Kernun Business Intelligence
Příručka administrátora

Trusted Network Solutions, a.s.

1. listopadu 2018

Obsah

Kapitola 1

Kernun Business Intelligence

Kernun Business Intelligence je nástroj pro uchovávání, zpracování, analýzu a prezentaci provozních záznamů ze zařízení Kernun Clear Web a Kernun UTM. Lze jej využít jako samostatné zařízení, modul pro Kernun Clear Web nebo cloudovou službu. Jeho hlavní funkce jsou:

Uchovávání záznamů Kernun Business Intelligence umožňuje centrální sběr provozních záznamů veškerých zařízení Kernun cílové organizace. Lze jej také využít jako dedikované úložiště pro jejich zálohu.

Detekce anomálií Algoritmy strojového učení a umělé inteligence jsou využity pro zpracování velkých objemům dat za účelem usnadnění detekce anomálního chování a ověření správného fungování prostředí.

Vizualizace dat Kernun Business Intelligence poskytuje různé typy grafického zobrazení výsledků analýz nad daty pro názorné a jednoduché zobrazení vlastností, vztahů a struktury. Takové výstupy jsou vhodné pro prezentaci informací širokému publiku.

Webové grafické rozhraní Uživatelé k funkcím Kernun Business Intelligence mohou přistupovat pomocí jednoduchého, intuitivního a uživatelsky přívětivého webového rozhraní.

Škálovatelnost Kernun Business Intelligence se dodává jako hardwarové zařízení v několika variantách podle výkonu nebo jako virtuální appliance do prostředí Oracle VirtualBox, VMware vSphere nebo MS Hyper-V. Také je možné ho využít jako modul pro Kernun Clear Web nebo jako cloudovou službu.

Kapitola 2

Uvedení do provozu

Kapitola obsahuje informace potřebné pro nasazení a zprovoznění zařízení Kernun Business Intelligence ve vaší síti. Zejména se jedná o nároky kladené na kompatibilitu prostředí, parametry pro prvotní konfiguraci nebo samotný režim nasazení.

2.1 Předpoklady kompatibility prostředí

Pro zaručení správné funkčnosti a dosažení nejlepších výsledků produktu Kernun Business Intelligence je nutné, aby se vlastnosti prostředí vaší sítě, kde má být Kernun Business Intelligence nasazen, pokud možno co nejlépe shodovaly s níže uvedenými předpoklady. Odchylky od těchto předpokladů nemusí nutně znamenat celkovou nefunkčnost zařízení, mohou však značně omezit některé jeho možnosti využití.

- Pro správné fungování zařízení Kernun Business Intelligence je nutné zajistit na mezilehlých prvcích vaší síťové infrastruktury (např. firewall) povolení následující komunikace ze zařízení Kernun Business Intelligence:
    1. port 22 (SSH) nebo 443 (HTTPS) na server `callhome.kernun.com` pro službu vzdálené pomoci
    2. port 443 (HTTPS) na server `download.kernun.com` pro aktualizaci systému Kernun Business Intelligence
    3. port 22 (SSH) na všechna zařízení Kernun pro získání jejich provozních záznamů
- Virtuální zařízení Kernun Business Intelligence může běžet na následujících platformách:
    1. VirtualBox 4.3
    2. VMware vSphere ESXi 5.5
    3. MS Hyper-V Windows Server 2012 R2

2.2 Příprava

Před zprovozněním systému Kernun Business Intelligence je potřeba provést několik kroků:

1. Zvolte si jméno počítače včetně jména domény (FQDN), pod kterým budete Kernun Business Intelligence identifikovat ve Vaší síti. Příklad: `kbi.example.com`.

2. Zvolte si unikátní IP adresu z vaší sítě (včetně masky), na které bude Kernun Business Intelligence komunikovat.

3. Zvolte si nové heslo pro administrátorský účet.

4. Zjistěte si IP adresu výchozí brány vaší sítě pro přístup do Internetu.

5. Zjistěte si IP adresu primárního (i sekundárního) doménového serveru pro překlad doménových jmen na IP adresy.

6. Připravte si platný licenční soubor produktu Kernun Business Intelligence.

7. Připravte si počítač s webovým prohlížečem (Mozilla Firefox, Microsoft Internet Explorer nebo Google Chrome) a ethernetovým síťovým kabelem.

8. Nastavte záznam typu A (pro převod jména počítače na IP adresu) a záznam typu PTR (pro zpětný převod IP adresy na jméno počítače) na svých interních DNS serverech pro jméno počítače a IP adresu z kroků 1 a 2.

9. Nastavte váš firewall a případné mezilehlé prvky vaší síťové infrastruktury tak, aby neblokovaly komunikaci z IP adresy z bodu 2 na port 22 (SSH) zařízení Kernun (získání provozních záznamů) a serveru `callhome.kernun.com` (služba vzdálené pomoci) a také port 443 (HTTPS) serveru `download.kernun.com` (aktualizace systému).

10. Připravte si hardware nebo v případě instalace jako virtuální zařízení pro VMware vSphere a Oracle VirtualBox OVF šablonu (např.: *kernun_clear_web-040102h00.201502050824.amd64.ova*) a pro MS Hyper-V soubor VHD (např.: *kernun_clear_web-040102h00.201502050824.amd64.vhd*).

2.3 Zapojení

Jakmile máte vše potřebné připraveno, můžete přistoupit ke zprovoznění systému Kernun Business Intelligence.

1. Jestliže instalujete hardwarové zařízení, propojte ho pomocí ethernetového síťového kabelu přímo s vaším počítačem. Počáteční IP adresa systému Kernun Business Intelligence nastavená z výroby je `192.168.1.2`. Jestliže je tato IP adresa použitelná ve vaší síti, můžete zařízení alternativně připojit rovnou do vaší sítě.

2. Zapněte zařízení Kernun Business Intelligence.

3. Pokud jste propojili Kernun Business Intelligence přímo s vaším počítačem, nastavte na vašem počítači IP adresu `192.168.1.3` a masku sítě `255.255.255.0`.

