Acronis

Acronis Cyber Cloud

Version 9.0

PŘÍRUČKA PRO PARTNERY

Revize: 23.3.2020

Obsah

1 O tomto dokumentu

Tento dokument je určen pro správce partnerů, kteří chtějí používat řešení Acronis Cyber Cloud k poskytování služeb svým klientům.

V tomto dokumentu naleznete informace o tom, jak nastavit a spravovat služby dostupné v řešení Acronis Cyber Cloud.

2 O službě Acronis Cyber Cloud

Acronis Cyber Cloud je cloudová platforma, která poskytovatelům služeb, prodejcům a distributorům umožňuje poskytovat služby ochrany dat jejich partnerům a zákazníkům.

Služba se poskytuje od partnerské úrovně až po úroveň zákaznických společností a koncových uživatelů.

Správa služeb je k dispozici prostřednictvím webových aplikací nazývaných konzole služeb. Správa tenantů a uživatelských účtů je k dispozici prostřednictvím webové aplikace nazývané portál pro správu.

Portál pro správu umožňuje správcům provádět následující činnosti:

- sledovat využití služeb a přístup ke konzolím služeb,
- spravovat tenanty,
- spravovat uživatelské účty,
- konfigurovat služby a kvóty pro tenanty,
- spravovat úložiště,
- spravovat budování značky,
- generovat zprávy o využití služby.

3 Nabízené položky a správa kvót

V této části naleznete odpovědi na následující dotazy:

- Jaké služby jsou k dispozici a co jsou nabídky a nabízené položky?
- Jak lze nabízené položky povolit nebo zakázat?
- Co jsou to měkké a tvrdé kvóty?
- Kdy lze překročit tvrdou kvótu?
- Co je to transformace kvóty pro zálohy?
- Jak ovlivňuje dostupnost nabízených položek dostupnost instalačního programu v konzoli služby?

3.1.1 Služby, nabídky a nabízené položky

Služby

Ve službě Acronis Cyber Cloud jsou k dispozici následující služby:

- **Cyber Protection**
- **File Sync & Share**
- **Cyber Infrastructure SPLA**
- **Cyber Notary Cloud**
- **Odesílání fyzických dat**

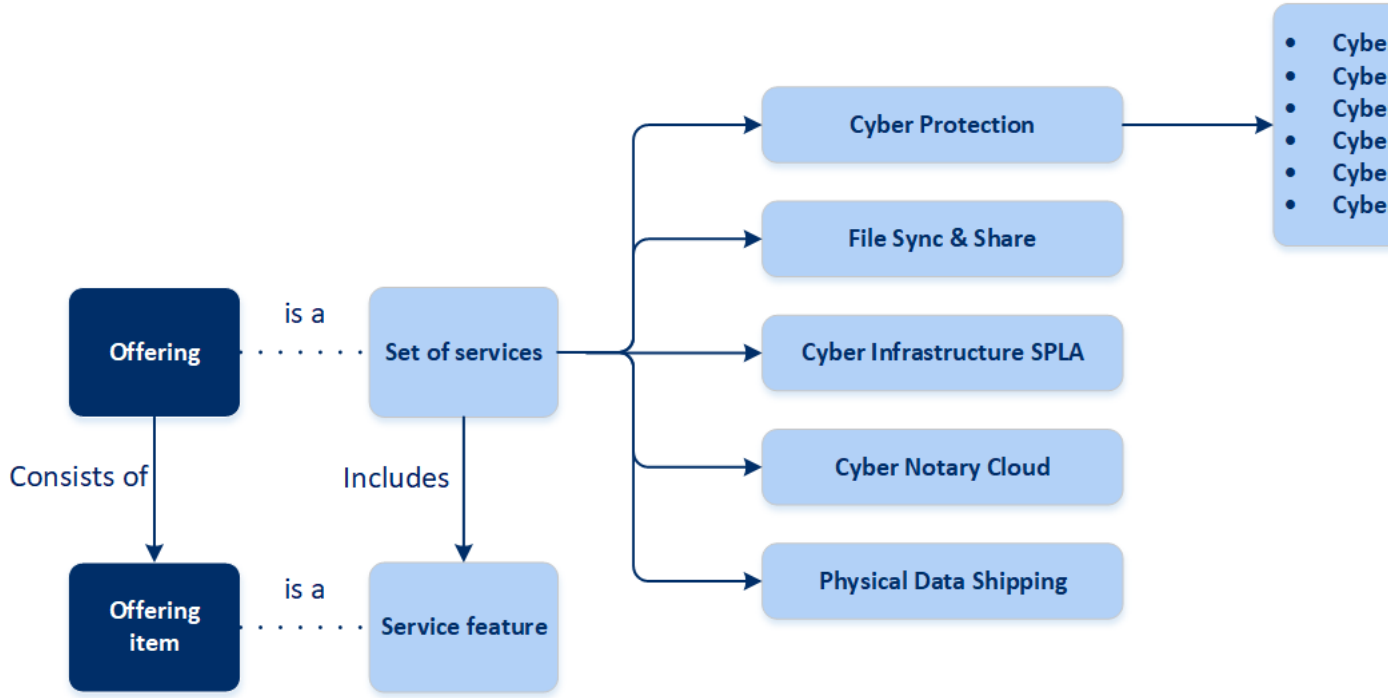
Povolením nebo zakázáním těchto služeb můžete určit, které z nich budou k dispozici vašim partnerům a zákazníkům.

Nabídky a nabízené položky

Acronis Cyber Cloud vám umožňuje připravovat nabídky na míru (sady služeb a různých funkcí nazývaných **nabízené položky**) pro vaše zákazníky a partnery.

Nabídky určují, které služby a funkce budou partnerům, zákazníkům a jejich koncovým uživatelům dostupné na portálu pro správu a v konzolích služeb. Veškeré funkce, které jsou z nabídky vyloučeny, budou skryté.

Abyste mohli dále upřesnit své nabídky, můžete stanovit kvóty pro konkrétní nabízené položky.



Verze služby Cyber Protection

Služba Cyber Protection má šest verzí, které určují funkce poskytované zákazníkům.

Verze	Popis
Cyber Backup – Standard	Poskytuje: ▪ Funkce zálohování a obnovení určené pro potřeby malých prostředí ▪ Posouzení ohrožení zabezpečení, základní vzdálená instalace, základní ochrana proti ransomwaru a těžbě kryptoměn ▪ Základní funkce vzdálené instalace
Cyber Backup – Advanced	Poskytuje: ▪ Funkce zálohování a obnovy sloužící k ochraně pokročilých pracovních úloh, například clustery Microsoft Exchange a Microsoft SQL, pro velká prostředí ▪ Správa skupin a plánů ▪ Posouzení ohrožení zabezpečení, vzdálená instalace, základní ochrana proti ransomwaru a těžbě kryptoměn ▪ Pokročilé funkce vzdálené instalace

Cyber Backup – Disaster Recovery	Poskytuje: ▪ Funkce zálohování a obnovy sloužící k ochraně pokročilých pracovních úloh, například clustery Microsoft Exchange a Microsoft SQL, pro velká prostředí ▪ Správa skupin a plánů ▪ Posouzení ohrožení zabezpečení, základní vzdálená instalace, základní ochrana proti ransomwaru a těžbě kryptoměn ▪ Pokročilé funkce vzdálené instalace ▪ Funkce obnovení po havárii určené pro společnosti, které mají vysoké požadavky na RTO.
Cyber Protect – Standard	Poskytuje: ▪ Funkce zálohování a obnovení určené pro potřeby malých prostředí ▪ Základní funkce vzdálené instalace ▪ Funkce posouzení ohrožení zabezpečení a správy oprav ▪ Pokročilé funkce antimalwarové ochrany a ochrany webu ▪ Funkce vzdálené plochy ▪ Funkce řízení zabezpečení, například správa programu Windows Defender ▪ Výstrahy založené na datech z Centra operací kybernetické ochrany ▪ Funkce zjišťování dat
Cyber Protect – Advanced	Poskytuje: ▪ Funkce zálohování a obnovy sloužící k ochraně pokročilých pracovních úloh, například clustery Microsoft Exchange a Microsoft SQL, pro velká prostředí ▪ Správa skupin a plánů ▪ Pokročilé funkce vzdálené instalace ▪ Funkce posouzení ohrožení zabezpečení a správy oprav ▪ Pokročilé funkce antimalwarové ochrany a ochrany webu ▪ Funkce vzdálené plochy ▪ Funkce řízení zabezpečení, například správa programu Windows Defender ▪ Výstrahy založené na datech z Centra operací kybernetické ochrany ▪ Funkce zjišťování dat

Cyber Protect – Disaster Recovery	Poskytuje: ▪ Funkce zálohování a obnovy sloužící k ochraně pokročilých pracovních úloh, například clustery Microsoft Exchange a Microsoft SQL, pro velká prostředí ▪ Správa skupin a plánů ▪ Pokročilé funkce vzdálené instalace ▪ Funkce posouzení ohrožení zabezpečení a správy oprav ▪ Pokročilé funkce antimalwarové ochrany a ochrany webu ▪ Funkce vzdálené plochy ▪ Funkce řízení zabezpečení, například správa programu Windows Defender ▪ Výstrahy založené na datech z Centra operací kybernetické ochrany ▪ Funkce zjišťování dat ▪ Funkce obnovení po havárii určené pro společnosti, které mají vysoké požadavky na RTO.

Verze umožňuje rozlišit nabídky ochrany dat pro vaše partnery a zákazníky a poskytovat funkce ochrany dat, které odpovídají jejich potřebám a rozpočtům.

Při vytváření partnera můžete povolením nebo zakázáním verze rozhodnout, která z verzí mu bude k dispozici. Každou verzi lze upravit konfigurací nabízených položek.

Můžete přiřadit jednu verzi na zákazníka. Později můžete na požádání přiřadit zákazníkům jinou verzi.

3.1.2 Správa verzí služby Cyber Protection pro partnery

Vypnutí verzí pro tenanty typu partner

Chcete-li vypnout verzi u tenanta typu partner, přejděte na kartu **Klienti** > **<konkrétní_partner>** > **Konfigurace** a zrušte výběr verze. Chcete-li toto vypnutí potvrdit, zadejte své přihlašovací údaje.

Vypnutí verze Cyber Backup – Disaster Recovery

Pro tohoto tenanta a jeho podřízené tenanty, kteří měli verzi Cyber Backup – Disaster Recovery, budou platit následující změny:

- Verze Cyber Backup – Disaster Recovery již nebude k dispozici.
- Všechny plány ochrany budou odvolány, registrace všech zařízení budou zrušeny a jejich zálohy budou odstraněny.
- Funkce Obnovení po havárii bude nedostupná: všechny servery pro obnovení, primární servery a síťové konfigurace funkce obnovení po havárii budou odstraněny. Zruší se registrace zařízení VPN; z cloudových serverů budou odvolány veřejné IP adresy a servery nebudou dostupné z internetu.

Vypnutí verze Cyber Backup – Advanced/Standard

Pro tohoto tenanta a jeho podřízené tenanty, kteří měli verzi Cyber Backup – Advanced/Standard, budou platit následující změny:

- Verze Cyber Backup – Advanced/Standard již nebude k dispozici.
- Všechny plány ochrany budou odvolány, registrace všech zařízení budou zrušeny a jejich zálohy budou odstraněny.

Vypnutí verze Cyber Protect – Disaster Recovery

Pro tohoto tenanta a jeho podřízené tenanty, kteří měli verzi Cyber Protect – Disaster Recovery, budou platit následující změny:

- Verze Cyber Protect – Disaster Recovery již nebude k dispozici.
- Všechny plány ochrany budou odvolány, registrace všech zařízení budou zrušeny a jejich zálohy budou odstraněny.
- Všechny funkce Cyber Protect budou zakázány.
- Funkce Obnovení po havárii bude nedostupná: všechny servery pro obnovení, primární servery a síťové konfigurace funkce obnovení po havárii budou odstraněny. Zruší se registrace zařízení VPN; z cloudových serverů budou odvolány veřejné IP adresy a servery nebudou dostupné z internetu.

Vypnutí verze Cyber Protect – Advanced/Standard

Pro tohoto tenanta a jeho podřízené tenanty, kteří měli verzi Cyber Protect – Advanced/Standard, budou platit následující změny:

- Verze Cyber Protect – Advanced/Standard již nebude k dispozici.
- Všechny plány ochrany budou odvolány, registrace všech zařízení budou zrušeny a jejich zálohy budou odstraněny.
- Všechny funkce Cyber Protect budou zakázány.

3.1.3 Přepnutí verzí služby Cyber Protection pro zákazníky

Upgradování verzí pro tenanty typu zákazník

Chcete-li upgradovat verzi u tenanta typu zákazník, přejděte na kartu **Klienti** > **<konkrétní_klient>** > **Konfigurace** a přepněte verzi. Upgrade verze může trvat až 10 minut.

<Aktuální> verze > <cílová> verze

Pro vybraného tenanta a jeho podřízené tenanty budou platit následující změny:

- Začnou být dostupné funkce <cílové> verze.
- Všechny plány ochrany, které používají funkce <aktuální> verze, budou dále funkční.
- Všechna registrovaná zařízení a jejich zálohy zůstanou zachovány.
- Statistiky využití a kvóty budou přeneseny do souvisejících nabízených položek <cílové> verze na portálu pro správu a ve zprávě o využití. Historické statistiky využití budou zachovány.

Downgradování verzí pro tenanty typu zákazník

Downgrade verze může trvat až 10 minut. Chcete-li tento downgrade potvrdit, zadejte své přihlašovací údaje.

Verze Advanced > verze Standard

Pro vybraného tenanta a jeho podřízené tenanty budou platit následující změny:

- Funkce verze Cyber Backup – Advanced již nebudou k dispozici.
- Všechny plány ochrany, které používají funkce verze Cyber Backup – Advanced, již nebudou aktivní.
- Všechna registrovaná zařízení a jejich zálohy zůstanou zachovány.

- Statistiky využití a kvóty budou migrovány do souvisejících nabízených položek verze Cyber Backup – Standard na portálu pro správu a do zprávy o využití. Historické statistiky využití budou zachovány.

Verze Disaster Recovery > verze Advanced/Standard

Pro vybraného tenanta a jeho podřízené tenanty budou platit následující změny:

- Funkce verze Cyber Backup – Disaster Recovery již nebudou k dispozici.
- Všechny plány ochrany, které používají funkce Cyber Backup – Disaster Recovery, již nebudou aktivní.
- Všechna registrovaná zařízení a jejich zálohy zůstanou zachovány.
- Všechny servery pro obnovení, primární servery a jejich zálohy zůstanou zachovány.
- Všechny síťové konfigurace funkce obnovení po havárii zůstanou zachovány.
- Registrace zařízení VPN zůstanou zachovány.
- Statistiky využití a kvóty budou migrovány do souvisejících nabízených položek verze Cyber Backup – Advanced/Standard na portálu pro správu a do zprávy o využití. Historické statistiky využití budou zachovány.

Verze Cyber Protect > verze Cyber Backup

Pro vybraného tenanta a jeho podřízené tenanty budou platit následující změny:

- Funkce verze Cyber Protect již nebudou k dispozici.
- Zbývající změny jsou popsány v tomto článku výše v závislosti na tom, mezi jakými verzemi přecházíte.

3.1.4 Povolení nebo zakázání nabízených položek

Informace o tom, jak pro tenanta povolit nebo zakázat nabízené položky, naleznete v tématu Vytvoření tenanta (str. 22).

V tabulce níže jsou uvedeny možnosti zakázání nabízených položek a výsledky těchto akcí.

Nabízená položka	Zakázání	Výsledek
Úložiště záloh	Lze zakázat, když se využití rovná nule.	Cloudové úložiště nebude dostupné jako cíl záloh v rámci tenanta zákazníka.
Místní záloha	Lze zakázat, když se využití rovná nule.	Místní úložiště nebude dostupné jako cíl záloh v rámci tenanta zákazníka.
Zdroje dat (včetně Office 365 a G Suite)	Lze zakázat, když se využití rovná nule.	Zdroje dat pro zálohování a obnovení (včetně Office 365 a G Suite) nebudou dostupné v rámci tenanta zákazníka.
Všechny nabízené položky služby Obnovení po havárii	Lze zakázat, když je využití vyšší než nula.	Podrobnosti naleznete v tématu Měkké a tvrdé kvóty (str. 11).
Všechny nabízené položky služby Notary	Lze zakázat, když se využití rovná nule.	Služba Notary nebude dostupná v rámci tenanta zákazníka.

Všechny nabízené položky služby File Sync & Share	Nabízené položky nelze povolit nebo zakázat samostatně.	Služba File Sync & Share bude pro tenanta zákazníka nedostupná.
Všechny nabízené položky služby Odesílání fyzických dat	Lze zakázat, když se využití rovná nule.	Služba Odesílání fyzických dat nebude dostupná v rámci tenanta zákazníka.

U nabízené položky, kterou nelze zakázat, když je její využití vyšší než nula, můžete ručně odebrat využití a poté odpovídající nabízenou položku zakázat.

3.1.5 Měkké a tvrdé kvóty

Kvóty vám umožňují omezit, jak tenant může využívat danou službu. Kvóty nastavíte tak, že vyberete klienta na kartě **Klienti**, vyberete kartu služby a potom kliknete **Upravit**.

Pokud je kvóta překročena, odešle se upozornění na e-mailovou adresu uživatele. Pokud nenastavíte překročení kvóty, bude kvóta považována za **měkkou**. To znamená, že se neuplatní omezení na používání služby Cyber Protection.

Když nastavíte překročení kvóty, bude kvóta považována za **tvrdou**. **Limit překročení** umožňuje uživateli překročit kvótu o zadanou hodnotu. Po překročení této hodnoty jsou použita omezení pro využívání příslušné služby.

Příklad

Měkká kvóta: Nastavili jste kvótu pro pracovní stanice na hodnotu 20. Když počet chráněných pracovních stanic zákazníka dosáhne 20, obdrží zákazník oznámení e-mailem, ale služba Cyber Protection bude dále k dispozici.

Tvrdá kvóta: Pokud jste nastavili kvótu pro pracovní stanice na hodnotu 20 a limit překročení na hodnotu 5, potom zákazník obdrží oznámení e-mailem, když počet chráněných pracovních stanic uživatele dosáhne 20, a služba Cyber Protection bude zakázána při dosažení hodnoty 25.

Úrovně, na kterých lze definovat kvóty

Kvóty lze nastavit na úrovních uvedených v následující tabulce.

Tenant/Uživatel	Měkká kvóta (pouze kvóta)	Tvrdá kvóta (kvóta a limit překročení)
Partner	ano	ne
Složka	ano	ne
Zákazník	ano	ano
Jednotka	ne	ne
Uživatel	ano	ano

Měkké kvóty lze nastavit na úrovních partnera a složky. Na úrovni jednotky nelze nastavit žádné kvóty. Tvrdé kvóty lze nastavit na úrovních zákazníka a uživatele.

Celkové množství tvrdých kvót, které jsou nastaveny na úrovni uživatele, nesmí překročit související tvrdou kvótu zákazníka.

3.1.5.1 Kvóty pro zálohy

Můžete zadat kvótu cloudového úložiště, kvótu pro místní zálohy a maximální počet počítačů, zařízení, nebo webových stránek, které může uživatel chránit. Jsou k dispozici následující kvóty.

Kvóty na zařízení

- **Pracovní stanice**
- **Servery**
- **Virtuální počítače**
- **Mobilní zařízení**
- **Webhostingové servery**
- **Webové stránky**

Počítač, zařízení nebo web se považují za chráněné, pokud používají aspoň jeden plán ochrany. Mobilní zařízení je chráněno po provedení první zálohy.

Pokud dojde k překročení u několika zařízení, nebude uživatel moct použít plán ochrany na více zařízeních.

Kvóty na cloudové zdroje dat

- **Licence Office 365**

  Tuto kvótu použije poskytovatel služby na celou společnost. Společnost může chránit soubory v **poštovních schránkách**, **soubory na OneDrivu** nebo oboje. Správci společnosti si mohou tuto kvótu a její využití prohlédnout na portálu pro správu, ale nemohou ji nastavit uživateli.

- **Office 365 SharePoint Online**

  Tuto kvótu použije poskytovatel služby na celou společnost. Tato kvóta zapíná nebo vypíná možnost ochrany webů SharePoint Online. Pokud je tato kvóta povolena, může být chráněn jakýkoli počet webů SharePoint Online. Správci společnosti si nemohou tuto kvótu prohlédnout na portálu pro správu, ale mohou ve zprávě o využití zobrazit velikost úložiště obsazenou zálohami SharePoint Online.

  Zálohování serverů SharePoint Online je k dispozici pouze pro zákazníky, kteří mají alespoň jednu další kvótu licencí Office 365. Tato kvóta je pouze ověřena a nebude využívána.

- **Počet licencí G Suite**

  Tuto kvótu použije poskytovatel služby na celou společnost. Společnost může chránit soubory v poštovních schránkách **Gmail** (včetně kalendáře a kontaktů), soubory **OneDrive** nebo oboje. Správci společnosti si mohou tuto kvótu a její využití prohlédnout na portálu pro správu, ale nemohou ji nastavit uživateli.

- **Sdílená jednotka G Suite**

  Tuto kvótu použije poskytovatel služby na celou společnost. Tato kvóta zapíná nebo vypíná možnost ochrany sdílených jednotek G Suite. Pokud je tato kvóta povolena, může být chráněn jakýkoli počet sdílených jednotek. Správci společnosti si nemohou tuto kvótu prohlédnout na portálu pro správu, ale mohou ve zprávě o využití zobrazit velikost úložiště obsazenou zálohami sdílených jednotek.

  Zálohování sdílených jednotek G Suite je k dispozici pouze pro zákazníky, kteří mají alespoň jednu další kvótu licencí G Suite. Tato kvóta je pouze ověřena a nebude využívána.

Licence Office 365 se považuje za chráněnou, pokud poštovní schránka uživatele nebo jeho OneDrive používají aspoň jeden plán ochrany. Licence G Suite se považuje za chráněnou, pokud poštovní schránka uživatele nebo jeho Disk Google používají aspoň jeden plán ochrany.

Pokud dojde k překročení u několika licencí, nebude správce společnosti moct použít plán ochrany u více licencí.

Kvóta na úložiště

- **Místní záloha**

  Kvóty na **místní zálohy** omezují celkovou velikost místních záloh vytvořených pomocí cloudové infrastruktury. Pro tuto kvótu nelze nastavit limit překročení.

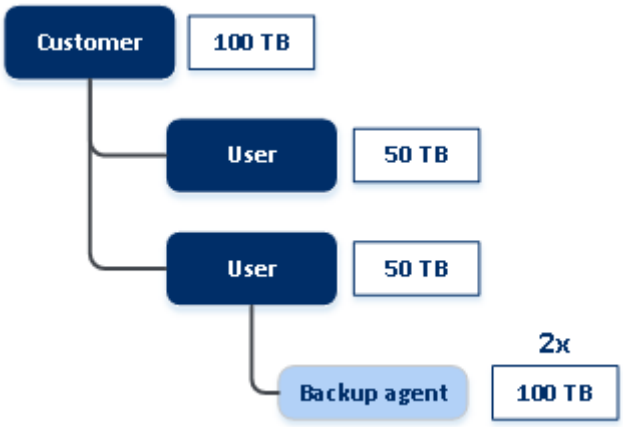
- **Cloudové zdroje**

Kvóta na **Cloudové zdroje** se skládá z kvóty na úložiště záloh a kvót na obnovení po havárii. Kvóta na úložiště záloh omezuje celkovou velikost záloh umístěných v cloudovém úložišti. Při překročení kvóty na úložiště záloh se nezdaří zálohování.

