Whalebone příručka

Vydání 3.2.1-12

29.02.2024

Contents

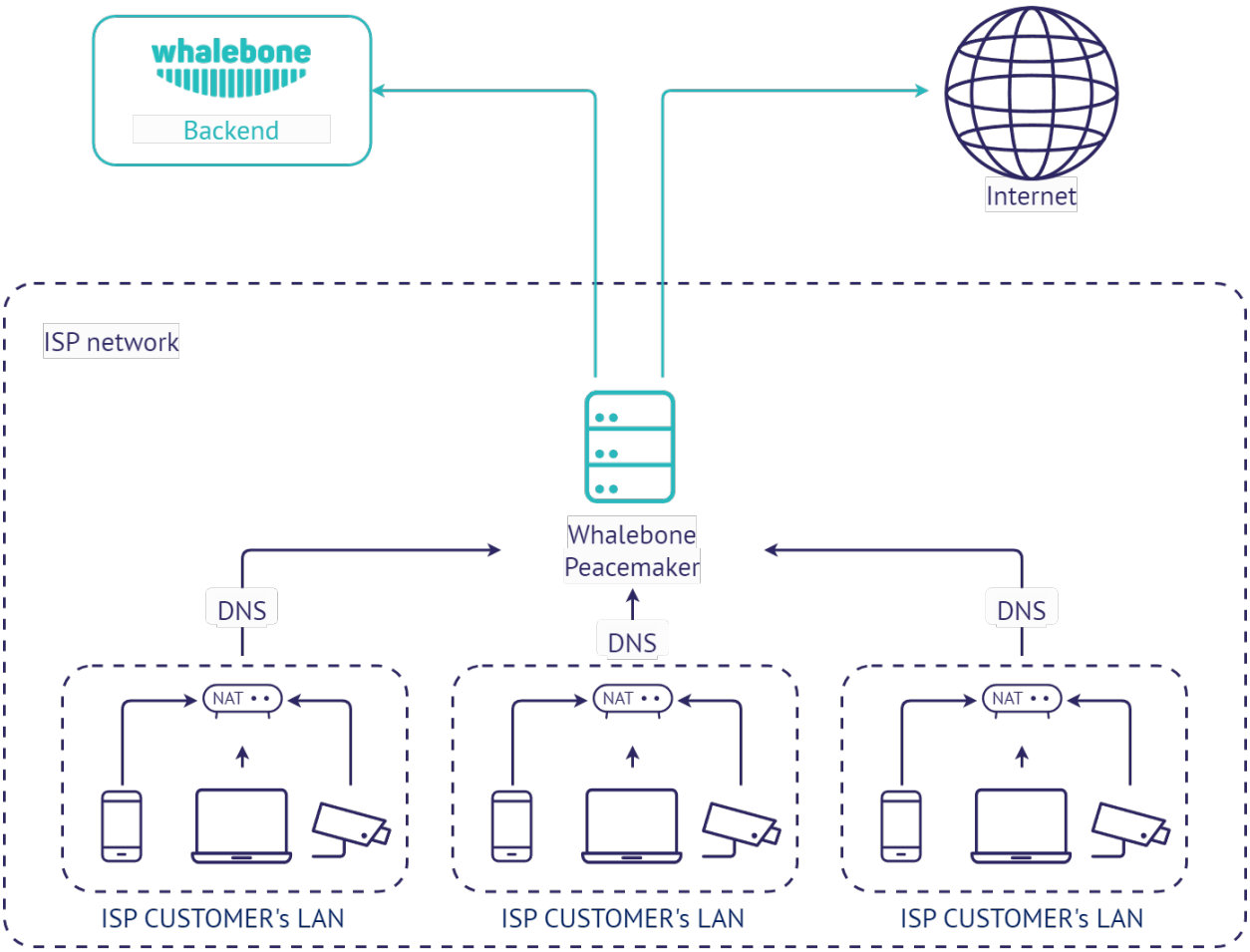
Whalebone je služba pro bezpečnostní filtrování provozu DNS. Využívá logiku nad vlastními DNS resolvery. Tyto resolvery mohou být buď cloudové, které jsou pod správou Whalebone, nebo lokální softwarové resolvery využívající cloud pouze pro aktualizace a hlášení informací o hrozbách. Při prevenci hrozeb se Whalebone spoléhá na externí zpravodajské zdroje i na vlastní metody. Další informace o produktu a společnosti jsou k dispozici na oficiálních stránkách Whalebone.

CHAPTER 1

Whalebone Peacemaker

1.1 Místní překladač DNS pro poskytovatele internetových služeb (ISP)

Tento scénář nasazení využívá lokální resolver Whalebone, který komunikuje s cloudem Whalebone prostřednictvím rozhraní API. Překlad DNS probíhá přímo na resolveru a je zcela nezávislý na dostupnosti cloudu. V případě, že resolver nebude schopen dosáhnout cloudové služby, nebude schopen aktualizovat informace o hrozbách a hlásit případné incidenty. Hlavní výhodou tohoto nasazení je viditelnost místní sítě a jednotlivých IP adres a nízká latence.


whalebone
Backend
Internet
ISP network
Whalebone
Peacemaker
DNS
DNS
DNS
NAT
NAT
NAT
ISP CUSTOMER's LAN
ISP CUSTOMER's LAN
ISP CUSTOMER's LAN

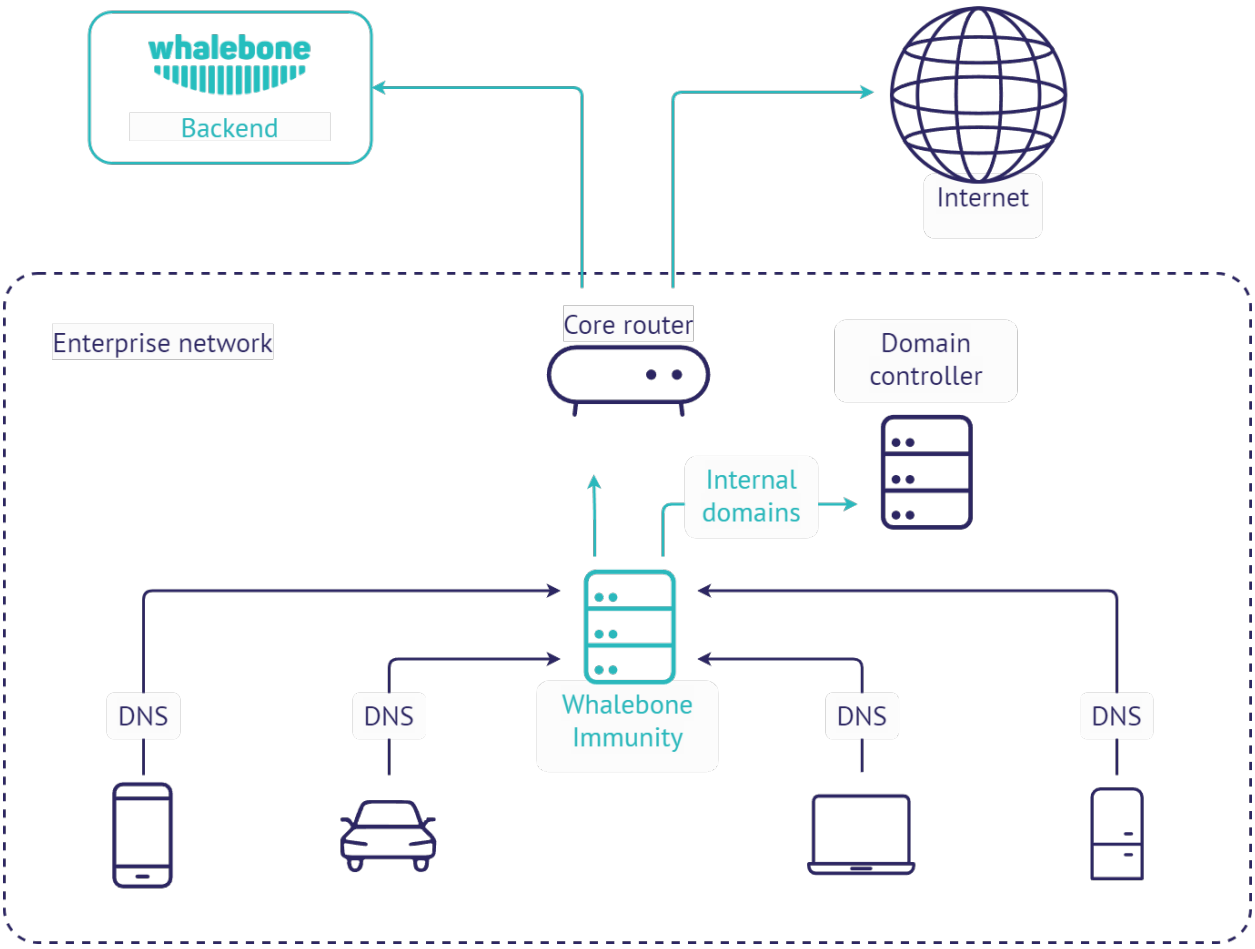
CHAPTER 2

Whalebone Immunity

2.1 Lokální DNS forwarder

Velmi podobný scénář nasazení jako u lokálního resolveru, avšak Whalebone pouze přeposílá lokální požadavky na předem nakonfigurované resolvery. Tento scénář je velmi užitečný v případě, že existují místní zóny DNS, které musí být klientům k dispozici (např. Active Directory), nebo v případech, kdy je nedávná konfigurace resolveru velmi specifická a musí být zachována. Toto nasazení má také nižší hardwarové nároky.