Jestliže instalujete virtuální zařízení, naimportujte tuto OVF šablonu do vašeho virtualizačního prostředí a nastavte virtuální síť tak, abyste z vašeho počítače mohli přistupovat k systému Kernun Business Intelligence používajícímu výchozí IP adresu (`192.168.1.2`). Podrobnější návod importu virtuální šablony do nejběžnějších virtualizačních platforem lze nalézt na: `http://www.kernun.cz/podpora/navody-kernun/`

2.4 První přihlášení

V tuto chvíli by měl systém Kernun Business Intelligence běžet a být dostupný po síti z vašeho počítače. Před zahájením běžného používání je potřeba se přihlásit do webového grafického rozhraní a systém nakonfigurovat.

1. Otevřete webový prohlížeč a do adresního řádku napište výchozí adresu zařízení `https://192.168.1.2`.

2. Zobrazí se informace o nedůvěryhodném spojení, protože prohlížeč nemůže ověřit platnost certifikátu. Akceptujte spojení s tímto certifikátem. Lze přidat výjimku pro tento certifikát ve vašem prohlížeči, abyste nemuseli akceptaci certifikátu znovu potvrzovat při každém přihlašování. Alternativně je možné importovat certifikační autoritu Kernun na adrese `http://192.168.1.2/ca` do seznamu důvěryhodných certifikačních autorit. Pro zvýšení bezpečnosti komunikace lze ověřit otisk certifikátu v prohlížeči s otiskem certifikátu ze systémové konzole zařízení. Pro přístup na systémovou konzolu připojte monitor (HW zařízení) nebo virtuálni obrazovku (virtuální zařízení).

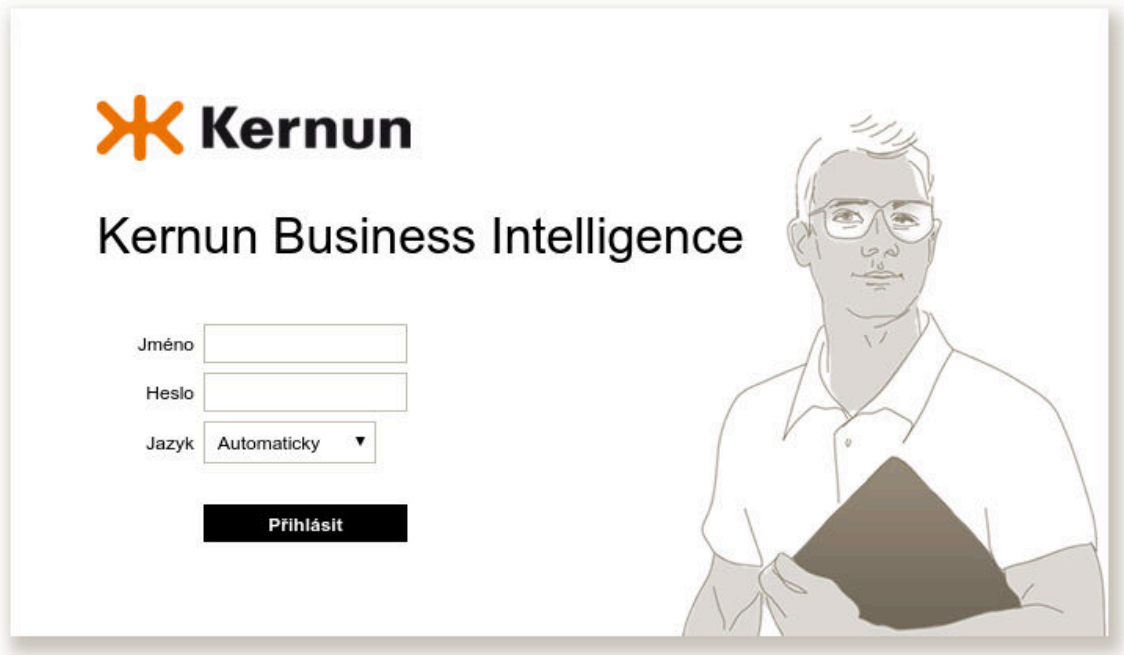
3. Objeví se přihlašovací obrazovka, viz obr. 2.1. Zadejte uživatelské jméno `admin` a heslo `admin`.

4. Po úspěšném přihlášení se objeví uvítací obrazovka. Jako první krok je potřeba nastavit nové heslo administrátora. Zvolte vhodné heslo, které nelze snadno uhodnout, a zapamatujte si ho nebo si ho zapište na bezpečné místo.

2.5 Počáteční konfigurace

Po nastavení hesla administrátora je nutné dokončit počáteční konfiguraci systému zadáním základních parametrů nastavení sítě. V konfiguračním dialogu (obr. 2.2) se nastavují dříve zvolené hodnoty, viz kap. 2.2:

- hostitelské jméno
- IP adresa a maska síťového rozhraní (ve formátu počet bitů masky 0–32)
- výchozí brána pro přístup do Internetu
- primární DNS server
- licenční soubor