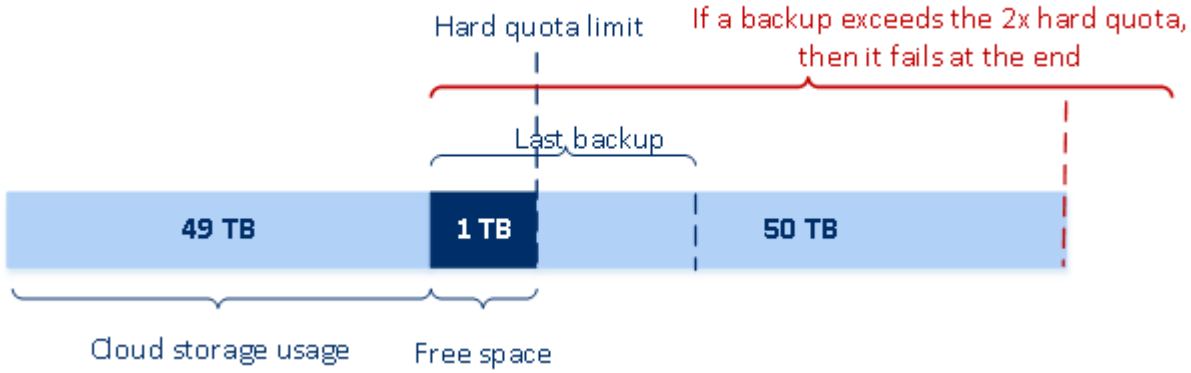
Překročení tvrdé kvóty pro úložiště záloh

U úložiště záloh může být jeho tvrdá kvóta překročena ve výši dvojnásobku definované tvrdé kvóty. Certifikát agenta ochrany má k dispozici dvojnásobek technické kvóty, což agentovi umožňuje překročit tvrdou kvótu tenanta, pokud ještě není dosažena během probíhajícího zálohování. Pokud bude kvóta tenanta překročena, další zálohu nebude možné zahájit. Pokud je během vytváření zálohy dosaženo dvojnásobku hodnoty kvóty (v certifikátu), záloha se nezdaří.

Příklad: Pro tenanta zákazníka jste definovali tvrdou kvótu cloudového úložiště ve výši 100 TB. To znamená, že celkový součet tvrdých kvót přidělených uživatelům tenanta nesmí překročit 100 TB. Rozhodli jste se tuto tvrdou kvótu rovnoměrně rozdělit mezi dva uživatele. Technicky vzato tak má agent každého uživatele k dispozici technickou kvótu 100 TB. Neznamená to však, že agent může zálohovat počítače, dokud není dosaženo všech 100 TB. Znamená to pouze, že pokud je tvrdá kvóta téměř dosažena při zahájení vytváření zálohy, bude záloha dokončena, pokud není její velikost příliš velká, aby nestačil dvojnásobek tvrdé kvóty.



Ve schématu níže má uživatel 1 TB volného místa, ale velikost zálohy je větší, například 3 TB. V tomto případě bude záloha úspěšně dokončena, i když limit tvrdé kvóty cloudového úložiště je překročen o 2 TB. Pokud by velikost zálohy byla 53 TB, pak by se sice zahájilo vytváření zálohy, ale po dosažení limitu cloudového úložiště (100 TB) by zálohování selhalo.



Transformace kvóty pro zálohy

Získávání kvóty pro zálohu a mapování nabízené položky k typu zdroje obecně funguje následovně: systém porovná dostupné nabízené položky s typem zdroje a poté získá kvótu pro odpovídající nabízenou položku.

Existuje však také možnost přiřadit k nabízené položce další kvótu, i když se přesně neshoduje s typem zdroje. Tento způsob se nazývá **transformace kvóty pro zálohy**. Pokud neexistuje žádná odpovídající nabízená položka, systém se pokusí najít nákladnější vhodnou kvótu pro typ zdroje (automatická transformace kvóty pro zálohy). Pokud není nalezena žádná vhodná kvóta, můžete ručně přiřadit kvótu služby k typu zdroje v konzoli služby.

Příklad

Chcete zálohovat virtuální počítač (pracovní stanice, s agentem).

Systém nejprve ověří, zda je přiřazena kvóta pro **virtuální počítače**. Pokud není tato kvóta nalezena, pokusí se systém automaticky získat kvótu pro **pracovní stanice**. Není-li nalezena ani tato kvóta, nebude automaticky získána žádná jiná kvóta. Pokud máte dostatek kvóty, která je cenově nákladnější než kvóta pro **virtuální počítače** a je použitelná pro virtuální počítač, můžete se přihlásit ke konzoli služby a ručně přiřadit kvótu pro **servery**.

3.1.5.2 Kvóty služby Obnovení po havárii

Poznámka *Nabízené položky služby Obnovení po havárii jsou dostupné pouze ve verzích s funkcí 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.
- **Výpočetní body**

Tato kvóta omezuje prostředky procesoru a paměti RAM využívané primárními servery a servery pro obnovení v průběhu zúčtovacího období. V případě dosažení limitu této kvóty se všechny primární servery a servery pro obnovení vypnou. Tyto servery nebude možné používat až do začátku příštího zúčtovacího období. Výchozí zúčtovací období je jeden celý kalendářní měsíc.

Pokud je kvóta vypnutá, nelze servery používat, a to bez ohledu na zúčtovací období.

- **Veřejné IP adresy**

  Tato kvóta omezuje počet veřejných IP adres, které lze přiřadit primárním serverům a serverům pro obnovení. V případě dosažení limitu této kvóty nebude možné povolit veřejné IP adresy pro další servery. Použití veřejné IP adresy můžete u serveru vypnout zrušením zaškrtnutí políčka **Veřejná IP adresa** v nastavení serveru. Potom můžete povolit použití veřejné IP adresy na jiném serveru, která většinou nebude stejná.

  Pokud je kvóta vypnutá, přestanou všechny servery používat veřejné IP adresy, a nebudou tak dostupné z internetu.

- **Cloudové servery**

  Tato kvóta omezuje celkový počet primárních serverů a serverů pro obnovení. V případě dosažení limitu této kvóty není možné vytvořit primární servery ani servery pro obnovení.

  Je-li kvóta vypnutá, budou servery viditelné v konzoli služby, ale jediná dostupná operace bude **Odstranit**.

- **Přístup k internetu**

  Tato kvóta zapíná nebo vypíná přístup k internetu z primárních serverů a serverů pro obnovení.

  Pokud je kvóta vypnutá, primární servery a servery pro obnovení nebudou moci navázat připojení k internetu.

3.1.5.3 Kvóty služby Synchronizace a sdílení souborů

Můžete definovat následující kvóty služby Synchronizace a sdílení souborů pro tenanta:

- **Uživatelé**

  Tato kvóta definuje počet uživatelů, kteří mají přístup k příslušné službě.

- **Cloudové úložiště**

  Cloudové úložiště sloužící k ukládání souborů uživatelů. Kvóta definuje místo přidělené tenantovi v cloudovém úložišti.

3.1.5.4 Kvóty služby Odesílání fyzických dat

Kvóty služby Odesílání fyzických dat jsou spotřebovány na základě počtu diskových jednotek. Počáteční zálohy více počítačů můžete ukládat na jeden disk.

Můžete definovat následující kvóty služby Odesílání fyzických dat pro tenanta:

- **Do cloudu**

  Umožňuje odeslání počáteční zálohy do cloudového datového centra na pevném disku. Tato kvóta definuje maximální počet disků, které lze přenést do cloudového datového centra.

3.1.5.5 Kvóty notarizace

Můžete definovat následující kvóty notarizace pro tenanta:

- **Notarizační úložiště**

Notarizační úložiště je cloudové úložiště, kde jsou uloženy notarizované soubory, podepsané soubory a soubory, u kterých probíhá proces notarizace nebo podepisování. Tato kvóta definuje maximální prostor, který mohou tyto soubory obsadit.

Chcete-li snížit využití této kvóty, můžete z notarizačního úložiště odstranit již notarizované nebo podepsané soubory.

- **Notarizace**

  Tato kvóta definuje maximální počet souborů, které lze notarizovat pomocí notarizační služby. Soubor je považován za notarizovaný, jakmile je nahrán do notarizačního úložiště a jeho stav notarizace se změní na Probíhá.

  Pokud je stejný soubor notarizován vícekrát, každá notarizace se počítá jako nová.

- **Elektronické podpisy**

  Tato kvóta definuje maximální počet souborů, které lze podepsat pomocí notarizační služby. Soubor je považován za podepsaný, jakmile je odeslán k podpisu.

3.1.6 Závislost instalačního programu agenta na nabízených položkách

V závislosti na povolených nabízených položkách bude v konzoli služby v části **Přidat zařízení** k dispozici odpovídající instalační program agenta. V tabulce níže si můžete prohlédnout instalační programy agentů a jejich dostupnost v konzoli služby v závislosti na povolených nabízených položkách.

Povolená nabízená položka / **Instalační program agenta**	**Servery**	**Pracovní stanice**	**Virtuální počítače**	**Licence Office 365**	**Počet licencí G Suite**	**Mobilní zařízení**	**Webhostingové servery**	**Webové stránky**
Pracovní stanice – Agent pro Windows		+	+					+
Pracovní stanice – Agent pro Mac		+	+					+
Servery – Agent pro Windows	+		+				+	+
Servery – Agent pro Linux	+		+				+	+
Agent pro Hyper-V			+					
Agent pro VMware			+					
Agent pro Virtuozzo			+					
Agent pro SQL	+		+					
Agent pro Exchange	+		+					

Agent pro Active Directory	+		+					
Agent pro Office 365				+				
Agent pro G Suite					+			
Úplný instalační program pro Windows	+	+	+				+	+
Mobilní zařízení (iOS a Android)						+		

3.2 Uživatelské účty a tenanty

Existují dva typy uživatelských účtů: účty správců a uživatelské účty.

- **Správci** mají přístup k portálu pro správu Mají roli správce ve všech službách.
- **Uživatelé** nemají přístup k portálu pro správu Přístup uživatelů ke službám a jejich roli ve službách definuje správce.

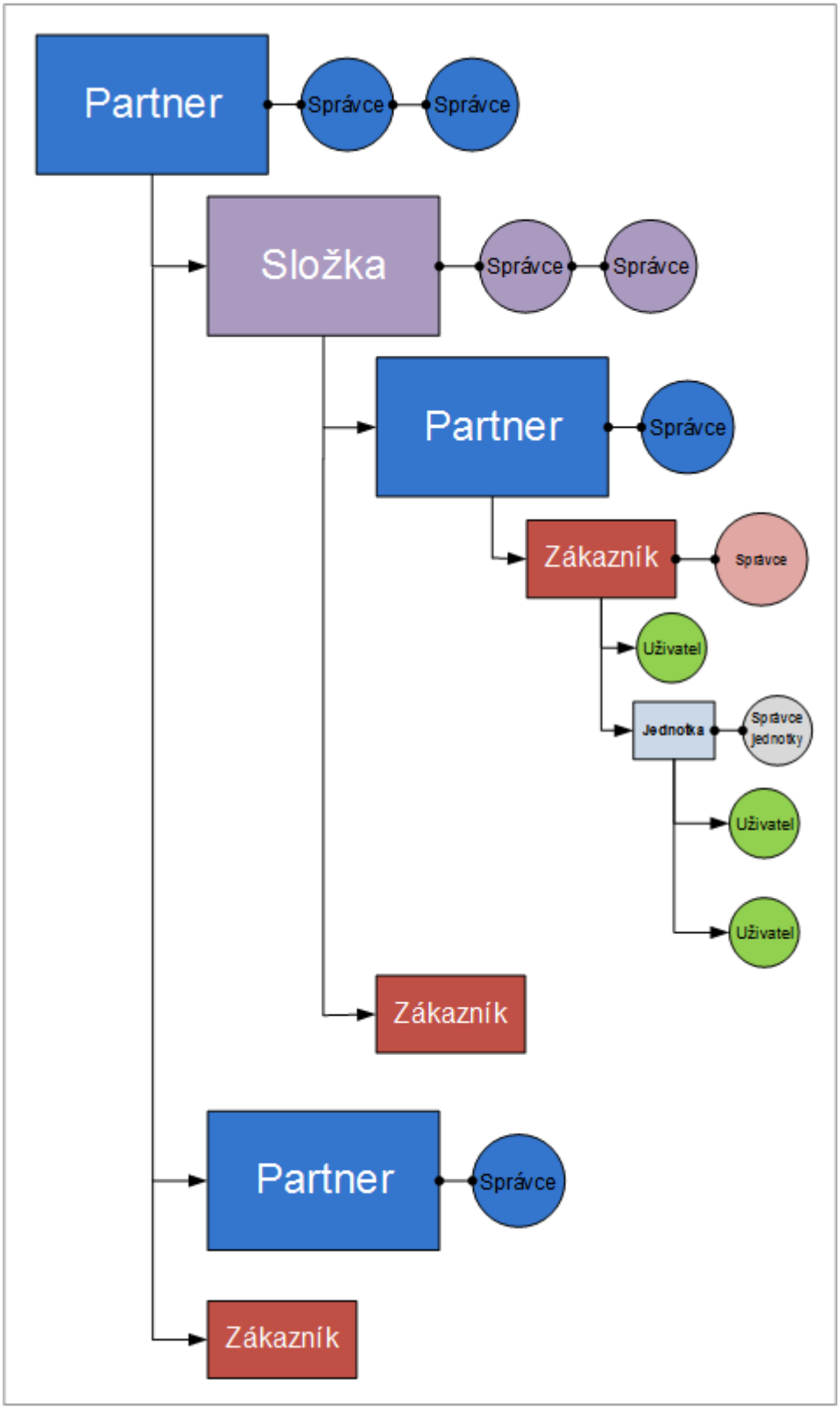
Každý účet náleží do nějakého tenantu. Tenant je součástí prostředků portálu pro správu (podobně jako uživatelské účty a podřízené tenanty) a nabídky služeb (povolené služby a jejich nabízené položky) vyhrazených pro partnera nebo zákazníka. Hierarchie tenanta by se měla shodovat se vztahy klient/prodejce mezi uživateli služby a poskytovateli.

- Tenant typu **Partner** typicky odpovídá poskytovatelům služeb, kteří prodávají služby.
- Tenant typu **Složka** je podpůrný tenant, který je obvykle používán správci partnerů k seskupení partnerů a zákazníků kvůli konfiguraci rozdílných nabídek nebo různých značek.
- Tenant typu **Zákazník** typicky odpovídá organizacím používajícím službu.
- Tenant typu **Jednotka** typicky odpovídá jednotkám nebo oddělením v rámci organizace.

Správce může vytvářet a spravovat tenanty, účty správců a uživatelské účty na jejich úrovni hierarchie nebo nižší.

Správci na úrovni zákazníka a vyšší mohou správcům vyšší úrovně omezit přístup ke svým tenantům (str. 62).

Následující diagram ukazuje úrovně hierarchie – tenanty partnerů, složek, zákazníků a jednotek.



Následující tabulka shrnuje operace, které mohou správci nebo uživatelé provést.

Operace	Uživatelé	Správci zákazníka a jednotek	Správci partnerů a složek

Operace	Uživatelé	Správci zákazníka a jednotek	Správci partnerů a složek
Tvorba tenantů	Ne	Ano	Ano
Tvorba účtů	Ne	Ano	Ano
Stahování a instalace softwaru	Ano	Ano	Ne*
Správa služeb	Ano	Ano	Ano
Tvorba zpráv o využití služby	Ne	Ano	Ano
Konfigurace značky	Ne	Ne	Ano

*Správce partnerů, které potřebuje provést tyto operace, si může pro sebe vytvořit účet správce zákazníka nebo uživatelský účet.

3.3 Podporované prohlížeče

Webové rozhraní podporuje následující prohlížeče:

- Google Chrome 29 nebo novější,
- Mozilla Firefox 23 nebo novější,
- Opera 16 nebo novější,
- Windows 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.

4 Používání portálu pro správu

V následujících krocích se seznámíte se základy používání portálu pro správu.

4.1 Aktivace účtu správce

Po podepsání partnerské smlouvy obdržíte e-mail obsahující následující informace:

- **Odkaz pro aktivaci účtu**. Klikněte na odkaz a nastavte heslo účtu správce. Zapamatujte si své přihlašovací jméno, které se zobrazuje na stránce aktivace účtu.
- **Odkaz na stránku pro přihlášení**. Přihlašovací jméno a heslo jsou stejné jako v předchozím kroku.

4.2 Přístup k portálu pro správu

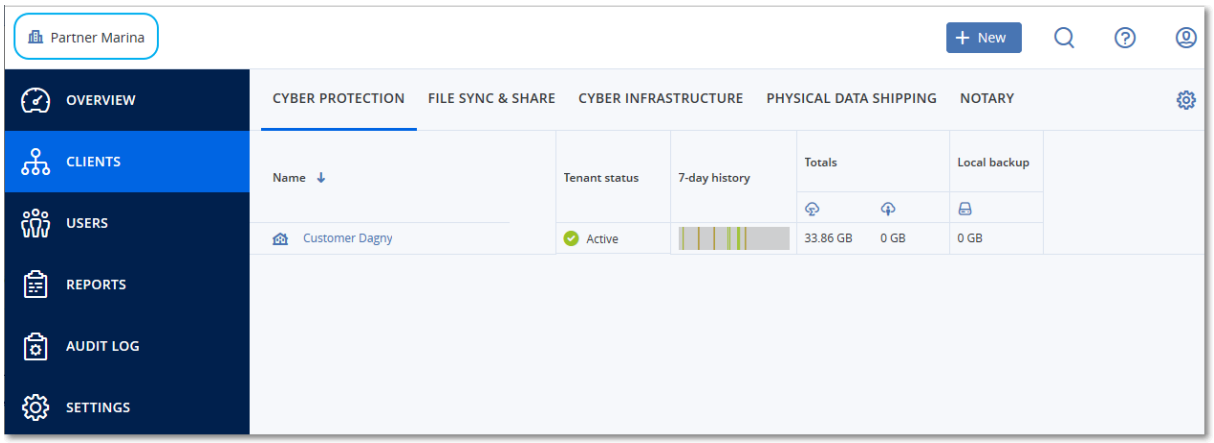
1. Přejděte na přihlašovací stránku služby. Adresa přihlašovací stránky je uvedena v aktivačním e-mailu.
2. Zadejte přihlašovací jméno a klikněte na tlačítko **Další**.
3. Zadejte heslo a klikněte na tlačítko **Další**.
4. Klikněte na možnost **Portál pro správu**.

U některých služeb lze přepnout do portálu pro správu z konzoly služby.

4.3 Navigace na portálu pro správu

Při používání portálu pro správu v kterémkoli okamžiku pracujete v rámci některého tenantu. To je označeno v levém horním rohu.

Ve výchozím nastavení je vybrán tenant nejvyšší dostupné úrovně. Kliknutím na název tenanta přejdete na nižší úroveň v hierarchii. Pro přechod zpět na vyšší úroveň klikněte na její název v levém horním rohu.



Všechny části uživatelského rozhraní zobrazují a ovlivňují pouze tenanta, ve kterém právě pracujete. Například:

- Karta **Klienti** zobrazuje pouze tenanty, které jsou přímo podřízeny tenantu, ve kterém právě pracujete.
- Karta **Uživatelé** zobrazuje pouze uživatelské účty, které existují v tenantu, ve kterém právě pracujete.
- Pomocí tlačítka **Nový** můžete vytvořit tenanta nebo nový uživatelský účet pouze v tenantu, ve kterém právě pracujete.

4.4 Přístup ke službě

Karta Přehled

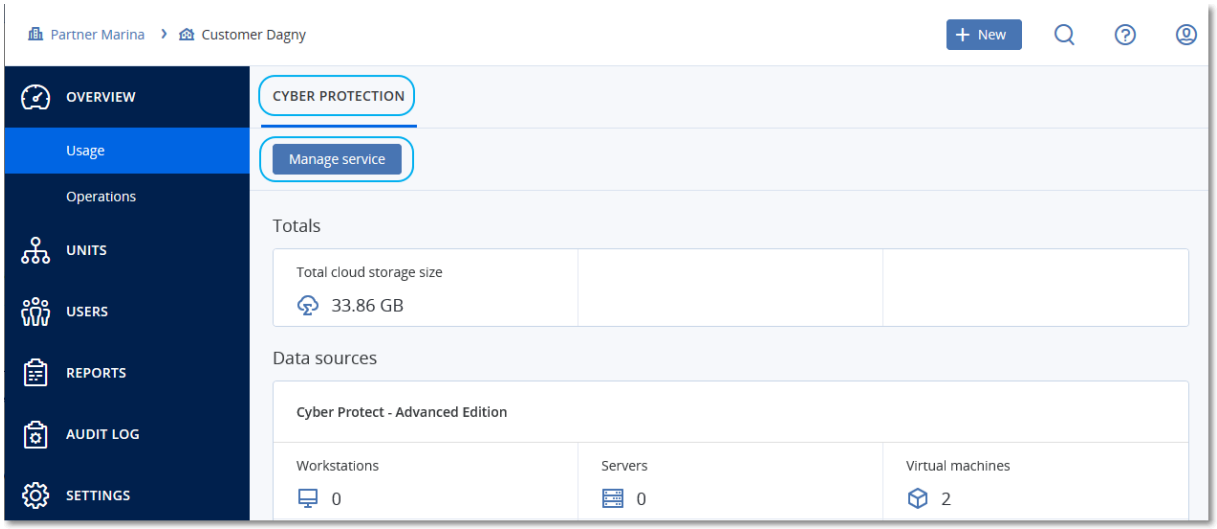
Část **Přehled** > **Použití** poskytuje přehledné informace o využívání služby a umožňuje přístup ke službám v rámci tenanta, ve kterém pracujete.

Správa služby pro tenanta na kartě Přehled

1. Přejděte do tenanta (str. 20), pro kterého chcete spravovat služby, a poté klikněte na možnost **Přehled** > **Použití**.

   Všimněte si, že některé služby lze spravovat na úrovních tenanta partnera a tenanta zákazníka, zatímco jiné služby lze spravovat na pouze úrovni tenanta zákazníka.
2. Klikněte na název služby, kterou chcete spravovat, a pak klikněte na **Spravovat službu** nebo **Konfigurovat službu**.

Další informace o používání služeb naleznete v uživatelských příručkách dostupných v konzolích příslušných služeb.