Varování: Nedoporučujeme předávat požadavky z místního resolveru na cloudové resolvery Whalebone. Taková konfigurace by vedla k duplicitní detekci incidentů, nepřidala by bezpečnost a u klientů by docházelo ke zbytečnému zpoždění požadavků.


whalebone
Backend
Internet
Enterprise network
Core router
Domain controller
Internal domains
DNS
DNS
Whalebone Immunity
DNS
DNS

CHAPTER 3

Coudové nasazení

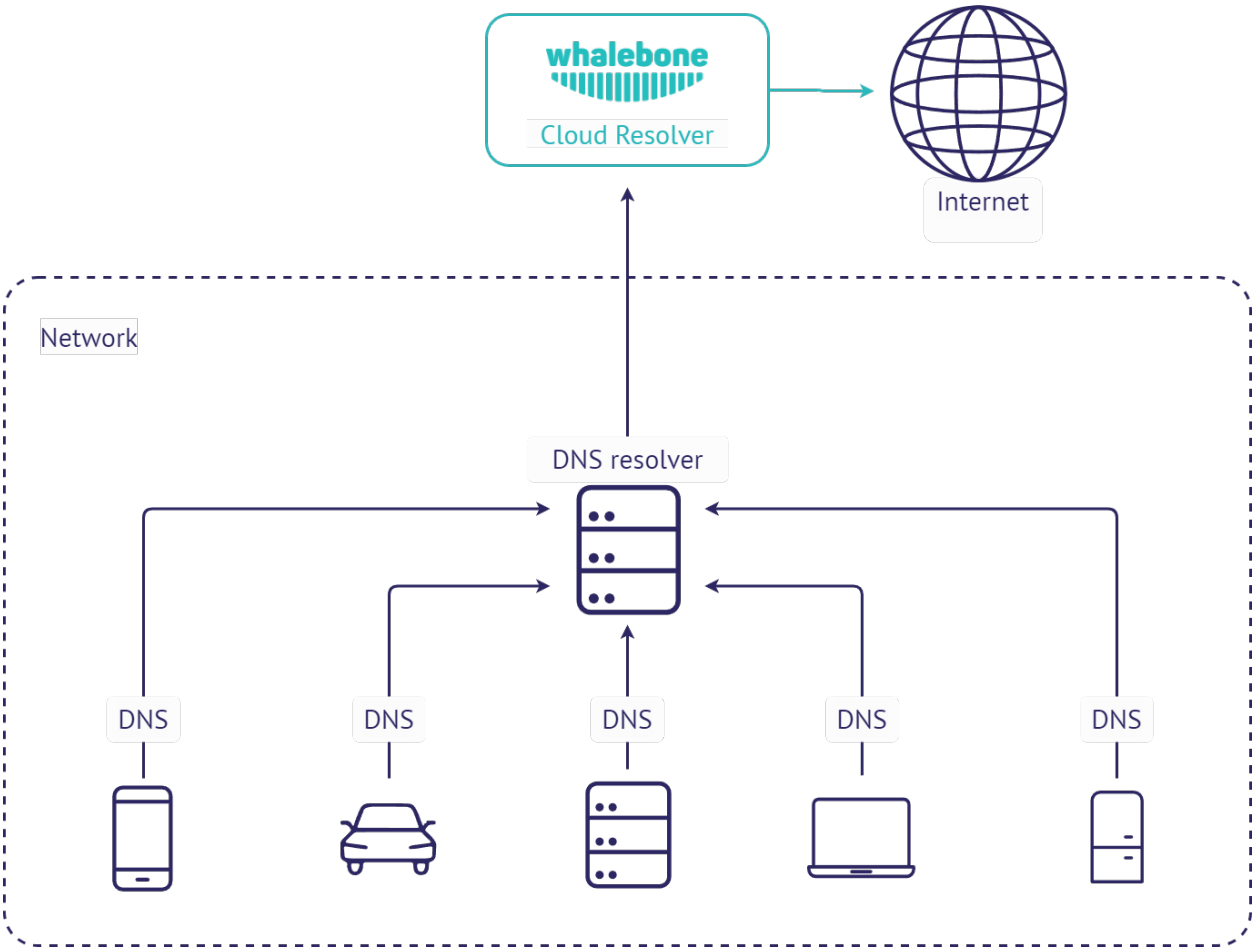
Whalebone lze nasadit v několika scénářích, které lze dokonce kombinovat tak, aby splňovaly požadavky konkrétních sítí. Kombinace cloudového a lokálního DNS resolveru s jediným portátálem pro správu je vhodná i v případě složitých, distribuovaných sítí.

Tip: Všechny níže uvedené možnosti lze kombinovat dohromady. Různé síťové segmenty a zóny mohou mít různé požadavky a možnosti.

Tip: Pokud ani jeden z níže uvedených scénářů konfigurace nevyhovuje Vašemu preferovanému případu použití, obraťte se na podporu společnosti Whalebone a my vám pomůžeme s návrhem architektury, která bude vyhovovat vašim potřebám a požadavkům.

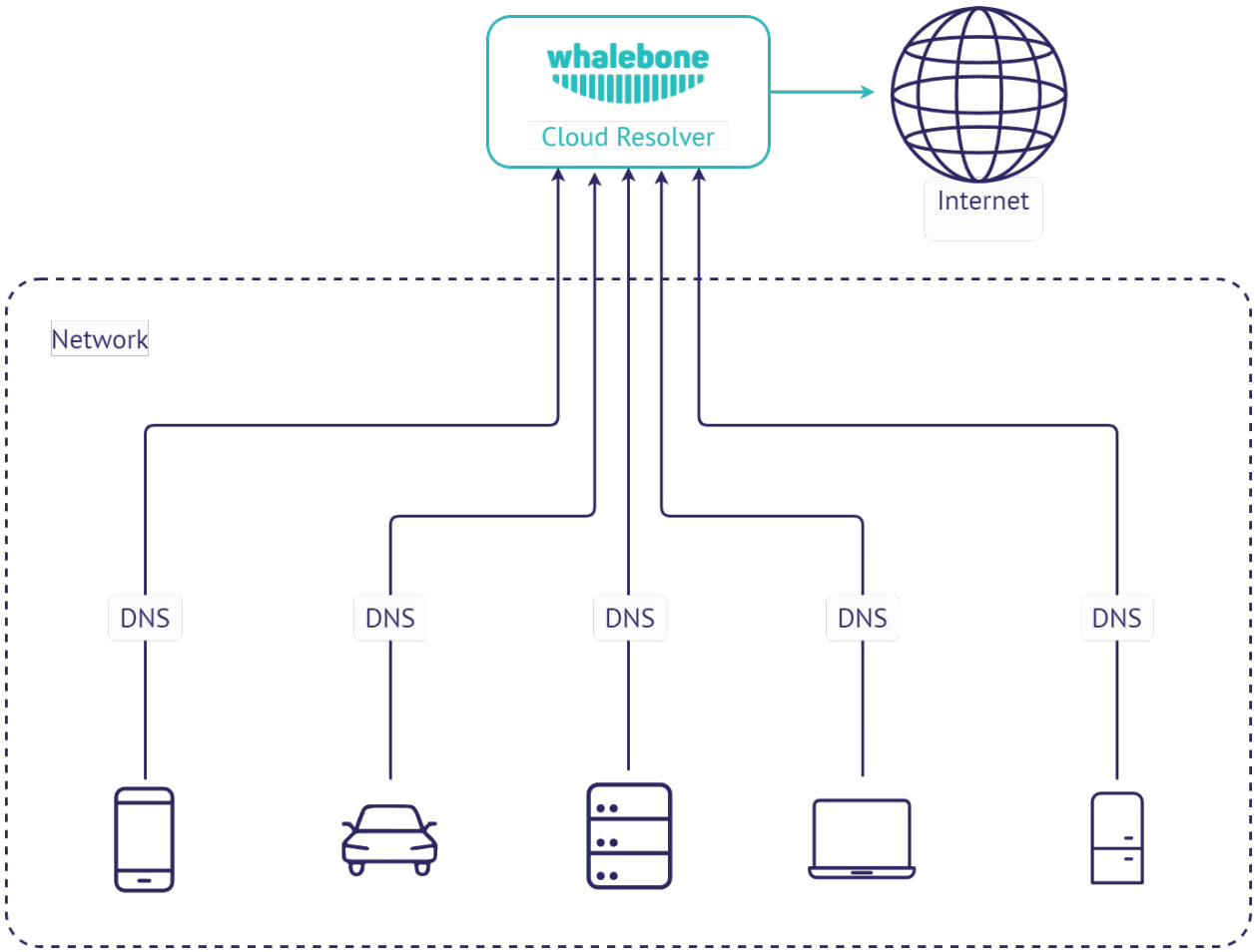
3.1 Použití stávající DNS pro přesměrování na Whalebone Cloud DNS

Jedná se o nejjednodušší způsob o nasazení. Chcete-li používat Whalebone resolver, stačí změnit konfiguraci vašich DNS resolverů a nasměrovat je na cloudové resolvery Whalebone. Nevýhodou tohoto nasazení je, že všechny incidenty budou viditelné se zdrojovou IP adresou DNS forwarderu namísto původní zdrojové IP adresy. Přesto se toto nasazení může hodit, pokud je prioritou zabránit hrozbám s co nejmenším úsilím a změnami infrastruktury.



3.2 Cloudové DNS (příme spojení)

Toto nasazení je podobné předávání požadavků na cloudové resolvery Whalebone, ale požadavky jsou odesílány přímo do cloudu bez místní mezipaměti DNS. To lze obvykle nastavit pro všechny koncové body prostřednictvím DHCP. Nepoužití místní mezipaměti DNS však znamená zvýšenou latenci způsobenou síťovou komunikací mezi klientem a cloudovým resolverem. Pokud nejsou jednotlivé počítače skryty za NAT, budou jejich IP adresy přímo viditelné v hlášení Whalebone a klienty lze snadno rozlišit.