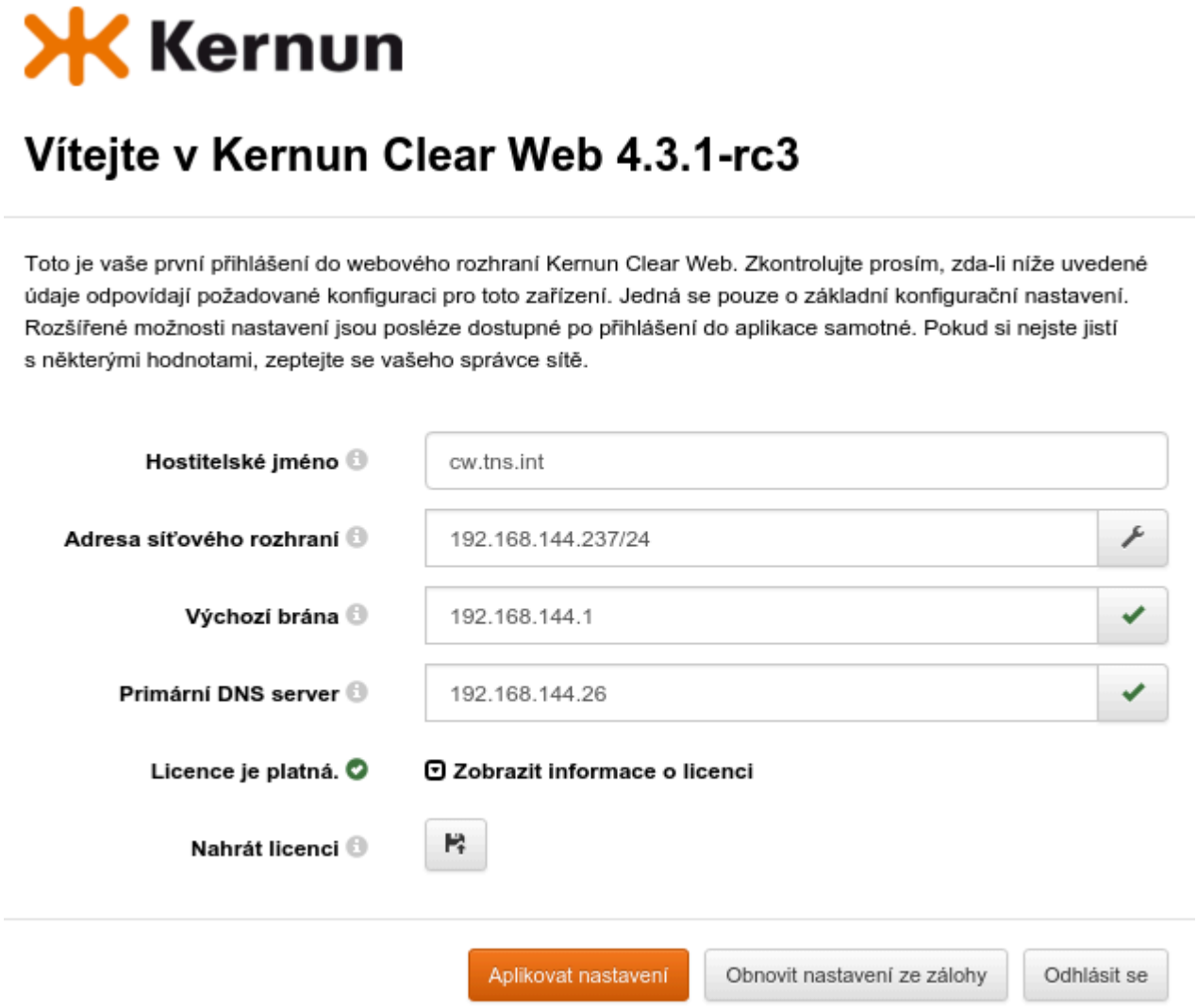
Obrázek 2.1: Přihlašovací obrazovka

Aby fungovalo DNS i bez nutnosti nastavovat adresy serverů, jsou ve výchozím nastavení jako primární a sekundární DNS server nastaveny adresy Google Public DNS `8.8.8.8`, viz `https://developers.google.com/speed/public-dns/`. V rámci počáteční konfigurace je možné nastavit pouze primární server. Oba servery je možné kdykoliv později změnit.

Po zadání hodnot klikněte na tlačítko Aplikovat nastavení. Nová konfigurace zařízení se uloží a aplikuje. Poté je vyžadováno nové přihlášení, tentokrát přímo do grafického uživatelského rozhraní produktu Kernun Business Intelligence. Jeho možnosti jsou popsány v následující kapitole.

Při novém přihlášení po aplikaci nastavení je nutné v prohlížeči zadat nově nastavené jméno počítače nebo IP adresu zařízení Kernun Business Intelligence.

2.6 Propojení se zařízeními Kernun



Obrázek 2.2: Počáteční konfigurace

Kapitola 3

Uživatelské rozhraní

Kapitola popisuje webové grafické rozraní pro administraci systému Kernun Business Intelligence společně se strukturou aktivit a sekcí rozhraní. S prvním přístupem k rozhraní vám pomůže návod pro přihlášení.

3.1 Přihlášení

Do grafického uživatelského rozhraní systému Kernun Business Intelligence se přistupuje pomocí webového prohlížeče (Mozilla Firefox, Microsoft Internet Explorer nebo Google Chrome). Přihlášení probíhá obdobně, jako první přihlášení po zapojení systému, viz kap. 2.4:

1. Otevřete webový prohlížeč a do adresního řádku napište doménové jméno zařízení, např. `https://kbi.example.com`. Jestliže jméno nebylo zavedeno do DNS, je potřeba místo jména zadat IP adresu síťového rozhraní systému Kernun Business Intelligence, např. `https://192.168.1.2`.

2. Jestliže se zobrazí informace o nedůvěryhodném spojení kvůli self-signed certifikátu, akceptujte spojení s tímto certifikátem. Lze přidat výjimku pro tento certifikát ve Vašem prohlížeči, abyste nemuseli akceptaci certifikátu znovu potvrzovat při každém přihlašování. Pro zvýšení bezpečnosti komunikace lze ověřit otisk certifikátu v prohlížeči s otiskem certifikátu ze systémové konzole zařízení. Pro přístup na systémovou konzoli připojte monitor (HW appliance) nebo virtuální obrazovku (virtuálni appliance).

   V každém prohlížeči, ze kterého se do rozhraní Kernun Business Intelligence přihlašujete, stačí certifikát akceptovat jednou. Při některých změnách konfigurace je vygenerován nový certifikát a je nutné ho znovu akceptovat. To se týká změny hostitelského jména nebo IP adresy zařízení.

3. Objeví se přihlašovací obrazovka, viz obr. 2.1. Zadejte uživatelské jméno `admin` a heslo.

4. Po chvíli se objeví centrální panel systému Kernun Business Intelligence, viz obr. 3.1.

3.2 Popis uživatelského rozhraní

Grafické uživatelské rozhraní produktu Kernun Business Intelligence je rozděleno do několika částí (aktivit). V této kapitole stručně popíšeme jednotlivé aktivity. Podrobnější vysvětlení klíčových aktivit a s nimi souvisejících funkcí produktu bude následovat v dalších kapitolách.

Po přihlášení se zobrazuje centrální panel (obr. 3.1), který podává rychlý přehled o stavu systému. Jednotlivá okna centrálního panelu obsahují:

Úspěšnost databáze Úspěšnost (procento nalezených serverů) databáze pro kategorizace webových serverů. Graf progrese zachycuje rozdíl mezi aktuální úspěšností a historickou úspěšností v době nasazení zařízení do provozu. Tlačítko Statistiky zobrazí podrobné statistiky provozu.

Síťový provoz Grafy objemu data přenášených po síti. Je možné se přepínat mezi pohledy za poslední měsíc, týden, den nebo hodinu. Tlačítko Monitoring vede na zobrazení právě probíhajících HTTP spojení od klientů.

