižší úrovni hierarchie.

Kdo jsou výchozí správci?

V systému Windows

Při instalaci serveru pro správu do počítače se děje následující:

- V počítači se vytvoří se skupina **Acronis Centralized Admins**.

  Na řadiči domény má skupina název *DCNAME* **$ Acronis Centralized Admins**; v tomto případě *DCNAME* zastupuje název řadiče domény NetBIOS.
- Všichni členové skupiny **Administrators** jsou přidáni do skupiny **Acronis Centralized Admins**. Pokud je počítač v doméně, ale není řadičem domény, místní uživatelé (kteří nejsou členy domény) jsou vyloučeni. V řadiči domény nejsou žádní uživatelé, kteří nejsou členy domény.
- Skupina **Acronis Centralized Admins** a skupina **Administrators** jsou přidány na server pro správu jako **správci organizace**. Pokud je počítač v doméně, ale není řadičem domény, skupina **Administrators** není přidána, takže místní uživatelé (kteří nejsou členy domény) se nestanou správci organizace.

Skupinu **Administrators** můžete ze seznamu správců organizace odstranit. Skupinu **Acronis Centralized Admins** ale odstranit nelze. V nepravděpodobném případě, ve kterém by byli všichni správci organizace odstraněni, můžete v systému Windows přidat ke skupině **Acronis Centralized Admins** účet, který lze pak použít pro přihlášení k webové konzoli Cyber Protect.

V systému Linux

Při instalaci serveru pro správu do počítače se uživatel **root** přidá do serveru pro správu jako **správce organizace**.

Do seznamu správců serveru pro správu můžete přidat další uživatele Linux, jak je popsáno níže, a potom odstranit uživatele **root** ze seznamu. Pokud dojde k odstranění všech správců organizace, což

je nepravděpodobné, můžete restartovat službu **acronis_asm**. Tím se uživatel **root** automaticky znovu přidá jako správce organizace.

Kdo může být správcem?

Pokud je server pro správu nainstalován na počítači se systémem Windows, který patří k doméně služby Active Directory, bude možné mezi správce serveru pro správu přidat kteréhokoli uživatele nebo skupinu uživatelů domény. V opačném případě bude možné přidat pouze místní uživatele a skupiny.

Více informací o přidání správce k serveru pro správu najdete v části Přidání správců (str. 446).

Role správce

K dispozici jsou dvě role správce:

- Správce – tato role poskytuje úplný přístup pro správu k organizaci nebo jednotce.
- Jen pro čtení – tato role poskytuje přístup k webové konzoli Cyber Protect. Umožňuje pouze shromažďování diagnostických dat, jako jsou systémové zprávy. Správce s rolí Jen pro čtení nemůže procházet zálohy ani obsah zálohovaných poštovních schránek.

  Tato role není k dispozici ve verzi Essentials.

Všechny změny rolí se zobrazí na kartě **Aktivity**.

Jednotky a správci jednotek

Skupina **Organizace** se vytvoří automaticky při instalaci serveru pro správu. S licencí Advanced aplikace Acronis Cyber Protect můžete vytvářet podřízené skupiny - jednotky, které obvykle odpovídají jednotkám nebo oddělením organizace, a přidávat těmto jednotkám správce.

Tímto způsobem můžete správou ochrany pověřit další uživatele, jejichž přístupová oprávnění budou přísně omezená na odpovídající jednotky.

Informace o vytvoření jednotky naleznete v části Vytváření jednotek (str. 446).

Každá jednotka může mít podřízené jednotky. Správci jednotky nadřazené jednotky mají stejná oprávnění ve všech podřízených jednotkách.

Skupina **Organizace** je nadřazené jednotky na nejvyšší úrovni a správci organizace mají ve všech jejích jednotkách stejná oprávnění.

Co když je účet přidán k několika jednotkám?

