Portál pro správu

Version 9.0

PŘÍRUČKA SPRÁVCE

Revize: 24.3.2020

Obsah

1 O tomto dokumentu

Tento dokument je určen pro správce, kteří chtějí používat portál pro správu.

2 Portál pro správu

Portál pro správu je webové rozhraní cloudové platformy, která poskytuje služby ochrany dat.

Zatímco jednotlivé služby mají své vlastní webové rozhraní nazývané konzola služby, portál pro správu umožňuje správcům řídit používání služeb, vytvářet uživatelské účty a jednotky, generovat zprávy a provádět další akce.

2.1 Účty a jednotky

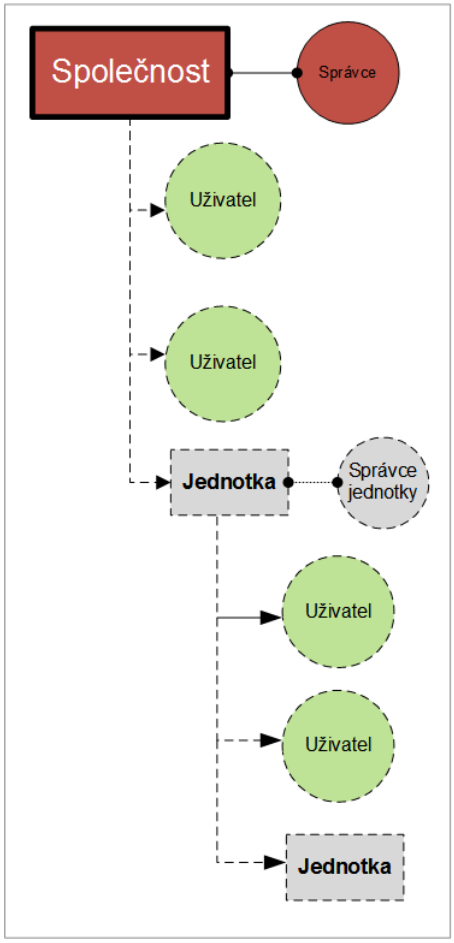
Existují dva typy uživatelských účtů: účty správců a uživatelské účty.

- **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.

Správci mohou vytvářet jednotky, které obvykle odpovídají jednotkám nebo oddělením organizace. Každá účet existuje buď na úrovni společnosti, nebo v jednotce.

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

Následující diagram ukazuje tři úrovně hierarchie – společnosti a dvou jednotek. Volitelné jednotky a účty jsou zobrazeny s tečkovanou čárou.



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

Operace	Uživatelé	Správci
Tvorba jednotky	Ne	Ano
Tvorba účtů	Ne	Ano
Stahování a instalace softwaru	Ano	Ano
Používání služeb	Ano	Ano
Tvorba zpráv o využití služby	Ne	Ano

2.2 Správa kvót

Kvóty omezují možnosti tetanta využívat danou službu.

Na portálu pro správu si můžete zobrazit kvóty služeb, které byly vaší organizaci přiděleny poskytovatelem služeb, ale nemůžete je spravovat.

Můžete však spravovat kvóty služeb pro své uživatele.

2.2.1 Zobrazení kvót pro organizaci

Na portálu pro správu přejděte na **Přehled** > **Využití**. Zobrazí se kontrolní panel s údaji o přidělených kvótách pro vaši organizaci. Kvóty pro jednotlivé služby jsou uvedeny na samostatných kartách.

2.2.1.1 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.

2.2.1.2 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.

2.2.1.3 Kvóty služby Synchronizace a sdílení souborů

Tyto kvóty používá poskytovatel služeb v rámci celé společnosti. Správci společnosti si mohou tyto kvóty a informace o využití zobrazit v portálu pro správu.

- **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.

2.2.1.4 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.

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.

- **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.

2.2.1.5 Kvóty notarizace

Tyto kvóty používá poskytovatel služeb v rámci celé společnosti. Správci společnosti si mohou tyto kvóty a informace o využití zobrazit v portálu pro správu.

- **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.

2.2.2 Definování kvót pro uživatele

Kvóty vám umožňují omezit, jak uživatel může využívat danou službu. Kvóty nastavíte tak, že vyberete uživatele na kartě **Uživatelé** a potom kliknete na ikonu tužky v oddílu **Kvóty**.

Pokud je kvóta překročena, odešle se upozornění na e-mailovou adresu uživatele. Pokud nenastavíte překročení kvóty, bude kvóta považována za **měkkou**. To znamená, že se neuplatní omezení na používání služby 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 uživatele dosáhne 20, uživatel obdrží oznámení e-mailem, ale služba Cyber Protection bude stále k dispozici.

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

2.2.2.1 Kvóty pro zálohy

Můžete zadat kvótu úložiště záloh a maximální počet počítačů, zařízení nebo webů, které může uživatel chránit. Jsou k dispozici následující kvóty.

Kvóty na zařízení

- **Pracovní stanice**
- **Servery**
- **Virtuální počítače**
- **Mobilní zařízení**
- **Webhostingové servery** (Fyzické a virtuální servery založené na Linuxu s ovládacími panely Plesk nebo cPanel)
- **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.

Kvóta na úložiště

- **Úložiště záloh**

Kvóta na úložiště záloh omezuje celkovou velikost záloh umístěných v cloudovém úložišti. Při překročení kvóty na úložiště záloh se nezdaří zálohování.

2.2.2.2 Kvóty služby Synchronizace a sdílení souborů

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

- **Osobní prostor úložiště**

Cloudové úložiště sloužící k ukládání souborů uživatele. Tato kvóta definuje místo přidělené uživateli v cloudovém úložišti.

2.2.2.3 Kvóty notarizace

Můžete definovat následující kvóty notarizace pro uživatele:

- **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.

2.3 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.

3 Pokyny krok za krokem

V části se seznámíte se základy používání portálu pro správu. Popisuje, jak provést následující úkony:

- Aktivovat váš účet správce.
- Přistupovat k portálu pro správu a ke službám.
- Vytvořit jednotku.
- Vytvořit uživatelský účet.

3.1 Aktivace účtu správce

Po registraci do služby 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.

3.2 Přístup k portálu pro správu a ke službám

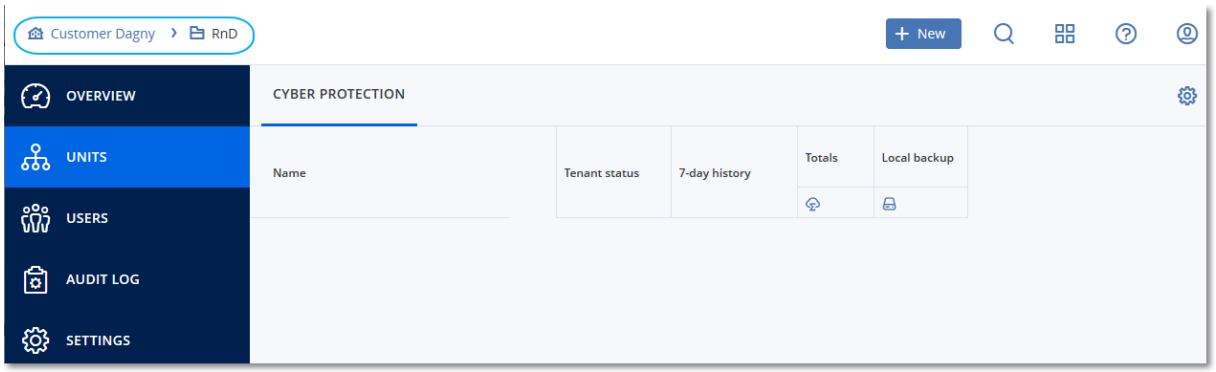
1. Přejděte na přihlašovací stránku. Adresa přihlašovací stránky je uvedena v aktivačním e-mailu.
2. Zadejte přihlašovací jméno a klikněte na tlačítko **Další**.
3. Zadejte heslo a klikněte na tlačítko **Další**.
4. Proveďte jeden z následujících úkonů:
   - Chcete-li se přihlásit do portálu pro správu, klikněte na možnost **Portál pro správu**.
   - Pokud se chcete přihlásit do služby, klikněte na název služby.