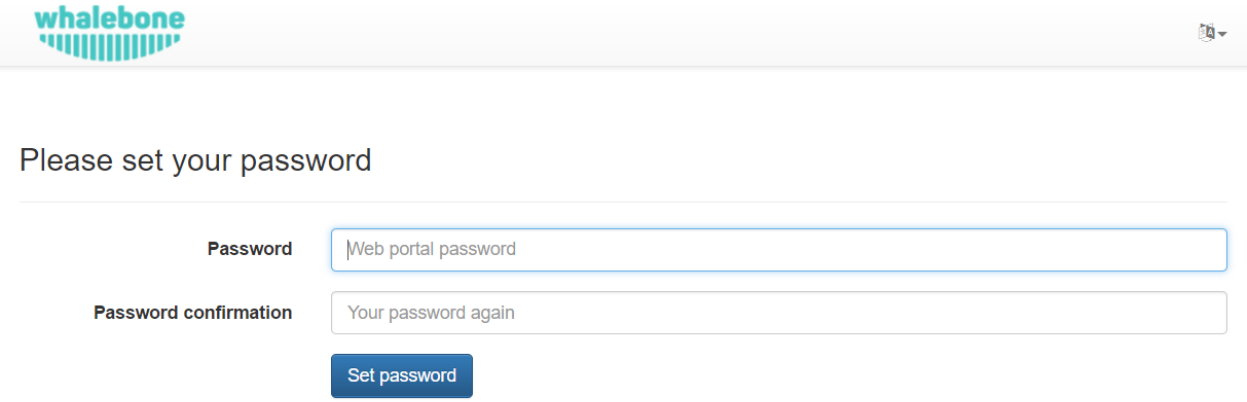

whalebone
Cloud Resolver
Internet
Network
DNS
DNS
DNS
DNS
DNS

CHAPTER 4

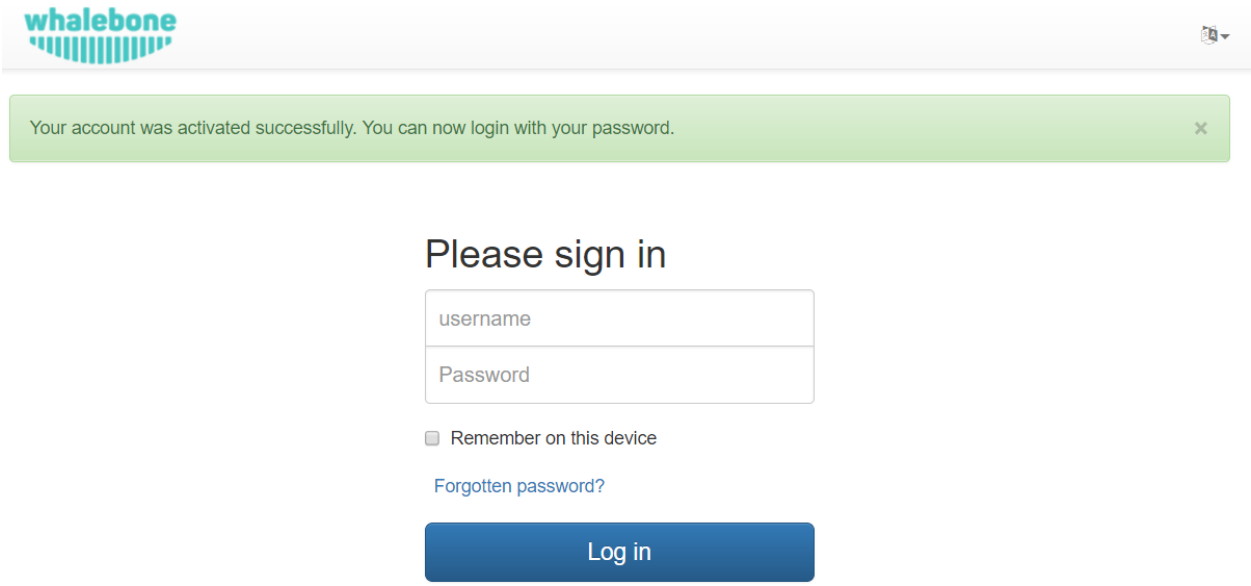
Quickstart

4.1 Vytvoření účtu v portálu

Po prostupu na URL z aktivačního e-mailu budete vyzváni k nastavení hesla k účtu. Na složitost hesla neklademe nároky, ale doporučujeme používat jedinečné a netriviální heslo. Neoprávněný přístup by ohrozil soukromí uživatelů a mohlo by dojít k poškození vaší sítě.

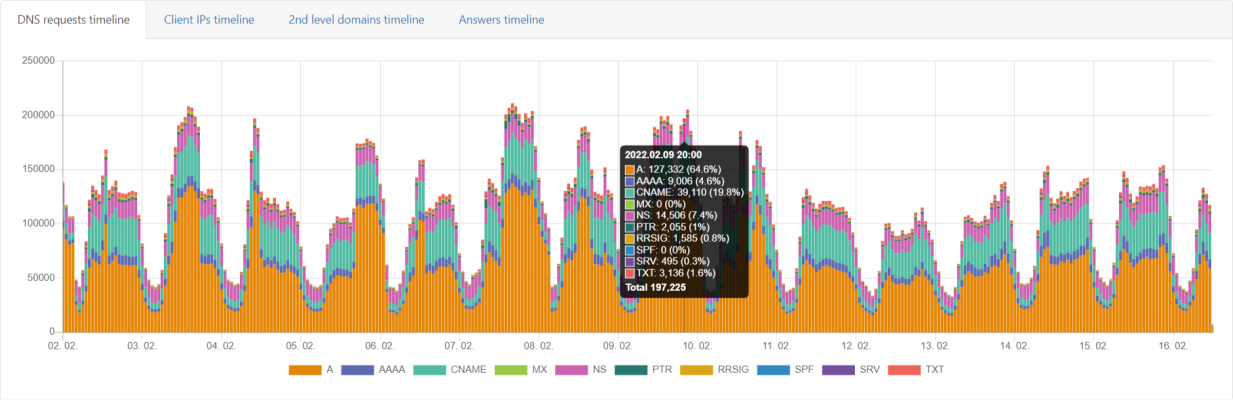


Po nastavení hesla budete vyzváni k přihlášení pomocí uživatelského jména a nově vytvořeného hesla.



4.2 Zobrazení DNS provozu

Pokud je provoz správně přesměrován na DNS resolvery Whalebone (cloudové nebo místní), bude provoz DNS viditelný v nabídce **DNS provoz**, kde jsou k dispozici jednotlivé dotazy a odpovědi pro další investigaci provozu. Provoz by měl být viditelný během několika minut poté, co bylo vše správně nastaveno. Pokud nebude provoz zaznamenán ani za několik hodin, neváhejte se obrátit na podporu společnosti Whalebone, která vám pomůže překontrolovat konfiguraci nebo jakýkoli druh problémů s resolvery.



Kontrolu překladu DNS lze v počítačích se systémem Windows nebo Linux provést také ručně pomocí nástroje `nslookup`. Nastavte IP adresu resolveru Whalebone a zkuste přeložit existující název domény.

```
localhost:~$ nslookup whalebone.io
Server:         193.32.92.32
Address:        193.32.92.32#53

Non-authoritative answer:
Name:   whalebone.io
Address: 75.2.70.75
```

(continues on next page)

(pokračujte na předchozí stránce)

```
Name:   whalebone.io
Address: 99.83.190.102
```

CHAPTER 5

Lokální resolver

Nasazení řešení Whalebone nasazeného jako **lokální resolver** přináší výhodu viditelnosti místních IP adres, které odesílají skutečné požadavky. Pokud pro vás nasazení lokálního řešení není vhodnou volbou, podívejte se na další Možnosti nasazení.

Whalebone resolver je založen na implementaci Knot Resolveru vyvinutého CZ.NIC.

5.1 Systémové požadavky na lokální resolver

Instalace lokálního resolveru je podporována na vyhrazeném (hardwarovém nebo virtuálním) stroji s jedním z níže uvedených operačních systémů.

- **Podporovaný operační systém** (64bitový, serverové edice následujících distribucí):
  - Red Hat Enterprise Linux 7, 8, 9
  - CentOS Linux 7, 8
  - CentOS Stream 8, 9
  - Debian 9, 10, 11, 12
  - Ubuntu 16.04, 18.04, 20.04, 22.04
- **Podporované souborové systémy**
  - ext4
  - xfs pouze s podporou d_type (ftype=1)
- **Minimální požadavky na hardware** (fyzického nebo virtuálního):
  - 2 jádra procesoru
  - 4 GB RAM
  - 40 GB HDD (alespoň 30 GB v oddílu /var)

Varování: Pozor, Whalebone podporuje pouze nasazení bez desktopových prostředí, jako je GNOME, KDE nebo Xfce, protože ty mohou ovlivnit dostupnou paměť a zpracování DNS na serveru.

- **Požadavky na nastavení sítě** (místní resolver potřebuje otevřené následující výstupní porty):

Směr	Protokol(y)	Port	Cílová IP/Doména	Popis
Odchozí	TCP+UDP	53	Jakákoli	DNS rekurze
Odchozí	TCP	443	resolverapi.whalebone.io	Aktualizace databáze hrozeb
Odchozí	TCP	443	stream.whalebone.io	Aktualizace databáze hrozeb
Odchozí	TCP	443	logger.whalebone.io	Logovací stream
Odchozí	TCP	443	agentapi.whalebone.io	Správa resolveru
Odchozí	TCP	443	transfer.whalebone.io	Sběr podpůrných protokolů
Odchozí	TCP	443	portal.whalebone.io	Portál správce
Odchozí	TCP	443	harbor.whalebone.io	Aktualizace resolveru
Odchozí	TCP	443	download.docker.com	Instalační proces
Odchozí	TCP	443	data.iana.org	DNSSEC klíče

Varování: Bez povolené komunikace na portu 443 s výše uvedenými doménami nebude resolver vůbec nainstalován (instalační skript se přeruší).

Hlavní funkcí resolveru je přijímat dotazy od uživatelů a odpovídat jim na ně, což vyžaduje, aby byly na resolveru otevřeny určité porty pro provoz pocházející z klientské podsítě nebo přicházející do zákaznického rozhraní.

Směr	Protokol(y)	Port	Cílová IP/Doména	Popis
Příchozí	TCP+UDP	53	Rozsah(y) podsítě zákazníka	DNS
Příchozí	TCP	853	Rozsah(y) podsítě zákazníka	DNS přes TLS (pokud se používá)
Příchozí	TCP	443	Rozsah(y) podsítě zákazníka	DNS přes HTTPS (pokud se používá)

Blokační stránky jsou hostovány **přímo** na resolverech, takže musí být použity IP adresy, které jsou přístupné klientům. Klienti pak budou při blokování přesměrováni na IP adresu resolveru. Doporučujeme povolit pouze podsítě přidělené zákazníkům nebo důvěryhodným sítím, jinak by mohly být zneužity k různým útokům nebo neoprávněným uživatelům.