Licence Informace o platnosti licence a také o počtu unikátních uživatelů a zařízení v síti za poslední týden. Okno obsahuje čas od poslední úspěšně aktualizace databáze pro kategorizaci webových serverů.

Povolené kategorie, BYPASS kategorie, Zakázané kategorie Přehledy počtů přístupů do nejčastěji navštěvovaných kategorií stránek. Samostatně se zobrazují kategorie, které jsou v konfiguraci politiky (v profilech) nastavené jako povolené, používající mechanismus bypass a zakázané. Grafy je možné zobrazit za poslední den, týden nebo měsíc. Tlačítko Statistiky zobrazí podrobné statistiky provozu.

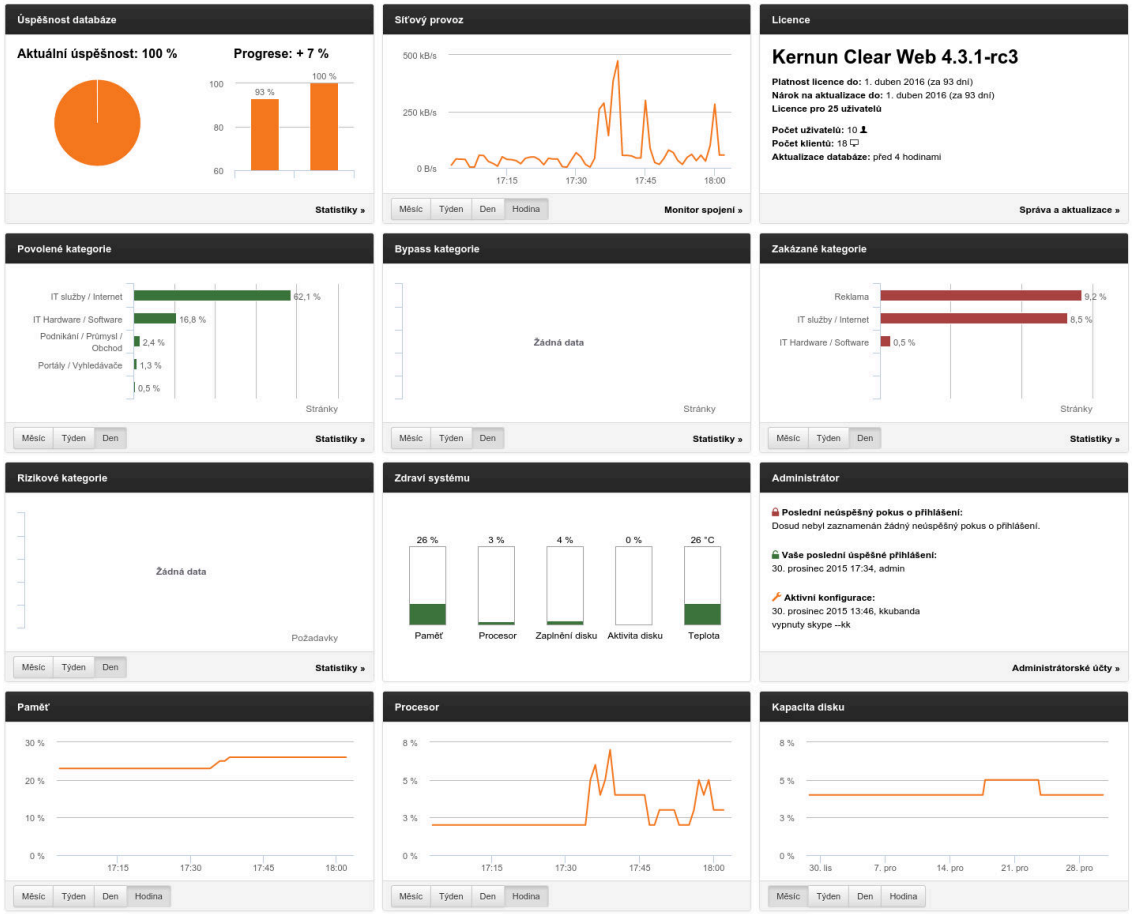
Rizikové kategorie Přehled uživatelů s největším počtem zachycených virů a přístupů na servery, které jsou zařazené do kategorií považovaných za bezpečností riziko.

Zdraví systému Aktuální hodnoty vybraných důležitých parametrů systému Kernun Business Intelligence.

Administrátor Informace o posledním přihlášení administrátora a o poslední změně konfigurace.

Paměť, Procesor, Kapacita disku Vývoj naměřených hodnot vybraných důležitých parametrů systému za poslední hodinu, den, týden nebo měsíc.

V horní části obrazovky je navigační lišta (obr. 3.2), která slouží pro přepínání mezi jednotlivými aktivitami (částmi) uživatelského rozhraní. Navigační lišta zároveň informuje o právě zobrazené aktivitě. V pravé části navigační lišty se nachází aktuální systémový čas a důležité akce, které může uživatel provést (aktivace konfigurace, uložení a obnovení uživatelského nastavení a odhlášení). Tlačítkem aktivace konfigurace se upravená konfigurace uloží a systém se podle ní začne chovat. Při ukládání každé nové verze konfigurace je možné vložit textovou poznámku popisující tuto verzi. Nápis Business Intelligence v levé části navigační lišty slouží pro přepnutí do rozhraní Kernun Clear Web, pokud zařízení obsahuje Kernun Business Intelligence pouze jako modul do Kernun Clear Web



Obrázek 3.1: Centrální panel

Obrázek 3.2: Navigační lišta

3.3 Struktura uživatelského rozhraní

Struktura dostupných aktivit v uživatelském rozhraní má dvě úrovně. První úroveň nazývaná aktivity se vybírá pomocí ikon na navigační liště. Názvy druhé úrovně nazývané sekce jsou v levém panelu.