Pokud chcete přepnout mezi portálem pro správu a konzolami služeb klikněte na ikonu v pravém horním rohu a vyberte **Portál pro správu** nebo službu, na kterou chcete přejít.

3.3 Navigace na portálu pro správu

Při používání portálu pro správu v kterémkoli okamžiku pracujete v rámci některé společnosti nebo jednotky. To je označeno v levém horním rohu.

Ve výchozím nastavení je vybrán tenant nejvyšší dostupné úrovně. Kliknutím na název jednotky 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 společnost nebo jednotku, ve které právě pracujete. Například:

- Pomocí tlačítka **Nový** můžete vytvořit jednotku nebo uživatelský účet pouze v této společnosti nebo jednotce.
- Na kartě **Jednotky** jsou zobrazeny pouze jednotky, které jsou přímo podřízeny této společnosti nebo jednotce.
- Karta **Uživatelé** zobrazuje pouze uživatelské účty, které existují v této společnosti nebo jednotce.

3.4 Vytvoření jednotky

Tento krok přeskočte, jestliže nechcete uspořádat účty do jednotek.

Pokud chcete jednotky vytvořit později, nezapomeňte, že existující účty nelze přesouvat mezi jednotkami nebo mezi společností a jednotkami. Nejprve je potřeba vytvořit jednotku a poté ji naplnit účty.

Vytvoření jednotky

1. Přihlaste se do portálu pro správu.
2. Přejděte do jednotky, ve které chcete vytvořit novou jednotku.
3. V pravém horním rohu klikněte na možnost **Nový** > **Jednotka**.
4. Do pole **Název** zadejte název nové jednotky.
5. [Volitelné] V části **Jazyk** změňte výchozí jazyk pro upozornění, zprávy a software, který se bude pro tuto jednotku používat.
6. Proveďte jeden z následujících úkonů:
   - Chcete-li vytvořit správce jednotky, klikněte na tlačítko **Další** a postupujte podle pokynů v části Vytvoření uživatelského účtu (str. 12) od kroku 4.
   - Jestliže chcete vytvořit jednotku bez správce, klikněte na možnost **Uložit a zavřít**. Správce a uživatele můžete do jednotky přidat později.

Nově vytvořená jednotka se zobrazí na kartě **Jednotky**.

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

3.5 Vytvoření uživatelského účtu

Tento krok přeskočte, jestliže nechcete vytvářet další uživatelské účty.

Další účty můžete chtít vytvářet v následujících případech:

- Účty správce společnosti – pro účely sdílení úkolů správy s dalšími uživateli.
- Účty správce jednotek – pokud potřebujete správou pověřit další uživatele, jejichž přístupová oprávnění budou omezená na odpovídající jednotky.
- Uživatelské účty – pokud chcete uživatelům povolit přístup pouze k určité podsadě služeb.

Vytvoření uživatelského účtu

1. Přihlaste se do portálu pro správu.
2. Přejděte do jednotky, ve které chcete vytvořit uživatelský účet.
3. V pravém horním rohu klikněte na možnost **Nový** > **Uživatel**.
4. Zadejte pro účet následující 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. Vyberte služby, k nimž bude mít uživatel přístup, a pro každou službu nastavte roli.

- Zaškrtnete-li políčko **Správce společnosti**, bude mít uživatel přístup k portálu pro správu a roli správce pro všechny služby.
- 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 upravit uživatelské nastavení nebo zadat nastavení upozornění a kvóty pro některého uživatele, 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.

3.6 Změna nastavení upozornění pro uživatele

Chcete-li změnit nastavení upozornění pro některého uživatele, vyberte daného uživatele na kartě **Uživatelé** a potom klikněte na ikonu tužky v oddílu **Nastavení**. K dispozici jsou následující nastavení upozornění:

- **Upozornění na překročení kvót** (ve výchozím nastavení zapnuté)

  Upozornění na překročené kvóty.
- **Naplánované zprávy o využití**

  Zprávy o využití, které jsou popsané níže, se odesílají první den každého měsíce.
- **Upozornění na chyby**, **Upozornění** a **Upozornění na úspěšné dokončení** (ve výchozím nastavení vypnuté)

  Oznámení o výsledcích spuštění plánů ochrany a výsledcích operací obnovení po havárii u každého zařízení.
- **Denní shrnutí aktivních výstrah** (ve výchozím nastavení zapnuto)

  Toto shrnutí informuje o nezdařených zálohách, vynechaných zálohách a dalších potížích. Shrnutí je odesláno v 10:00 (čas datového centra). Pokud to této chvíle nenastaly žádné potíže, shrnutí se neodešle.

Všechna upozornění se odesílají na e-mailovou adresu uživatele.

3.7 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**.

3.8 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. 13).

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.

3.9 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.

3.10 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 poskytnutého platformou.

Jak to funguje

1. Povolíte dvojúrovňové ověřování (str. 17) 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.

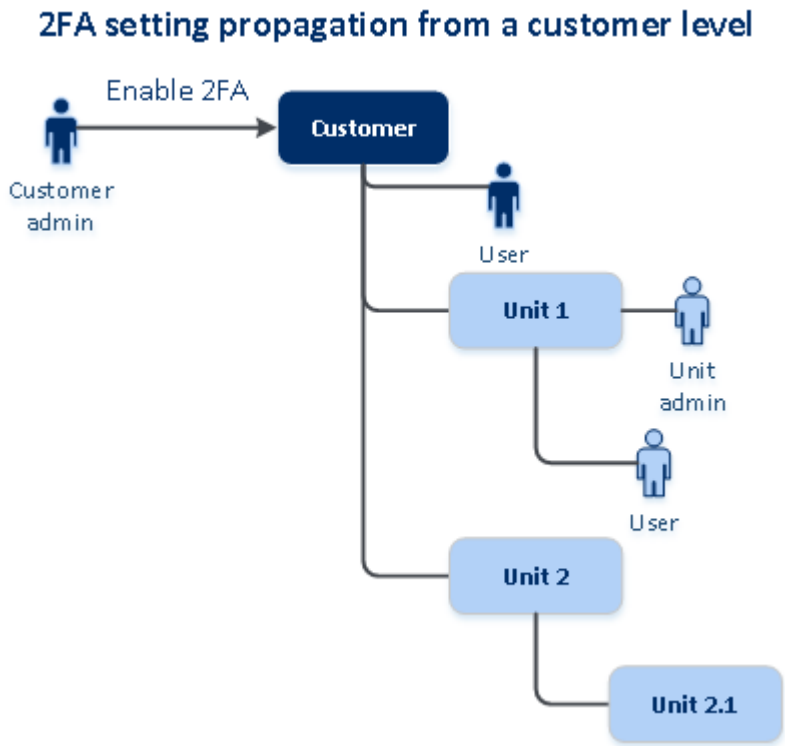
Když se nyní uživatelé přihlásí do systému, budou požádáni o zadání přihlašovacího jména a hesla a jednorázového kódu TOTP vygenerovaného v aplikaci pro ověřování. Uživatelé si při přihlášení do systému mohou označit svůj prohlížeč jako důvěryhodný. Díky tomu nebudou muset při dalších přihlášeních pomocí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

3.10.1 Šíření nastavení dvojúrovňového ověřování v úrovních tenanta

Dvojúrovňové ověřování je nastaveno na úrovni **organizace**. Můžete si ho nastavit jen pro svou vlastní organizaci.