Směr	Protokol(y)	Port	Cílová IP/Doména	Popis
Příchozí	TCP	80	Rozsah(y) podsítě zákazníka	Stránka přesměrování/blokování
Příchozí	TCP	443	Rozsah(y) podsítě zákazníka	Stránka přesměrování/blokování

Procesy resolveru musí komunikovat na localhostu. V případě, že je v provozu nějaký firewall, ujistěte se, že je provoz povolen, tj. `iptables -A INPUT -s 127.0.0.1 -j ACCEPT`

Příchozí TCP ANY 127.0.0.1 Procesy řešitele

Poznámka: Pro odhad HW požadavků u nasazení vr velkých sítích ISP nebo podnikových sítích se neváhejte obrátit na společnost Whalebone. Lokální resolver Whalebone bude potřebovat přibližně dvojnásobek paměti RAM a procesoru než běžný resolver (BIND, Unbound).

5.2 Instalace nového lokálního resolveru

Můžete se podívat na videonávod krok za krokem o postupu instalace zde.

V záložce **Resolvery** stiskněte tlačítko **Vytvořit nový**. Zvolte název (identifikátor) nového resolveru. Zadání je čistě informativní a nebude mít vliv na funkčnost. Po zadání názvu klikněte na tlačítko **Přidat resolver**. Po kliknutí na tlačítko se zobrazí informativní okno se seznamem podporovaných platforem a **jednořádkovým příkazem pro instalaci**. Příkaz zkopírujte a spusťte na stroji (VM) určeném pro místní resolver. Příkaz spustí instalační skript a předá jednorázový token použitý pro aktivaci resolveru (stejný příkaz nelze použít opakovaně).

Po spuštění příkazu probíhá kontrola operačního systému a instalace požadavků. Skript vás bude informovat o průběhu a vytvoří podrobný protokol s názvem `wb_install.log` v aktuálním adresáři. Úspěšné spuštění instalačního skriptu je ukončeno oznámením `` `Finální ladění operačního systému`` `` s hodnotou `[ OK ]`. Hned po instalaci proběhne také inicializace a může trvat několik minut, než resolver spustí služby.

Varování: Lokální resolver je nakonfigurován jako otevřený resolver. Odpoví na jakýkoli zaslaný požadavek. To je poměrně pohodlné z hlediska dostupnosti služeb, ale také to může představovat riziko, pokud je služba dostupná z vnějších sítí. Ujistěte se, že jste omezili přístup k místnímu resolveru na port 53 (UDP a TCP) pouze z důvěryhodných sítí, jinak může být zneužit k různým DoS útokům.

Důležité: The resolver's processes need to communicate on localhost. In case some firewall is in place please make sure that the traffic is allowed, i.e. `iptables -A INPUT -s 127.0.0.1 -j ACCEPT`

5.2.1 Ověření správnosti instalace

Whalebone diponuje řadou neškodných testovacích domén, které jsou interně klasifikovány jako testovací domény pro ověření funkčnosti resolveru. Pomocí těchto domén se můžete ujistit, že Whalebone resolver pracuje správně:

- `http://malware.test.attacker.online`
- `http://c2server.test.attacker.online`
- `http://spam.test.attacker.online`
- `http://phishing.test.attacker.online`
- `http://coinminer.test.attacker.online`

Při přístupu na tyto domény by se měla zobrazit podobná blokační stránka podobná s následující:

V případě, že narazíte na níže uvedenou stránku, znamená to, že požadavek nebyl zablokován, a tedy není použit resolver Whalebone. Zkontrolujte prosím své nastavení a pokud problém přetrvává, kontaktujte prosím podporu.

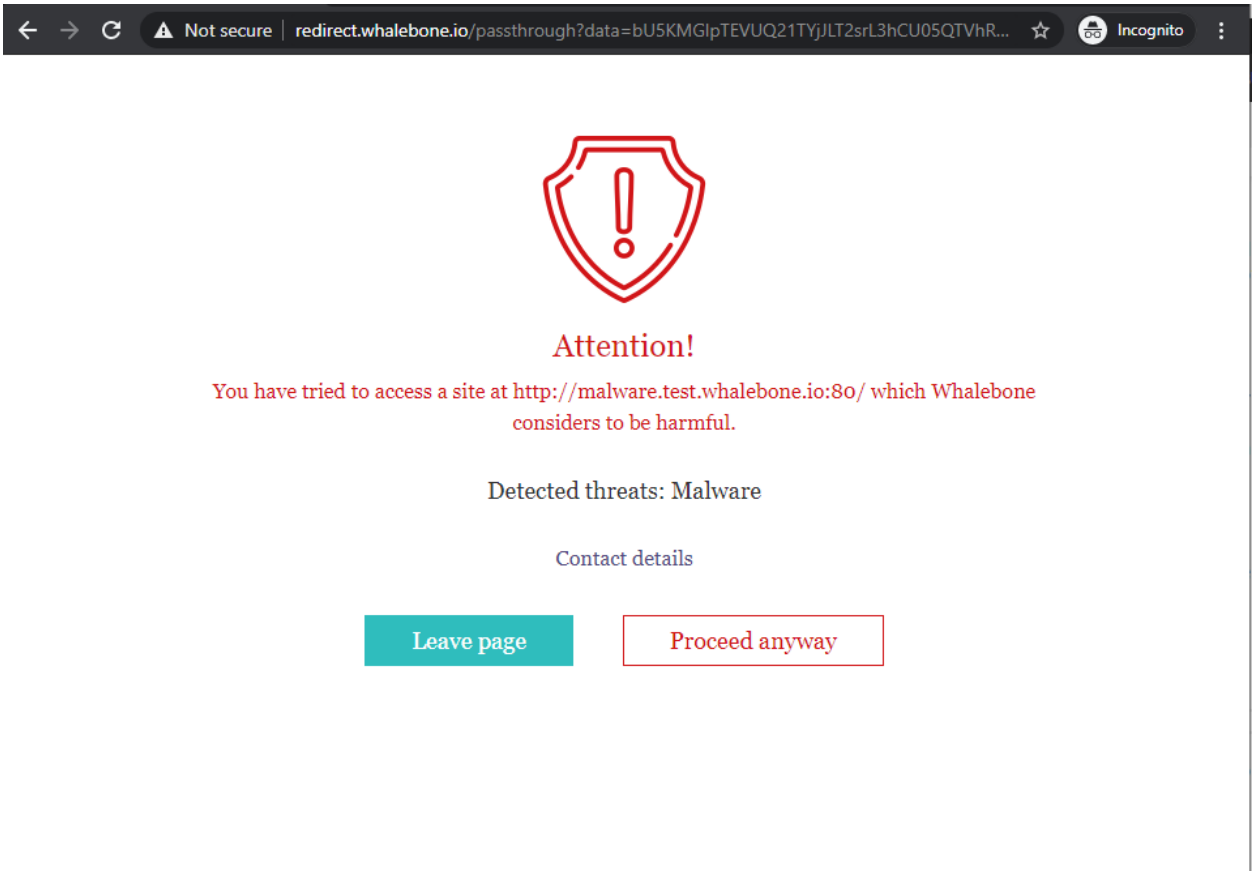


Figure1: Blokační stránka - správná funkce resolveru.

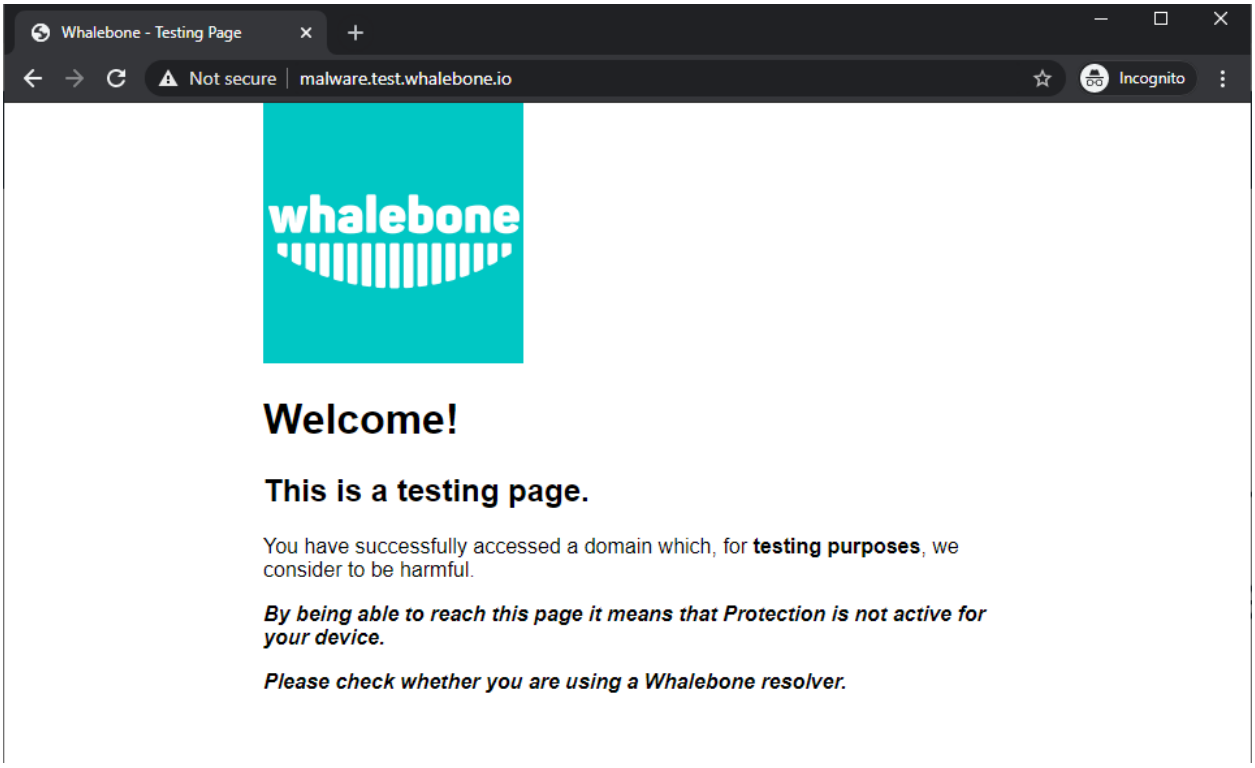


Figure2: Blokační stránka - resolver nefunguje správně.