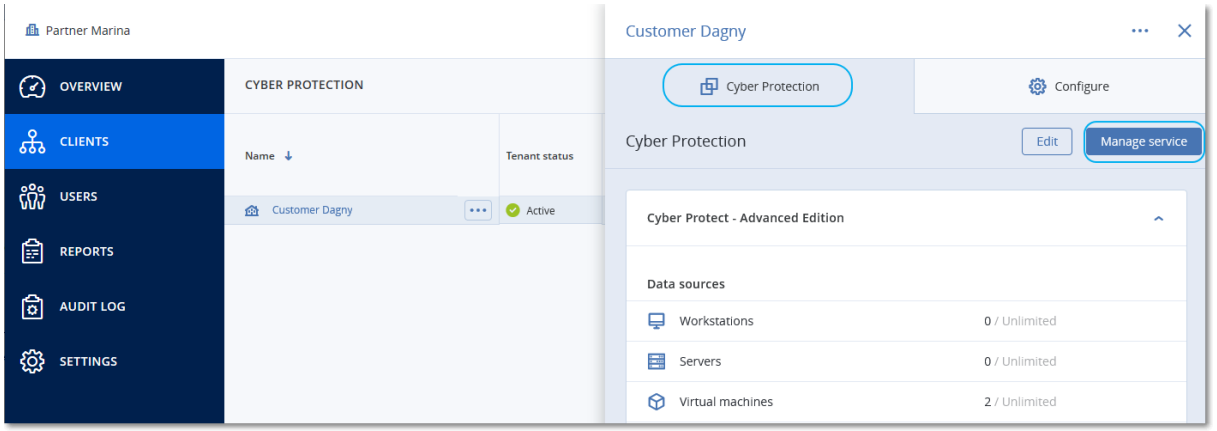


Karta Klienti

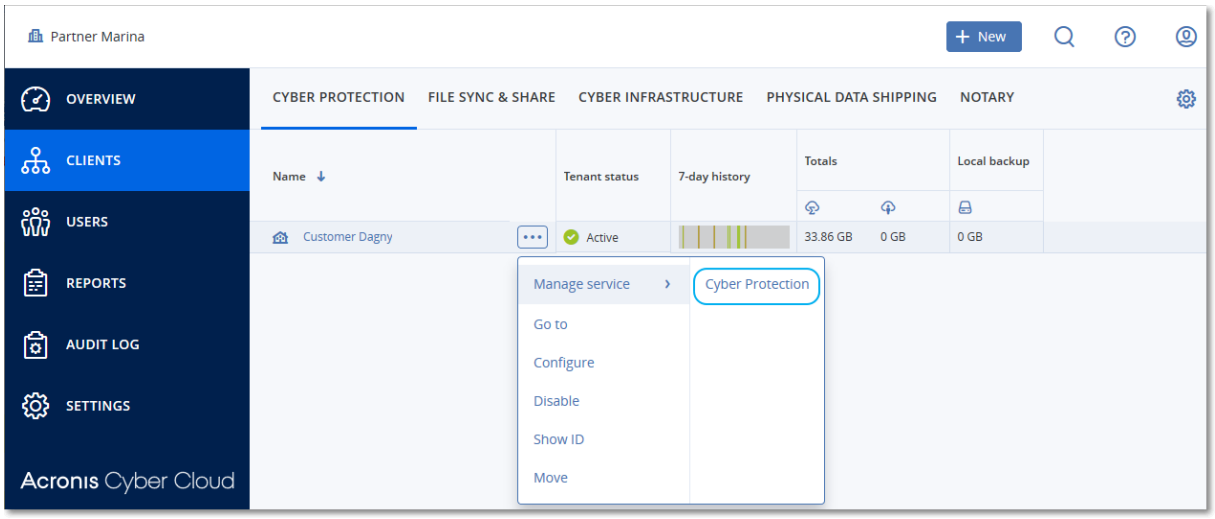
Karta **Klienti** zobrazuje podřízené tenanty pro tenanta, ve kterém pracujete, a umožňuje přístup k jejich službám.

Správa služby pro tenanta na kartě Klienti

1. Proveďte jeden z následujících úkonů:
   - Kliknutím na **Klienti** vyberte tenanta, pro kterého chcete službu spravovat, klikněte na název nebo ikonu služby, kterou chcete spravovat, a pak klikněte na **Spravovat službu** nebo **Konfigurovat službu**.



- Klikněte na **Klienti**, klikněte na ikonu se třemi tečkami vedle názvu tenanta, pro kterého chcete službu spravovat, klikněte na **Spravovat službu** a vyberte službu, kterou chcete spravovat.



Všimněte si, že některé služby lze spravovat na úrovních tenanta partnera a tenanta zákazníka, zatímco jiné služby lze spravovat na pouze úrovni tenanta zákazníka.

Další informace o používání služeb naleznete v uživatelských příručkách dostupných v konzolích příslušných služeb.

4.5 Vytvoření tenanta

Tenant typu **Partner** se obvykle vytváří pro každého partnera, který podepíše dohodu o partnerství.

Tenant typu **Složka** se obvykle vytváří kvůli seskupení partnerů a zákazníků za účelem konfigurace rozdílných nabídek nebo různých značek.

Tenant typu **Zákazník** se obvykle vytváří pro každou organizaci, která si zaregistruje nějakou službu.

Při rozšiřování služby na novou organizační jednotku můžete v rámci tenanta zákazníka vytvořit nový tenant **jednotky**.

Vytvoření tenanta

1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), ve kterém chcete vytvořit tenanta.
3. V pravém horním rohu klikněte na možnost **Nový** a poté klikněte na jednu z následujících možností (v závislosti na typu tenanta, který chcete vytvořit):
   - **Zákazník**
   - **Partner**
   - **Složka**
   - **Jednotka**

   Dostupnost typů závisí na typu nadřazeného tenanta.
4. Do pole **Název** zadejte název nového tenanta.
5. [Jen při vytváření tenanta zákazníka] V části **Režim** vyberte, zda tenant používá službu ve zkušebním, nebo v produkčním režimu. Měsíční zprávy o využití služby nezahrnují data o využití pro tenanty ve zkušebním režimu.

Důležité *Pokud režim přepnete ze zkušebního na produkční uprostřed měsíce, započítá se do měsíční zprávy o využití služby celý měsíc. Proto doporučujeme režimy přepínat první den v měsíci. Režim se automaticky přepne na produkční ve chvíli, kdy tenant zůstane ve zkušebním režimu celý jeden měsíc.*

6. [Volitelné] V části **Jazyk** změňte výchozí jazyk pro upozornění, zprávy a software, který se bude pro tenant používat.
7. Proveďte jeden z následujících úkonů:
   - Chcete-li vytváření tenanta dokončit, klikněte na možnost **Uložit a zavřít**. V tomto případě bude mít tenant povolené všechny služby. Tenant nebude mít správce, dokud jej nevytvoříte.
   - Chcete-li pro tenanta konfigurovat služby pro a vytvořit správce, klikněte na tlačítko **Další**.
8. [Volitelné, neplatí pro tenanta jednotky] Vypněte přepínače služeb, které chcete tenantovi zakázat. Zakázané služby budou skryty uživatelům v příslušném tenantu a jeho podřízených tenantech.

   [Pokud vytváříte partnera] Vyberte, které verze služby Cyber Protection budou k dispozici.

   [Pokud vytváříte zákazníka] Vyberte jednu verzi služby Cyber Protection, která bude k dispozici.

   Po dokončení výběru klikněte na **Další**.
9. [Volitelné, neplatí pro tenanta jednotky] Nakonfigurujte nabízené položky tenanta:
   a. V jednotlivých službách zrušte zaškrtnutí políček pro nabízené položky, které chcete zakázat. Funkce odpovídající zakázaným nabízeným položkám nebudou dostupné uživatelům v příslušném tenantu a jeho podřízených tenantech.
   b. U některých služeb můžete vybrat úložiště, která budou dostupná pro nový tenant. Úložiště jsou seskupená podle umístění. Vybírat můžete ze seznamu umístění a úložišť, které má tenant dostupné.
      - Při vytváření tenanta nadřízené položky/složky můžete pro každou službu vybrat více umístění a úložišť.
      - Při vytváření tenanta zákazníka musíte vybrat jedno umístění a potom v tomto umístění vybrat pro službu jedno úložiště. Úložiště přiřazená zákazníkovi můžete později změnit, ale pouze pokud je jejich využití 0 GB. To znamená buď před tím, než je zákazník začne využívat, nebo poté, co z nich zákazník odstraní všechny zálohy. Informace o využití prostoru úložiště nejsou aktualizovány v reálném čase. Aktualizace informací může trvat až 24 hodin.

      Další informace o úložištích naleznete v části Správa umístění a úložišť (str. 38).
   c. Chcete-li zadat kvótu pro položku, klikněte na odkaz **Neomezeno** vedle nabízené položky. Tyto kvóty jsou „měkké“. Pokud dojde k překročení některé z těchto hodnot, bude správcům tenanta a správcům nadřazeného tenanta zasláno e-mailové upozornění. Neuplatní se omezení využívání služby. V případě tenanta partnera se očekává, že využití položky nabídky může kvótu překročit, protože limit překročení nelze nastavit při vytváření tenanta partnera.
   d. [Jen při vytváření tenanta zákazníka] Určete limity překročení kvót. Limit překročení umožňuje tenantu zákazníka překročit kvótu až o určenou hodnotu. Po překročení této hodnoty jsou použita omezení pro využívání příslušné služby.
10. Proveďte jeden z následujících úkonů:
    - Chcete-li vytvořit správce tenanta, klikněte na tlačítko **Další** a postupujte podle pokynů v části Vytvoření uživatelského účtu (str. 25) od kroku 4. Pokud si to rozmyslíte, můžete vytváření správce zrušit kliknutím na možnost **Přeskočit a zavřít**.
    - Jestliže chcete vytvořit tenanta bez správce, klikněte na možnost **Uložit a zavřít**. Správce tenanta můžete přidat později.

Nově vytvořený tenant se zobrazí na kartě **Klienti**.

Chcete-li upravit nastavení tenanta nebo zadat kontaktní informace, vyberte tenanta na kartě **Klienti** a poté klikněte na ikonu tužky v části, kterou chcete upravit.

4.6 Povolení a zakázání tenanta

Někdy je třeba tenanta dočasně zakázat. Příkladem může být případ, kdy má tenant dluhy za používání služeb.

Jak zakázat tenanta

1. Na portálu pro správu přejděte na **Klienti**.
2. Vyberte tenanta, kterého chcete zakázat, a potom klikněte na ikonu se třemi tečkami > **Zakázat**.
3. Akci potvrďte kliknutím na **Zakázat**.

Výsledek:

- Tenant a jeho podřízení tenanti budou zakázáni a zastaví se jejich služby.
- Za tenanta a všechny jeho podřízené tenaty se budou i nadále účtovat poplatky, protože jejich data se ukládají do Acronis Cyber Cloud.
- Všichni klienti API v rámci tenanta a jeho podřízených tenantů budou zakázáni a všechny integrace využívající tyto klienty přestanou fungovat.

Tenanta povolíte tak, že ho vyberete ze seznamu klientů a kliknete na ikonu se třemi tečkami > **Povolit**.

4.7 Odstranění tenanta

Pokud potřebujete uvolnit prostředky, které určitý tenant používá, můžete ho odstranit. Statistika využití bude aktualizována do jednoho dne od odstranění. V případě velkých tenantů může tato akce trvat déle.

Před odstraněním je nutné tenanta zakázat. Pokyny k provedení tohoto postupu naleznete v tématu Zakázání a povolení tenanta (str. 24).

Důležité *Odstranění tenanta je nevratné!*

Odstranění tenanta

1. Na portálu pro správu přejděte na **Klienti**.
2. Vyberte zakázaného tenanta, kterého chcete odstranit, klikněte na ikonu se třemi tečkami a na položku **Odstranit**.
3. Za účelem potvrzení akce zadejte své přihlašovací jméno a klikněte na tlačítko **Odstranit**.

Výsledek:

- Tenant a jeho podřízení tenanti budou odstraněni.
- Všechny služby, které byly povoleny v rámci tenanta a jeho podřízených tenantů, budou zastaveny.
- Všichni uživatelé v rámci tenanta a jeho podřízených tenantů budou odstraněni.
- Bude zrušena registrace všech počítačů v tenantovi a jeho podřízených tenantech.
- Veškerá data týkající se služby, například zálohy a synchronizované soubory, v tenantovi a jeho podřízených tenantech budou odstraněna.

- Všichni klienti API v rámci tenanta a jeho podřízených tenantů budou odstraněni a všechny integrace využívající tyto klienty přestanou fungovat.

4.8 Vytvoření uživatelského účtu

Další účty můžete chtít vytvářet v následujících případech:

- Účty správce partnerů/složek – pro účely sdílení úkolů správy služby s dalšími uživateli.
- Účty správce zákazníků/jednotek – pokud potřebujete správou služby pověřit další uživatele, jejichž přístupová oprávnění budou přísně omezená na odpovídající zákazníky/jednotky.
- Uživatelské účty v tenantech zákazníka nebo jednotky – pokud chcete uživatelům povolit přístup pouze k určité podsadě služeb.

Nezapomeňte, že existující účty nelze přesouvat mezi tenanty. Nejprve je potřeba vytvořit tenanta a poté jej naplnit účty.

Vytvoření uživatelského účtu

1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), ve kterém chcete vytvořit uživatelský účet.
3. V pravém horním rohu klikněte na možnost **Nový** > **Uživatel**.
4. Zadejte pro účet následující kontaktní informace:
   - **E-mailová adresa**
   - [Volitelné] **Jméno**
   - [Volitelné] **Příjmení**
   - [Volitelné] Chcete-li zadat přihlašovací jméno, které se liší od zadané e-mailové adresy, zrušte zaškrtnutí políčka **Použít e-mailovou adresu jako přihlašovací jméno** a poté zadejte požadované přihlašovací jméno.

     Důležité *Každý účet musí mít jedinečné přihlašovací jméno.*
5. [Volitelné] V části **Jazyk** změňte výchozí jazyk pro upozornění, zprávy a software, který se bude pro tento účet používat.
6. [Není k dispozici při vytváření účtu v tenantu partnera/složky.] Vyberte služby, k nimž bude mít uživatel přístup, a pro každou službu nastavte roli.

   Dostupné služby závisí na službách, které jsou povoleny pro tenanta, v němž je vytvořen uživatelský účet.
   - Zaškrtnete-li políčko **Správce společnosti**, bude mít uživatel přístup k portálu pro správu a roli správce pro všechny služby, které jsou aktuálně povoleny v daném tenantu. Uživatel bude mít také roli správce ve všech službách, které budou pro daný tenant povoleny v budoucnosti.
   - Zaškrtnete-li políčko **Správce jednotky**, bude mít uživatel přístup k portálu pro správu, ale podle nastavení služby může nebo nemusí mít roli správce služby.
   - V ostatních případech bude mít uživatel role, které vyberete v zvolených službách.
7. Klikněte na tlačítko **Vytvořit**.

Nově vytvořený uživatelský účet se zobrazí na kartě **Uživatelé**.

Chcete-li pro uživatele upravit uživatelská nastavení nebo zadat nastavení upozornění a kvóty (není k dispozici pro správce složek a partnerů), vyberte požadovaného uživatele na kartě **Uživatelé** a klikněte na ikonu tužky v části, kterou chcete upravit.

Resetování hesla uživatele

1. Na portálu pro správu přejděte do části **Uživatelé**.
2. Vyberte uživatele, jehož heslo chcete resetovat, klikněte na ikonu se třemi tečkami a na položku **Resetovat heslo**.
3. Akci potvrďte kliknutím na tlačítko **Resetovat**.

Uživatel může nyní dokončit proces resetování podle pokynů v obdrženém e-mailu.

4.9 Zakázání a povolení uživatelského účtu

K dočasnému omezení přístupu na cloudovou platformu může být nutné zakázat uživatelský účet.

Zakázání uživatelského účtu

1. Na portálu pro správu přejděte do části **Uživatelé**.
2. Vyberte uživatelský účet, který chcete zakázat, klikněte na ikonu se třemi tečkami a na položku **Zakázáno**.
3. Akci potvrďte kliknutím na tlačítko **Zakázat**.

Tento uživatel pak nebude moct využívat cloudovou platformu ani přijímat oznámení.

Chcete-li zakázaný uživatelský účet povolit, vyberte ho na seznamu uživatelů, klikněte na ikonu se třemi tečkami a na položku **Povolit**.

4.10 Odstranění uživatelského účtu

Pokud potřebujete uvolnit prostředky, které určitý uživatelský účet využívá, například úložiště nebo licenci, můžete ho trvale odstranit. Statistika využití bude aktualizována do jednoho dne od odstranění. V případě účtů s velkým objemem dat může tato akce trvat déle.

Před odstraněním je nutné uživatelský účet zakázat. Pokyny k provedení tohoto postupu naleznete v tématu Zakázání a povolení uživatelského účtu (str. 26).

Důležité *Odstranění uživatelského účtu je nevratné!*

Odstranění uživatelského účtu

1. Na portálu pro správu přejděte do části **Uživatelé**.
2. Vyberte zakázaný uživatelský účet, klikněte na ikonu se třemi tečkami a na položku **Odstranit**.
3. Za účelem potvrzení akce zadejte své přihlašovací jméno a klikněte na tlačítko **Odstranit**.

Výsledek:

- Tento uživatelský účet bude odstraněn.
- Všechna data náležející k tomuto uživatelskému účtu budou odstraněna.
- Zruší se registrace všech počítačů asociovaných s tímto uživatelským účtem.

4.11 Převod vlastnictví uživatelského účtu

Pokud si chcete uchovat přístup k datům zakázaného uživatele, může být nutné převést vlastnictví uživatelského účtu.

Důležité *Obsah odstraněného účtu nelze přiřadit jinému uživateli.*

Převod vlastnictví uživatelského účtu:

1. Na portálu pro správu přejděte do části **Uživatelé**.
2. Vyberte uživatelský účet, jehož vlastnictví chcete převést, a klikněte na ikonu tužky v části **Obecné informace**.
3. Nahraďte existující e-mail e-mailem budoucího vlastníka účtu a klikněte na tlačítko **Hotovo**.
4. Potvrďte akci kliknutím na tlačítko **Ano**.
5. Požádejte budoucího vlastníka účtu o ověření své e-mailové adresy podle pokynů, které byly na adresu zaslány.
6. Vyberte uživatelský účet, jehož vlastnictví převádíte, klikněte na ikonu se třemi tečkami a na položku **Resetovat heslo**.
7. Akci potvrďte kliknutím na tlačítko **Resetovat**.
8. Požádejte budoucího vlastníka účtu o resetování hesla podle pokynů, které byly zaslány na jeho e-mailovou adresu.

Nový vlastník má nyní přístup k tomuto účtu.

4.12 Nastavení dvojúrovňového ověřování

Dvojúrovňové ověřování (2FA) je typ vícefaktorového ověřování, které kontroluje identitu uživatele pomocí kombinace dvou různých faktorů:

- Něco, co uživatel zná (PIN nebo heslo)
- Něco, co uživatel má (token)
- Něco, co uživatele definuje (biometrické údaje)

Dvojúrovňové ověřování poskytuje vyšší úroveň ochrany před neoprávněným přístupem k vašemu účtu.

Tato platforma podporuje ověřování **TOTP (Time-based One-Time Password)**. Pokud je v systému povoleno ověřování TOTP, musí uživatelé, kteří chtějí získat přístup k systému, zadat své tradiční heslo a jednorázový kód TOTP. Jinými slovy, uživatel zadá heslo (první úroveň ověřování) a kód TOTP (druhá úroveň ověřování). Kód TOTP je generován v aplikaci pro ověřování na uživatelském zařízení určeném pro druhou úroveň ověřování na základě aktuálního času a tajného klíče (QR kód nebo alfanumerický kód) poskytnutého platformou.

Jak to funguje

1. Povolíte dvojúrovňové ověřování (str. 30) na úrovni organizace.
2. Všichni uživatelé v organizaci si musí nainstalovat aplikaci pro ověřování na svých zařízeních určených pro druhou úroveň ověřování (mobilní telefony, notebooky, stolní počítače nebo tablety). Tato aplikace bude použita pro generování jednorázových kódů TOTP. Doporučené aplikace pro ověřování jsou:
   - Google Authenticator

     Verze pro iOS (https://itunes.apple.com/sg/app/google-authenticator/id388497605?mt=8)

Verze pro Android (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=cs)

- Microsoft Authenticator

  Verze pro iOS (https://app.adjust.com/n094ls?campaign=appstore_ios&fallback=https://itunes.apple.com/app/microsoft-authenticator/id983156458)

  Verze pro Android (https://app.adjust.com/n094ls?campaign=appstore_android&fallback=https://play.google.com/store/apps/details?id=com.azure.authenticator)

Důležité *Uživatelé musí zajistit, aby byl v zařízení, kde je instalována aplikace pro ověřování, správně nastaven čas a aby odpovídal skutečnému aktuálnímu času.*

3. Uživatelé ve vaší organizaci se musí znovu přihlásit do systému.
4. Po zadání přihlašovacího jména a hesla budou vyzváni k nastavení dvojúrovňového ověřování pro svůj uživatelský účet.
5. Pomocí své aplikace pro ověřování musí naskenovat QR kód. Pokud QR kód nelze naskenovat, mohou použít tajný klíč TOTP uvedený pod QR kódem a přidat jej ručně do aplikace pro ověřování.

Důležité *Důrazně doporučujeme tyto údaje uložit (vytisknout QR kód, zapsat si tajný klíč TOTP, popř. použít aplikaci, která podporuje zálohování kódů v cloudu). Tajný klíč TOTP je vyžadován k obnovení dvojúrovňového ověřování v případě ztráty zařízení určeného pro druhou úroveň ověřování.*

6. Aplikace pro ověřování vygeneruje jednorázový kód TOTP. Kód bude automaticky vygenerován každých 30 sekund.
7. Uživatelé musí zadat kód TOTP na obrazovce Nastavení dvojúrovňového ověřování poté, co zadají své heslo.
8. Tím bude nastaveno dvojúrovňové ověřování pro uživatele.

Když se nyní uživatelé přihlásí do systému, budou požádáni o zadání přihlašovacího jména a hesla a jednorázového kódu TOTP vygenerovaného v aplikaci pro ověřování. Uživatelé si při přihlášení do systému mohou označit svůj prohlížeč jako důvěryhodný. Díky tomu nebudou muset při dalších přihlášeních pomocí tohoto prohlížeče zadávat kód TOTP.