Nastavení dvojúrovňového ověřování je šířeno napříč úrovněmi tenanta následujícím způsobem:

- Jednotky automaticky zdědí nastavení dvojúrovňového ověřování od organizace zákazníka.



Poznámka
1. Dvojúrovňové ověřování není možné nastavit na úrovni jednotky.
2. Nastavení dvojúrovňového ověřování můžete spravovat pro uživatele podřízených organizací (jednotek).

3.10.2 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**.

3.10.3 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.

3.10.4 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. 17).

3.10.5 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).

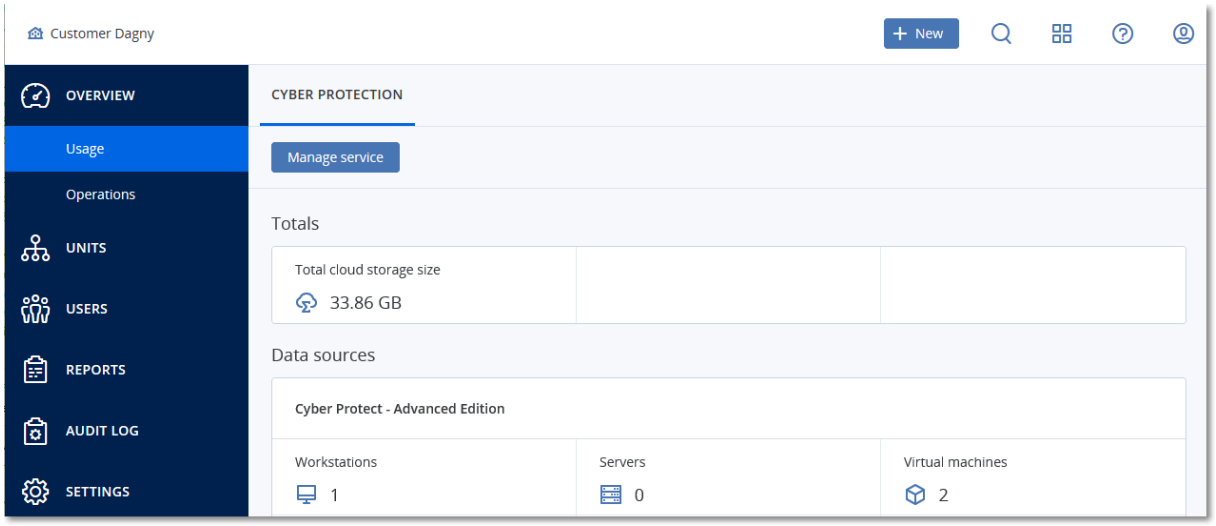
Pokusy o zadání kódu TOTP se registrují na uživatele, nikoli na zařízení. To znamená, že i když se uživatel pokusí zadat kód TOTP z různých zařízení, bude i přesto zablokován.

4 Monitorování

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

4.1 Využití

Karta **Využití** poskytuje přehled o využívání služeb (včetně případných kvót) a umožňuje přístup ke konzolám služeb.



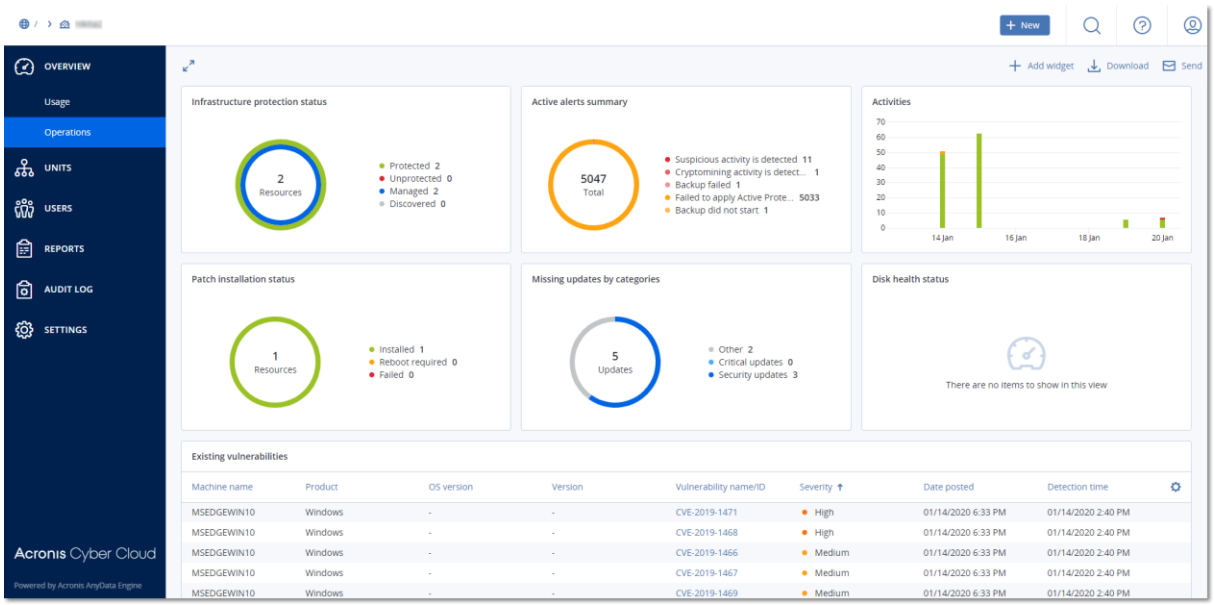
4.2 Operace

Kontrolní panel **Operace** je k dispozici pouze správcům společnosti při práci na úrovni společnosti.

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.

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 nebo ho poslat e-mailem ve formátu PDF nebo XLSX.

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 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 časový rozsah a nastavit u něj filtry.

Jak přidat ovládací prvek

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

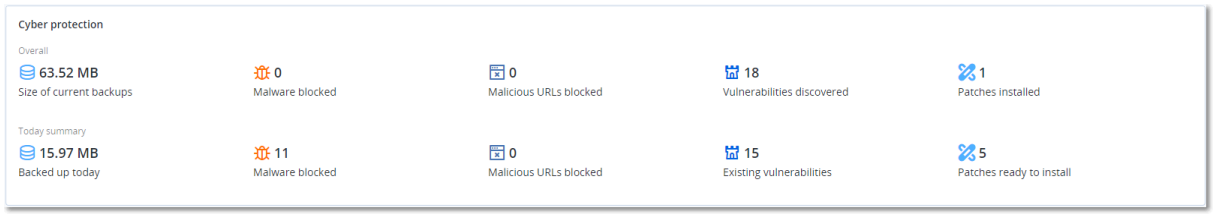
- Klikněte na ovládací prvek, který chcete přidat. Ovládací prvek se přidá s výchozím nastavením.
- Chcete-li ovládací prvek před přidáním upravit, vyberte jej a klikněte na ikonu tužky. Po úpravě ovládacího prvku klikněte na tlačítko **Hotovo**.