5.2.2 Zabezpečení resolveru

Při první instalaci je resolver nakonfigurován jako otevřený resolver. Odpoví na jakýkoli požadavek, který je mu zaslán, bez ohledu na to, odkud požadavek pochází. To je poměrně pohodlné z hlediska dostupnosti služeb, ale může být také rizikem, pokud je služba dostupná z vnějších sítí. Ujistěte se, že jste omezili přístup k místnímu resolveru na portu 53 (UDP a TCP) pouze z důvěryhodných sítí, jinak může být zneužit k různým DoS útokům.

CHAPTER 6

Správa resolveru

V záložce **Resolvery** je přehled vytvořených resolverů. Správce může upravovat konfiguraci, nasazovat aktualizace a instalovat nové resolvery.

6.1 Přehled resolverů

V hlavním přehledu resolverů jsou dlaždice s podrobnostmi o resolveru. Přehled obsahuje informace o operačním systému a zdrojích jako využití CPU, paměti a HDD. Je zde také stav komunikačního kanálu mezi resolverem a cloudem označený barevnou tečkou.

Resolver se může nacházet v jednom z těchto stavů:

- **Aktivní** - Tento stav se očekává v produkčních prostředích a signalizuje, že vše běží správně.
- **Problém s překladem** - Resolver není schopen překládat požadavky DNS.
- **Nedostupný** - Resolver ztratil spojení se službou Whalebone Cloud. Tento stav nemá vliv na překlad DNS, nicméně resolver nemůže získávat aktualizace databáze hrozeb a nemusí reagovat na změny zásad nebo konfigurace iniciované z portálu.
- **Upgrading** - Resolveru byl vydán příkaz k aktualizaci. Tento stav by neměl přetrvávat déle než několik minut.
- **Není nainstalován** - Resolver ještě nebyl nainstalován.

6.2 Nahrání konfigurace

Pokud došlo ke změnám konfigurace, které mají vliv na překlad DNS, je třeba následně **Nahrát konfiguraci**. Jinak se změny neprojeví. V případě, že jsou k dispozici nějaké změny konfigurace, které lze nasadit, bude na kartě resolveru viditelná **červená ikona** se šipkou vpravo. Po kliknutí na ni bude webová stránka požádána o potvrzení a v pravém horním rohu bude oznámeno úspěšné nasazení.

Poznámka: Pokud nasazení skončilo chybou, zkuste akci zopakovat. Důvodem chyby může být krátkodobý výpadek komunikace mezi cloudem a resolverem.

6.3 Nastevení bezpečnostní politky pro jednotlivé segmenty

Zásady zabezpečení a obsahu lze granulárním způsobem přiřadit různým segmentům sítě.

Nastavení se vztahuje na jednotlivé resolvery a lze je nakonfigurovat v části **Resolvery** → `Název resolveru` → **Přiřazení politik**.

Poznámka: Konfigurace se vztahuje na zvlášť **pro každý resolver**. V případě, že chcete konfiguraci použít pro více resolverů, upravte konfiguraci u všech resolverů.

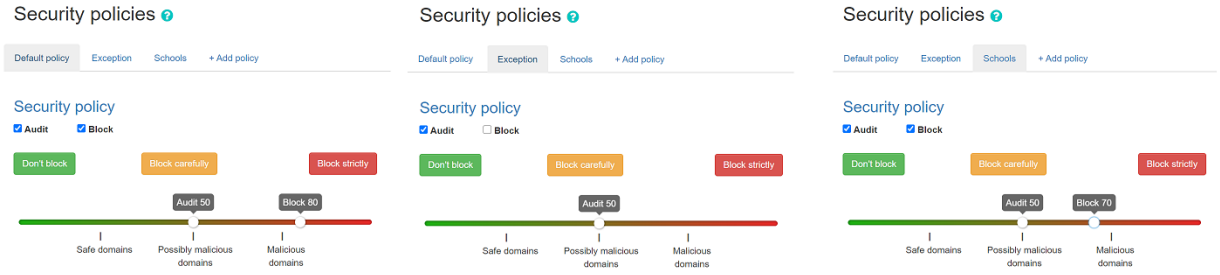
Bezpečnostní politiky lze aplikovat přidáním rozsahů IP ve vstupních oknech:

Pro lepší pochopení uvažujme příklad s rozsahem sítě `10.10.0.0/16`. Vytvořili jsme 3 různé politiky:

Pro lepší pochopení uvažujme příklad s rozsahem sítě `10.10.0.0/16`.

Vytvořili jsme 3 různé zásady:

- **Default**: zásada, kterou chceme použít pro celou síť, jedná se o nejobecnější zásadu.
- **Exception**: zásada, která musí být použita na konkrétní segment v síti, který bude mít zakázáno veškeré zabezpečení a filtrování obsahu.
- **School**: zásada, kterou chceme použít na 2 různé podsítě, které byly přiřazeny školnímu prostředí. V tomto případě jsme zvolili přísnější blokování.

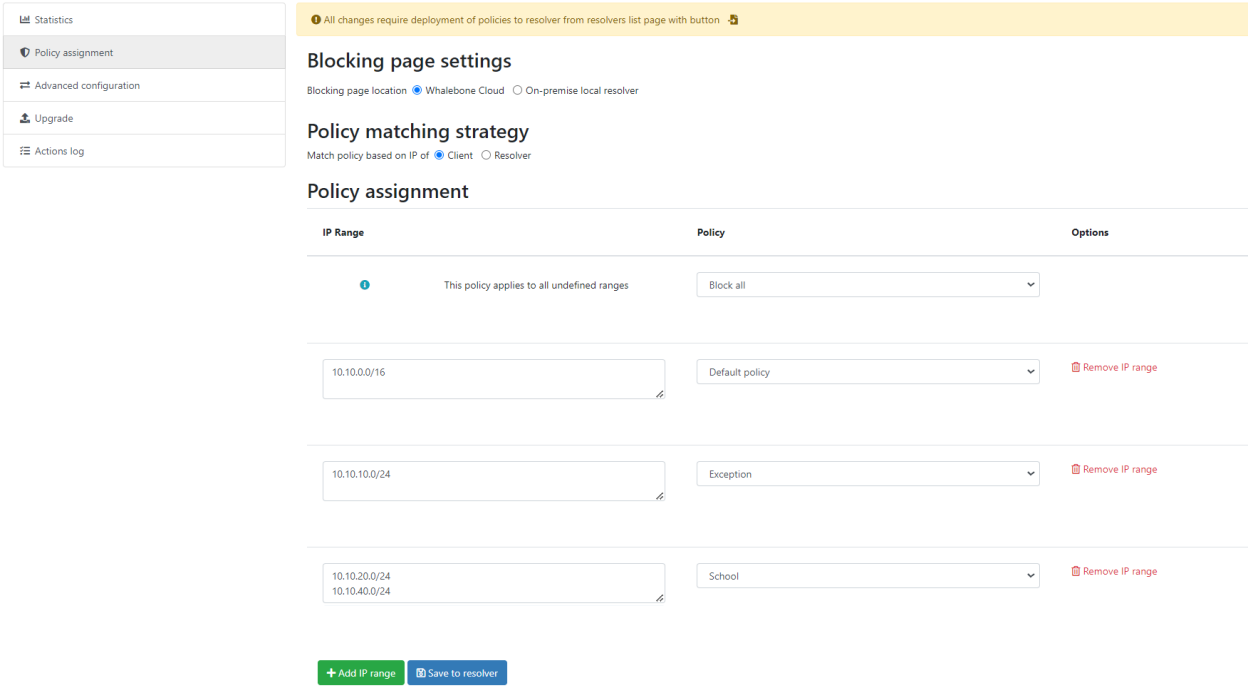


Poznámka: První možnost nastavení zásad je pro všechny nedefinované rozsahy. V případě různých zásad ovlivňujících stejný rozsah se použije ta, která je více granulární.

Shrňme požadavky do následující tabulky:

Bezpečnostní politika	Síťový rozsah
Default	10.10.0.0/16
Exception	10.10.10.0/24
School	10.10.20.0/24 a 10.10.40.0/24

Následující obrázek ukazuje proces přiřazování bezpečnostních politik k rozsahům.



Poznámka: Po přidání politik k rozsahům je nutné kliknout na **Uložit do resolveru**, aby se přidání projevilo. Poté budou změny ověřeny a vyskakovací zpráva poskytne další informace.

Pro přiřazení dalších položek ke stávajícímu přiřazení lze přidat nový rozsah sítí pomocí **enteru** jako oddělovače. V návaznosti na předchozí příklad bychom v případě, že bychom chtěli přidat podsíť `10.10.30.0/24` do bezpečnostní politiky **Exception**:

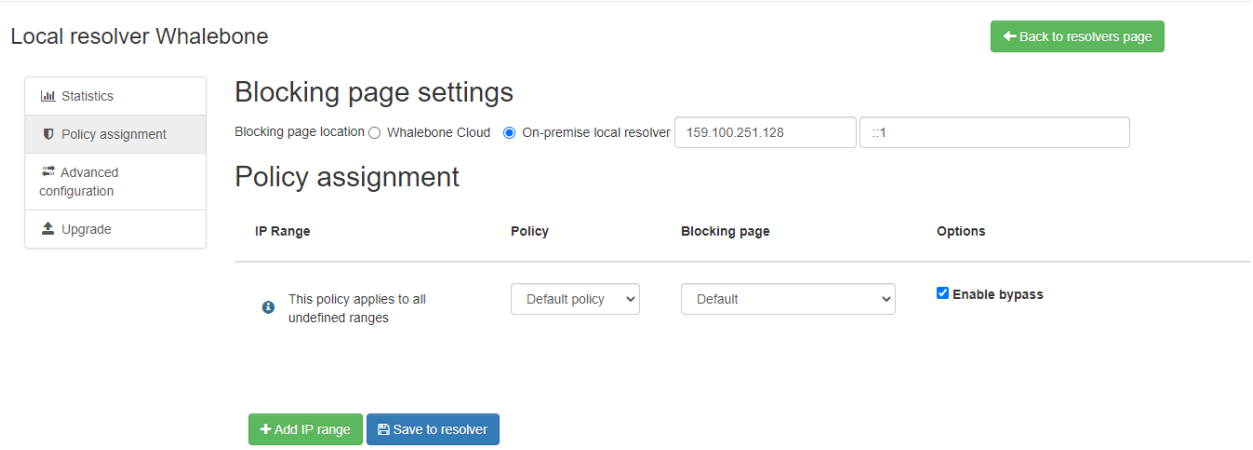
6.4 Konfigurace blokačních stránek

Podobně jako zásady zabezpečení lze k určitým rozsahům přiřadit i různé blokační stránky.