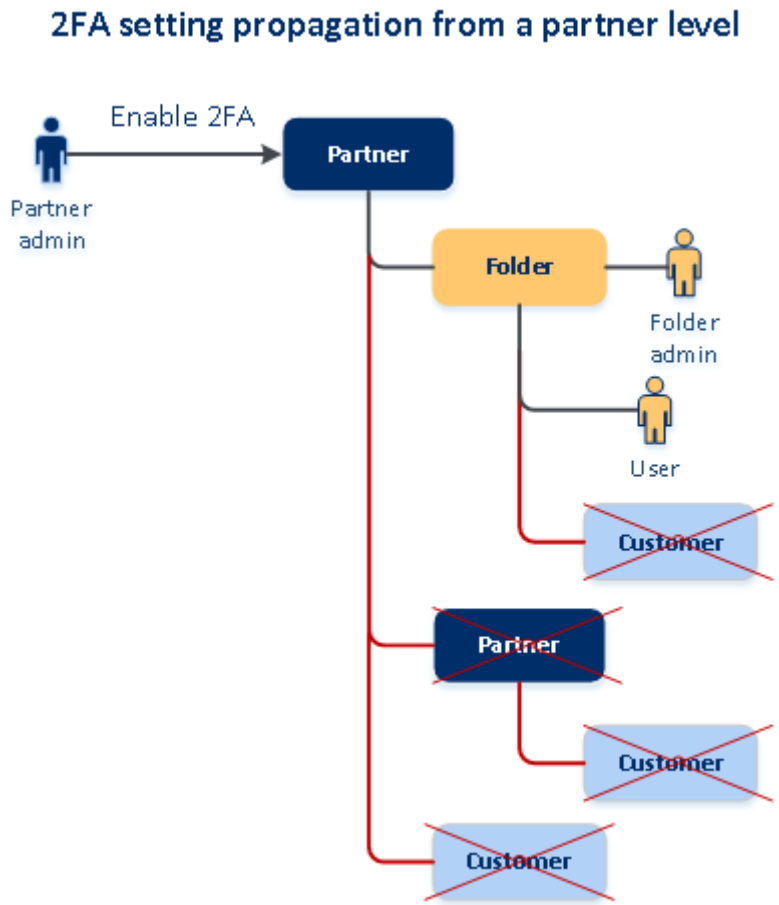
4.12.1 Šíření nastavení dvojúrovňového ověřování v úrovních tenanta

Dvojúrovňové ověřování je nastaveno na úrovni **organizace**. Dvojúrovňové ověřování můžete zapnout nebo vypnout:

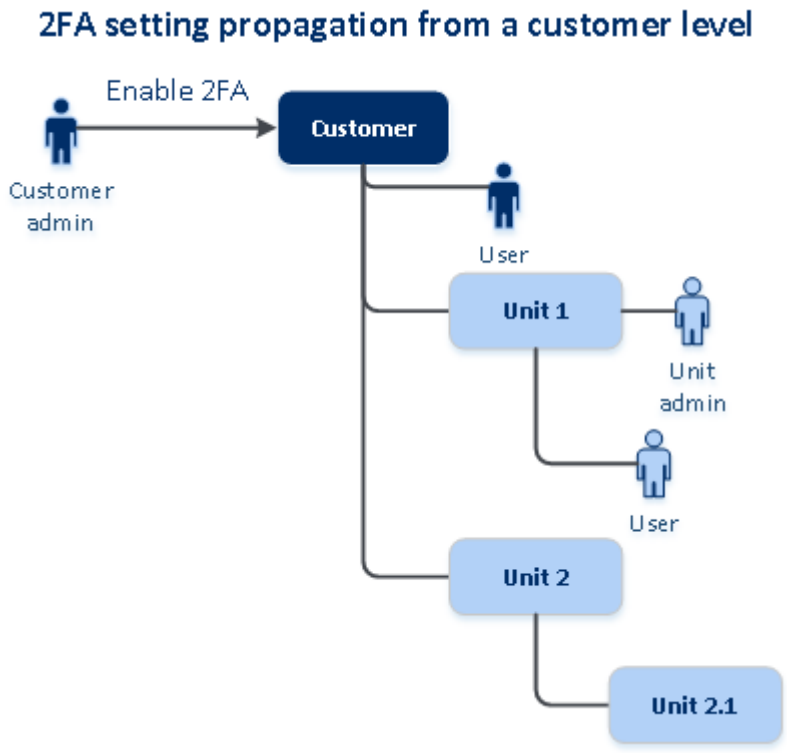
- pro svou vlastní organizaci,
- pro podřízeného tenanta (pouze pokud je v rámci tohoto podřízeného tenanta povolená možnost **Přístup k podpoře**).

Nastavení dvojúrovňového ověřování je šířeno napříč úrovněmi tenanta následujícím způsobem:

- Složky automaticky zdědí nastavení dvojúrovňového ověřování od organizace partnera. Červené čáry ve schématu níže znamenají, že šíření nastavení dvojúrovňového ověřování není možné.



- Jednotky automaticky zdědí nastavení dvojúrovňového ověřování od organizace zákazníka.



Poznámka
*1. Pro podřízené organizace můžete zapnout nebo vypnout dvojúrovňové ověřování, pouze pokud je v rámci dané podřízené organizace povolená možnost **Přístup k podpoře**.*
*2. Pro uživatele v podřízených organizacích můžete spravovat nastavení dvojúrovňového ověřování, pouze pokud je v rámci dané podřízené organizace povolená možnost **Přístup k podpoře**.*
3. Dvojúrovňové ověřování není možné nastavit na úrovni složky nebo jednotky.
4. Nastavení dvojúrovňového ověřování můžete nakonfigurovat, i když vaše nadřízená organizace toto nastavení nemá povoleno.

4.12.2 Nastavení dvojúrovňového ověřování pro tenanta

Postup povolení dvojúrovňového ověřování pro tenanta

1. Na portálu pro správu přejděte na **Nastavení** > **Zabezpečení**.
2. Povolte dvojúrovňové ověřování přetáhnutím posuvníku do polohy Zapnuto. Potvrďte akci kliknutím na **Povolit**.

Ukazatel průběhu zobrazuje, kolik uživatelů má nastaveno dvojúrovňové ověřování pro své účty. Tímto je pro vaši organizaci povoleno dvojúrovňové ověřování. Nyní si musí všichni uživatelé v organizaci ve svých účtech nastavit dvojúrovňové ověřování. Když se poté uživatelé přihlásí do systému, budou požádáni o zadání přihlašovacího jména a hesla a kódu TOTP.

Na kartě **Uživatelé** se zobrazí sloupec **Stav dvojúrovňového ověřování**. Můžete zde sledovat, kteří uživatele mají nastaveno dvojúrovňové ověřování pro své účty.

Postup zakázání dvojúrovňového ověřování pro tenanta

1. Na portálu pro správu přejděte na **Nastavení** > **Zabezpečení**.
2. Zakažte dvojúrovňové ověřování přetáhnutím posuvníku do polohy Vypnuto. Potvrďte akci kliknutím na **Zakázat**.
3. [Pokud alespoň jeden uživatel nakonfiguroval dvojúrovňové ověřování v rámci organizace] Zadejte kód TOTP vygenerovaný aplikací pro ověřování ve vašem mobilním zařízení.

Tím se pro vaši organizaci zakáže dvojúrovňové ověřování, odstraní se tajné klíče a důvěryhodné prohlížeče se zapomenou. Všichni uživatelé se do systému přihlásí pouze pomocí svého přihlašovacího jména a hesla. Na kartě **Uživatelé** bude skryt sloupec **Stav dvojúrovňového ověřování**.

4.12.3 Správa dvojúrovňového ověřování pro uživatele

Na portálu pro správu můžete na kartě **Uživatelé** monitorovat a obnovit nastavení dvojúrovňového ověřování všech uživatelů.

Monitorování

Na portálu pro správu na kartě **Uživatelé** naleznete seznam všech uživatelů v organizaci. Ve sloupci **Stav dvojúrovňového ověřování** si můžete prohlédnout, zda je pro uživatele nastaveno dvojúrovňové ověřování.

Obnovení dvojúrovňového ověřování pro vybraného uživatele

1. Na portálu pro správu na kartě **Uživatelé** vyhledejte uživatele, pro kterého chcete změnit nastavení, a potom klikněte na ikonu se třemi tečkami.
2. Klikněte na **Obnovit dvojúrovňové ověřování**.

3. Zadejte kód TOTP vygenerovaný aplikací pro ověřování ve vašem zařízení určeném pro druhou úroveň ověřování a potom klikněte na **Obnovit**.

Tím uživateli umožníte znovu nastavit dvojúrovňové ověřování.

Obnovení důvěryhodného prohlížeče pro vybraného uživatele

1. Na portálu pro správu na kartě **Uživatelé** vyhledejte uživatele, pro kterého chcete změnit nastavení, a potom klikněte na ikonu se třemi tečkami.
2. Klikněte na **Obnovit všechny důvěryhodné prohlížeče**.
3. Zadejte kód TOTP vygenerovaný aplikací pro ověřování ve vašem zařízení určeném pro druhou úroveň ověřování a potom klikněte na **Obnovit**.

Uživatel, pro kterého jste obnovili všechny důvěryhodné prohlížeče, bude muset při dalším přihlášení zadat kód TOTP.

Uživatelé mohou obnovit všechny důvěryhodné prohlížeče a obnovit nastavení dvojúrovňového ověřování sami. To lze provést po přihlášení do systému kliknutím na příslušný odkaz a zadáním kódu TOTP k potvrzení operace.

Zakázání dvojúrovňového ověřování pro vybraného uživatele

Je možné, že někdy budete chtít zakázat dvojúrovňové ověřování pro některého uživatele, a ponechat ho povolené pro ostatní uživatele. To je nutné v případě, že daný uživatel používá přístup k rozhraní API.

Důležité *Kvůli zakázání dvojúrovňového ověřování nepřepínejte normální uživatele na uživatele služby, protože by se uživatelé nebyli schopni přihlásit.*

1. Na portálu pro správu na kartě **Uživatelé** vyhledejte uživatele, pro kterého chcete změnit nastavení, a potom klikněte na ikonu se třemi tečkami.
2. Klikněte na **Označit jako účet služby**. Výsledkem je, že k příslušnému uživateli je přiřazen zvláštní stav dvojúrovňového ověřování označovaný jako **účet služby**.
3. [Pokud má alespoň jeden uživatel v tenantu nakonfigurováno dvojúrovňové ověřování.] Potvrďte zákaz zadáním kódu TOTP vygenerovaném aplikací pro ověřování ve vašem zařízení určeném pro druhou úroveň ověřování.

Povolení dvojúrovňového ověřování pro vybraného uživatele

Je možné, že budete chtít povolit dvojúrovňové ověřování konkrétnímu uživateli, kterému jste ho dříve zakázali.

1. Na portálu pro správu na kartě **Uživatelé** vyhledejte uživatele, pro kterého chcete změnit nastavení, a potom klikněte na ikonu se třemi tečkami.
2. Klikněte na **Označit jako běžný účet**. Výsledkem je, že daný uživatel si při přihlášení do systému bude muset nastavit dvojúrovňové ověřování nebo zadat kód TOTP.

4.12.4 Obnovení dvojúrovňového ověřování v případě ztráty zařízení určeného pro druhou úroveň ověřování

Chcete-li obnovit přístup ke svému účtu v případě ztráty zařízení určeného pro druhou úroveň ověřování, postupujte podle jednoho z doporučených přístupů:

- Obnovte svůj tajný klíč TOTP (QR kód nebo alfanumerický kód) ze zálohy.

  Použijte jiné zařízení a přidejte uložený tajný klíč TOTP do aplikace pro ověřování nainstalované v tomto zařízení.

- Požádejte správce, aby pro vás obnovil nastavení dvojúrovňového ověřování (str. 30).

4.12.5 Ochrana před útoky hrubou silou

Útok hrubou silou je útok, kdy se narušitel pokouší získat přístup do systému tím, že odešle mnoho hesel s nadějí, že jedno bude správné.

Mechanismus ochrany platformy před útoky hrubou silou se zakládá na souborech cookie zařízení.

Nastavení ochrany před útoky hrubou silou použitá na platformě jsou předdefinovaná:

Parametr	Zadání hesla	Zadání kódu TOTP
Limit počtu pokusů	10	5
Časový limit počtu pokusů (po uplynutí daného času se limit obnoví)	15 min (900 s)	15 min (900 s)
K uzamčení dojde při	Limit počtu pokusů + 1 (11. pokus)	Limit počtu pokusů
Doba uzamčení	5 min (300 s)	5 min (300 s)

Pokud jste povolili dvojúrovňové ověřování, je soubor cookie zařízení vydán klientovi (prohlížeči) až po úspěšném ověření pomocí obou úrovní (heslo a kód TOTP).

V případě důvěryhodných prohlížečů je soubor cookie zařízení vydán po úspěšném ověření pomocí jediného faktoru (heslo).

Pokusy o zadání kódu TOTP se registrují na uživatele, nikoli na zařízení. To znamená, že i když se uživatel pokusí zadat kód TOTP z různých zařízení, bude i přesto zablokován.

4.13 Konfigurace scénářů upsellingu pro vaše zákazníky

Upselling je proces přesvědčení zákazníka, aby si zakoupil doplňující nebo nákladnější produkt.

Cyber Protection má šest verzí, které se liší funkcemi a cenou. Svým zákazníkům, kteří využívají základní verze, můžete nabídnout dražší verze s rozšířenými funkcemi.

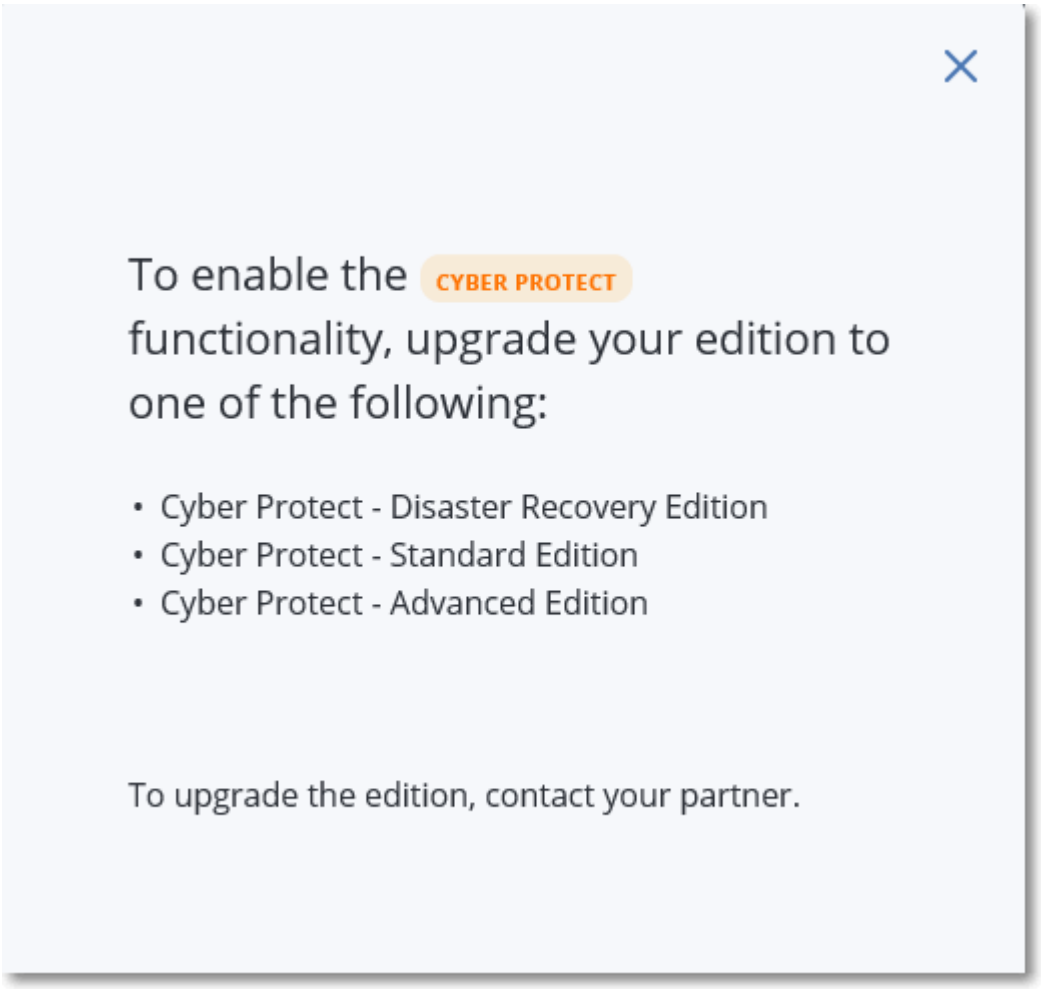
Možnost upsellingu můžete pro jednotlivé zákazníky povolit nebo zakázat. Ve výchozím nastavení je tato možnost povolena. Pokud upselling pro zákazníka povolíte, uvidí další funkce, které nebudou k dispozici, dokud si zákazník nabízenou vyšší verzi nezakoupí. Doplňkové funkce jsou označeny popisky, které uvádějí název nebo ikony podporované verze. Vše je zvýrazněno oranžově. Tyto body upsellingu se zobrazí zákazníkům, aby je motivovaly ke koupi dražší verze. Kliknutím na body se zákazníkovi zobrazí dialogové okno navrhující nákup dražší verze, která požadované funkce zahrnuje.

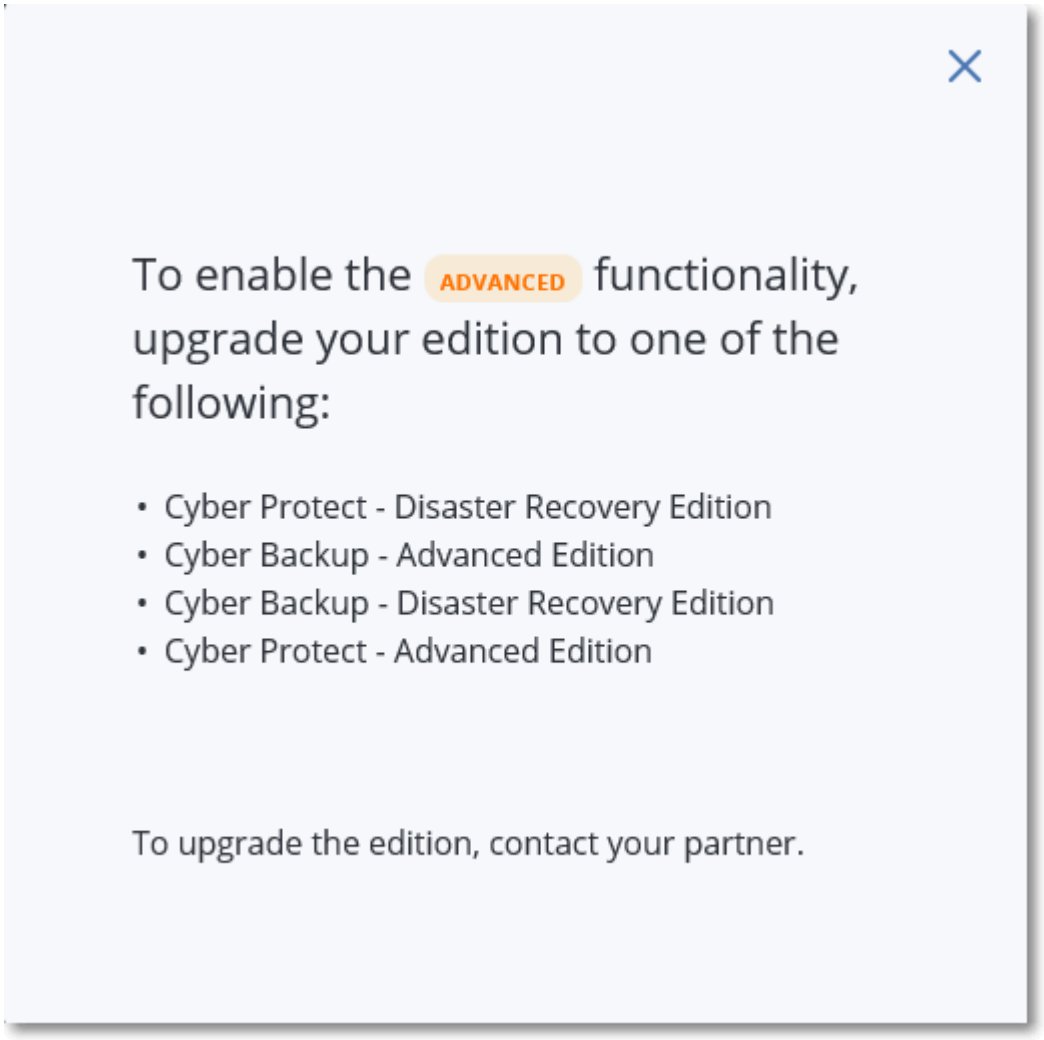
Položka akce závisí na typu uživatele zákazníka. Typ uživatelů (kupující nebo nekupující) lze nakonfigurovat pomocí uživatelského rozhraní API platformy. Podrobnosti naleznete v dokumentaci k rozhraní API. Další informace o položkách akce, které se zobrazí vašim zákazníkům, naleznete v tabulce níže:

Typ uživatelů v tenantu zákazníka	Položka akce
Správce; kupující	V uživatelském rozhraní se zobrazí tlačítko **Koupit**.*

Správce; nekupující	V uživatelském rozhraní se zobrazí zpráva „Chcete-li upgradovat verzi, obraťte se na svého partnera.“
Uživatel; kupující	V uživatelském rozhraní se zobrazí zpráva „Chcete-li upgradovat verzi, obraťte se na svého partnera.“
Uživatel; nekupující	V uživatelském rozhraní se zobrazí zpráva „Chcete-li upgradovat verzi, obraťte se na svého partnera.“

* Odkaz pro tlačítko **Koupit**, které přesměruje zákazníka na web, kde si bude moct zakoupit rozšířenou verzi, lze nakonfigurovat v nabídce **Nastavení** > **Budování značky**. V části **Upselling** můžete zadat **adresu URL tlačítka Koupit**. Nastavení budování značky budou použita na všechny přímé a nepřímé podřízené partnery/složky a zákazníky tenanta, kde je nakonfigurováno budování značky.





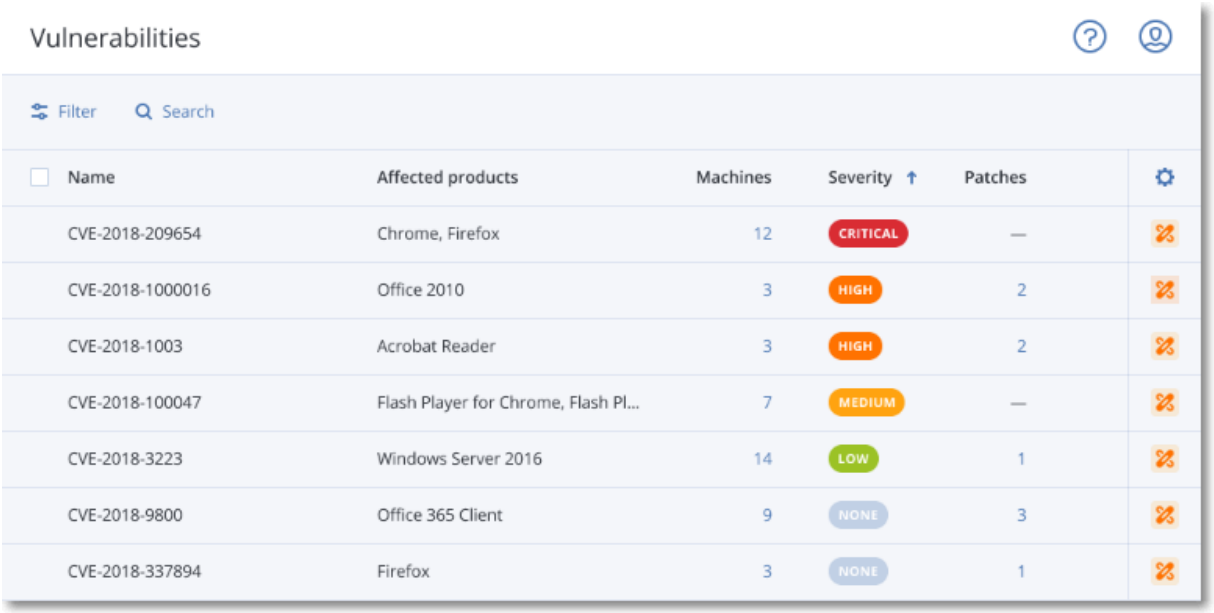
Povolení nebo zakázání možnosti upsellingu pro jednotlivé zákazníky

1. Na portálu pro správu přejděte na **Klienti**.
2. Vyberte zákazníka, přejděte na levý panel a přepněte na kartu **Nastavení**.
3. V části **Upselling** proveďte následující:
   - Povolením možnosti **Propagovat pokročilejší verze** zapněte pro zákazníky scénář upsellingu.
   - Zakázáním možnosti **Propagovat pokročilejší verze** vypněte pro zákazníky scénář upsellingu.