Jak odstranit ovládací prvek

Klikněte na znak X vedle názvu ovládacího prvku.

4.2.1 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

4.2.2 Stav ochrany

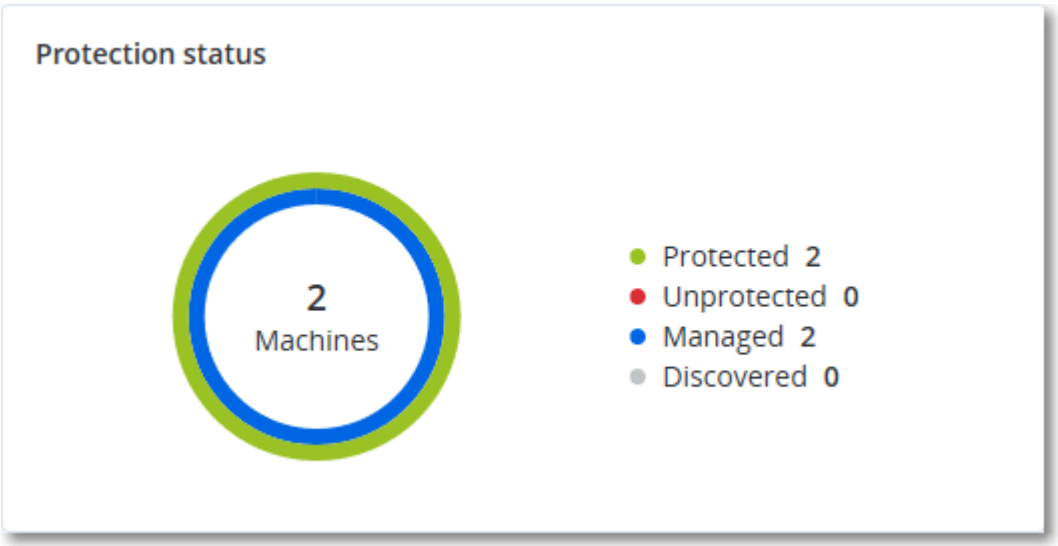
Stav ochrany

Tento ovládací prvek ukazuje aktuální stav ochrany všech počítačů.

Počítač se může nacházet v jednom z následujících stavů:

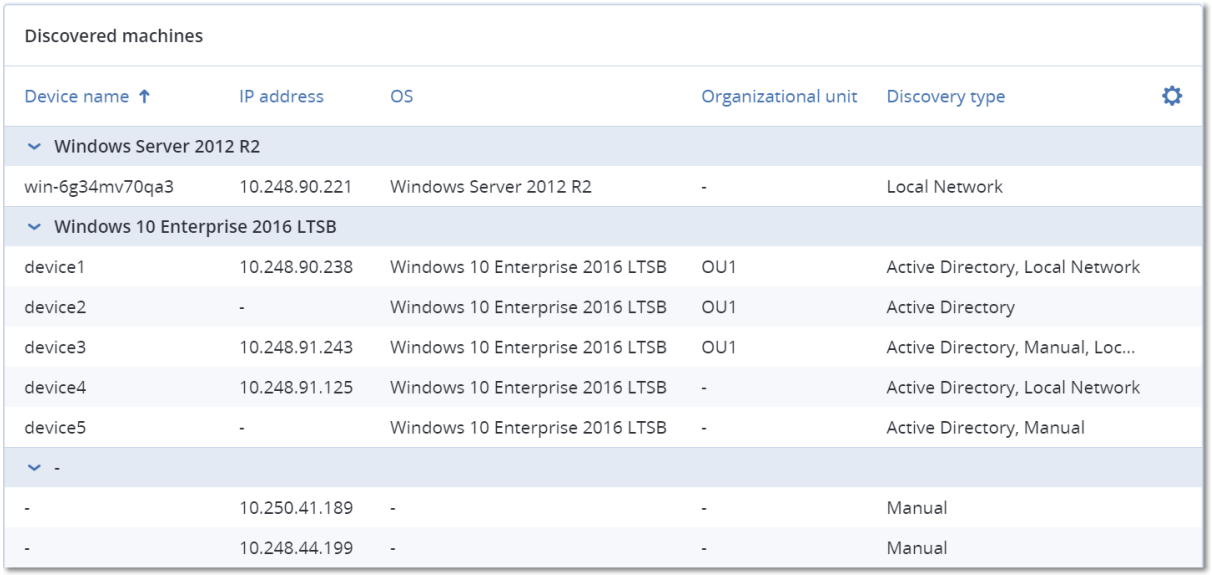
- **Chráněno** – počítače s nainstalovaným agentem ochrany a aktivním plánem ochrany
- **Nechráněno** – počítače s nainstalovaným agentem ochrany, ale bez aktivního plánu ochrany
- **Spravováno** – počítače s nainstalovaným agentem ochrany
- **Zjištěno** – počítače bez nainstalovaného agenta ochrany

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.



4.2.3 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

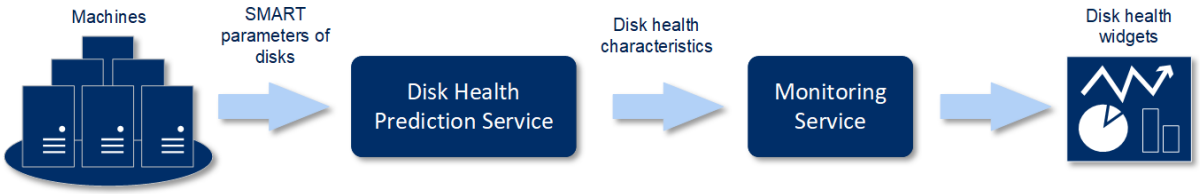
Jak to funguje

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:

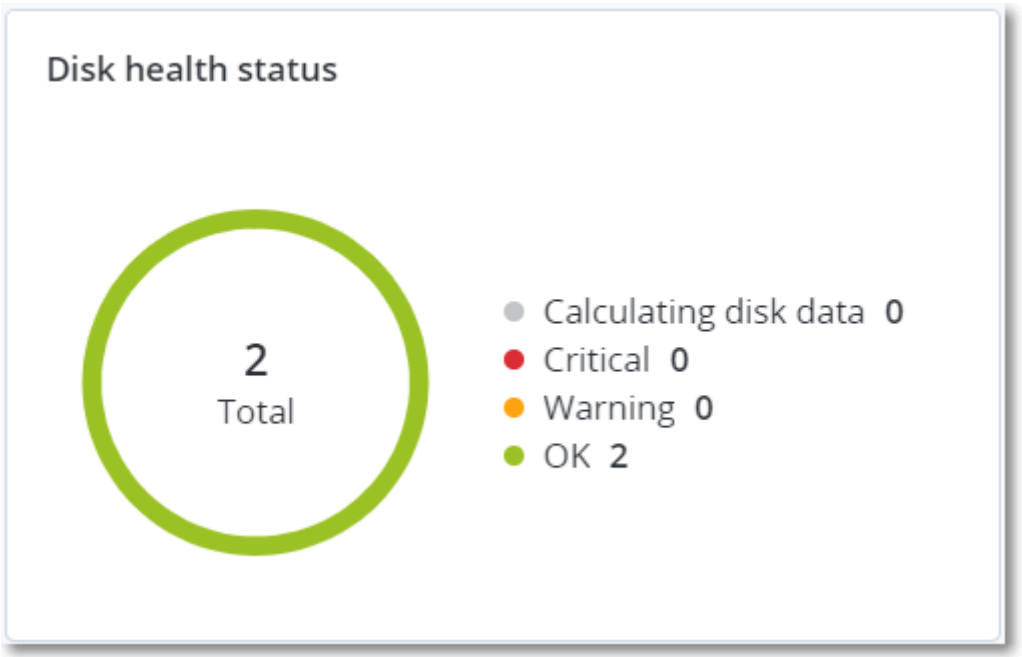
- **Přehled stavu disku** – ovládací prvek stromové mapy se dvěma úrovněmi detailů, které lze přepínat procházením:

- 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 vybraný počítač. Každý blok disku zobrazuje předpověď změny stavu disku:
  - Zhorší se (pravděpodobnost předpovědi stavu disku v procentech)
  - Zůstane stabilní (pravděpodobnost předpovědi stavu disku v procentech)

- Zlepší se (pravděpodobnost předpovědi stavu disku v procentech)

- **Stav disku** – ovládací prvek kruhového diagramu zobrazující počet disků pro každý stav.



Výstrahy stavu disku

Kontrola stavu disku probíhá každých 30 minut a odpovídající výstraha se generuje jednou denně. Když se stav disku změní z Upozornění na Kritický, zobrazí se také výstraha, i když se během dne již nějaká výstraha zobrazila.

Název výstrahy	Závažnost	Stav disku	Popis
Může dojít k selhání disku.	Upozornění	[30;70)	Disk [název_disku] na počítači [název_počítače] v budoucnu pravděpodobně selže. Co nejdříve spusťte plnou zálohu bitové kopie, nahraďte ji a pak ji obnovte na nový disk.
Brzy dojde k selhání disku.	Kritická	(0;30)	Disk [název_disku] na počítači [název_počítače] je v kritickém stavu a velmi pravděpodobně brzy selže. Záloha bitové kopie tohoto disku není momentálně doporučena, protože zátěž navíc může způsobit selhání disku. Zálohujte ihned všechny nejdůležitější soubory na tomto disku a disk vyměňte.

4.2.4 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.

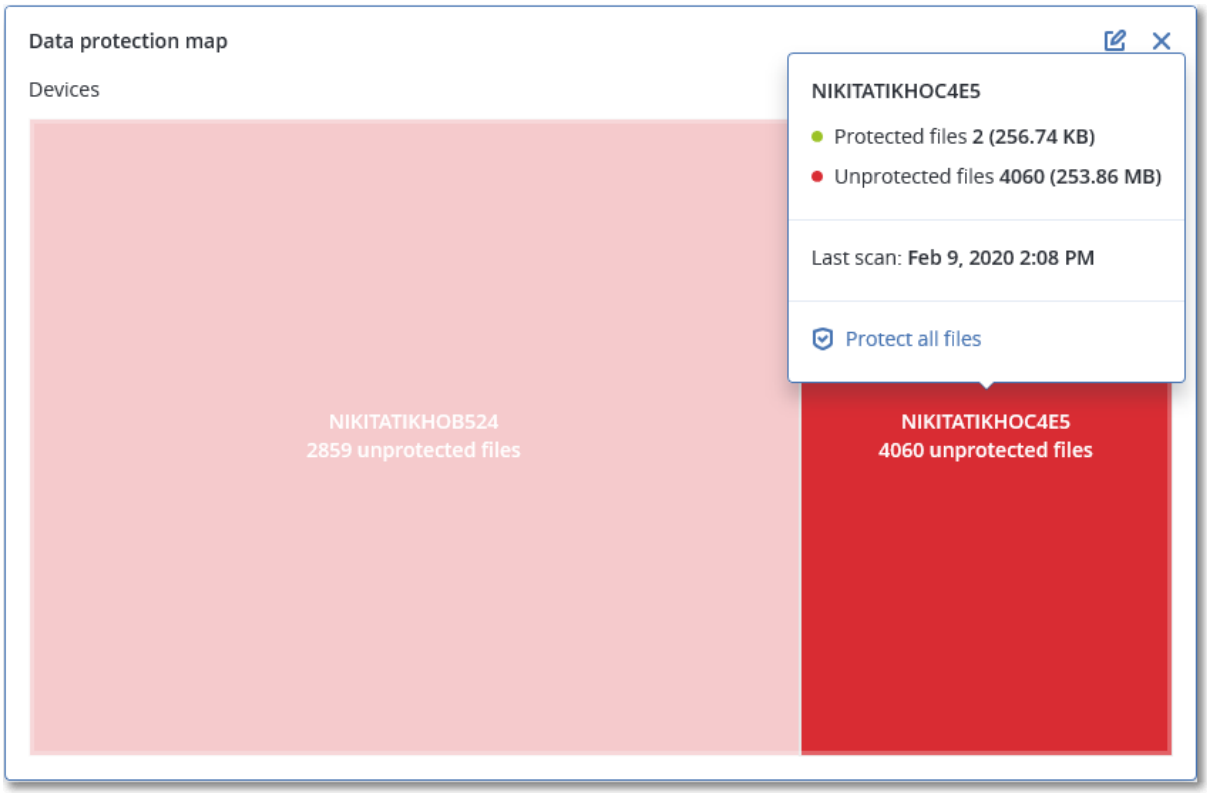
Velikost každého bloku závisí na celkovém počtu/velikosti všech důležitých souborů, které náleží zákazníkovi/počítači.

Soubory mohou mít jeden z následujících stavů ochrany:

- **Kritický** – existuje 51–100 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.
- **Nízký** – existuje 21–50 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.
- **Střední** – existuje 1–20 % nechráněných souborů se zadanými příponami, které nejsou pro vybraný počítač/umístění zálohovány a nebudou zálohovány s použitím stávajícího nastavení zálohování.
- **Vysoký** – všechny soubory se zadanými příponami jsou pro vybraný počítač/umístění chráněny (zálohovány).

Výsledky kontroly ochrany dat naleznete na kontrolním panelu v ovládacím prvku Mapa ochrany dat, což je prvek stromové mapy zobrazující podrobnosti na úrovni počítače:

- 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.