Prvním krokem je v detailu **Lokálního resolveru** v záložce **Přiřazení politik** v části **Nastavení blokační stránky**. Jsou dostupná dvě pole, do kterých je třeba vyplnit adresy IPv4 a IPv6 blokačních stránek.

Tip: Blokační stránky jsou umístěny **přímo** na resolverech, takže je třeba použít IP adresy, které jsou inzerovány klientům. Klienti pak budou při blokování přesměrováni na IP adresu resolveru. Zajistěte, aby byly na firewallu přístupné porty 80 a 443.

Pro každý přidaný rozsah IP adres je v rozevírací nabídce uvedena přiřazená blokační stránka.

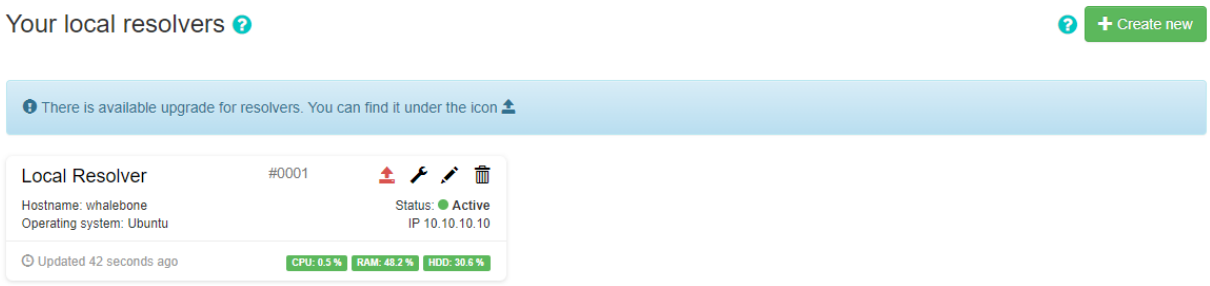


Důležité: První položka v **Policy Assignment** je považována za Default/Fallback. V případě, že klient přistupuje k resolveru z nedefinovaného rozsahu IP bude spadat pod politiku a blokační stránků z daného defaultního rozsahu.

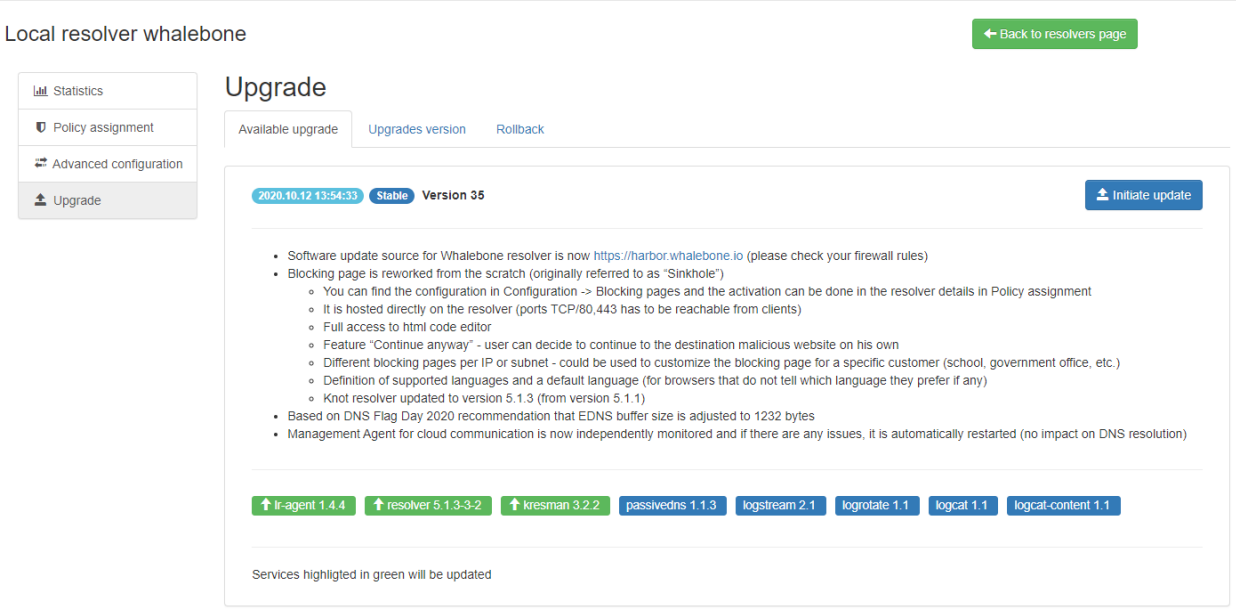
Poznámka: Po provedení potřebných změn v nastavení stránky blokování zkontrolujte, zda je třeba resolvery znovu nasadit.

6.5 Aktualizace/obnovení resolveru

Po vydání nové verze resolveru se v rozhraní pro správu resolveru zobrazí **červená ikona upgradu**.



Po kliknutí na ikonu **Upgrade** se vybere příslušná nabídka a zobrazí se důležité informace o nové verzi.



Z této nabídky lze zahájit aktualizaci resolveru.

V případě, že instalace nové verze nepřinese očekávaný výsledek, je možné se kdykoli vrátit k předchozí verzi na kartě **Vrácení změn**:

CHAPTER 7

Bezpečnostní politiky

Videoprůvodce základní konfigurací bezpečnostních politiky krok za krokem si můžete prohlédnout zde.

Videoprůvodce krok za krokem s hlubším vysvětlením jak nastavovat bezpečnostní politiky naleznete zde.

Chcete-li pomocí Whalebone provádět filtraci provozu, musíte nakonfigurovat bezpečnostní politiku. Při instalaci je Whalebone dodáván s **výchozí** bezpečnostní politikou, která je nastavena tak, aby zahrnovala všechny typy hrozeb a nastavuje prahové hodnoty na hodnotu **80/50**. Tato politika se také automaticky aplikuje na každý nově nainstalovaný resolver. V každé politice lze nakonfigurovat několik možností:

7.1 Prahové hodnoty pro filtrování škodlivých domén

Každá doména v naší databázi hrozeb má určitou hodnotu skóre. Skóre vyjadřuje, jak škodlivá je podle nás daná doména. V zásadách upravujete dvě hodnoty související se skóre:

- **Blokace** - Domény se skóre vyšším nebo rovným této hodnotě budou Whalebone resolverem blokovány a na požadavek klienta bude odpovězeno IP adresou blokující stránky.
- **Audit** - Domény se skóre vyšším nebo rovným této hodnotě, ale nižším, než je prahová hodnota pro blokování, budou monitorovány. Požadavek na překlad bude povolen a odpověď bude doručena buď z mezipaměti, nebo provedením úplné rekurze DNS. Požadavky však budou logovány v panelu hrozeb pro případné pozdější prošetření.

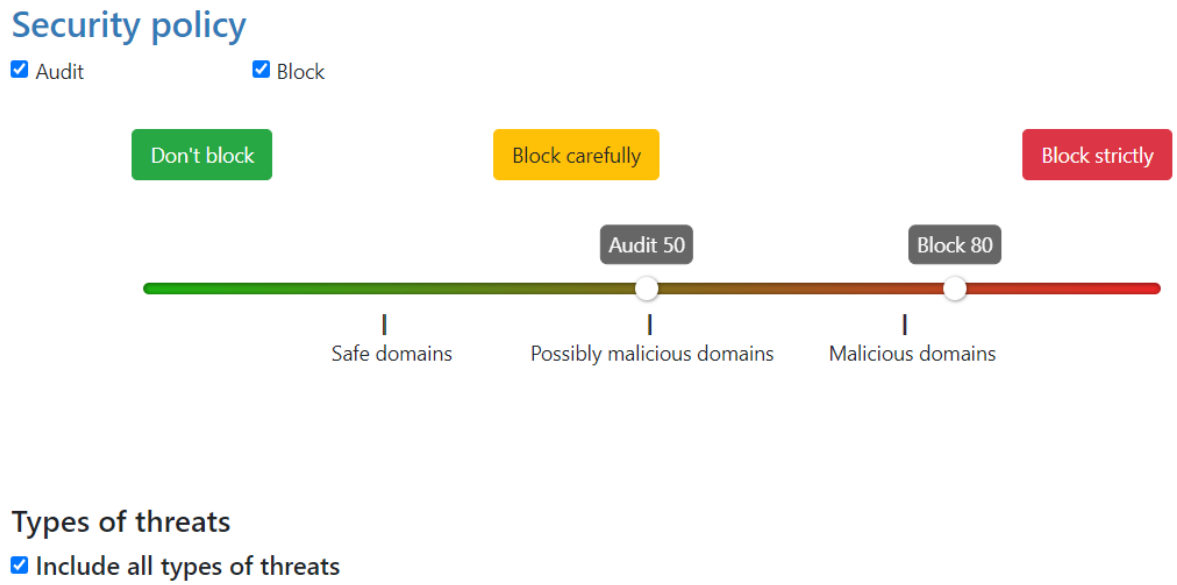
Jednotlivé akce lze vypnout - např. vypnout blokování pro účely testování.