Body upsellingu, které se zobrazí zákazníkovi

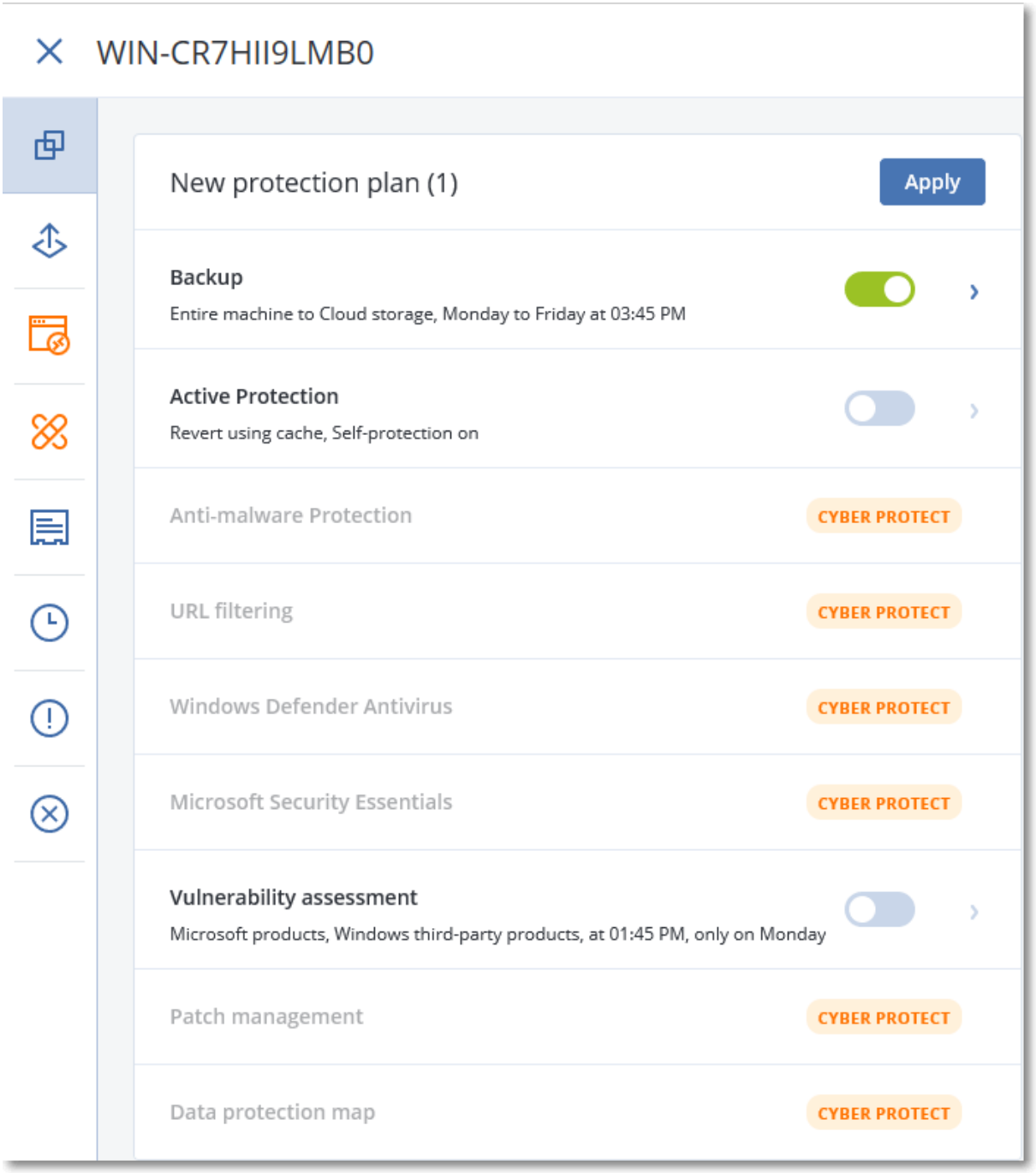
Seznam ohrožení zabezpečení

V konzoli služby naleznete seznam ohrožení zabezpečení v nabídce **Správa softwaru** > **Ohrožení zabezpečení**. Když uživatel klikne na ikonu jehly, otevře se dialogové okno propagace verze, kde bude uživatel vyzván k zakoupení dražší verze.



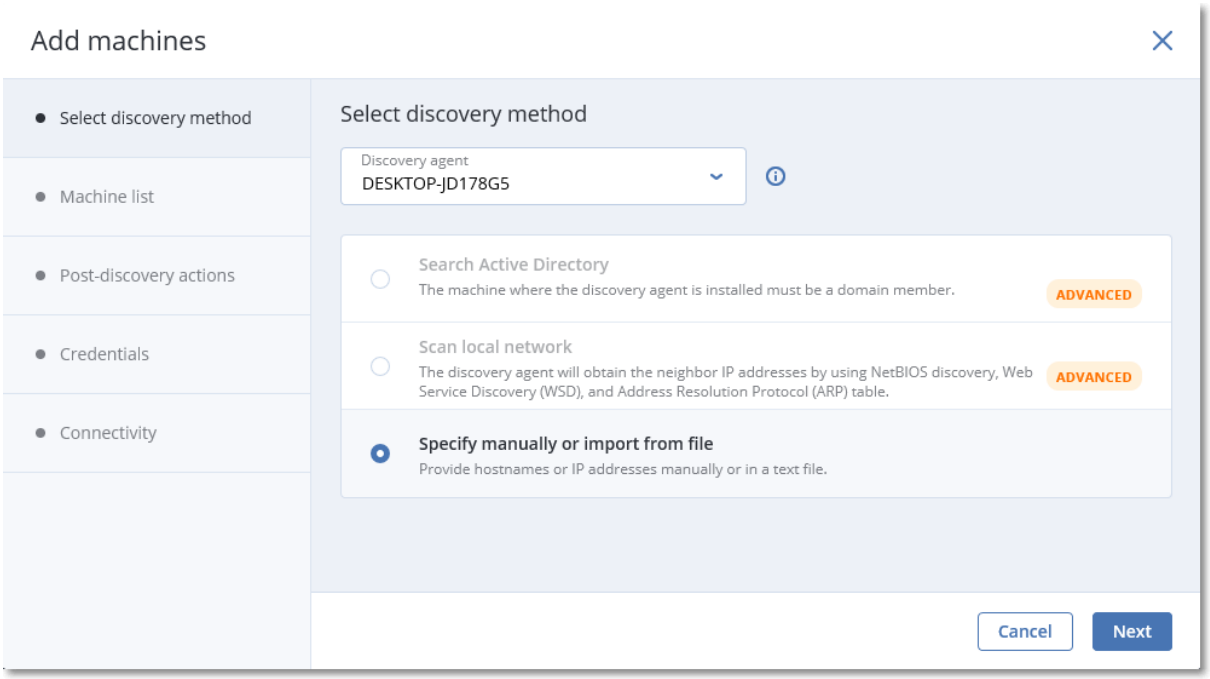
Vytvoření nebo úprava plánu ochrany

V konzoli služby naleznete plán ochrany v nabídce **Plány** > **Ochrana**. Klikněte na **Vytvořit plán**. Verze Cyber Backup mají povoleny pouze moduly **Backup** a **Vulnerability**. Zbytek modulů je k dispozici pouze ve verzích Cyber Protect. Váš zákazník bude mít všechny moduly aktivní po zakoupení jedné z verzí Cyber Protect.



Průvodce automatickým zjišťováním

V konzoli služby naleznete průvodce v nabídce **Zařízení** > **Všechna zařízení**. Váš zákazník by měl průvodce automatickým zjišťováním spustit kliknutím na tlačítko **Přidat**. V části **Více zařízení** by pak měl kliknout na možnost **Pouze Windows**. Metody automatického zjišťování počítačů budou k dispozici pouze ve verzích Advanced.

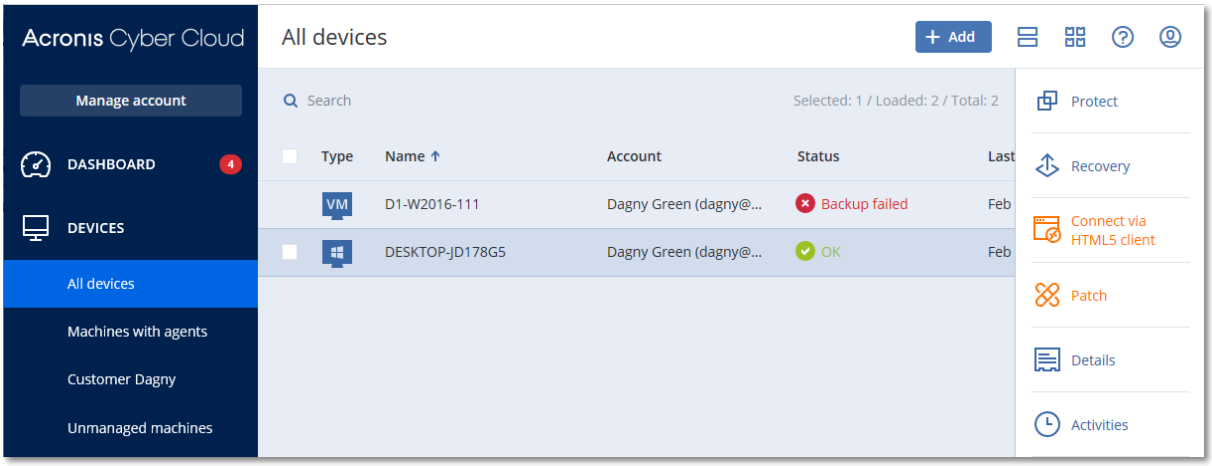


Akce v seznamu zařízení

V konzoli služby naleznete tento seznam v nabídce **Zařízení** > **Všechna zařízení**. Váš zákazník by měl vybrat počítač. Následně se mu na levém panelu zobrazí dvě další možnosti:

- **Připojit pomocí klienta HTML5**
- **Oprava**

Tyto možnosti budou k dispozici, pouze pokud si zákazník koupí verzi dražší, než je verze stávající.



4.14 Správa umístění a úložišť

V části **Nastavení** > **Umístění** se zobrazují cloudová úložiště a infrastruktura obnovení po havárii. Můžete je použít k poskytnutí služeb **Cyber Protection** a **File Sync & Share** svým partnerům a zákazníkům.

Úložiště konfigurovaná pro jiné služby se v budoucích verzích zobrazí v části **Umístění**.

Umístění

Umístění je kontejner, který umožňuje pohodlně seskupovat cloudová úložiště s infrastrukturou pro obnovení po havárii. Můžete vybrat cokoli, například určité datové centrum nebo geografické umístění se součástmi vaší infrastruktury.

Můžete vytvořit libovolný počet umístění a naplnit je úložišti záloh, infrastrukturou obnovení po havárii a úložišti služby **File Sync & Share**. Umístění může obsahovat více cloudových úložišť, ale jenom jednu infrastrukturu pro obnovení po havárii.

Další informace o operacích s úložišti najdete v části Správa úložišť (str. 38).

Volba umístění a úložišť pro partnery a zákazníky

Při vytváření tenanta partnera/složky (str. 22) můžete pro službu vybrat více umístění a v nich více úložišť, které bude mít nový tenant k dispozici.

Při vytváření tenanta zákazníka (str. 22) musíte vybrat jedno umístění a potom v tomto umístění vybrat pro službu jedno úložiště. Úložiště přiřazená zákazníkovi můžete později změnit, ale pouze pokud je jejich využití 0 GB. To znamená buď před tím, než je zákazník začne využívat, nebo poté, co z nich zákazník odstraní všechny zálohy.

Informace o úložištích přiřazených k tenantu zákazníka se zobrazují na panelu s podrobnostmi o tenantu, když je tenant vybrán na kartě **Klienti**. Informace o využití prostoru úložiště nejsou aktualizovány v reálném čase. Aktualizace informací může trvat až 24 hodin.

Operace s umístěními

Pokud chcete vytvořit nové umístění, klikněte na **Přidat umístění** a zadejte jeho název.

Pokud chcete úložiště nebo infrastrukturu obnovení po havárii přesunout jinam, vyberte úložiště nebo infrastrukturu, klikněte v poli **Umístění** na ikonu tužky a vyberte cílové umístění.

Pokud chcete umístění přejmenovat, klikněte na ikonu se třemi tečkami vedle názvu úložiště, klikněte na **Přejmenovat** a zadejte název nového úložiště.

Pokud chcete umístění odstranit, klikněte na ikonu se třemi tečkami vedle názvu úložiště, klikněte na **Odstranit** a potvrďte volbu. Odstranit můžete jenom prázdná umístění.

4.14.1 Správa úložišť

Přidání nových úložišť

- Služba **Cyber Protection**:
  - Ve výchozím nastavení jsou úložiště umístěna v datových centrech Acronis.
  - Pokud správce vyšší úrovně povolí tenantovi partnera nabízenou položku **Úložiště pro zálohování vlastněné partnerem**, mohou správci partnera k uspořádání úložiště ve vlastním datovém centru partnera použít software Acronis Cyber Infrastructure. Kliknutím na **Přidat**

úložiště záloh v části **Umístění** zjistíte informace o uspořádání úložiště záloh ve svém datovém centru.

- Pokud správce vyšší úrovně povolí tenantovi partnera nabízenou položku **Infrastruktura obnovení po havárii vlastněná partnerem**, mohou správci partnera uspořádat infrastrukturu obnovení po havárii v partnerově vlastním datovém centru. Informace o přidání infrastruktury pro obnovení po havárii poskytuje technická podpora pro Acronis na webu Argentina/support.

- Chcete-li získat informace o přidávání dalších úložišť, která budou využívána dalšími službami, kontaktujte technickou podporu Acronis na webu Argentina/support.

Odstranění úložišť

Úložiště přidaná vámi nebo vašimi podřízenými tenanty můžete odstranit.

Pokud je úložiště přiřazeno tenantům zákazníka, musíte napřed vypnout službu, která ho používá, a teprve potom můžete úložiště odstranit.

Jak odstranit úložiště

1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), do kterého bylo přidáno úložiště.
3. Klikněte na **Nastavení** > **Umístění**.
4. Vyberte úložiště, které chcete odstranit.
5. Na panelu vlastností úložiště klikněte na ikonu tří teček a potom na možnost **Odstranit úložiště**.
6. Potvrďte své rozhodnutí.

4.15 Konfigurace značky

V části **Nastavení** > **Budování značky** mohou správci partnerů přizpůsobit uživatelské rozhraní portálu pro správu a služby **Cyber Protection** tak, aby odstranili všechna spojení se společností Acronis nebo partnery vyšší úrovně.

Budování značky lze nakonfigurovat na úrovni partnerů a složek. Budování značky se použije u všech přímých a nepřímých podřízených partnerů, složek a zákazníků tenanta, kde je budování značky nakonfigurováno.

V budoucích verzích budou k dispozici možnosti konfigurace značky pro všechny služby. Některé služby nabízejí vlastní možnosti budování značky. Další informace naleznete v uživatelských příručkách dostupných v konzolích příslušných služeb.

Položky značky

Vzhled

- **Název služby**. Tento název se používá ve všech e-mailových zprávách odeslaných portálem pro správu (zprávy o aktivaci účtu, e-mailová provozní upozornění), v **uvítacím** okně po prvním přihlášení a jako název karty portálu pro správu v prohlížeči.
- **Logo**. Logo se zobrazuje na portálu pro správu a ve službách. Kliknutím na logo nahrajte soubor obrazu.
- **Barevné schéma**. Barevné schéma definuje kombinaci barev, která je použita ve všech prvcích uživatelského rozhraní. Klikněte na schéma a vyberte jedno předdefinovaných schémat, které nejlépe vyhovuje vašim potřebám.

Tip *Kliknutím na možnost* ***Zobrazit náhled schématu na nové kartě*** *zobrazíte, jak bude vypadat rozhraní pro vaše podřízené tenanty. Budování značky nebude použito, dokud na panelu* ***Zvolit barevné schéma*** *nekliknete na tlačítko* ***Hotovo****.*

Dokumentace a podpora

- **Adresa URL domovské stránky**. Tato stránka se otevře, když uživatel klikne na název společnosti na panelu **Informace**.
- **Adresa URL podpory**. Tato stránka se otevře, když uživatel klikne na odkaz **Kontaktovat podporu** na panelu **Informace** nebo v -mailové zprávě odeslané portálem pro správu.
- **Telefonní číslo podpory**. Toto telefonní číslo se zobrazí na panelu **Informace**.
- **Adresa URL znalostní databáze**. Tato stránka se otevře, když uživatel klikne odkaz **Znalostní databáze** v chybové zprávě.
- **Příručka správce portálu pro správu**. Tato stránka se otevře, když uživatel klikne na ikonu otazníku v pravém horním rohu portálu pro správu a poté na možnost **Informace** > **Příručka správce**.
- **Nápověda pro správce portálu pro správu**. Tato stránka se otevře, když uživatel klikne na ikonu otazníku v pravém horním rohu portálu pro správu a poté na možnost **Nápověda**.

Nastavení právních dokumentů

- **Adresa URL licenční smlouvy s koncovým uživatelem**. Tato stránka se otevře, když uživatel klikne na odkaz **Licenční smlouva s koncovým uživatelem** na panelu **Informace** nebo na **uvítací okno** po prvním přihlášení.
- **Adresa URL podmínek platformy**. Tato stránka se otevře, když správce partnera klikne na odkaz **Podmínky platformy** na panelu **Informace** nebo na **uvítací okno** po prvním přihlášení.
- **Adresa URL prohlášení o ochraně soukromí**. Tato stránka se otevře, když uživatel klikne na odkaz **Prohlášení o ochraně soukromí** v **uvítacím okně** po prvním přihlášení.

Upselling

- **Adresa URL tlačítka Koupit**. Tato stránka se zobrazí, když uživatel klikne na tlačítko **Koupit**, aby provedl upgrade na vyšší verzi služby Cyber Protection. Další informace o scénářích upsellingu naleznete v tématu „Konfigurace scénářů upsellingu pro vaše zákazníky (str. 32)“.

Mobilní aplikace

- **App Store**. Tato stránka se otevře, když uživatel klikne na možnost **Přidat** > **iOS** ve službě **Cyber Protection**.
- **Google Play**. Tato stránka se otevře, když uživatel klikne na možnost **Přidat** > **Android** ve službě **Cyber Protection**.

Nastavení e-mailového serveru

Můžete určit vlastní e-mailový server, který se bude používat k posílání e-mailových upozornění z portálu pro správu a ze služeb. Chcete-li zadat vlastní e-mailový server, klikněte na možnost **Přizpůsobit** a poté zadejte následující nastavení:

- V části **Od** zadejte jméno, které se zobrazí v poli **Od** v e-mailových upozorněních.
- Do pole **SMTP** zadejte název serveru odchozí pošty (SMTP).
- V části **Port** zadejte port odchozí pošty. Implicitně je tento port nastaven na 25.
- V části **Šifrování** vyberte, jestli se má používat šifrování SSL nebo TLS. Výběrem možnosti **Žádné** šifrování zakážete.
- V části **Uživatelské jméno** a **Heslo** zadejte pověření účtu, který se bude používat pro odesílání zpráv.

Konfigurace značky

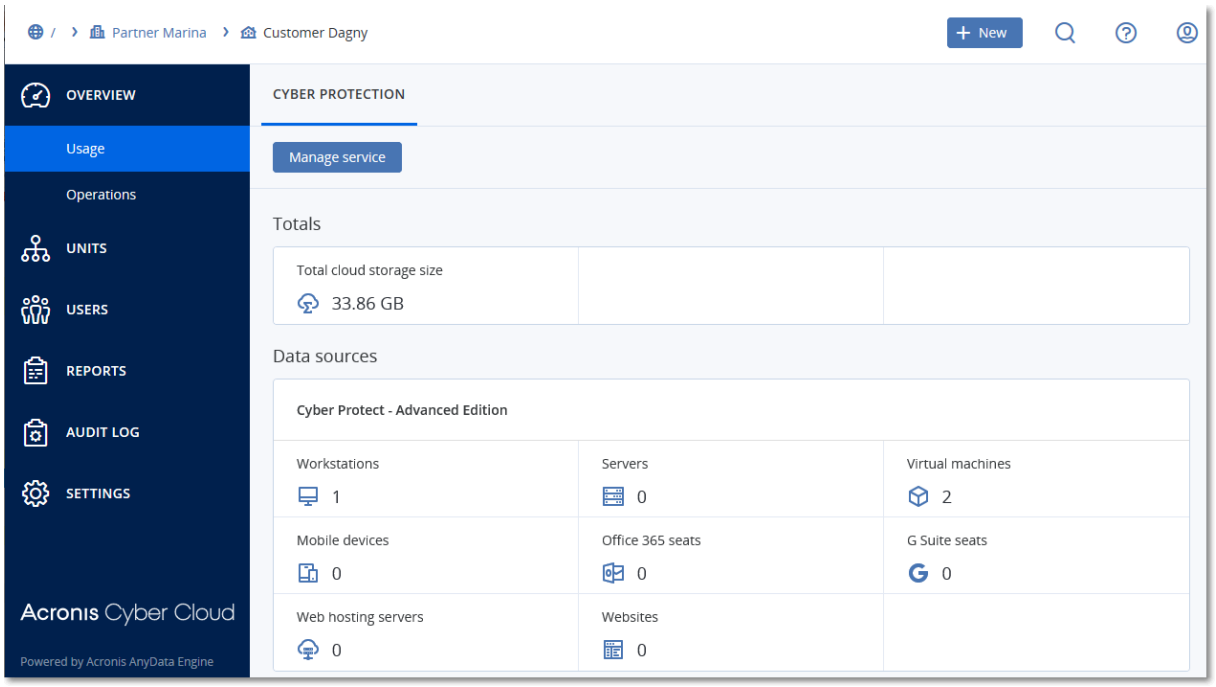
1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), ve kterém chcete konfigurovat budování značky.
3. Klikněte na **Nastavení** > **Budování značky**.
4. Klikněte na **Povolit budování značky**.
5. Proveďte jeden z následujících úkonů:
   - Konfigurujte výše uvedené položky budování značky.
   - Kliknutím na **bílý štítek** vymažte všechny položky budování značky, kromě **názvu služby**, **adresy URL licenční smlouvy s koncovým uživatelem**, **příručky správce pro portál správy**, **nápovědy správce pro portál správy** a **nastavení e-mailového serveru**.
   - Chcete-li obnovit všechny položky budování značky na výchozí hodnoty, klikněte na možnost **Obnovit výchozí nastavení**.

4.16 Monitorování

Informace o použití a provozu služeb získáte kliknutím na **Přehled**.

4.16.1 Využití

Karta **Využití** poskytuje přehled o využívání služeb a umožňuje přístup ke službám v rámci tenanta, ve kterém pracujete.



4.16.2 Operace

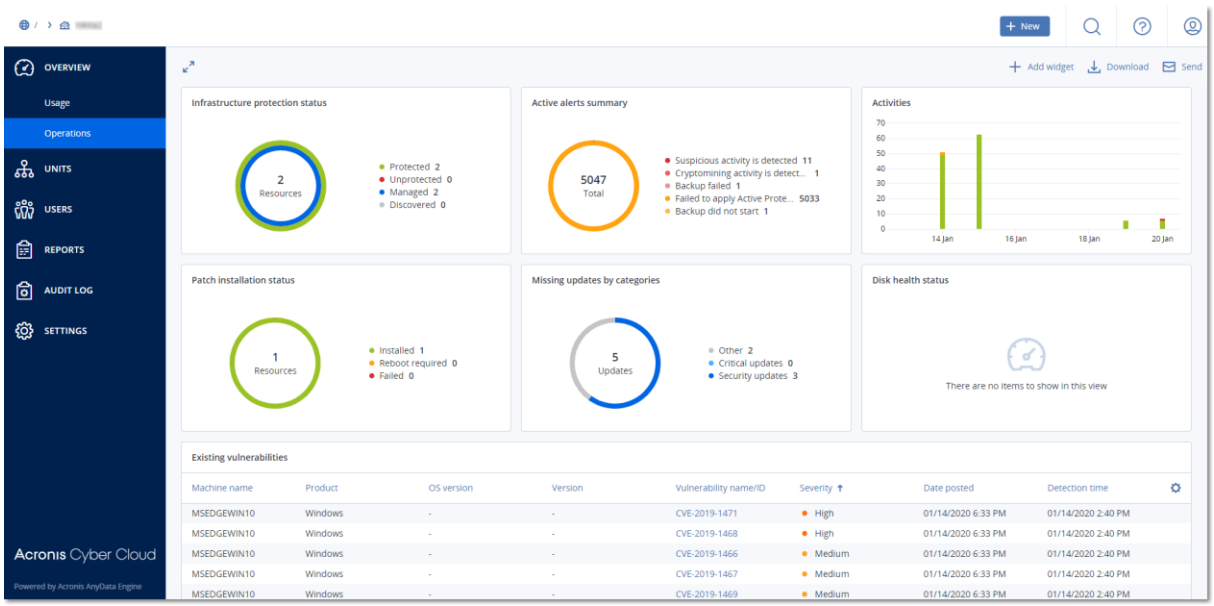
Kontrolní panel **Operace** nabízí celou řadu přizpůsobitelných ovládacích prvků, které poskytují přehled o operacích souvisejících se službou Cyber Protection. Ovládací prvky dalších služeb budou dostupné v příštích verzích.