Jakýkoli účet lze jako **správce jednotky** přidat k neomezenému počtu jednotek. U takového účtu, stejně jako u správců organizace, se ve webové konzoli Cyber Protect zobrazuje správce výběru jednotek. Použitím tohoto nástroje pro výběr může správce zobrazovat a spravovat každou jednotku odděleně.

Účet s oprávněním ke všem jednotkám nemá oprávnění pro organizaci. Správci organizace musí být zvlášť přidáni do skupiny **Organizace**.

Jak naplnit jednotky počítači

Když správce přidá počítač přes webové rozhraní (str. 42), daný počítač se přidá do jednotky spravované tímto správcem. Pokud správce spravuje několik jednotek, počítač se přidá do vybrané jednotky ve správci výběru jednotek. Správce tedy musí zvolit jednotku ještě před kliknutím na tlačítko **Přidat**.

Když správce provádí lokální instalaci agentů (str. 48), poskytne své vlastní pověření. Počítač se potom přidá do jednotky spravované tímto správcem. Pokud správce spravuje více jednotek, instalační program zobrazí výzvu pro výběr jednotky, do které má být počítač přidán.

Dědění rolí

Role v nadřazené jednotce jsou zděděny podřízenými jednotkami. Pokud má stejný uživatelský účet v nadřazené a podřízené jednotce přiřazeny různé role, bude mít obě role.

Role lze explicitně přiřadit konkrétnímu uživatelskému účtu nebo je lze zdědit ze skupiny uživatelů. Uživatelský účet tak může mít konkrétní přiřazenou roli a zároveň i zděděnou roli.

Pokud má uživatelský účet různé role (přiřazené nebo zděděné), má přístup k objektům a může provádět akce povolené jakoukoli z těchto rolí. Například uživatelský účet s přiřazenou rolí jen pro čtení a zděděnou rolí správce bude mít oprávnění správce.

Poznámka *Ve webové konzoli Cyber Protect se zobrazují pouze explicitně přiřazené role pro aktuální jednotku. Možné nesoulady se zděděnými rolemi se nezobrazí. Důrazně doporučujeme přiřadit role správce a role jen pro čtení odděleným účtům nebo skupinám, aby nedošlo k možným problémům se zděděnými rolemi.*

30.1.2 Přidání účtů správce

Přidání účtů

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

   Software zobrazí seznam správců serveru pro správu a strom jednotek (pokud je k dispozici).
2. Vyberte možnost **Organizace** nebo vyberte jednotku, do které chcete správce přidat.
3. Klikněte na tlačítko **Přidat účet**.
4. V části **Doména** vyberte doménu obsahující uživatelské účty, které chcete přidat. Pokud není server pro správu zahrnutý v doméně služby Active Directory nebo je nainstalovaný v systému Linux, bude možné přidat pouze místní uživatele.
5. Vyhledejte uživatelské jméno nebo název skupiny uživatelů.
6. Klikněte na znaménko + vedle jména uživatele nebo názvu skupiny.
7. Vyberte roli pro účet.
8. Chcete-li přidat více uživatelů nebo skupin, opakujte kroky 4–6.
9. Po dokončení klikněte na **Hotovo**.
10. [Pouze v systému Linux] Přidejte uživatelská jména do modulu Acronis Linux Pluggable Authentication Module (PAM) podle pokynů níže.

Jak přidat uživatelská jména do modulu Acronis Linux PAM

1. Na počítači se serverem pro správu otevřete jako uživatel root soubor **/etc/security/acronisagent.conf** v textovém editoru.
2. Do tohoto souboru zadejte uživatelská jména, která jste přidali jako správce serveru pro správu, vždy jedno jméno na jeden řádek.
3. Soubor uložte a zavřete.

30.1.3 Vytváření jednotek

1. Klikněte na možnost **Nastavení** > **Účty**.
2. Software zobrazí seznam správců serveru pro správu a strom jednotek (pokud je k dispozici).
3. Vyberte možnost **Organizace** nebo pro novou jednotku vyberte nadřazenou jednotku.
4. Klikněte na možnost **Vytvořit jednotku**.