- *Přehled*
- *Sestavy* — Bude podrobně vysvětleno v kap. 4.
  - *Moje sestavy* — Uživatelem vytvořené sestavy
  - *Výchozí sestavy* — Sestavy dodávané společně s produktem
- *Reporty* — Bude podrobně vysvětleno v kap. 4.
  - *Reporty* — Uživatelem vytvořené reporty a přehled reportů dodávaných společně s produktem
  - *E-maily* — Zasílání pravidelně generovaných reportů a sestav
  - *Detekce* — Zasílání pravidelně generovaných reportů za předpokladu, že platí zadaná podmínka
- *Správa*
  - *Databáze* — Stav a správa databáze.
  - *Síťové nastavení* — Jméno počítače a parametry sítě.
  - *Parametry systému* — Nastavení času, zasílání zpráv a správa záznamů.
  - *Zdraví systému* — Grafy stavu systému
  - *Správa a aktualizace* — Správa verzí a aktualizace systému, licence, zálohování konfigurace a obnova ze zálohy, restart a vypnutí zařízení, služba vzdálené pomoci, systémové komponenty
  - *Účty* — Správa administrátorských účtů
- *Nápověda*
  - *Příručka administrátora* — Zobrazí tuto příručku administrátora
  - *Poznámky k vydání*
  - *Seznam změn*
  - *O aplikaci*

Kapitola 4

Reporty a sestavy

Report (obr. 4.1) v kontextu Kernun Business Intelligence představuje jeden nezávislý pojmenovaný pohled na data z databáze. Slouží zejména k získání a následné prezentaci důležitých informací ze zpracovávaných dat o síťové komunikaci. Reporty lze sdružit do pojmenovaných sestav (obr. 4.2) a vytvořit tak širší pohled na zkoumanou oblast se souvisejícími informacemi. Samotná definice reportu je nezávislá na konkrétních datech a report tak lze opakovaně použít ve vícerých sestavách s různými typy dat.

Příkladem je výchozí sestava Síťový provoz obsahující reporty s daty za posledních 31 dnů s informacemi o množství provozu po jednotlivých hodinách, o použití pravidel politiky za celé období, množství provozu jednotlivých uživatelů nebo klientů a také s informacemi o zachycených virech a struktuře provozu přes jednotlivé kategorie, domény a servery.

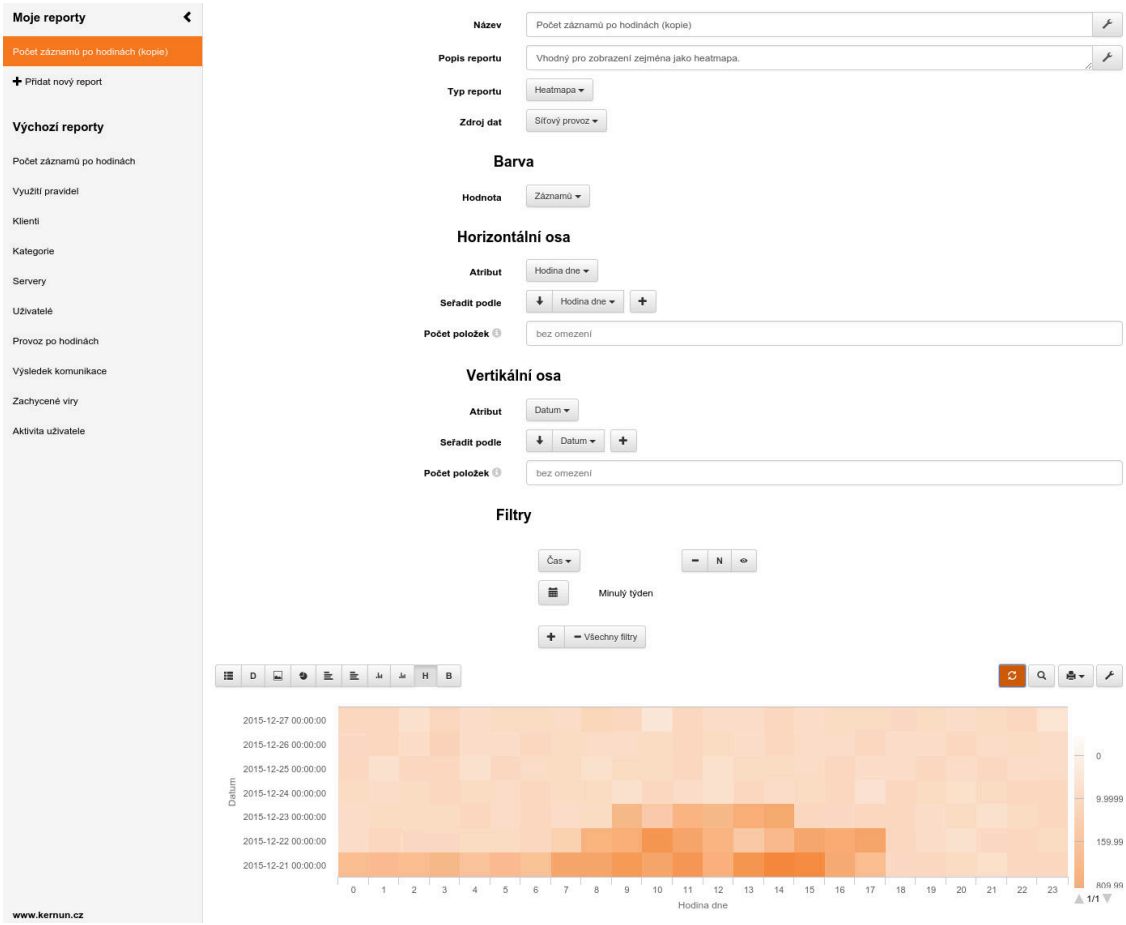
Nové sestavě lze nastavit název společně s popisem, přidat nové nebo existující reporty, které má obsahovat a omezit zdrojová data reportů pomocí filtrů sestavy. Takto vytvořenou sestavu lze následně vytisknout nebo stáhnout ve formátech PDF a XSLT pomocí tlačítka Exportovat sestavu. Periodické zasílání sestav pomocí mailu se nastavuje v aktivitě Správa v sekci E-maily.

Novému reportu lze nastavit název společně s upřesňujícím popisem. Výběrem typu reportu se zobrazí nastavitelné parametry reportu pro výběr a zpracování dat. Tyto parametry definují zdroj a filtry pro výběr zpracovávaných dat, způsob seskupování, řazení a zobrazení hodnot a výsledku. Hodnoty zobrazitelné v reportu jsou počet záznamů, množství přijatých nebo odeslaných dat a doba trvání komunikace.