Ve výchozím nastavení se zobrazují data tenanta, ve kterém pracujete (str. 20). Zobrazovaného tenanta můžete změnit úpravou každého ovládacího prvku jednotlivě. Zobrazí se také souhrnné

informace o přímých podřízených tenantech zákazníků vybraného tenanta, včetně těch, kteří jsou umístění ve složkách. Na kontrolním panelu se *nezobrazují* informace o podřízených partnerech a jejich podřízených tenantech; k zobrazení kontrolního panelu konkrétního partnera je třeba k němu přejít níže v hierarchii. Pokud však převedete podřízeného tenanta typu partner na tenanta typu složka (str. 62), zobrazí se informace o podřízených zákaznících tohoto tenanta v kontrolním panelu nadřízeného tenanta.

Ovládací prvky se aktualizují každé dvě minuty. Ovládací prvky obsahují prokliknutelné prvky, které vám umožní prozkoumat a řešit různé problémy. Aktuální stav kontrolního panelu si můžete stáhnout ve formátu PDF nebo XLSX nebo ho poslat e-mailem na jakoukoli adresu, včetně externích příjemců.

Můžete vybírat z mnoha různých ovládacích prvků v podobě tabulek, výsečových grafů, pruhových grafů, seznamů a stromových map. Můžete přidávat více ovládacích prvků stejného typu pro různé tenanty nebo s různými filtry.



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 časové období, vybrat tenanta, pro kterého se mají zobrazit data, a nastavit filtry.

Jak přidat ovládací prvek

Klikněte na **Přidat ovládací prvek** a proveďte jeden z následujících úkonů:

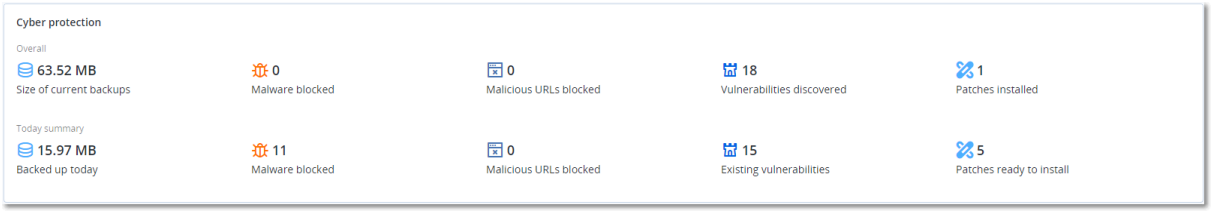
- Klikněte na ovládací prvek, který chcete přidat. Ovládací prvek se přidá s výchozím nastavením.
- Chcete-li ovládací prvek před přidáním upravit, klikněte na ikonu ozubeného kola po vybrání ovládacího prvku. Po úpravě ovládacího prvku klikněte na tlačítko **Hotovo**.

Jak odstranit ovládací prvek

Klikněte na znak X vedle názvu ovládacího prvku.

4.16.2.1 Kybernetická ochrana

Tento ovládací prvek obrazuje souhrnné informace o zablokovaném malwaru, škodlivých adresách URL, nainstalovaných opravách a velikosti záloh.



Na horním řádku je uvedena celková statistika:

- **Velikost aktuálních záloh** – aktuální velikost všech záloh
- **Zablokovaný malware** – počet zablokovaných položek malwaru na všech počítačích
- **Zablokované škodlivé adresy URL** – počet zablokovaných škodlivých adres URL na všech počítačích
- **Zjištěná ohrožení zabezpečení** – počet zjištěných ohrožení zabezpečení na všech počítačích
- **Nainstalované opravy** – počet nainstalovaných aktualizací/oprav na všech počítačích

Na dolním 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 škodlivé adresy URL** – počet aktuálních aktivních výstrah týkajících se zablokovaných škodlivých adres URL
- **Existující ohrožení zabezpečení** – počet aktuálních ohrožení zabezpečení
- **Opravy připravené k instalaci** – počet oprav aktuálně dostupných k instalaci

4.16.2.2 Stav ochrany

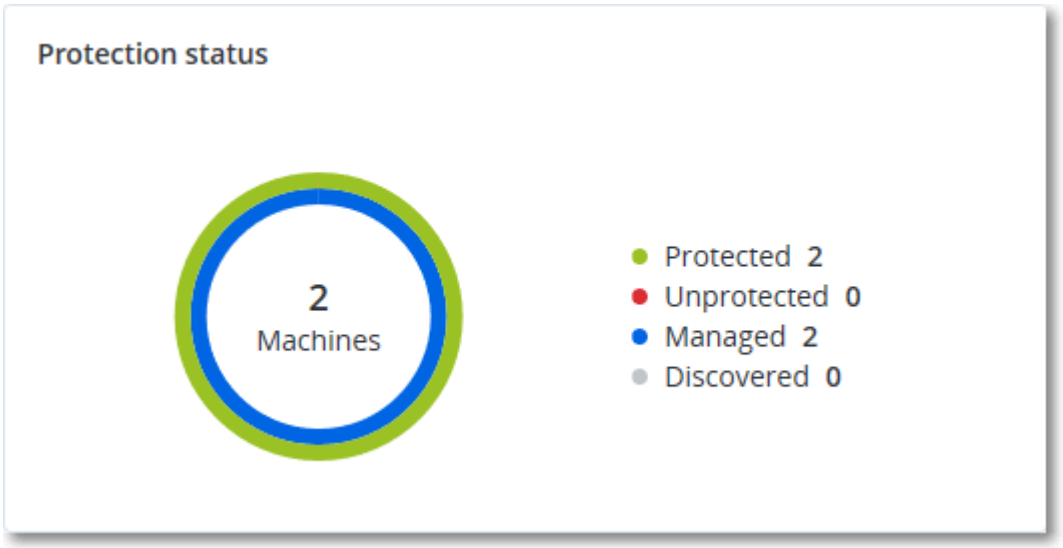
Stav ochrany

Tento ovládací prvek ukazuje aktuální stav ochrany všech počítačů.

Počítač se může nacházet v jednom z následujících stavů:

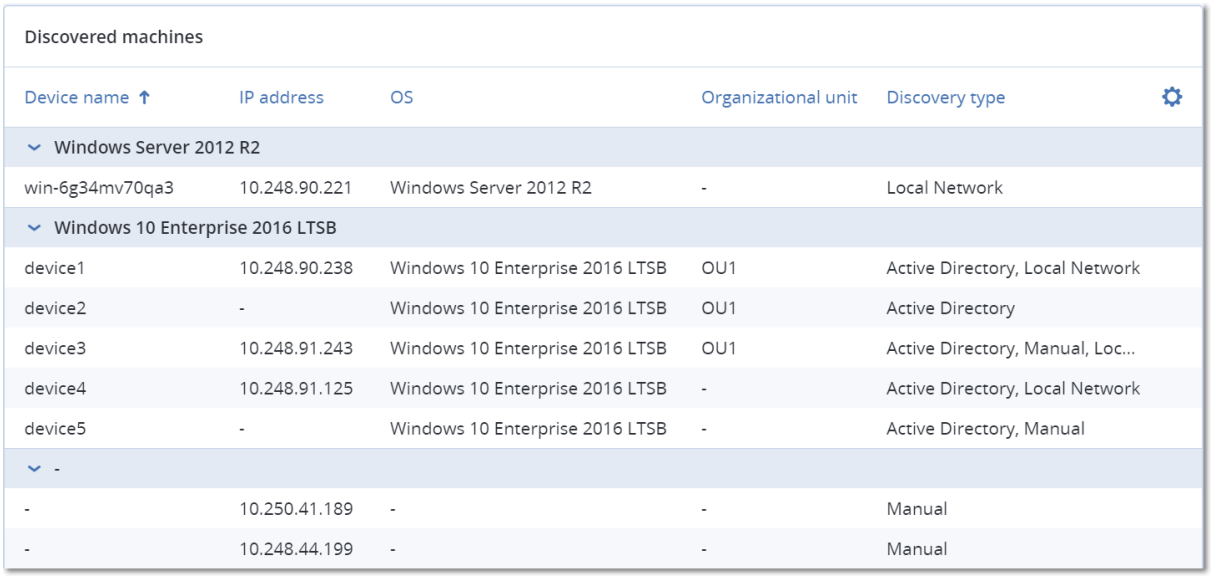
- **Chráněno** – počítače s nainstalovaným agentem ochrany a aktivním plánem ochrany
- **Nechráněno** – počítače s nainstalovaným agentem ochrany, ale bez aktivního plánu ochrany
- **Spravováno** – počítače s nainstalovaným agentem ochrany
- **Zjištěno** – počítače bez nainstalovaného agenta ochrany

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.



4.16.2.3 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 %

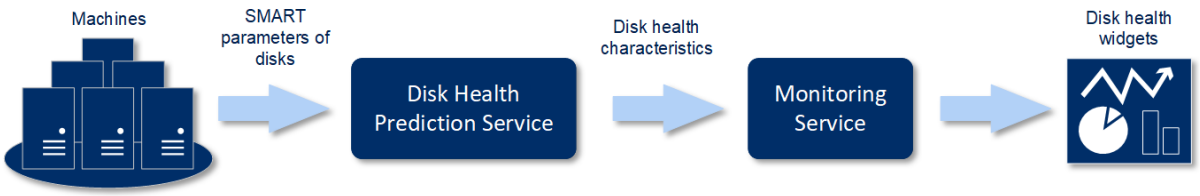
- **Upozornění** – stav disku je 30–70 %
- **Kritický** – stav disku je 0–30 %
- **Probíhá výpočet dat na disku** – probíhá výpočet aktuálního stavu disku a předpovědi

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 získá charakteristiky stavu disku a použije tato data v ovládacích prvcích stavu disku, které se zobrazí uživateli v konzoli.

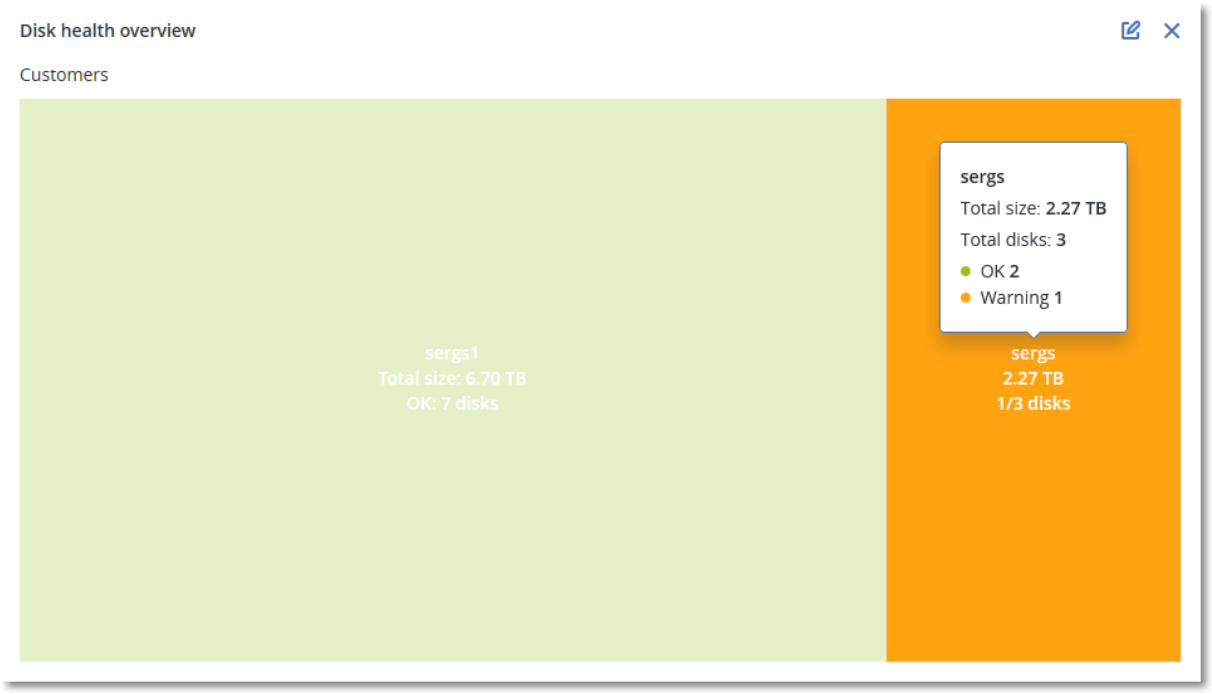


Ovládací prvky stavu disku

Výsledky sledování stavu disku naleznete na kontrolním panelu v ovládacích prvcích souvisejících se stavem disku:

- **Přehled stavu disku** – ovládací prvek stromové mapy se třemi úrovněmi detailů, které lze přepínat procházením:

- Úroveň tenanta zákazníka – zobrazuje souhrnné informace o stavu disku pro vybrané zákazníky. Ovládací prvek obsahuje údaje o nejkritičtějším stavu disku. Ostatní stavy se zobrazí v popisku po umístění kurzoru na konkrétní blok. Velikost bloku zákazníka závisí na celkové velikosti všech disků daného zákazníka. Barva bloku zákazníka závisí na zjištěném nejkritičtějším stavu disku.

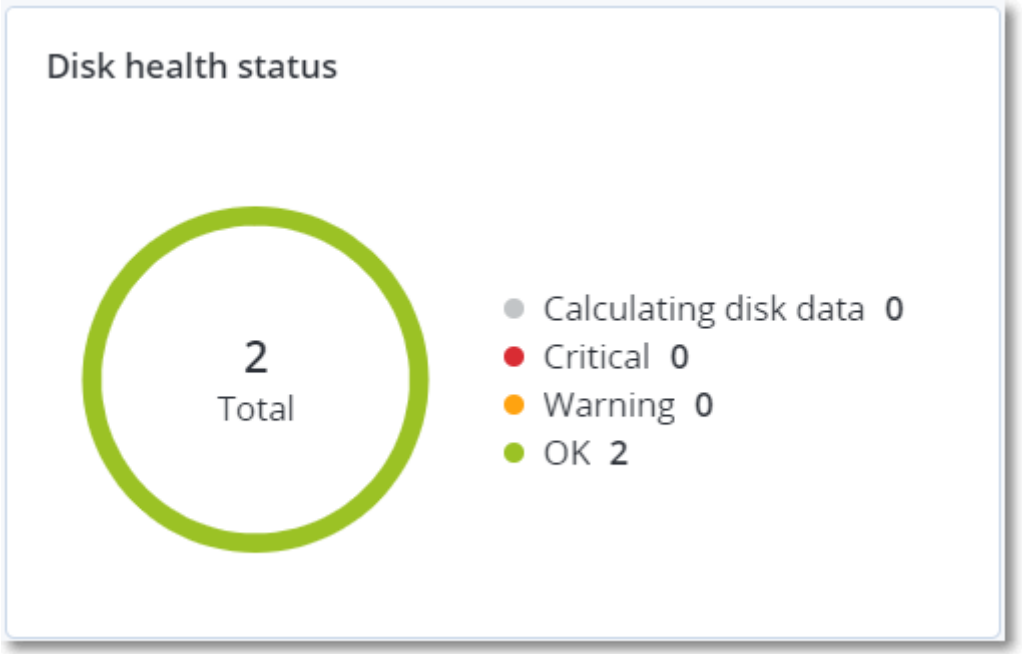


- Úroveň počítače – zobrazuje souhrnné informace o stavu disku pro vybrané počítače zákazníka. Ovládací prvek obsahuje údaje o nejkritičtějším stavu disku. Ostatní stavy se zobrazí v popisku po umístění kurzoru na konkrétní blok. Velikost bloku počítače závisí na celkové velikosti všech disků daného počítače. Barva bloku počítače závisí na zjištěném nejkritičtějším stavu disku.

- Úroveň disku – zobrazuje aktuální stav disku ze všech disků pro vybraného zákazníka a 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.



4.16.2.4 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.

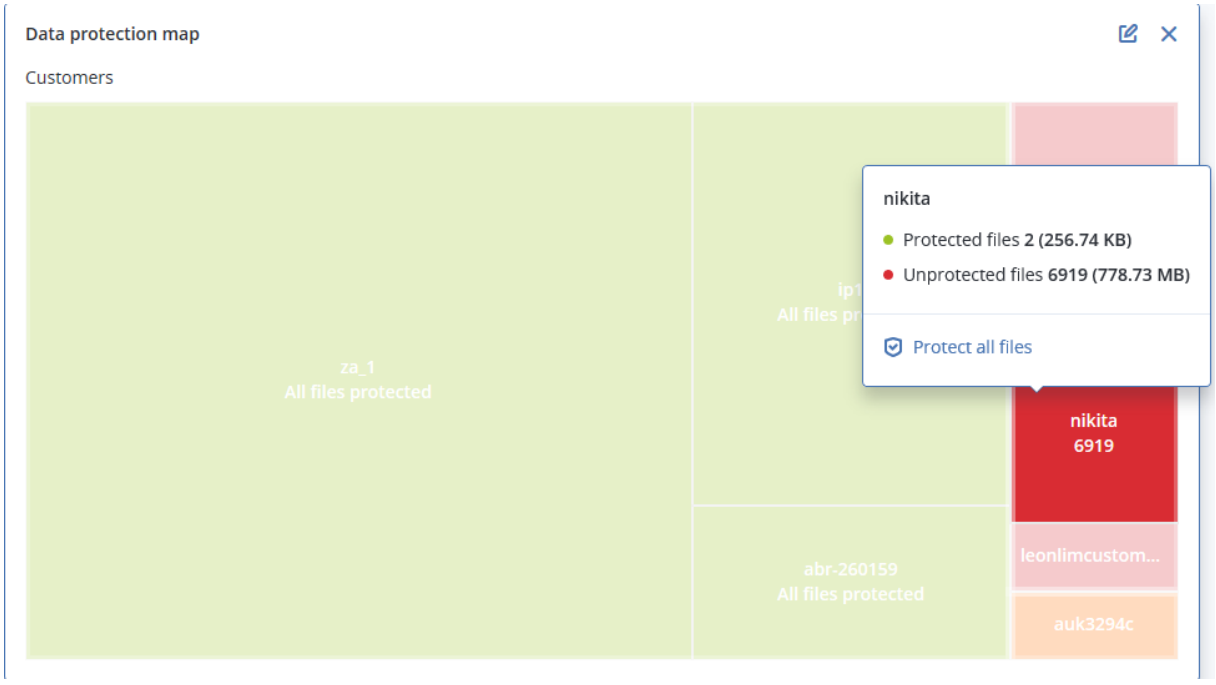
Velikost každého bloku závisí na celkovém počtu/velikosti všech důležitých souborů, které náleží zákazníkovi/počítači.

Soubory mohou mít jeden z následujících stavů ochrany:

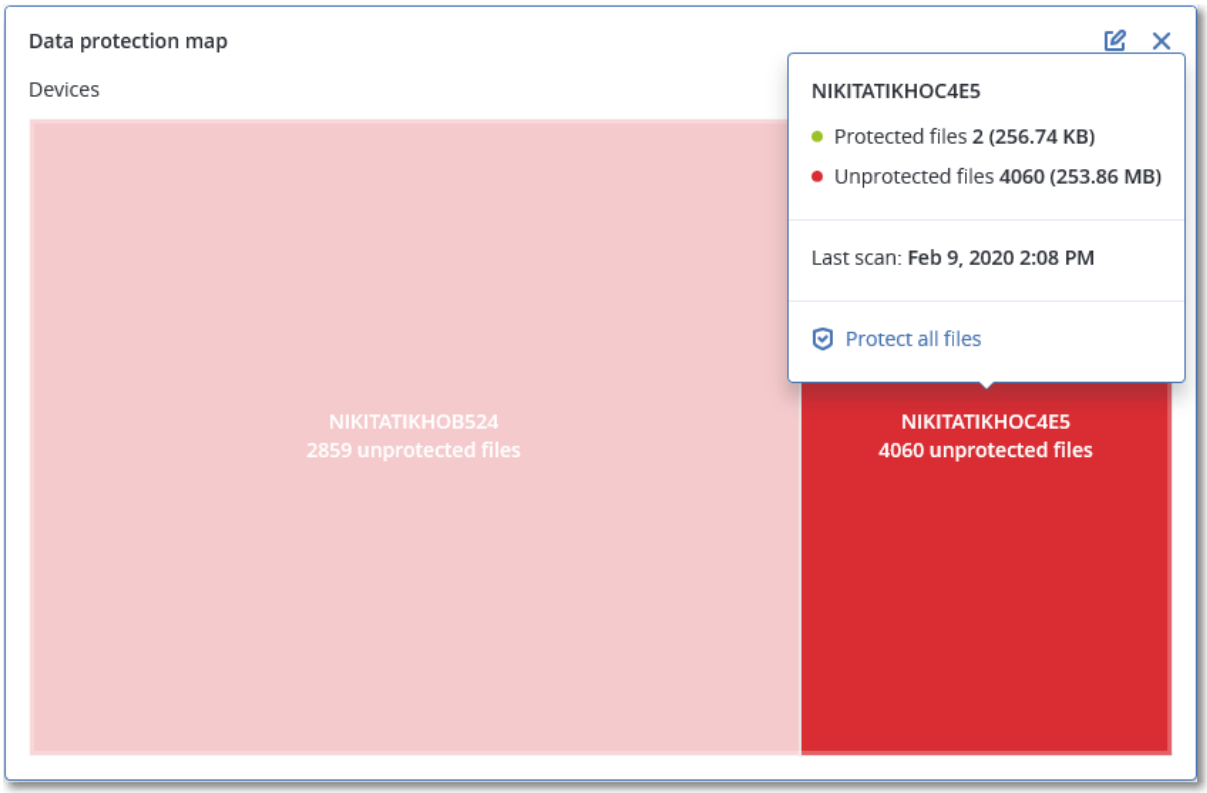
- **Kritický** – existuje 51–100 % nechráněných souborů se zadanými příponami, které nejsou pro vybraného tenanta/počítač/umístění zákazníka zálohovány.
- **Nízký** – existuje 21–50 % nechráněných souborů se zadanými příponami, které nejsou pro vybraného tenanta/počítač/umístění zákazníka zálohovány.
- **Střední** – existuje 1–20 % nechráněných souborů se zadanými příponami, které nejsou pro vybraného tenanta/počítač/umístění zákazníka zálohovány.
- **Vysoký** – všechny soubory se zadanými příponami jsou pro vybraného tenanta/počítač/umístění zákazníka chráněny (zálohovány).

Výsledky kontroly ochrany dat naleznete na kontrolním panelu v ovládacím prvku Mapa ochrany dat, což je prvek stromové mapy se dvěma úrovněmi detailů, které lze přepínat procházením:

- Úroveň tenanta zákazníka – zobrazuje souhrnné informace o stavu ochrany důležitých souborů pro vybrané zákazníky.