4.2.5 Ovládací prvky posouzení ohrožení zabezpečení

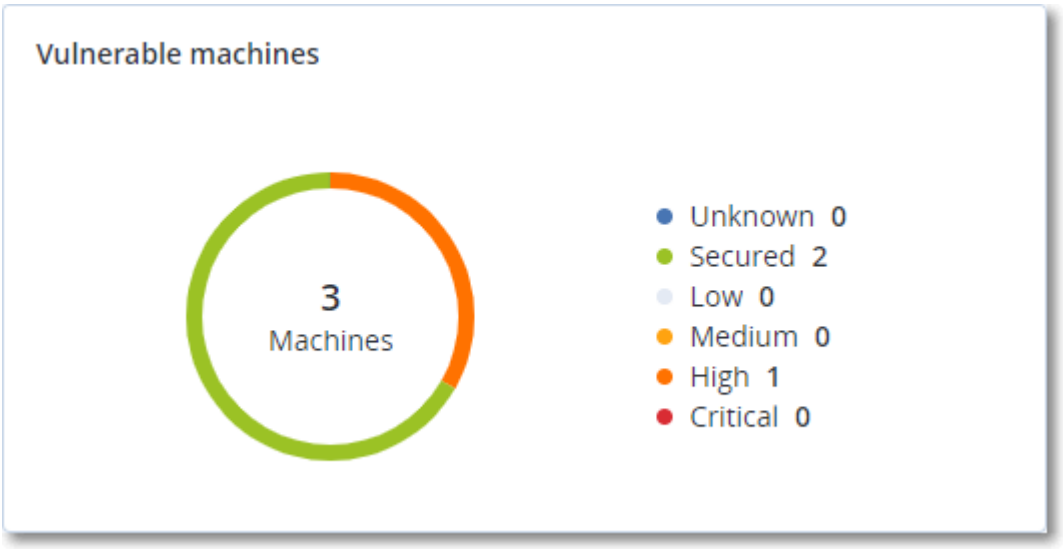
Ohrožené počítače

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

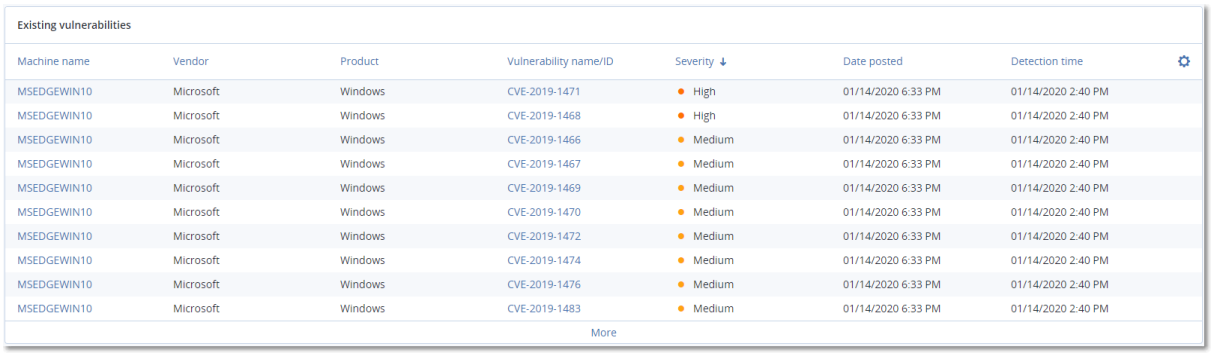
- Neznámý



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

4.2.6 Ovládací prvky instalace oprav

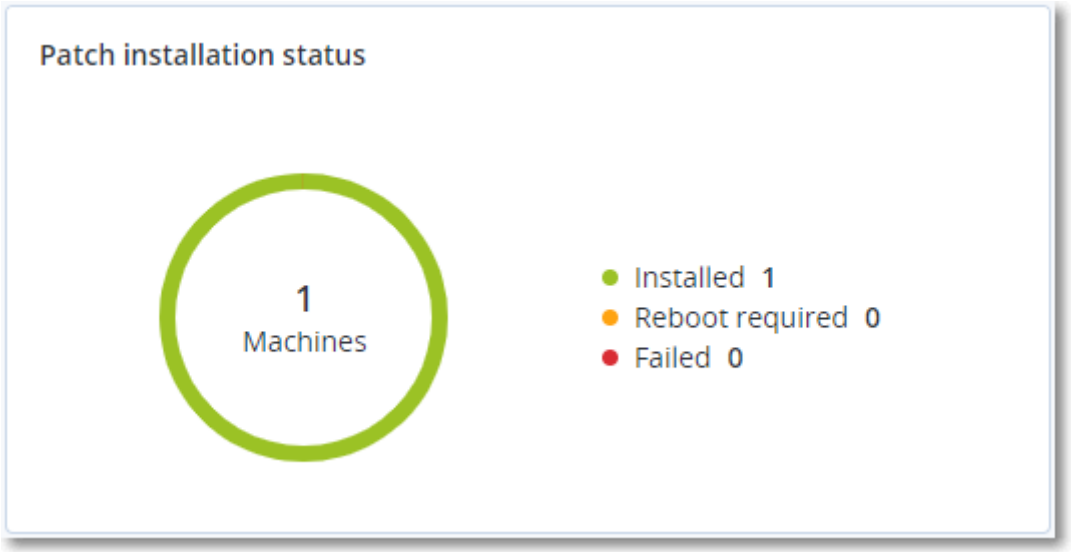
Pro funkci správy oprav jsou k dispozici čtyři ovládací prvky.

Stav instalace opravy

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

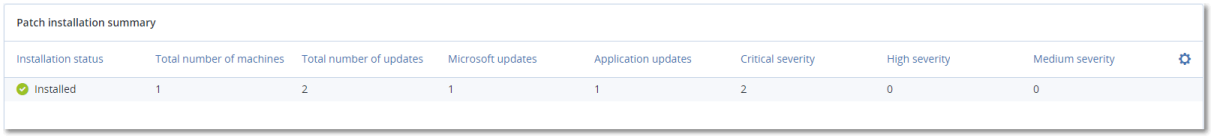
- **Nainstalováno** – všechny dostupné opravy jsou nainstalovány na počítači
- **Nutný restart** – po instalaci opravy je vyžadován restart počítače

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



Souhrn instalace opravy

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



Historie instalace oprav

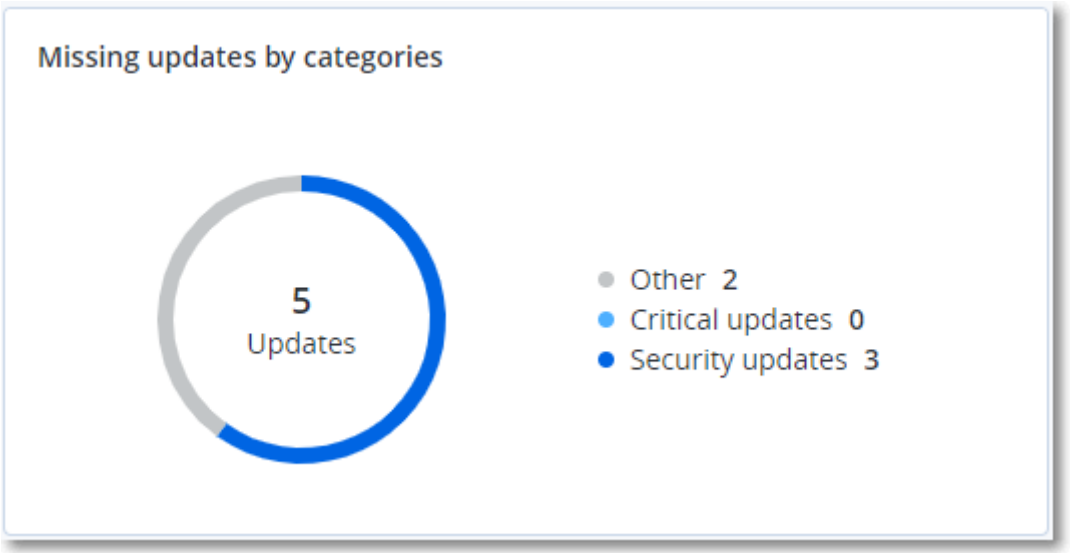
Tento ovládací prvek zobrazuje podrobné informace o opravách na počítačích.