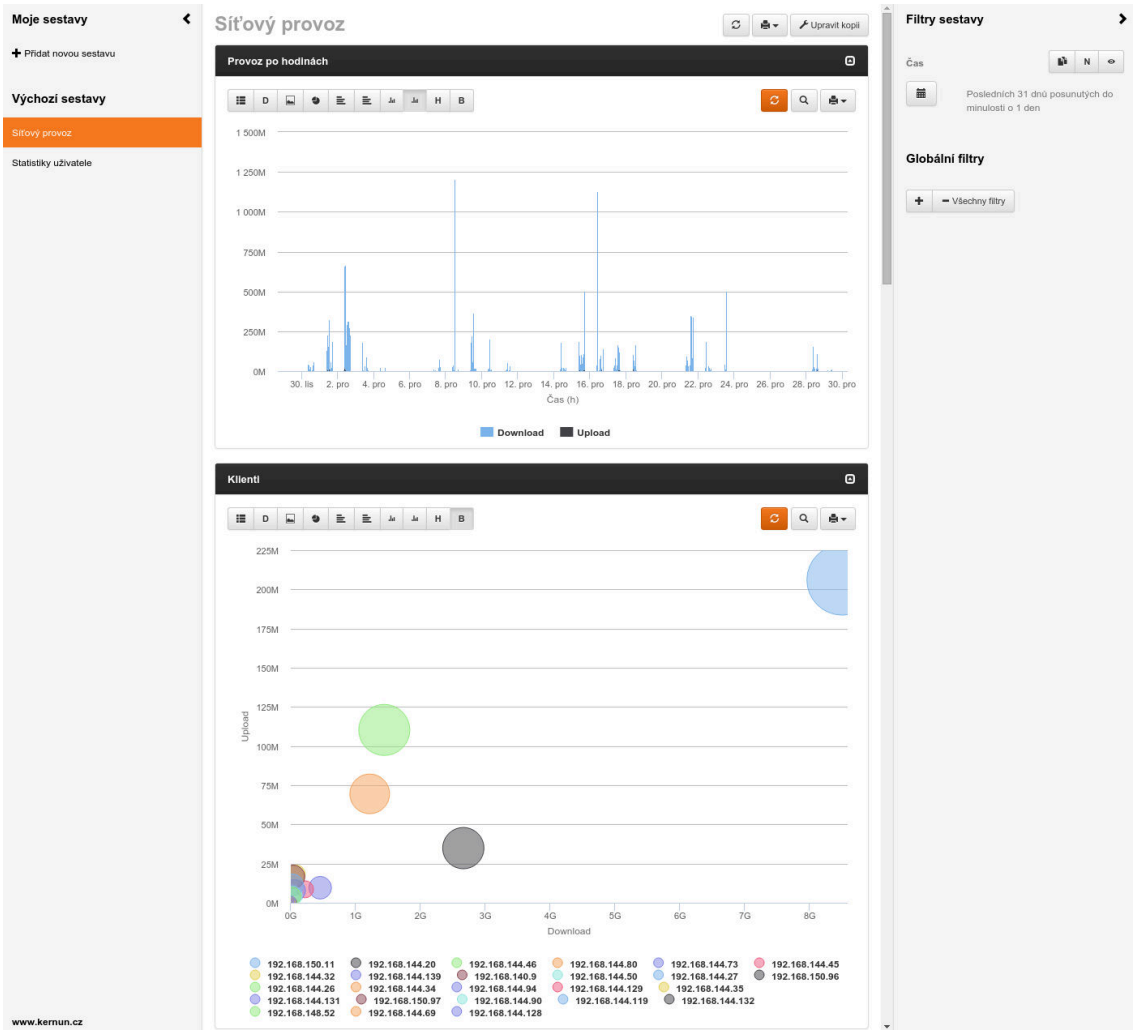
Nový report lze vytvořit buď prázdný, jako kopii jiného již existujícího reportu nebo pomocí funkce Prozkoumat. Tlačítko Exportovat report umožnuje stáhnout report ve formátu PDF a XSLT, vytisknout report nebo ho odeslat mailem ve formátu PDF.

Pro interaktivní práci se sestavami a reporty slouží globální filtry a funkce Prozkoumat. Jejich hlavním posláním je získat přesnější informace omezením zpracovávaných dat. Po kliknutí na zobrazenou entitu v grafu nebo na tlačítko lupy v reportu se objeví samostatné okno pro úpravu kopie reportu. Report lze libovolně upravovat přidáváním filtrů nebo změnou parametrů. Lze také změnit aktuální report na jeden z uložených v levém rohu okna. Výsledný report interaktivní analýzy je možné uložit mezi ostatní reporty.

Aby se projevily změny filtrů, nastavení reportu nebo nahrání nových dat do databáze, je nutné Report obnovit tlačítkem Obnovit data. Po vytvoření a nastavení reportů je nutné uložit



Obrázek 4.1: Reporty



Obrázek 4.2: Sestavy

změny tlačítkem Uložit uživatelské nastavení v horní liště, jinak budou provedené změny po odhlášení ztraceny.

4.1 Zdroje dat

Databáze Kernun Business Intelligence obsahuje data z různých zdrojů, která se liší položkami. Jednotlivé typy zdrojů jsou hierarchicky uspořádané tak, aby bylo možné pracovat se záznamy různých typů zdrojů, které obsahují společné typy položek.

Hierarchie zdrojů dat:

Všechny události Všechny záznamy v databázi. Obsahují pouze čas, počet událostí, název zařízení Kernun a identifikaci jeho funkcionality, která záznam vytvořila.

IDP/IPS Záznamy systému prevence a detekce průniku, který monitoruje a analyzuje síťový provoz na úrovni paketů a zakazuje podezřelý provoz.

Síťový provoz Všechny záznamy síťového provozu. Kromě informací obsažených ve *Všech událostech* obsahují identifikaci zdroje a cíle komunikace, množství přijatých a odeslaných dat, výsledek události a uplatněné pravidlo (například název profilu nebo výjimky).

Překlad doménových jmen (DNS) Navíc obsahují jméno a operační kód DNS dotazu a jeho odpověď.

Virtuální privátní síť (VPN) Navíc obsahují virtuální IP adresu.

Webový provoz (HTTP) Navíc obsahují typ obsahu, HTTP metodu a informace o Kernun Clear Web kategoriích.

Webový provoz (ICAP) Webový provoz, který byl zkontrolován antivirem. Obsahuje navíc ICAP metodu.

Telefonní hovory (SIP) Hovory prostřednicvím internetových telefonů. Navíc obsahují indentifikaci volajícího a příjemce.

E-mail (SMTP) Jednotlivé e-maily. Záznamy navíc obsahují identifikace odesílatele a příjemce, typy příloh a informace o přítomnosti viru a o stavu metody grey-listing.