- Úroveň počítače – zobrazuje informace o stavu ochrany důležitých souborů pro počítače vybraného zákazníka.



Chcete-li chránit nechráněné soubory, umístěte kurzor na blok a klikněte na příkaz **Chránit všechny soubory**. V dialogovém okně naleznete informace o počtu nechráněných souborů a jejich umístění. Chcete-li je chránit, klikněte na položku **Chránit všechny soubory**.

Můžete si také stáhnout podrobnou zprávu ve formátu CSV.

4.16.2.5 Ovládací prvky posouzení ohrožení zabezpečení

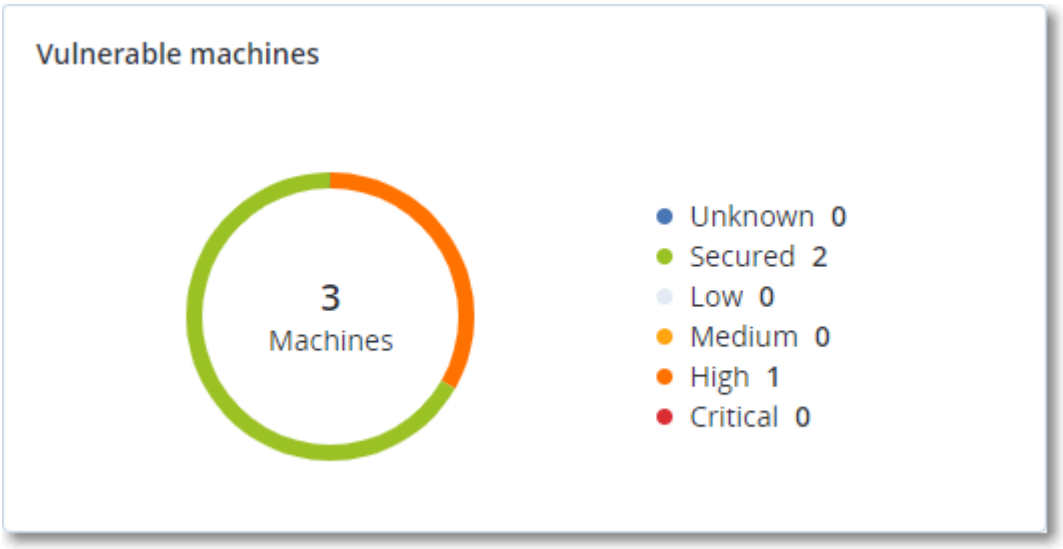
Ohrožené počítače

Tento ovládací prvek zobrazuje ohrožené počítače podle závažnosti ohrožení zabezpečení.

Zjištěné ohrožení zabezpečení může mít jednu z následujících úrovní závažnosti podle rámce CVSS (Common Vulnerability Scoring System):

- Kritická: 9–10 CVSS
- Vysoká: 7–9 CVSS
- Střední: 3–7 CVSS
- Nízká: 0–3 CVSS
- Zabezpečeno: nebyla zjištěna žádná ohrožení zabezpečení

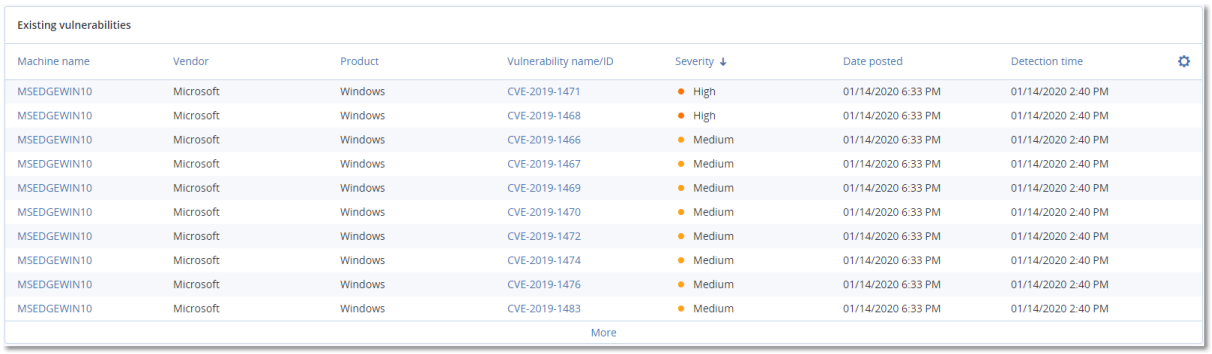
- Neznámý



Stávající zranitelnosti

Tento ovládací prvek zobrazuje aktuální ohrožení zabezpečení na počítačích. V ovládacím prvku **Existující ohrožení zabezpečení** uvidíte dva sloupce s časovými razítky:

- **Čas detekce** – datum a čas, kdy bylo ohrožení zabezpečení na počítači zjištěno poprvé.
- **Datum publikování** – datum a čas, kdy bylo ohrožení zabezpečení na počítači zjištěno naposledy.



Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Date posted	Detection time
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1471	High	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1468	High	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1466	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1467	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1469	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1470	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1472	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1474	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1476	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM
MSEDGEWIN10	Microsoft	Windows	CVE-2019-1483	Medium	01/14/2020 6:33 PM	01/14/2020 2:40 PM

More

4.16.2.6 Ovládací prvky instalace oprav

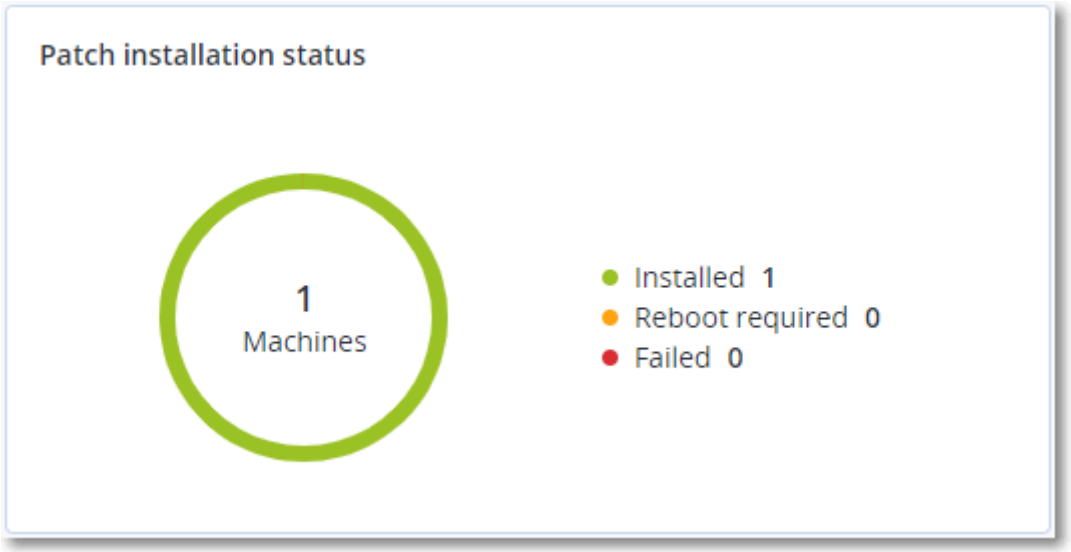
Pro funkci správy oprav jsou k dispozici čtyři ovládací prvky.

Stav instalace opravy

Tento ovládací prvek zobrazuje počet počítačů seskupených podle stavu instalace opravy.

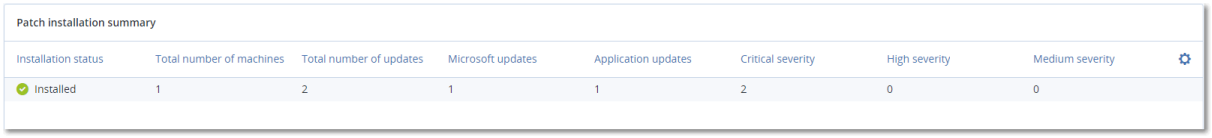
- **Nainstalováno** – všechny dostupné opravy jsou nainstalovány na počítači
- **Nutný restart** – po instalaci opravy je vyžadován restart počítače

- **Nezdařilo se** – instalace opravy se nezdařila



Souhrn instalace opravy

Tento ovládací prvek zobrazuje souhrn oprav na počítačích podle stavu instalace opravy.



Historie instalace oprav

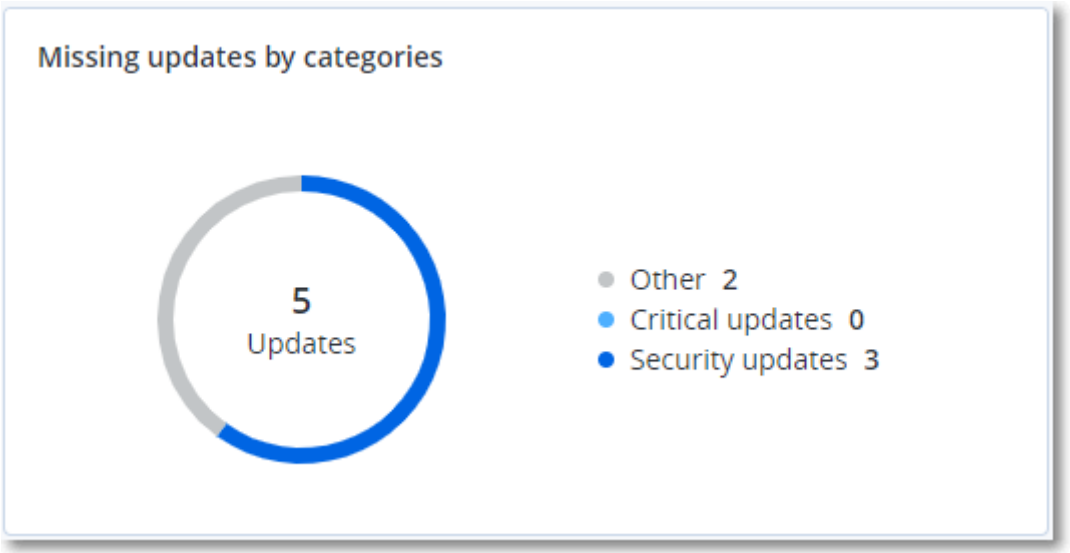
Tento ovládací prvek zobrazuje podrobné informace o opravách na počítačích.

Chybějící aktualizace podle kategorie

Tento ovládací prvek zobrazuje počet chybějících oprav podle kategorie. Zobrazeny jsou následující kategorie:

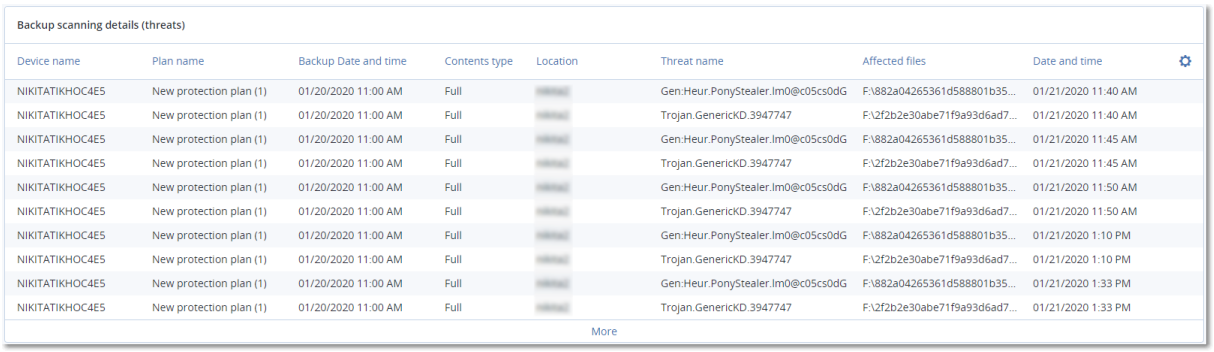
- Aktualizace zabezpečení
- Kritické aktualizace

- Jiné



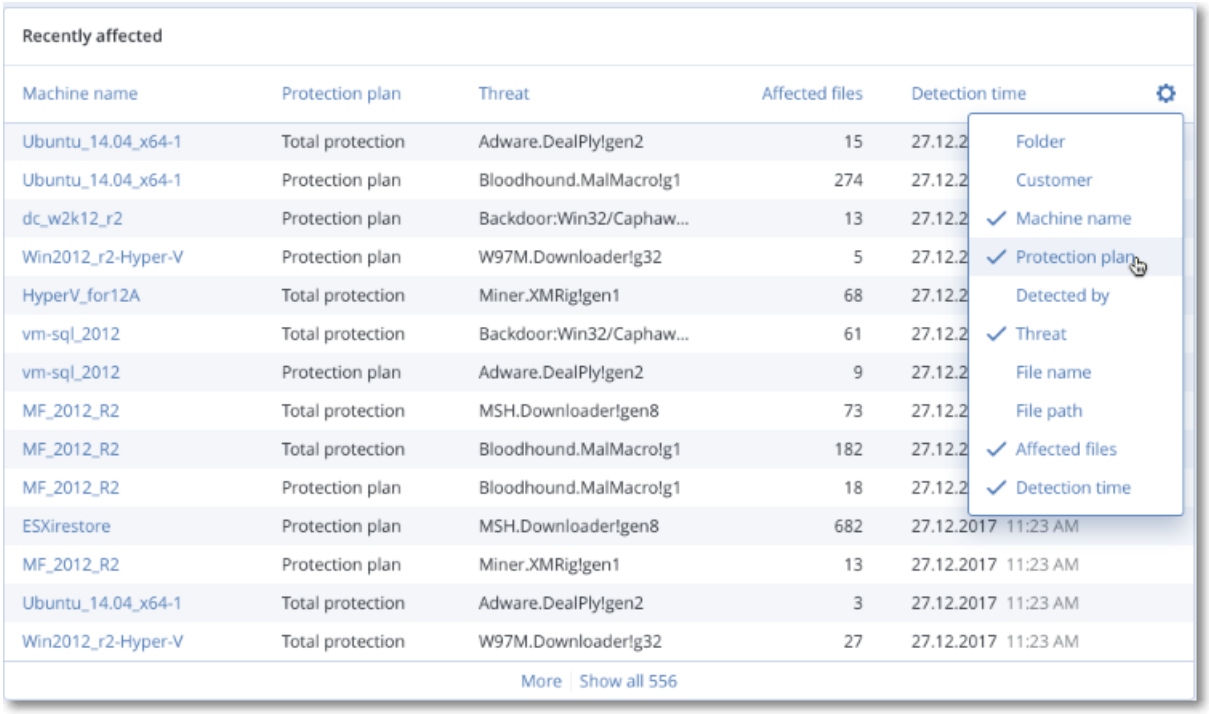
4.16.2.7 Podrobnosti kontroly zálohy

Tento ovládací prvek zobrazuje podrobné informace o zjištěných hrozbách v zálohách.



4.16.2.8 Nedávno napadeno

Tento ovládací prvek zobrazuje podrobné informace o nedávno napadaných počítačích. Naleznete zde informace o zjištěných hrozbách a o počtu infikovaných souborů.



4.17 Zprávy

Chcete-li vytvořit zprávy o použití a operacích služeb, klikněte na **Zprávy**.

4.17.1 Využití

Zprávy o využití obsahují historická data týkající se používání služby.

Typ zprávy

Je možné vybrat jednu z následujících typů zpráv:

- **Aktuální využití**

  Zpráva obsahuje metriky využití aktuální služby.

  Metriky využití jsou vypočítávány v rámci zúčtovacích období jednotlivých podřízených tenantů. Pokud mají tenaty zahrnuté ve zprávě odlišná zúčtovací období, může se využití nadřízeného tenanta lišit od součtu využití podřízených tenantů.
- **Distribuce aktuálního využití**

  Tato práva je k dispozici pouze pro tenanty partnerů spravovaných externím systémem poskytování. Tato zpráva je užitečná, když se zúčtovací období podřízených tenantů neshodují se zúčtovacím obdobím nadřízeného tenanta. Zpráva obsahuje metriky využití aktuální služby pro podřízené tenanty, které jsou vypočítané v rámci aktuálního zúčtovacího období nadřízeného tenata. Využití nadřízeného tenanta je zaručeně rovno součtu využití podřízených tenantů.
- **Souhrn pro období**

Zpráva obsahuje metriky využití služby na konci zadaného období a rozdíly mezi metrikami na začátku a na konci zadaného období.

- **Po dnech pro období**

  Zpráva obsahuje metriky využití služby a jejich změny za každý den v uvedeném období.

Rozsah zprávy

Jako rozsah zprávy můžete vybrat některou z těchto hodnot:

- **Přímí zákazníci a partneři**

  Výpis bude obsahovat metriky využití služby pouze pro přímé podřízené tenanty tenanta, ve kterém pracujete.
- **Všichni zákazníci a partneři**

  Výpis bude obsahovat metriky využití služby pro všechny podřízené tenanty tenanta, ve kterém pracujete.
- **Všichni zákazníci, partneři a uživatelé**

  Výpis bude obsahovat metriky využití služby pro všechny podřízené tenanty tenanta, ve kterém pracujete, a pro všechny uživatele v tenantech.

Naplánované zprávy

Naplánovaná zpráva obsahuje metriky využití služby za poslední celý kalendářní měsíc. Zprávy se generují ve 23:59:59 UTC vždy první den v měsíci a odesílají se druhý den stejného měsíce. Zprávy se posílají všem správcům tenanta, kteří mají v uživatelském nastavení zaškrtnuté políčko **Naplánované zprávy o využití**.

Povolení nebo zakázání naplánované zprávy

1. Přihlaste se do portálu pro správu.
2. Zkontrolujte, že se nacházíte v tenantu nejvyšší úrovně, který máte k dispozici.
3. Klikněte na možnost **Zprávy** > **Použití**.
4. Klikněte na možnost **Naplánované**
5. Zaškrtněte nebo zrušte zaškrtnutí políčka **Odeslat měsíční souhrnnou zprávu**.
6. V části **Úroveň podrobnosti** vyberte rozsah zprávy, jak je popsáno výše.

Vlastní zprávy

Tento typ zprávy je možné vygenerovat na požádání a nelze jej naplánovat. Zpráva bude zaslána na vaši e-mailovou adresu.

Generování vlastní zprávy

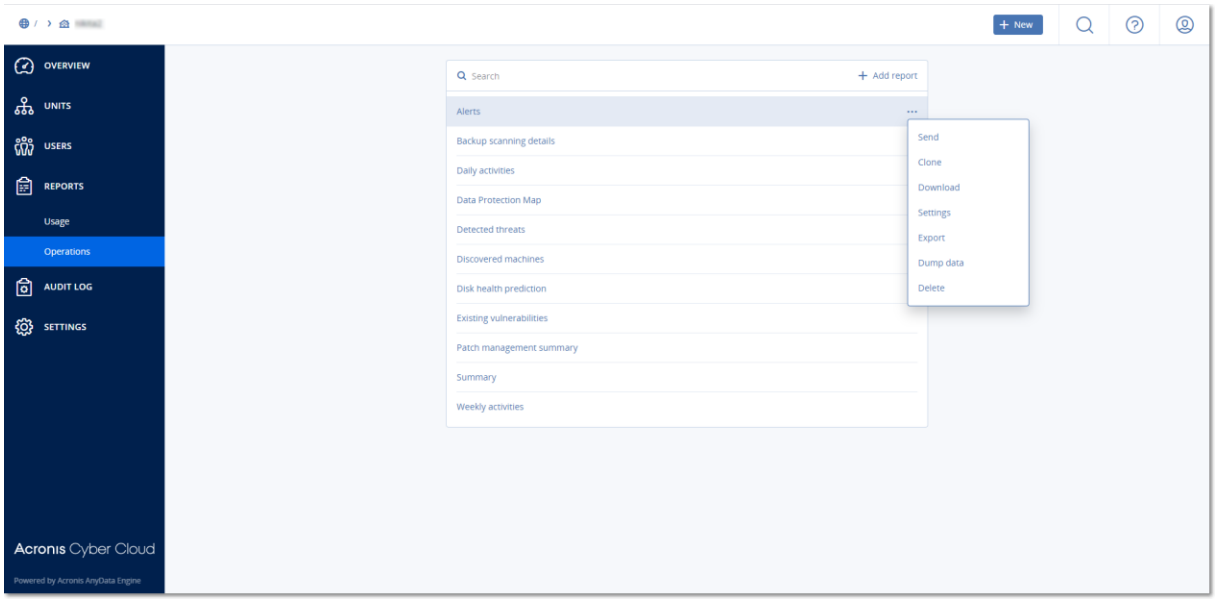
1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), pro který chcete vytvořit zprávu.
3. Klikněte na možnost **Zprávy** > **Použití**.
4. Vyberte kartu **Vlastní**.
5. V části **Typ** vyberte typ zprávy, jak je popsáno výše.
6. [Není k dispozici pro typ zprávy **Aktuální využití**.] V části **Období** vyberte období pro zprávu:
   - **Aktuální kalendářní měsíc**
   - **Předchozí kalendářní měsíc**
   - **Vlastní**
7. [Není k dispozici pro typ zprávy **Aktuální využití**.] Pokud chcete zadat vlastní období pro zprávu, vyberte počáteční a koncové datum. Jinak tento krok přeskočte.

8. V části **Úroveň podrobnosti** vyberte rozsah zprávy, jak je popsáno výše.
9. Zprávu vygenerujete kliknutím na možnost **Generovat a odeslat**.

4.17.2 Operace

Zpráva o operacích může obsahovat jakoukoli sadu ovládacích prvků kontrolního panelu (str. 41) **Operace**. Ve výchozím nastavení zobrazují všechny ovládací prvky shrnující informace za tenanta, ve kterém pracujete. Změny můžete provést jednotlivě úpravou každého ovládacího prvku nebo najednou v nastavení zpráv. Všechny ovládací prvky zobrazují parametry za stejný časový rozsah. Tento rozsah můžete změnit v nastavení zpráv.

Můžete použít výchozí zprávy nebo vytvořit vlastní.



Výchozí zprávy jsou uvedeny níže:

Název zprávy	Popis	K dispozici v edici služby
Výstrahy	Zobrazuje výstrahy, ke kterým došlo během zadaného časového období.	Cyber Backup, Cyber Protect
Podrobnosti kontroly zálohy	Zobrazuje podrobné informace o zjištěných hrozbách v zálohách.	Cyber Protect
Denní aktivity	Zobrazuje souhrnné informace o aktivitách provedených během zadaného časového období.	Cyber Backup, Cyber Protect
Mapa ochrany dat	Zobrazuje podrobné informace o počtu, velikosti, umístění a stavu ochrany všech důležitých souborů na počítačích.	Cyber Protect
Zjištěné hrozby	Zobrazuje podrobnosti dotčených počítačů podle počtu zablokovaných hrozeb a počtu ohrožených počítačů a počítačů, které ohroženy nejsou.	Cyber Backup, Cyber Protect
Zjištěné počítače	Zobrazuje všechny počítače nalezené v síti organizace.	Cyber Backup, Cyber Protect

Předpověď stavu disku	Zobrazuje předpovědi výpadku vašeho pevného disku nebo disku SSD a aktuální stav disku.	Cyber Protect
Stávající zranitelnosti	Zobrazuje existující ohrožení zabezpečení pro operační systém a aplikace ve vaší organizaci. Zobrazuje také podrobnosti dotčených počítačů ve vaší síti pro každý uvedený produkt.	Cyber Backup, Cyber Protect
Souhrn správy oprav	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.	Cyber Protect
Shrnutí	Zobrazuje souhrnné informace o chráněných zařízeních pro zadané časové období.	Cyber Backup, Cyber Protect
Týdenní aktivity	Zobrazuje souhrnné informace o aktivitách provedených během zadaného časového období.	Cyber Backup, Cyber Protect

Zprávu zobrazíte kliknutím na její název.