Hodnoty posuvníku definují pravděpodobnost, že daná doména je škodlivá, na stupnici od **0** do **100**, přičemž **100** je nejškodlivější.

Tip: V základním nastavením je prahová hodnota pro blokaci nastavena na **80**, což je bezpečné i pro větší sítě s volnější politikou vůči uživatelům. Pro restriktivnější politiku doporučujeme nastavit práh pro blokování na **70-75**, ve velmi restriktivních sítích dokonce až na **60**. Audit má čistě informativní charakter, nicméně příliš nízké nastavení prahu může vést k příliš velkému počtu zaznamenaných incidentů.

K dispozici jsou předkonfigurované zásady, které pokrývají nejběžnější případy. Jedná se o tyto případy: Tyto případy jsou následující: **Neblokovat**, **Blokovat opatrně** a **Blokovat striktně**.

- Nastavení **Blokovat opatrně** upřednostňuje nízkou míru falešně pozitivních výsledků a je vhodné pro poskytovatele internetových služeb.
- Nastavení **Blokovat striktně** maximalizuje míru detekce a je vhodné pro většinu firemních nasazení.
- Nastavení **Neblokovat** zcela vypne blokování a způsobí, že Whalebone bude pracovat v transparentním/permisivním režimu, kdy bude incidenty pouze zaznamenávat (kontrolovat), ale nebude je aktivně blokovat.



Další politiky můžete nakonfigurovat kliknutím na kartu **Přidat politiku**. Nejprve vyberete, na které ze stávajících zásad má být nová zásada založena. Poté klikněte na tlačítko s tužkou pod položkou **Název zásady**, abyste ji zřetelně odlišili od ostatních. Poté můžete upravit citlivost blokování a auditu, přidat seznamy odmítnutí nebo nastavit regulační filtrování. Nová zásada se uloží až po kliknutí na tlačítko **Uložit**.

Tip: Zásada není aktivní, pokud není přiřazena některým resolverům (místním nebo cloudovým). Chcete-li zahájit vynucování zásad, přejděte do části **Resolvery** → **Přiřazení politik** a přiřaďte je konkrétní **podsíti** nebo **resolveru**.

7.2 Typy hrozeb

Ve výchozím nastavení jsou zahrnuty všechny typy hrozeb. Pokud chcete některé z nich vyloučit, můžete tak učinit zrušením zaškrtnutí políčka **zahrnout všechny typy hrozeb**. V rozevírací nabídce nyní můžete vybrat konkrétní kategorie kontrolovaných/blokovaných hrozeb. K dispozici jsou tyto kategorie: **blacklist**, **c&c**, **coinminer**, **compromised**, **malware**, **phishing** a **spam**.

Úplný seznam toho, co jednotlivé kategorie zahrnují, naleznete níže:

- **C&C (Command and Control)**: domény, které usnadňují komunikaci botnetu a koordinují jeho činnost. Botnet je síť infikovaných počítačů, které jsou řízeny jako skupina.
- **Malware**: domény, které hostují a distribuují jakýkoli druh škodlivého kódu.
- **Phishing**: domény, jejichž cílem je oklamat uživatele a získat z nich citlivé informace, jako jsou údaje o kreditních kartách, přihlašovací údaje atd.
- **Blacklist**: domény, o kterých je známo, že slouží k více nekalým účelům současně nebo po určitou dobu.

- **Spam**: domény, které jsou spojeny s šířením nevyžádaných e-mailů a podvodných schémat.
- **Kompromitované**: jinak legitimní domény, které byly napadeny hackery a jsou dočasně používány ke škodlivým účelům.
- **Coinminer**: domény, které přebírají výpočetní a energetické zdroje pro nevyžádanou těžbu kryptoměn.

Poznámka: Veškeré změny v zásadách zabezpečení se na resolvery aplikují přibližně za 2-3 minuty. Uložená konfigurace se používá při přípravě balíčku dat o hrozbách pro resolvery, které tyto balíčky v pravidelných intervalech stahují a aplikují.

7.3 Povolené

- Domény, které nebudou nikdy blokovány (pokud nejsou také přítomny v seznamu domén podléhajícím právnímu omezení).
- Seznam povolených domén má při vyhodnocování způsobu překladu domény druhou nejvyšší prioritu.
- Seznam povolených se použije na doménu a všechny subdomény, např.: povolená doména `whalebone.io` povolí také `docs.whalebone.io`, ale ne naopak.
- Seznam lze nakonfigurovat na kartě **Blokované / Povolené** na levé straně stránky **Konfigurace**.
- Jeden seznam může obsahovat až 10 000 domén.

7.4 Blokované

- Domény, které budou vždy blokovány (pokud se stejná doména nenachází také v seznamu povolených domén).
- Seznam deny se vztahuje na doménu a všechny subdomény, např.: zakázaná doména `malware.ninja` bude zakázána také `super.malware.ninja`, ale ne naopak.
- Seznam lze nakonfigurovat na kartě **Blokované / Povolené** na levé straně stránky **Konfigurace**.
- Jeden seznam může obsahovat až 10 000 domén.

Seznamy podporují zásadu *Lex specialis derogat legi generali*, podle níž má specifičtější seznam domén přednost před obecnějším seznamem domén. Tímto způsobem můžete mít celou doménu `malware.ninja` v seznamu Deny. ale pokud máte doménu `friendly.malware.ninja` v seznamu Allow, bude mít tato doména přednost a komunikace s touto stránkou bude fungovat jako výjimka a resolver ji povolí.

Varování: Po vytvoření seznamu povolených nebo zakázaných položek je třeba jej přiřadit ke konkrétní zásadě zabezpečení, jinak se změny neprojeví.

7.5 Právní omezení

- Integrovaný seznam domén, které musí být použity, aby byly v souladu s regulačními omezeními dané země.
- Příklady těchto domén zahrnují případy nelegálního hazardu nebo dětské pornografie.
- Domény na seznamu regulačních omezení budou vždy blokovány, pokud je tento seznam použit v zásadách zabezpečení.
- Mají nejvyšší prioritu a jejich filtrování nelze zrušit. Ani přidání domény do seznamu povolených domén nezpůsobí, že ji resolver přestane blokovat.

Varování: Každá země má jiné seznamy domén podléhající právnímu omezení. V případě nasazení ve více zemích lze použít různé zásady, aby bylo možné uplatnit správná regulační omezení.

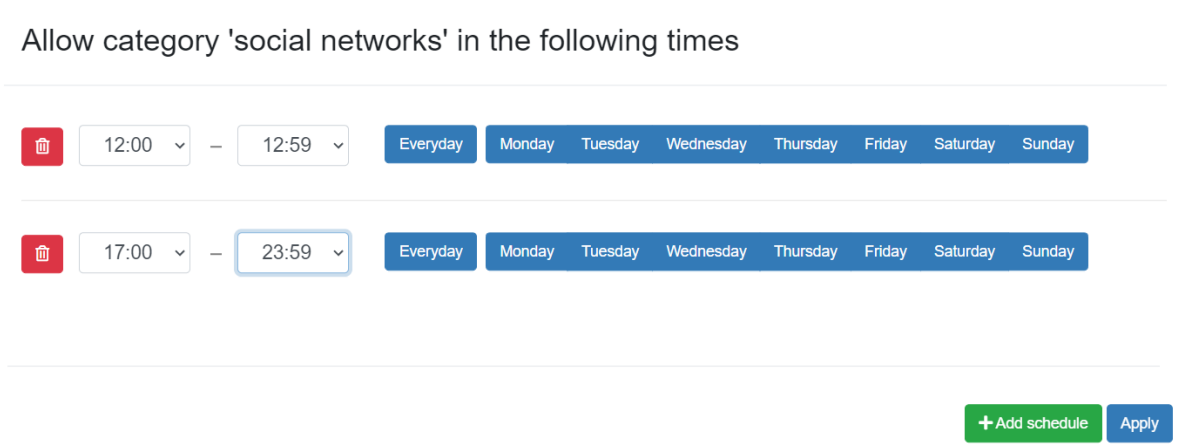
7.6 Obshahová filtrace

Jednotlivé kategorie obsahu lze použít na úrovni jednotlivých politik. To je užitečné v případě, že různé segmenty sítí mají různé požadavky. Například v případě školního prostředí lze povolit všechny kategorie **Pro dospělé** a omezit přístup k příslušnému obsahu.

K dispozici je rozmanitá sada kategorií filtrování obsahu:

- **Sexuální obsah**: Sexuální a pornografický materiál,
- **Gambling**: hry a činnosti zahrnující sázení peněz,
- **Zbraně**: zbraně a stránky týkající se zbraní,
- **Audio-video**: služby streamování audia a videa,
- **Hry**: online hry a herní webové stránky,
- **Chat**: aplikace pro zasílání rychlých zpráv a chatování,
- **Sociální sítě**: stránky a aplikace sociálních sítí,
- **Zneužívání dětí**: webové stránky týkající se zneužívání dětí, šíření dětské pornografie,
- **Drogy**: webové stránky týkající se drog včetně alkoholu a tabáku,
- **Rasismus**: obsah související s rasismem a xenofobií,
- **Násilí**: explicitní násilí a gore,
- **Terorismus**: domény spojené s podporou terorismu,
- **Reklamy**: bannery, kontextové reklamy a další reklamní systémy,
- **Těžba kryptoměn**: domény spojené s těžbou kryptoměn,
- **DoH**: DNS přes HTTPS. Jedná se o domény, které zajišťují obfuskaci požadavků DNS v provozu HTTP,
- **P2P**: domény spojené s peer to peer sítěmi, kde uživatelé sdílejí multimediální obsah,
- **Sledování**: webové a e-mailové sledovací systémy.

Filtr obsahu lze použít i pro konkrétní denní dobu. Po zaškrtnutí určité kategorie se vedle ní zobrazí ikona hodin. Pokud na ikonu hodin kliknete, můžete pro tuto kategorii přidat nový plán. Pro stejnou kategorii může být aktivních více rozvrhů. Takto můžete povolit přístup k sociálním sítím pouze během polední přestávky a po skončení pracovní doby. Nastavení dokončete kliknutím na tlačítko **Použít** a **Uložit** zásady zabezpečení.