Chybějící aktualizace podle kategorie

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

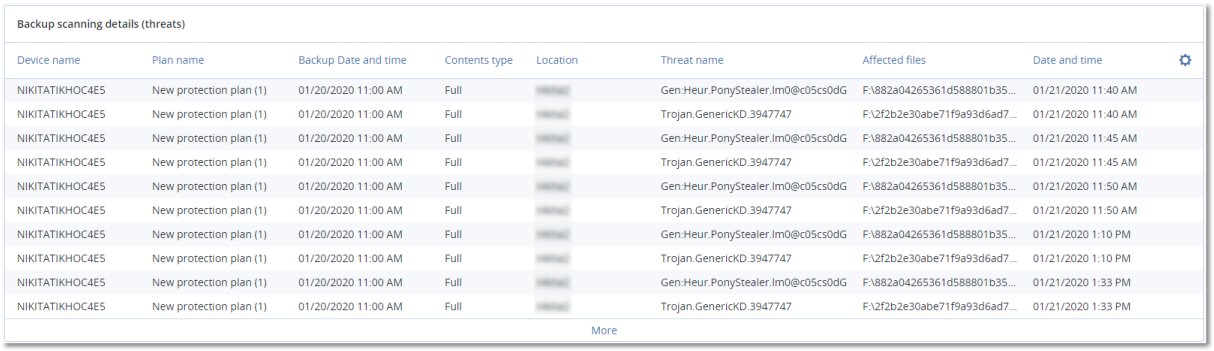
- Aktualizace zabezpečení
- Kritické aktualizace

- Jiné



4.2.7 Podrobnosti kontroly zálohy

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



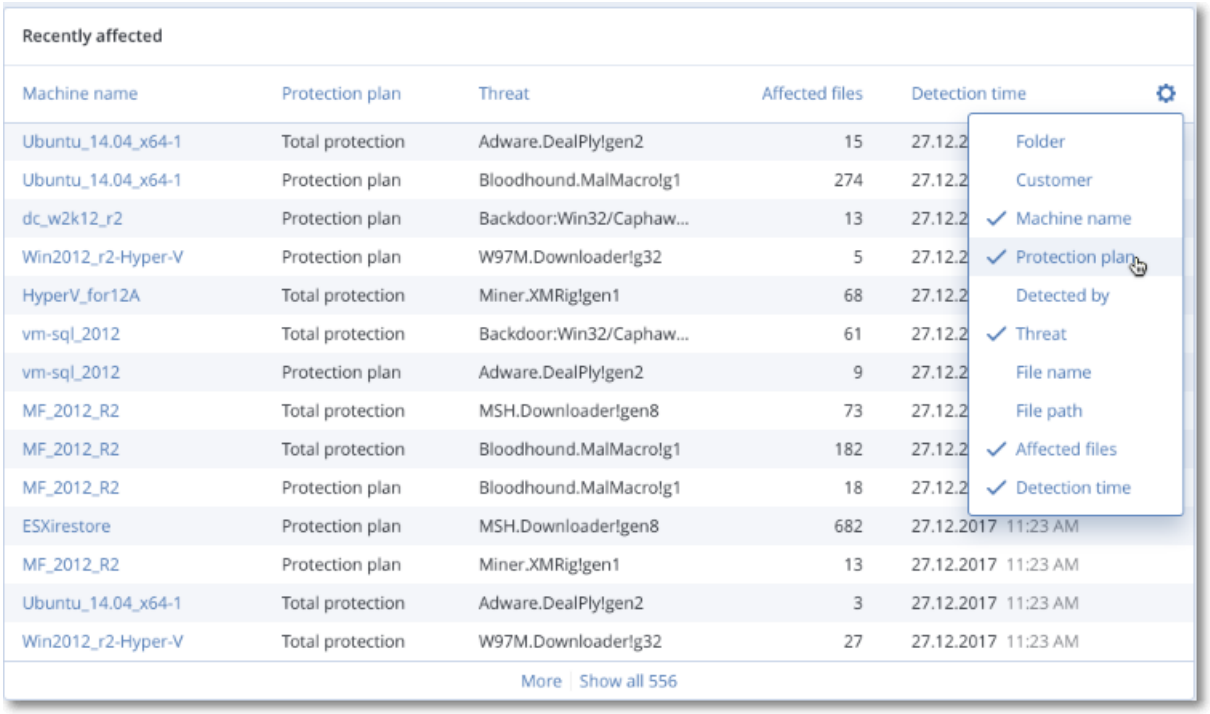
Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

4.2.8 Nedávno napadeno

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



5 Zprávy

Chcete-li se dostat ke zprávám o použití a operacích služeb, klikněte na **Zprávy**.

Poznámka *Tato funkce není k dispozici ve verzích Standard služby Cyber Protection.*

5.1 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.
- **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 jednotky společnosti, ve které pracujete.
- **Všichni zákazníci a partneři**

  Výpis bude obsahovat metriky využití služby pro všechny podřízené jednotky společnosti nebo jednotky, ve které pracujete.
- **Všichni zákazníci, partneři a uživatelé**

  Výpis bude obsahovat metriky využití služby pro všechny podřízené jednotky společnosti nebo jednotky, ve které pracujete, a pro všechny uživatele v jednotkách.

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. Posílají se všem správcům společnosti nebo jednotkám, které 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 ve společnosti nebo jednotce nejvyšší úrovně, kterou 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

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

Generování vlastní zprávy

1. Přihlaste se do portálu pro správu.
2. Přejděte do jednotky (str. 11), pro kterou chcete vytvořit zprávu.
3. Klikněte na možnost **Zprávy** > **Použití**.
4. Klikněte na možnost **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**.

5.1.1 Zprávy o využití

Zpráva o využití služby Cyber Protection obsahuje následující data o společnosti nebo jednotce:

- Velikost záloh podle jednotky, uživatele a typu zařízení.
- Počet chráněných zařízení podle jednotky, uživatele a typu zařízení.
- Cena podle jednotky, uživatele a typu zařízení.
- Celková velikost záloh.
- Celkový počet chráněných zařízení.
- Celková cena.

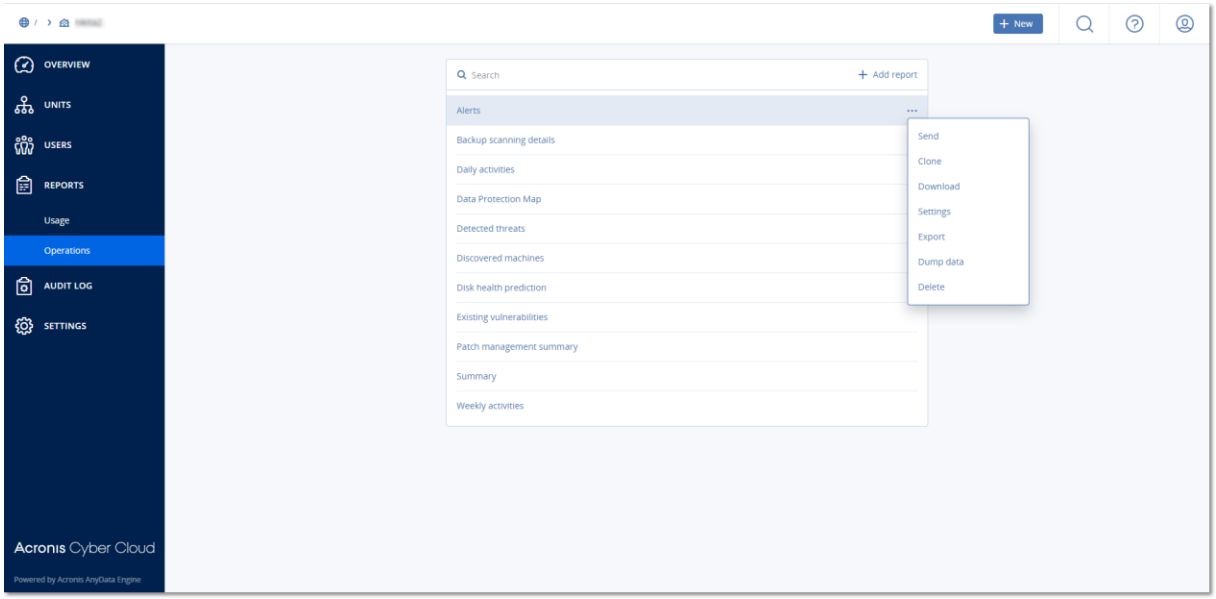
5.2 Operace

Zprávy o **Operacích** jsou k dispozici pouze správcům společnosti při práci na úrovni společnosti.