5. Zadejte název nové jednotky a pak klikněte na **Vytvořit**.

30.2 Cloudové nasazení

Správa uživatelských účtů a organizačních jednotek je k dispozici na portálu pro správu. Pokud chcete získat přístup k portálu pro správu, klikněte při přihlašování ke službě kybernetické ochrany na **Portál pro správu** nebo klikněte  na ikonu v pravém horním rohu a pak klikněte na **Portál pro správu**. Na tento portál mají přístup pouze uživatelé s oprávněním správce.

Informace o správě uživatelských účtů a organizačních jednotek získáte v Příručce správce portálu pro správu. Dokument zpřístupníte kliknutím na ikonu otazníku na portálu pro správu.

Tato část obsahuje další informace související se správou služby kybernetické ochrany.

Kvóty

Kvóty vám umožňují omezit, jak uživatelé používají danou službu. Kvóty nastavíte tak, že vyberete uživatele na kartě **Uživatelé** a potom kliknete na ikonu tužky v oddílu **Kvóty**.

Pokud je kvóta překročena, odešle se upozornění na e-mailovou adresu uživatele. Pokud nenastavíte překročení kvóty, bude kvóta považována za měkkou. To znamená, že se neuplatní omezení používání služby kybernetické ochrany.

Je také možné určit překročení kvóty. Limit překročení umožňuje uživateli překročit kvótu o zadanou hodnotu. Po překročení této hodnoty jsou použita omezení pro využívání služby kybernetické ochrany.

Zálohování

Můžete zadat kvótu cloudového úložiště, kvótu pro místní zálohy a maximální počet počítačů, zařízení a poštovních schránek, které může uživatel chránit. Jsou k dispozici následující kvóty:

- **Cloudové úložiště**
- **Pracovní stanice**
- **Servery**
- **Windows Server Essentials**
- **Virtuální hostitelé**
- **Univerzální**

  Tuto kvótu je možné použít místo kterékoliv z výše uvedených kvót: Pracovní stanice, servery, Windows Server Essentials, virtuální hostitelé.
- **Mobilní zařízení**
- **Poštovní schránky Office 365**
- **Místní záloha**

Počítač, zařízení nebo poštovní schránka jsou považovány za chráněné, pokud je pro ně použit aspoň jeden plán ochrany. Mobilní zařízení je chráněno po provedení první zálohy.

Při překročení kvóty cloudového úložiště bude zálohování neúspěšné. Pokud dojde k překročení u několika zařízení, nebude uživatel moct použít plán ochrany na více zařízeních.

Kvóty na **místní zálohy** omezují celkovou velikost místních záloh vytvořených pomocí cloudové infrastruktury. Pro tuto kvótu nelze nastavit limit překročení.

Obnovení po havárii

Tyto kvóty používá poskytovatel služeb v rámci celé společnosti. Správce společnosti může tyto kvóty a využití zobrazit v portálu pro správu, ale nemůže nastavit kvóty pro uživatele.

- **Úložiště obnovení po havárii**

  Toto úložiště používají primární servery a servery pro obnovení. V případě dosažení limitu této kvóty není možné vytvořit primární servery a servery pro obnovení nebo přidat/rozšířit disky existujících primárních serverů. V případě překročení limitu této kvóty není možné zahájit převzetí služeb při selhání ani jen spustit zastavený server. Spuštěné servery zůstanou v činnosti.

  V případě vypnutí kvóty se všechny servery odstraní. Karta **Cloudový server pro obnovení** zmizí z webové konzole Cyber Protect.

- **Výpočetní body**

  Tato kvóta omezuje prostředky procesoru a paměti RAM využívané primárními servery a servery pro obnovení v průběhu zúčtovacího období. V případě dosažení limitu této kvóty se všechny primární servery a servery pro obnovení vypnou. Tyto servery nebude možné používat až do začátku příštího zúčtovacího období. Výchozí zúčtovací období je jeden celý kalendářní měsíc.

  Pokud je kvóta vypnutá, nelze servery používat, a to bez ohledu na zúčtovací období.