E-mail přílohy (SMTP AT) Jednotlivé přílohy e-mailů. Obsahují navíc velikost přílohy.

Síťový provoz / Paketový filtr Provoz paketového filtru. Záznamy neobsahují navíc žádné informace.

4.2 Filtry

Reportem zpracovávaná vstupní data lze omezit pomocí výběru zdroje dat v reportu nebo pomocí některého z filtrů. V Kernun Business Intelligence jsou filtry čtyř typů:

Časový filtr Nastavuje časový interval, za který se zobrazí data. Lze možné vybrat jeden z přednastavených intervalů, nebo zvolit vlastní interval. Přednastavené intervaly se každý den

automaticky posunují o jeden den, aby například filtr na včera vždy vybíral události ze včerejšího dne. Toto nastavení lze vypnout odznačením Automaticky posouvat filtr v horní části dialogového okna nastavení filtru.

Číselný filtr Umožňuje omezit hodnoty daného číselného sloupce.

Výčtový filtr Vybírá hodnoty nečíselného sloupce z předem známé skupiny hodnot. Například hodnota sloupce Akce proxy může být buď accepted nebo rejected.

Filtr na textovou hodnotu Umožňuje určit hodnoty, kterých může nabývat daný textový sloupec. Pro omezení hodnot na předpony a přípony lze použít zástupný znak %. Po vepsání prvního písmene se zobrazí seznam hodnot, kterých daný sloupec nabývá.

Filtry je možné dočasně deaktivovat kliknutím na tlačítko s ikonou oka. Také lze celý filtr negovat, čímž se obrátí jeho význam.

Filtry jsou rozděleny na Filtry reportu, které jsou nedílnou součástí každého reportu, Filtry sestavy, které jsou vlastní každé sestavě, Globální filtry, které jsou společné pro všechny sestavy, a Filtry funkce Prozkoumat, které jsou podrobněji vysvětleny v sekci kap. 4.4.

4.3 Vizualizace výsledků reportu

Výsledkem reportu jsou data v podobě tabulky, kterou je možné zobrazit v grafické podobě pro rychlejší a intuitivnější pochopení dat. Některé typy grafů vyžadují sloupce určitého typu, jinak je není možné zobrazit, například pro zobrazení výsečového grafu je nutný alespoň jeden číselný sloupec, jinak není možné spočítat velikosti jednotlivých výsečí.

Dostupné typy grafů:

Tabulka Pro jednoduchost je tabulka považována za typ grafu. Zobrazuje přímo výsledek dotazu do databáze, proto například u typu reportu Heatmapa není příliš přehledná. Typ reportu Přehled webové aktivity má význam zobrazit pouze jako tabulku.

Dvouúrovňová tabulka Speciální typ zobrazení pro typ reportu Dvouúrovňová tabulka.

Čárový graf Každý číselný sloupec zobrazuje jako jednu čáru v grafu. První nečíselný sloupec je zobrazen jako souřadnice x. Pokud je jediným nečíselným sloupcem čas a data jsou podle něj seřazená vzestupně, je možné graf přiblížit kliknutím a táhnutím myši.

Výsečový graf Zobrazuje data jako výseče. Velikost výseče je určena první číselnou hodnotou, další číselné hodnoty se zobrazí pouze při najetí myší.

Řádkový a sloupcový graf Každý číselný sloupec zobrazuje jako jeden řádek, respektive sloupec v grafu. První nečíselný sloupec je zobrazen jako popisek řádku (případně sloupce). U vrstvového grafu jsou jednotlivé řádky (sloupce) navrstveny na sobě, jinak se nacházejí vedle sebe.

Heatmapa Zobrazuje data v dvourozměrné tabulce, ve které sytost barvy představuje velikost prvního číselného sloupce. Pro jednodušší nastavení reportu slouží typ reportu Heatmapa.

Bublinový graf Jednotlivé body jsou zobrazeny jako kružnice o různém poloměru v ploše. Pozice na x-ové ose je určena první číselnou hodnotu, pozice na y-ové ose eprezentuje druhou číselnou hodnotu a velikost je určena třetí číselnou hodnotou. Graf lze přibližovat kliknutím a táhnutím myši nebo skrýváním jednotlivých kružnic po kliknutí na název kružnice pod grafem.

Kliknutí na oblast grafu představující jednu informaci (jeden bod čárového grafu, jeden sloupec sloupcového grafu, jeden obdélník heatmapy) způsobí otevření dialogového okna, ve kterém se zobrazí filtr na každou položku informace. Vedle filtru se nacházejí tlačítka Přidat filtr, které přidá vybraný filtr ke globálním filtrům, a Prozkoumat, které otevře nové dialogové okno stejnojmenné funkce, jež je podrobněji rozebrána v následující sekci.

4.4 Funkce Prozkoumat

Pro jednorázové bližší prozkoumání dat daného reportu slouží funkce Prozkoumat, která je dostupná po kliknutí na část grafu nebo na ikonu lupy. V samostatném okně se zobrazí kopie reportu, jehož parametry je možné libovolně upravovat, aniž by se změny promítly do existujících reportů. Hledanou informaci lze dále upřesňovat přidáváním filtrů nebo rozšiřovat výběrem dalších sloupců. Výsledný report lze přidat k již existujícím tlačítkem s ikonou diskety v záhlaví okna. V záhlaví okna je také možné vybrat z existujících reportů, což nahradí právě upravovaný report kopií vybraného, ale zachová Filtry funkce Prozkoumat. Tak lze snadno změnit pohled na právě vybraná data.

4.5 Výchozí reporty a sestavy

Kernun Business Intelligence obsahuje výchozí sadu reportů a sestav, které jsou dodané spolu se zařízením. Výchozí reporty a sestavy nelze přímo upravovat, ale lze použít jejich kopii jako základ při vytvářeních vlastních reportů a sestav.

Výchozí sestavy v Kernun Business Intelligence jsou:

Síťový provoz Poskytuje celkový přehled provozu v síti. Obsahuje heatmapu provozu po hodinách dne a jednotlivých dnech, vrstvový sloupcový report provozu po hodinách, dvouúrovňovou tabulku využitých pravidel a akcí proxy, bublinové grafy klientů a uživatelů, vrstvový řádkový graf jednotlivých kategorií, dvouúrovňovou tabulku serverů podle L2 domény a kompletní domény, tabulku zachycených virů a výsečový graf výsledku komunikace.