Zpráva o operacích může obsahovat jakoukoli sadu ovládacích prvků kontrolního panelu (str. 19) **Operace**. Všechny ovládací prvky zobrazují shrnující informace za celou společnost. Všechny ovládací prvky zobrazují parametry za stejný časový rozsah. Tento rozsah můžete změnit v nastavení zpráv.

Zprávu zobrazíte kliknutím na její název.

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



Můžete použít předdefinované zprávy nebo vytvořit vlastní.

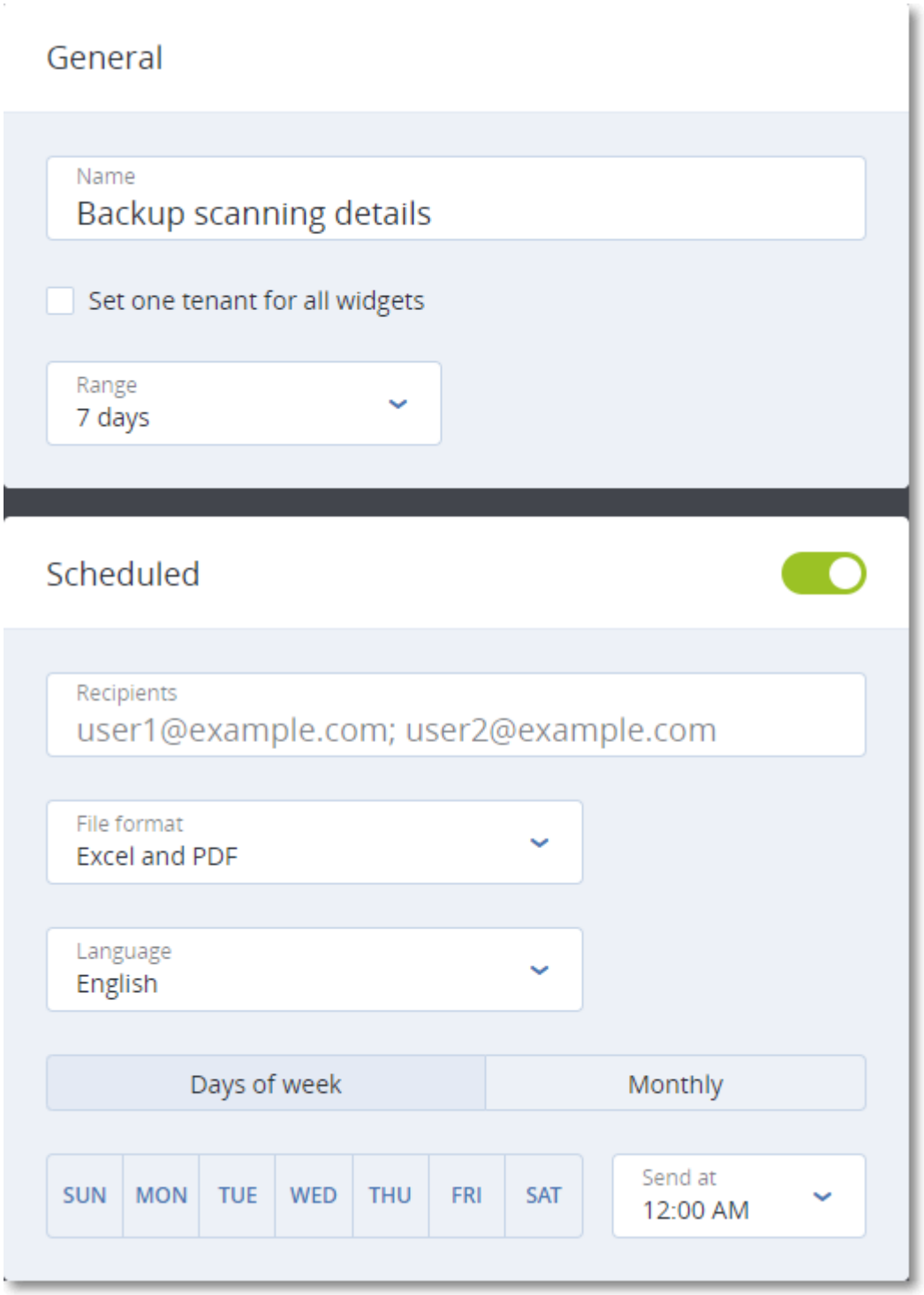
Přidání zprávy

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 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.

Chcete-li exportovat strukturu zprávy, klikněte na ikonu tří teček v pravém horním rohu a 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 tří teček v pravém horním rohu a na možnost **Vypsat data**.
3. Zadejte e-mailové adresy příjemců.
4. V části **Časový rozsah** zadejte časový rozsah.
5. Klikněte na možnost **Odeslat**.

5.3 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.

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 (ovládací prvky)	▪ Čas vygenerování zprávy je v časovém pásmu počítače, kde je spuštěný prohlížeč. ▪ Časové pásmo aktivit zobrazených ve zprávě je UTC.
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.

6 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 organizaci nebo jednotce, ve které právě pracujete, a v jejích podřízených jednotkách. Kliknutím na libovolnou událost zobrazíte podrobnější informace o této události.

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 jednotky, do které náleží objekt. Například tenantem události **Uživatel byl aktualizován** je jednotka, ve které je uživatel umístěn. Tenantem události **Byla dosažena kvóta** je uživatel, jehož kvóta byla dosažena.

- **Spouštěč**

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

- **Tenant spouštěče**

  Název jednotky, do které 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.

7 Pokročilé scénáře

7.1 Omezení přístupu k webovému rozhraní

Přístup k webovému rozhraní můžete omezit zadáním seznamu IP adres, ze kterých se mohou uživatelé přihlašovat.

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

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

Jak omezit přístup k webovému rozhraní

1. Přihlaste se do portálu pro správu.
2. Přejděte do jednotky (str. 11), ve které chcete omezit přístup.
3. Klikněte na **Nastavení** > **Zabezpečení**.
4. Zaškrtněte políčko **Povolit správu 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**.

7.2 Omezení přístupu ke společnosti

Správci společnosti mohou správcům vyšší úrovně omezit přístup ke společnosti.

Pokud je přístup ke společnosti omezen, mohou správci vyšší úrovně pouze upravovat vlastnosti společnosti. Uživatelské účty a podřízené jednotky vůbec nevidí.

Omezení přístupu ke společnosti

1. Přihlaste se do portálu pro správu.
2. Klikněte na **Nastavení** > **Zabezpečení**.
3. Vypněte možnost **Podpora přístupu**.
4. Klikněte na tlačítko **Uložit**.

7.3 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.

7.3.1 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**.

7.3.2 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**.

7.3.3 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.

7.3.4 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.

7.3.5 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.*