- **Veřejné IP adresy**

  Tato kvóta omezuje počet veřejných IP adres, které lze přiřadit primárním serverům a serverům pro obnovení. V případě dosažení limitu této kvóty nebude možné povolit veřejné IP adresy pro další servery. Použití veřejné IP adresy můžete u serveru vypnout zrušením zaškrtnutí políčka **Veřejná IP adresa** v nastavení serveru. Potom můžete povolit použití veřejné IP adresy na jiném serveru, která většinou nebude stejná.

  Pokud je kvóta vypnutá, přestanou všechny servery používat veřejné IP adresy, a nebudou tak dostupné z internetu.

- **Cloudové servery**

  Tato kvóta omezuje celkový počet primárních serverů a serverů pro obnovení. V případě dosažení limitu této kvóty není možné vytvořit primární servery ani servery pro obnovení.

  Je-li kvóta vypnutá, budou servery viditelné ve webové konzoli Cyber Protect, ale jediná dostupná operace bude **Odstranit**.

- **Přístup k internetu**

  Tato kvóta zapíná nebo vypíná přístup k internetu z primárních serverů a serverů pro obnovení.

  V případě vypnutí kvóty se primární servery a servery pro obnovení ihned odpojí od internetu. Přepínač **Přístup k internetu** ve vlastnostech serveru nebude vybraný a bude neaktivní.

Upozornění

Chcete-li změnit nastavení upozornění pro některého uživatele, vyberte daného uživatele na kartě **Uživatelé** a potom klikněte na ikonu tužky v oddílu **Nastavení**. K dispozici jsou následující nastavení upozornění:

- **Upozornění na překročení kvót** (ve výchozím nastavení zapnuté)

  Upozornění na překročené kvóty.

- **Naplánované zprávy o využití**

  Zprávy o využití, které jsou popsané níže, se odesílají první den každého měsíce.

- **Upozornění na chyby**, **Upozornění** a **Upozornění na úspěšné dokončení** (ve výchozím nastavení vypnuté)

  Oznámení o výsledcích spuštění plánů ochrany a výsledcích operací obnovení po havárii u každého zařízení.

- **Denní shrnutí aktivních výstrah** (ve výchozím nastavení zapnuto)

  Toto shrnutí informuje o nezdařených zálohách, vynechaných zálohách a dalších potížích. Shrnutí je odesláno v 10:00 (čas datového centra). Pokud to této chvíle nenastaly žádné potíže, shrnutí se neodešle.

Všechna upozornění se odesílají na e-mailovou adresu uživatele.

Zprávy

Zpráva o využití služby kybernetické ochrany obsahuje následující data o organizaci nebo jednotce:

- Velikost záloh podle jednotky, uživatele a typu zařízení.
- Počet chráněných zařízení podle jednotky, uživatele a typu zařízení.
- Cena podle jednotky, uživatele a typu zařízení.
- Celková velikost záloh.
- Celkový počet chráněných zařízení.
- Celková cena.

31 Referenční příručka

Referenční příručka příkazového řádku je samostatný dokument dostupný na stránce Argentina/support/documentation/AcronisCyberBackup_12.5_Command_Line_Reference

32 Odstraňování problémů

Tato část popisuje, jak uložit protokol agenta do souboru .zip. Pokud zálohování selže z nejasného důvodu, tento soubor pomůže personálu technické podpory identifikovat problém.

Jak shromáždit protokoly

1. Proveďte jeden z následujících úkonů:
   - V nabídce **Zařízení** vyberte počítač, ze kterého chcete shromáždit protokoly, a potom klikněte na **Aktivity**.
   - V nabídce **Nastavení** > **Agenti** vyberte počítač, ze kterého chcete shromáždit protokoly, a potom klikněte na **Podrobnosti**.
2. Klikněte na možnost **Shromáždit informace o systému**.
3. Určete umístění, kam se má soubor uložit, pokud k tomu budete webovým prohlížečem vyzváni.