Chcete-li ze zprávy přejít na operace, klikněte na ikonu svislých tří teček na řádku zprávy. Stejné operace jsou k dispozici uvnitř zprávy.

Přidání zprávy

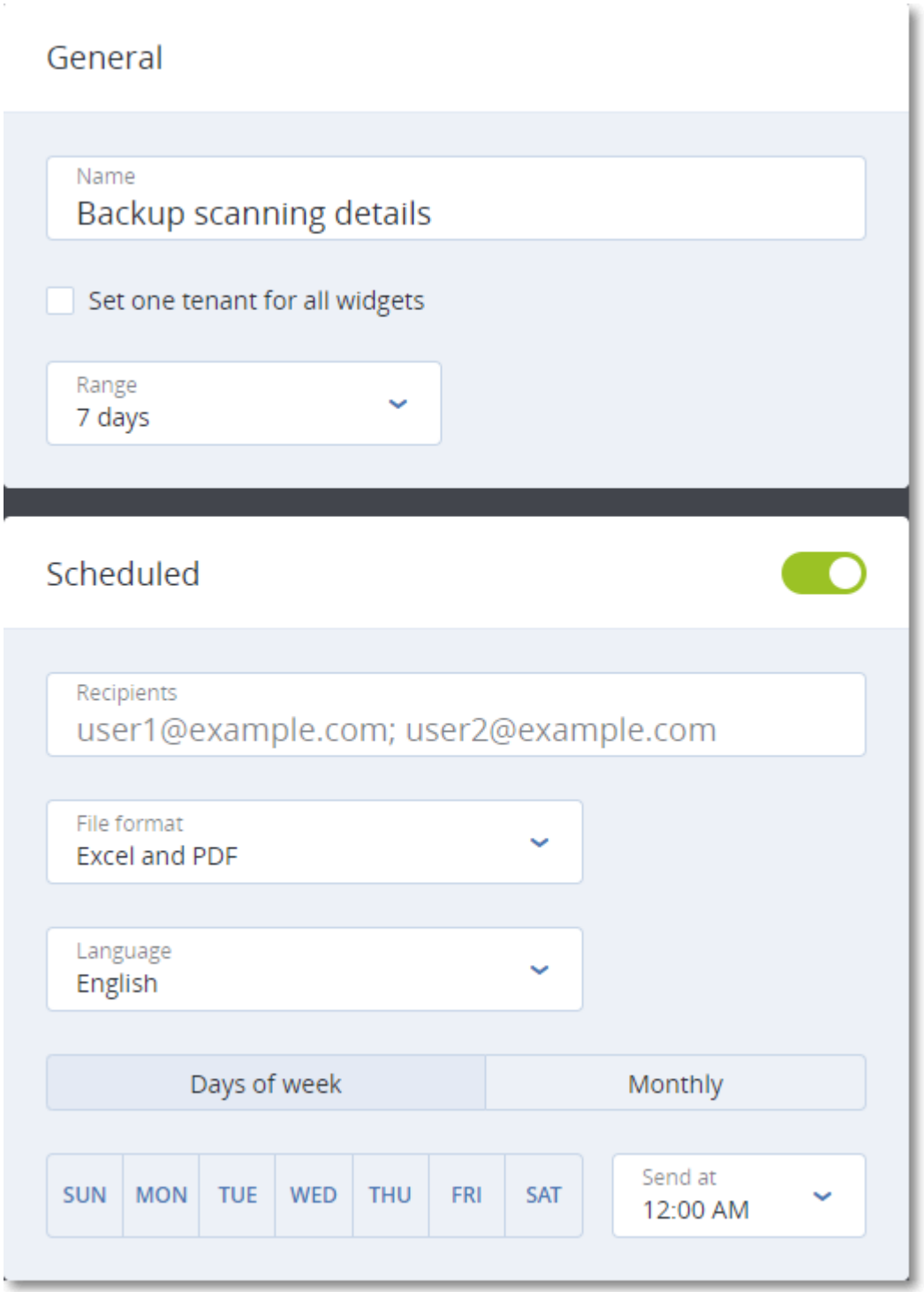
1. Klikněte na **Přidat zprávu**.
2. Proveďte jeden z následujících úkonů:
   - Předdefinovanou zprávu přidáte kliknutím na její název.
   - Chcete-li přidat vlastní zprávu, klikněte na **Vlastní**, na název zprávy (výchozí přiřazené názvy jsou například **Vlastní(1)**) a potom do zprávy přidejte ovládací prvky.
3. [Volitelné] Ovládací prvky přesunete kliknutím a přetažením.
4. [Volitelné] Zprávu upravíte podle kroků popsaných níže.

Úprava zprávy

Zprávu upravíte kliknutím na její název a potom na možnost **Nastavení**. Při úpravách zprávy můžete:

- zprávu přejmenovat,
- změnit zobrazeného tenanta pro všechny ovládací prvky obsažené ve zprávě,
- změnit časový rozsah pro všechny ovládací prvky obsažené ve zprávě,

- naplánovat odesílání zprávy e-mailem ve formátu PDF nebo XLSX.



Naplánování zprávy

1. Klikněte na název zprávy a potom na **Nastavení**.
2. Zvolte přepínač **Plánovaná**.
3. Zadejte e-mailové adresy příjemců.
4. Vyberte formát zprávy: .pdf, .xlsx nebo oba.
5. Vyberte dny a čas odesílání zprávy.
6. Klikněte na **Uložit** v pravém horním rohu.

Export a import struktury zprávy

Strukturu zprávy (sadu ovládacích prvků a nastavení zprávy) můžete exportovat a importovat ze souboru JSON. Může to být užitečné při kopírování struktury zprávy z jednoho tenanta do jiného.

Chcete-li exportovat strukturu zprávy, klikněte na ikonu svislých tří teček v pravém horním rohu a potom na možnost **Exportovat**.

Strukturu zprávy naimportujete kliknutím na možnost **Přidat zprávu** a potom na možnost **Importovat**.

Výpis dat ze zprávy

Výpis dat ze zprávy můžete odeslat e-mailem v souboru CSV. Výpis zahrnuje veškerá data ze zprávy (bez filtrování) pro vlastní časový rozsah. Časové značky ve zprávách CSV jsou ve formátu UTC, zatímco ve zprávách ve formátu Excel nebo PDF jsou v aktuálním systémovém časovém pásmu.

Software generuje výpis dat průběžně. Pokud zadáte dlouhé časové období, může tato akce trvat poměrně dlouho.

Jak vytvořit výpis dat ze zprávy

1. Klikněte na název zprávy.
2. Klikněte na ikonu svislých tří teček v pravém horním rohu a potom na možnost **Vypsat data**.
3. Zadejte e-mailové adresy příjemců.
4. V části **Časový rozsah** zadejte časový rozsah.
5. Klikněte na možnost **Odeslat**.

4.17.3 Časová pásma ve zprávách

Časová pásma použitá ve zprávách se liší v závislosti na typu zprávy. Následující tabulka obsahuje referenční informace.

Umístění a typ zprávy	Časové pásmo použité ve zprávě
Portál pro správu > Přehled > Operace (ovládací prvky)	Čas vygenerování zprávy je v časovém pásmu počítače, kde je spuštěný prohlížeč.
Portál pro správu > Přehled > Operace (exportováno do PDF nebo xslx)	▪ Časová značka exportované zprávy je v časovém pásmu počítače, který byl použit k exportu zprávy. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.
Portál pro správu > Zprávy > Využití > Naplánované zprávy	▪ Zpráva se generuje ve 23:59:59 UTC vždy první den v měsíci. ▪ Zpráva se odesílá druhý den v měsíci.
Portál pro správu > Zprávy > Využití > Vlastní zprávy	Časové pásmo a datum zprávy je UTC.
Portál pro správu > Zprávy > Operace (ovládací prvky)	▪ Čas vygenerování zprávy je v časovém pásmu počítače, kde je spuštěný prohlížeč. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.

Umístění a typ zprávy	Časové pásmo použité ve zprávě
Portál pro správu > Přehled > Operace (ovládací prvky)	Čas vygenerování zprávy je v časovém pásmu počítače, kde je spuštěný prohlížeč.
Portál pro správu > Zprávy > Operace (exportováno do PDF nebo xslx)	▪ Časová značka exportované zprávy je v časovém pásmu počítače, který byl použit k exportu zprávy. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.
Portál pro správu > Zprávy > Operace (naplánované doručení)	▪ Časové pásmo doručení zprávy je UTC. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.
Portál pro správu > Uživatelé > Denní shrnutí aktivních výstrah	▪ Tato zpráva se odesílá jednou denně od 10:00 do 23:59 UTC. Čas odeslání zprávy závisí na pracovním zatížení datového centra. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.
Portál pro správu > Uživatelé > Oznámení o stavu kybernetické ochrany	▪ Tato zpráva se odesílá po dokončení aktivity. ***Poznámka*** *V závislosti na pracovním zatížení datového centra mohou být některé zprávy zasílány s prodlením.* ▪ Časové pásmo aktivity ve zprávě je UTC.

4.18 Protokol auditu

Chcete-li zobrazit protokol auditu, klikněte na možnost **Protokol auditu**.

Protokol auditu obsahuje chronologický záznam následujících událostí:

- Operace provedené uživateli na portálu pro správu
- Systémové zprávy o dosažených kvótách a využití kvót

Tento protokol zobrazuje události v tenantovi, ve které právě pracujete, a v jeho podřízených tenantech. Kliknutím na libovolnou událost zobrazíte podrobnější informace o této události.

Protokoly auditu jsou uchovávány v datovém centru Acronis a na jejich dostupnost nemají vliv problémy na počítačích koncového uživatele.

Protokol je denně čištěn. Události jsou z protokolu odebrány po 180 dnech.

Pole protokolu auditu

Pro každou událost protokol zobrazuje následující informace:

- **Událost**

  Stručný popis události. Příklady: **Tenant byl vytvořen**, **Tenant byl odstraněn**, **Uživatel byl vytvořen**, **Uživatel byl odstraněn**, **Byla dosažena kvóta**.
- **Závažnost**

  Může být uvedena jedna z následujících možností:
  - **Chyba**

Označuje chybu.

- **Upozornění**

  Označuje potenciálně negativní akci. Příklady: **Tenant byl odstraněn**, **Uživatel byl odstraněn**, **Byla dosažena kvóta**.

- **Poznámka**

  Označuje událost, která může vyžadovat pozornost. Příklady: **Tenant byl aktualizován**, **Uživatel byl aktualizován**.

- **Informační**

  Označuje neutrální informativní změnu nebo akci. Příklady: **Tenant byl vytvořen**, **Uživatel byl vytvořen**, **Kvóta byla aktualizována**.

- **Datum**

  Datum a čas, kdy došlo k události.

- **Název objektu**

  Objekt, se kterým byla operace provedena. Například objektem události **Uživatel byl aktualizován** je uživatel, jehož vlastnosti byly změněny. Pro události, které se týkají kvóty, je objektem kvóta.

- **Tenant**

  Název tenanta, do kterého náleží objekt.

- **Spouštěč**

  Přihlašovací jméno uživatele, který spustil událost. U systémových zpráv a událostí spuštěných správci vyšší úrovně je spouštěč zobrazen jak **Systém**.

- **Tenant spouštěče**

  Název tenanta, do kterého náleží spouštěč. U systémových zpráv a událostí spuštěných správci vyšší úrovně je toto pole prázdné.

- **Metoda**

  Určuje, jestli událost pochází z webového rozhraní nebo z rozhraní API.

- **IP**

  IP adresa počítače, ze které událost pochází.

Filtrování a hledání

Události můžete filtrovat podle popisu, závažnosti nebo data. Události můžete dále vyhledávat podle objektu, jednotky, spouštěče a jednotky spouštěče.

5 Pokročilé scénáře

5.1 Přesunutí tenanta do jiného tenanta

Na portálu pro správu můžete přesunout tenanta z jednoho nadřazeného tenanta do jiného. To je užitečné, pokud chcete přesunout zákazníka z jednoho partnera do jiného, nebo pokud jste si vytvořili tenanta složky kvůli uspořádání klientů a chcete některé z klientů přesunout do nově vytvořené složky.

Omezení

- Partnera / tenanta složky můžete přesunout pouze do partnera / tenanta složky.

- Tenanta zákazníka můžete přesunout pouze do partnera / složky tenanta.
- Tenanta nelze přesunout do jeho podřízeného tenanta.
- Tenanta jednotky nelze přesunout.
- Tenanta lze přesunout, pouze pokud cílový nadřazený tenant má stejnou nebo větší sadu služeb a nabízených položek jako původní nadřazený tenant.
- Partner nemůže přesouvat tenanty mezi skupinami se stejnou úrovní hierarchie.
- Při přesouvání tenanta zákazníka musí v cílovém nadřazeném tenantu existovat všechna úložiště, která jsou k tenantu zákazníka přiřazena v původním nadřazeném tenantu. Důvodem je to, že data zákazníka související se službou nelze přesouvat mezi úložišti.

Jak přesunout tenanta

1. Přihlaste se do portálu pro správu.
2. Na kartě **Klienti** vyberte cílového tenanta, do kterého chcete provést přesun.
3. Na panelu vlastností tenanta klikněte na ikonu svislých tří teček a potom na možnost **Zobrazit ID**.
4. Zkopírujte text zobrazený v poli **Interní ID** a klikněte na tlačítko **Zrušit**.
5. Na kartě **Klienti** vyberte tenanta, kterého chcete přesunout.
6. Na panelu vlastností tenanta klikněte na ikonu svislých tří teček a potom na možnost **Přesunout**.
7. Vložte interní ID cílového tenanta a potom klikněte na možnost **Přesunout**.

5.2 Převod tenanta typu partner na tenanta typu složka a naopak

Tento portál pro správu umožňuje převést tenanta typu partner na tenanta typu složka.

Je to užitečné, když jste použili tenanta typu partner k vytvoření skupin a nyní chcete správně uspořádat infrastrukturu tenanta. Je to také výhodné, pokud chcete, aby operační kontrolní panel (str. 41) zahrnoval souhrnné informace o tenantovi.

Můžete také převést tenanta typu složka na tenanta typu partner.

Poznámka *Převod je bezpečná operace a nemá vliv na uživatele v rámci tenanta ani na žádná data související se službami.*

Jak převést tenanta

1. Přihlaste se do portálu pro správu.
2. Na kartě **Klienti** vyberte tenanta, kterého chcete převést.
3. Proveďte jeden z následujících úkonů:
   - Klikněte na ikonu tří teček vedle názvu tenanta.
   - Vyberte tenanta a potom klikněte na ikonu tří teček na panelu vlastností tenanta.
4. Klikněte na možnost **Převést na složku** nebo **Převést na partnera**.
5. Potvrďte své rozhodnutí.

5.3 Omezení přístupu k webovému rozhraní

Správci mohou omezit přístup k webovému rozhraní zadáním seznamu IP adres, ze kterých se mohou členové tenantu přihlašovat.

Toto omezení platí také pro přístup k portálu pro správu prostřednictvím API.

Toto omezení platní pouze pro úroveň, ve které bylo nastaveno. Toto omezení *neplatí* pro členy podřízených tenantů.

Jak omezit přístup k webovému rozhraní

1. Přihlaste se do portálu pro správu.
2. Přejděte do tenanta (str. 20), ve kterém chcete omezit přístup.
3. Klikněte na **Nastavení** > **Zabezpečení**.
4. Zapněte přepínač **Ovládací prvek pro přihlášení**.
5. V části **Povolené IP adresy** zadejte povolené IP adresy.

   Můžete zadat libovolné z následujících parametrů (oddělené středníkem):

   - IP adresy, například: 192.0.2.0
   - Rozsahy IP adres, například: 192.0.2.0-192.0.2.255
   - Podsítě, například: 192.0.2.0/24
6. Klikněte na tlačítko **Uložit**.

5.4 Omezení přístupu k vašemu tenantu

Správci na úrovni zákazníka a vyšší mohou správcům vyšší úrovně omezit přístup ke svým tenantům.

Pokud je přístup k tenantu omezen, mohou správci nadřazeného tenanta pouze upravovat vlastnosti tenanta. Účty a podřízené tenanty vůbec nevidí.

Zabránění přístupu správcům vyšší úrovně k vašemu tenantu

1. Přihlaste se do portálu pro správu.
2. Klikněte na **Nastavení** > **Zabezpečení**.
3. Zakažte přepínač **Podpora přístupu**.

5.5 Integrace se systémy třetích stran

Poskytovatel služby může platformu Acronis Cyber Cloud integrovat se systémem třetí strany, a to následovně:

- Nastavením rozšíření platformy v tomto systému (str. 63).

  Na stránce **Integrace** portálu pro správu jsou uvedena rozšíření pro nejoblíbenější systémy PSA (Professional Services Automations) (PSA) a RMM (Remote Monitoring and Management).

  Toto je doporučený způsob integrace platformy.
- Vytvořením klienta API pro systém (str. 64) a povolením přístupu k rozhraním API platformy a jejím službám pro systém. Klienti API jsou součástí autorizačního prostředí OAuth 2.0 platformy. Další informace o ověřování OAuth 2.0 viz https://tools.ietf.org/html/rfc6749.

  Toto je základní způsob integrace platformy, který vyžaduje znalost programování. Doporučujeme ho využít, pokud pro systém neexistuje žádné rozšíření platformy nebo pokud má být systém přizpůsoben pro takové případy správy platformy a jejích služeb, na které se nevztahuje dostupné rozšíření.

5.5.1 Nastavení rozšíření Acronis Cyber Cloud

1. Přihlaste se do portálu pro správu.
2. Klikněte na **Nastavení** > **Integrace**.
3. Klikněte na název systému třetí strany, se kterým chcete povolit integraci.

4. Postupujte podle pokynů na obrazovce.

Další informace o integraci se systémy třetích stran jsou dostupné v části týkající se integrace na webu Acronis.

5.5.2 Správa klientů API

Systémy třetích stran lze s platformou Acronis Cyber Cloud integrovat pomocí rozhraní API. Přístup k těmto rozhraním API je povolen prostřednictvím klientů API, které tvoří nedílnou součást autorizačního prostředí OAuth 2.0 platformy.

Co je klient API?

Klient API je speciální účet platformy reprezentující systém třetí strany, který potřebuje provést ověření a mít oprávnění pro přístup k datům v rozhraních API platformy a jejích službách.

Přístup klienta je omezen na tenanta, kde správce vytvoří klienta a jeho podřízené tenanty.

Při vytváření klient zdědí role služby účtu správce, které nelze později změnit. Změna rolí účtu správce nebo zakázání tohoto účtu nemá na klienta vliv.

Pověření klienta zahrnují jedinečný identifikátor (ID) a tajný kód. Platnost pověření nevyprší a nelze je použít k přihlášení na portále pro správu ani ke konzoli služby. Tajný kód lze resetovat.

Pro klienta nelze povolit dvojúrovňové ověřování.

Typický postup integrace

1. Správce vytvoří klienta API v tenantovi, který bude spravovat systém třetí strany.
2. Správce v systému třetí strany povolí tok pověření klienta OAuth 2.0.

   Podle tohoto toku by měl systém před přístupem k tenantovi a jeho službám prostřednictvím rozhraní API nejprve na platformu odeslat pověření vytvořenému klientovi s využitím autorizačního rozhraní API. Platforma vygeneruje a zpět zašle token zabezpečení, což je jedinečný kryptický řetězec přiřazený tomuto konkrétnímu klientovi. Systém pak musí tento token přidat do všech požadavků API.

   Díky tokenu zabezpečení není nutné s požadavky API předávat pověření klienta. Pro účely většího zabezpečení je platnost tokenu dvě hodiny. Po uplynutí této doby všechny požadavky API s vypršelým tokenem selžou a systém bude muset na platformě vyžádat nový token.

Další informace o používání autorizačních rozhraní API a rozhraní API platformy naleznete v příručce pro vývojáře na adrese https://developer.acronis.com/doc/platform/management/v2.

5.5.2.1 Vytvoření klienta API

1. Přihlaste se do portálu pro správu.
2. Klikněte na položky **Nastavení** > **Klienti API** > **Vytvořit klienta API**.
3. Zadejte název klienta API.
4. Klikněte na tlačítko **Další**.

   Klient API je vytvořen se stavem **Aktivní** (výchozí nastavení).
5. Zkopírujte a uložte ID a tajný kód klienta a adresu URL datového centra. Budete je potřebovat při povolování toku pověření klienta OAuth 2.0 v systému třetí strany.

   Důležité *Z bezpečnostních důvodů se tajný kód zobrazí pouze jednou. Pokud tento kód ztratíte, nebude možné ho znovu zobrazit. Můžete ho pouze resetovat.*

6. Klikněte na tlačítko **Hotovo**.

5.5.2.2 Resetování tajného kódu klienta API

1. Přihlaste se do portálu pro správu.
2. Klikněte na položky **Nastavení** > **Klienti API**.
3. Vyhledejte v seznamu požadovaného klienta.
4. Pokračujte kliknutím na tlačítko a na položku **Resetovat tajný kód**.
5. Potvrďte své rozhodnutí kliknutím na tlačítko **Další**.

   Vygeneruje se nový tajný klíč. ID klienta a adresa URL datového centra se nezmění.

   Všechny tokeny zabezpečení přiřazené k tomuto klientovi okamžitě vyprší a požadavky API s těmito tokeny selžou.
6. Zkopírujte a uložte nový tajný kód klienta.

   Důležité *Z bezpečnostních důvodů se tajný kód zobrazí pouze jednou. Pokud tento kód ztratíte, nebude možné ho znovu zobrazit. Můžete ho pouze resetovat.*
7. Klikněte na tlačítko **Hotovo**.

5.5.2.3 Zakázání klienta API

1. Přihlaste se do portálu pro správu.
2. Klikněte na položky **Nastavení** > **Klienti API**.
3. Vyhledejte v seznamu požadovaného klienta.
4. Pokračujte kliknutím na tlačítko  a potom klikněte na **Vypnout**.
5. Potvrďte své rozhodnutí.

   Stav klienta se změní na **Zakázáno**.

   Požadavky API s tokeny zabezpečení, které jsou přiřazeny tomuto klientovi, selžou, ale tokeny nevyprší okamžitě. Zakázání klienta nemá vliv na čas vypršení platnosti tokenů.

   Klienta bude možné kdykoli znovu povolit.

5.5.2.4 Povolení a zakázání klienta API

1. Přihlaste se do portálu pro správu.
2. Klikněte na položky **Nastavení** > **Klienti API**.
3. Vyhledejte v seznamu požadovaného klienta.
4. Pokračujte kliknutím na tlačítko  a potom klikněte na **Povolit**.

   Stav klienta se změní na **Aktivní**.

   Požadavky API s tokeny zabezpečení, které jsou přiřazeny tomuto klientovi, budou úspěšné, pokud tokeny ještě nevypršely.

5.5.2.5 Odstranění klienta API

1. Přihlaste se do portálu pro správu.
2. Klikněte na položky **Nastavení** > **Klienti API**.
3. Vyhledejte v seznamu požadovaného klienta.

4. Pokračujte kliknutím na tlačítko  a potom klikněte na **Odstranit**.
5. Potvrďte své rozhodnutí.

   Všechny tokeny zabezpečení přiřazené k tomuto klientovi okamžitě vyprší a požadavky API s těmito tokeny selžou.

Důležité *Neexistuje žádný způsob, jak obnovit odstraněného klienta.*