Statistiky uživatele Umožňuje analyzovat daného síťovou aktivitu uživatele, který se vybírá vyplněním filtru na Jméno uživatele. Obsahuje heatmapu provozu po hodinách dne a jednotlivých dnech, vrstvový sloupcový graf provozu po hodinách, podrobnou aktivitu uživatele, vrstvový řádkový graf provozu po jednotlivých kategoriích, dvouúrovňovou tabulku serverů podle L2 domény a kompletní domény, dvouúrovňovou tabulku využitých pravidel a akcí proxy a výsečový graf výsledku komunikace.

Kapitola 5

Správa

Kapitola vysvětluje funkce systému Kernun Business Intelligence z aktivity Správa. Jedná se zejména o správu systému a databáze a nastavení automatického zasílání vybraných reportů a sestav.

5.1 Správa a aktualizace

Systém Kernun Business Intelligence periodicky kontroluje dostupnost nových verzí a aktualizací. V případě zaškrtnuté možnosti Povolit automatickou přípravu aktualizací se automaticky, bez nutnosti zásahu administrátora, stáhne dostupná aktualizace a připraví se lokálně na zařízení. Tím se čas samotné aktualizace zařízení zkrátí na co nejkratší možnou dobu. V případě nepovedené aktualizace je možné se vždy vrátit k předešlé funkční verzi pomocí tlačítka Obnovit.

Platnost licence je možné zkontrolovat v sekci Správa a aktualizace aktivity Správa, kde je navíc možnost nahrát do zařízení novou licenci. V této sekci se také nachází funkce pro zálohování a obnovu konfigurace, restart a vypnutí zařízení nebo obnovy do továrního nastavení zařízení Kernun Business Intelligence. Pro rychlejší analýzu a řešení nekonzistentností systému lze spustit službu vzdálené pomoci, která umožní přímý přístup technikům výrobce na konkrétní zařízení Kernun Business Intelligence. Pro fungování této služby nastavte váš firewall a případné mezilehlé prvky vaší síťové infrastruktury tak, aby neblokovaly komunikaci ze zařízení na port 22 (SSH) serveru `callhome.kernun.com`.

V této části je také možné zařízení obnovit do továrního nastavení. K tomu slouží tlačítko Obnovit tovární nastavení. V takovém případě dojde ke smazání veškerých uživatelských dat (konfigurace a její historie, statistiky, logy, databáze pro grafy systémové zátěže a podobně) a zařízení bude restartováno s výchozí tovární konfigurací. Na hardwarovém modelu "Appliance KBI 1"je k dispozici také hardwarové tlačítko, které slouží rovněž pro reset do továrního nastavení podobně, jako tlačítko v grafickém rozhraní. K provedení resetu pomocí hardwarového tlačítka je nutné je podržet alespoň po dobu čtyř vteřin. Následně se ozve potvrzovací tón a zařízení se restartuje.

Dále lze v této sekci změnit HTTPS certifikát administračního rozhraní. Ve výchozím nastavení je certifikát vygenerován automaticky. Při změně hostitelského jména systému je výchozí certifikát vygenerován nově a může být nezbytné znovu pro něj přidat výjimku v prohlížeči. Lze zadat

vlastní certifikát, který se použije místo výchozího certifikátu.

5.2 Pravidelné zasílání reportů a sestav e-mailem

Sekce E-maily aktivity Správa umožňuje nastavit pravidelné automatické zasílání vybraných reportů a sestav. Po kliknutí na tlačítko Přidat nový periodický e-mail lze vybrat čas a periodicitu zasílání, adresu příjemce, seznam reportů a sestav a jednorázově vyzkoušet zaslání e-mailu. V sekci Síťové nastavení je nutné mít správně nakonfiguranou vychozí bránu a DNS servery, v sekci Parametry systému lze nastavit poštovní server, přes který se doručují zprávy, jinak se budou doručovat přímo poštovnímu serveru adresáta.

5.3 Správa databáze

Po provedení aktualizace na novou verzi Kernun Business Intelligence nebo návratu k předchozí verzi může být nutné reinicializovat databázi, pokud došlo ke změně její verze. Tato situace je signalizována vykřičníkem vedle času v horní liště. Sekce Databáze aktivity Správa zobrazuje stav a velikost databáze. Také umožnuje reinicializovat databázi a nahrát události ze zařízení. K automatickému nahrávání událostí ze zařízení dochází pravidelně každý den ve tři hodiny ráno.

5.4 Single Sign-on

Pro přihlášení do webového rozhraní bez nutnosti zadávat uživatelské jméno a heslo lze použít funkcionalitu Single Sign-on (SSO). Ta v prostředí Microsoft Active Directory využívá protokol Kerberos a LDAP.

Podmínkou funkčnosti SSO je správně nakonfigurovaná proxy autentizace pomocí metody Kerberos a správně nastavené prostředí klienta.

Microsoft Internet Explorer a Google Chrome:

- V nastaveních Možnosti Internetu, v záložce "Zabezpečení", v sekci "Důvěryhodné weby"přidat hostitelské jméno KBI (např. https://kernun.example.com) do seznamu "Weby".
- Nastavit ve "Vlastní úroveň...", v sekci "Ověření uživatele", v podsekci "Přihlášení"možnost "Automatické přihlášení pod aktuálním uživatelským jménem a heslem".

Mozilla Firefox:

- Zobrazit pokročilá nastavení zadáním adresy about:config do adresního řádku prohlížeče.
- Hodnotu položky s názvem "network.negotiate-auth.trusted-uris"nastavit na hostitelské jméno KBI (např. https://kernun.example.com).

Single Sign-on lze nastavit v sekci "Účty". Poté lze do webového rozhraní autentizovat dvěma způsoby:

Pomocí účtu v Active Directory: Konkrétnímu lokálnímu účtu lze nastavit jeden AD účet z domény. Tento AD účet lze následně využít pro přihlášení pomocí SSO k tomuto lokálnímu účtu.

Pomocí skupin v Active Directory: V tabulce mapování AD skupin na role je možné k jednotlivým rolím přiřadit AD skupiny, jejichž členové po přihlášení pomocí SSO obdrží oprávnění dané role bez nutnosti vytvářet lokální účet. Jestliže je možné uživateli přiřadit více rolí, použije se role s nejvyššími oprávněními.