Prohlášení o autorských právech

Technologie patentované Acronis

33 Slovníček

A

Acronis Startup Recovery Manager (ASRM)

Úprava spouštěcího agenta, který se nachází na systémovém disku a je konfigurován, aby se spustil stisknutím klávesy F11 při spouštění. Acronis Startup Recovery Manager odstraňuje potřebu záchranného média nebo síťového připojení ke spuštění záchranného spouštěcího nástroje.

Acronis Startup Recovery Manager je praktický zejména pro mobilní uživatele. Pokud dojde k havárii a restartujete počítač, stiskněte při výzvě „Stisknutím klávesy F11 spustíte Acronis Startup Recovery Manager...“ klávesu F11 a proveďte obnovu dat stejným způsobem jako s běžným spustitelným médiem.

Omezení: Vyžaduje znovu aktivovat zavaděče jiné než zavaděče Windows a GRUB.

J

Jednosouborový formát zálohy

Jedná se o nový formát zálohy, ve kterém se počáteční plná a následující přírůstkové zálohy uloží do jednoho souboru .tib, namísto řetězce souborů. Tento formát využívá rychlosti přírůstkové metody zálohování a vyhýbá se tak své hlavní nevýhodě – obtížnému odstraňování neaktuálních záloh. Software označí bloky použité neaktuálními zálohami jako „volné“ a nové zálohy poté zapisuje do těchto bloků. Výsledkem je velmi rychlé vyčištění s minimální spotřebou zdrojů.

Jednosouborový formát zálohy není dostupný při zálohování do umístění, která nepodporují čtení a zápis s náhodným přístupem, jako jsou například servery SFTP.

P

Plná záloha

Je to samostatná záloha obsahující veškerá data vybraná k zálohování. Pokud chcete obnovit data z plné zálohy, není nutné mít přístup k jiným zálohám.

Přírůstková záloha

Je to záloha, která ukládá změny dat vzhledem k poslední záloze. Pokud chcete obnovit data z přírůstkové zálohy, potřebujete přístup k ostatním zálohám.

R

Rozdílová záloha

Rozdílová záloha ukládá změnu dat vzhledem k poslední plné záloze (str. 451). Pro obnovu dat z rozdílové zálohy potřebujete přístup k odpovídající plné záloze.

S

Sada záloh

Skupina záloh, na kterou je možné použít jednotlivá pravidla zachování.

U schématu zálohování **Vlastní** sady záloh odpovídají metodám zálohování (**Plná**, **Rozdílová** a **Přírůstková**).

Ve všech ostatních případech jsou sady záloh **Měsíčně**, **Denně**, **Týdně** a **Po hodině**.

- Měsíční záloha se vytvoří jako první po začátku měsíce.
- Týdenní záloha se vytvoří jako první v den, který vyberete pomocí možnosti **Týdenní zálohování** (klikněte na ikonu ozubeného kola a poté na možnost **Možnosti zálohování** > **Týdenní zálohování**).

  Pokud se týdenní záloha vytvoří jako první po začátku měsíce, je tato záloha považována za měsíční. V takovém případě bude týdenní záloha vytvořena ve vybraný den příštího týdne.
- Denní záloha je první záloha vytvořená po začátku dne, pokud tato záloha nespadá do definice měsíční nebo týdenní zálohy.
- Hodinová záloha je první záloha vytvořená po začátku hodiny, pokud tato záloha nespadá do definice měsíční, týdenní nebo denní zálohy.

Spravované umístění

Umístění záloh spravované pomocí uzlu úložišť.

Fyzicky se může spravované umístění nacházet ve sdílené síťové složce, SAN, NAS, na místním pevném disku uzlu úložišť nebo v knihovně pásek místně připojené k uzlu úložišť. Uzel úložišť provádí vyčištění a ověřování (pokud jsou součástí plánu ochrany) pro všechny zálohy uložené ve spravovaném úložišti. Můžete určit další operace, které bude uzel úložišť provádět (deduplikaci, šifrování).