Poznámka: Použitím plánu **povolíte** přístup k doménám z dané kategorie obsahu v daném časovém období.

CHAPTER 8

Konfigurace překladu DNS

Možnosti konfigurace resolveru najdete v zíložce **Konfigurace** na kartě **DNS Překlad**. Tato záložka umožňuje provést základní konfiguraci bez znalosti konfigurační syntaxe. Dále je zde textová oblast umožňující definovat libovolnou konfiguraci k základnímu Knot Resolveru.

Dostupné možnosti konfigurace:

- **Používat IPv6 pro dotazy na autoritativní servery**
  - Pokud je systém správně nakonfigurován, je možné povolit IPv6.
  - V opačném případě by aktivace protokolu IPv6 mohla mít negativní vliv na výkon a latenci resolveru.
- **Přesměrovat dotazy na nadřazené resolvery**
  - Tato možnost umožňuje přesměrovat všechny nebo vybrané dotazy na předřazené resolvery nebo autoritativní servery DNS (vhodné např. pro přesměrování na řadiče domény služby Active Directory).
  - **Zakázat DNSSEC validaci**
    - Pokud je tato možnost zaškrtnuta, odpovědi z přesměrovaných dotazů nebudou ověřovány pomocí DNSSEC.
    - Tuto možnost doporučujeme zaškrtnout v případě, že předávací server nemá správně nakonfigurován DNSSEC.
  - **Všechny dotazy na**
    - Možnost předání všech dotazů jednomu nebo více resolverům.
    - Toto nastavení ukládá všechny odpovědi do mezipaměti!
  - **Následující domény**
    - Možnost vybrat konkrétní domény, které mají být předávány na jeden ,nebo více resolverů.
    - Pro různé domény lze definovat různé resolvery.
    - Ukládání do mezipaměti pro vybrané domény bude vypnuto!
- **Statické záznamy**

  - Předdefinované odpovědi, které mají být vráceny pro konkrétní domény.
  - Mohly by sloužit pro speciální účely, jako je monitorování nebo velmi jednoduché nahrazování záznamů na autoritativním serveru.
- **Nastavení DNS překladu**
  - Textová oblast pro pokročilou konfiguraci.
  - Slouží k přímé konfiguraci Knot Resolveru.
  - Kompletní konfigurace Knot Resolveru
  - Podporuje skriptování v jazyce Lua.

Poznámka: Po stisknutí tlačítka **Uložit** jsou změny v nastavení překladu DNS uloženy a připraveny k nasazení na resolvery. Samotné nasazení je třeba provést v záložce **Resolvery**. Je možné provést více změn a použít je všechny najednou, aby se minimalizoval počet nasazení na resolver.

Varování: Chybná konfigurace může ovlivnit stabilitu, výkon nebo bezpečnostní funkce resolveru. V případě chybné syntaxe se po spuštění **Nahrát konfiguraci** zobrazí chybový kód.

CHAPTER 9

Knot Resolver - Tipy a Triky

Pokročilá konfigurace Whalebone resolveru umožňuje přímou konfiguraci Knot Resolveru. V této části popíšeme nejčastější případy použití a příklady takových konfigurací. Zásady a akce se vyhodnocují v pořadí, v jakém jsou definovány (s výjimkou speciálních řetězových akcí, které jsou popsány v oficiální dokumentaci Knot Resolveru). První shoda provede akci, zbytek pravidel zásad se nevyhodnocuje. Pokud budete kombinovat různé fragmenty konfigurace, můžete stejný modul načíst jen jednou na začátku konfigurace.

9.1 Povolení konkrétních rozsahů IP adres

Nastaví seznam rozsahů IP, které budou mít povoleno používat tento DNS resolver. Dotazy ze všech ostatních rozsahů budou odmítnuty.

```
--načtení modulů
modules = {'policy', 'view'}

--definuje seznam povolených rozsahů
--127.0.0.1 by měl být vždy povolen
allowed = {
  '127.0.0.1/32',
  '10.10.20.5/32',
  '10.30.10.0/24'
}

--cyklus procházející seznam pololených rozsahů
for i,subnet in ipairs(allowed) do
  view:addr(subnet, policy.all(policy.PASS))
end

--ostatní rozsahy jsou zablokovány
view:addr('0.0.0.0/0', policy.all(policy.DENY))
```

9.2 Odmítnutí určitých rozsahů IP

Nastaví seznam rozsahů IP, které budou blokovány pro použití tohoto DNS resolveru. Dotazy ze všech ostatních rozsahů budou povoleny.

```
--načtení modulů
modules = {'policy', 'view'}

--definuje seznam blokovaných rozsahů
blocked = {
  '10.10.20.5/32',
  '10.30.10.0/24'
}

--cyklus procházející seznam blokovaných rozsahů
for i,subnet in ipairs(blocked) do
  view:addr(subnet, policy.all(policy.REFUSE))
end
```

9.3 Povolit seznam domén

```
--načtení modulů
modules = {'policy'}

--definuje seznam povolených domén
domains = {
  'example.com',
  'anotherexample.org'
}

--cyklus procházející seznam povolených domén
for i,domain in ipairs(domains) do
  policy.add(policy.suffix(policy.PASS, {todname(domain)}))
end
```

9.4 Zamítnout seznam domén

```
-- load modules
modules = {'policy'}

--definuje seznam blokovaných domén
domains = {
  'example.com',
  'anotherexample.org'
}

--cyklus procházející seznam blokovaných domén vracející NXDOMAIN
for i,domain in ipairs(domains) do
```

(continues on next page)

(pokračujte na předchozí stránce)

```
  policy.add(policy.suffix(policy.DENY, {todname(domain)}))
end
```

9.5 Globální vypnutí DNSSEC validace

```
trust_anchors.negative = { '.' }
```

9.6 Vypnutí DNSSEC validace pro konkrétní doménu

```
trust_anchors.set_insecure({ 'domain.com' })
```

9.7 Zákaz náhodného výběru dotazů

```
policy.add(policy.suffix(policy.FLAGS('NO_0X20'), {todname('domain.com')}))
```

9.8 Zakáz minimalizace QNAME

```
policy.add(policy.suffix(policy.FLAGS('NO_MINIMIZE'), {todname('domain.com')}))
```

9.9 Zakáz ukládání domény do mezipaměti

```
policy.add(policy.suffix(policy.FLAGS('NO_CACHE'), {todname('domain.com')}))
```

9.10 Povolení metrik Prométheus

Resolver může vystavit své metriky v textovém formátu Prometheus. Následující skript povolí modul HTTP a zpřístupní příslušný endpoint `/metrics`.

Další informace a možnosti konfigurace naleznete na stránce Dokumentace k Knot Resolveru.

```
modules.load('http')
function startHttp ()
net.listen('127.0.0.1', 8453, { kind = 'webmgmt' })
end
pcall(startHttp)
```

CHAPTER 10

Blokační stránky

Zde si můžete prohlédnout videonávod.

V případě blokování přístupu k doméně (z důvodů bezpečnosti, obsahu nebo regulace) odpovídají resolvery klientům konkrétní IP adresou, která vede na jednu z blokovacích stránek. Zatímco klienti iniciují HTTP(S) spojení směrem k blokované doméně, jsou jim zobrazeny vlastní blokační stránky s různým obsahem na základě důvodu blokování. Pro blokační Stránky Whalebone poskytuje vzorovou šablonu, avšak není nutné ji dodržovat a prakticky každá úprava, branding a copywriting je možný. Kód šablony je napsán tak, aby byl kompatibilní s co nejširším rozsahem prohlížečů, aby se předešlo problémům se staršími verzemi.

Různé verze **Blokačních Stránek** mohou být přiřazeny různým segmentům sítí v **Resolvery** → **Přiřazení politiky**.

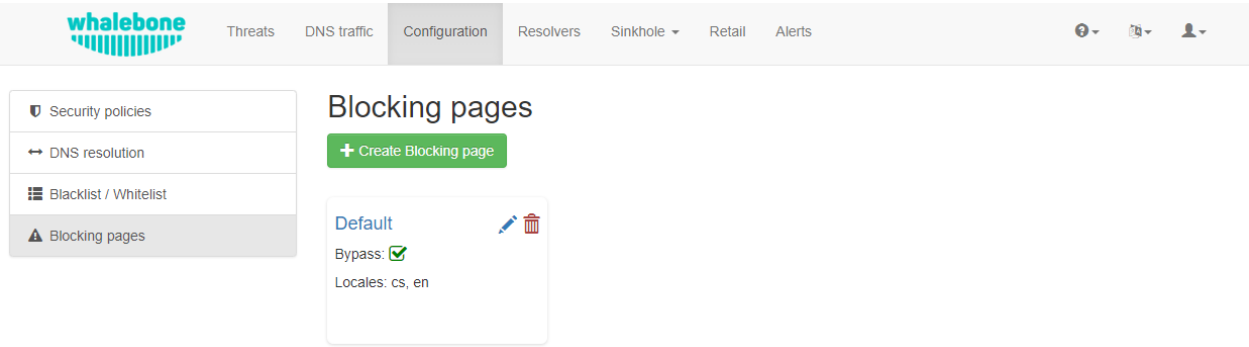


Figure1: Blocking Pages Overview

Pro každou verzi, na základě nasazení, jsou dostupné a mohou být nakonfigurovány čtyři varianty blokačních stránek:

- **Bezpečnost**: zobrazeno, když je přístup blokován z bezpečnostních důvodů
- **Blacklist**: zobrazeno, když je přístup blokován Administrátory
- **Právní**: zobrazeno, když je přístup regulován na základě zákona nebo soudního příkazu

- **Obsah**: zobrazeno, když je přístup blokován kvůli obsahu domény

Navíc, každá verze může mít různé možnosti lokalizace. Jazyk blokační stránky se odvíjí od jazyka prohlížeče ze kterého je na ni přistupováno. Nové lokalizace mohou být snadno přidány.

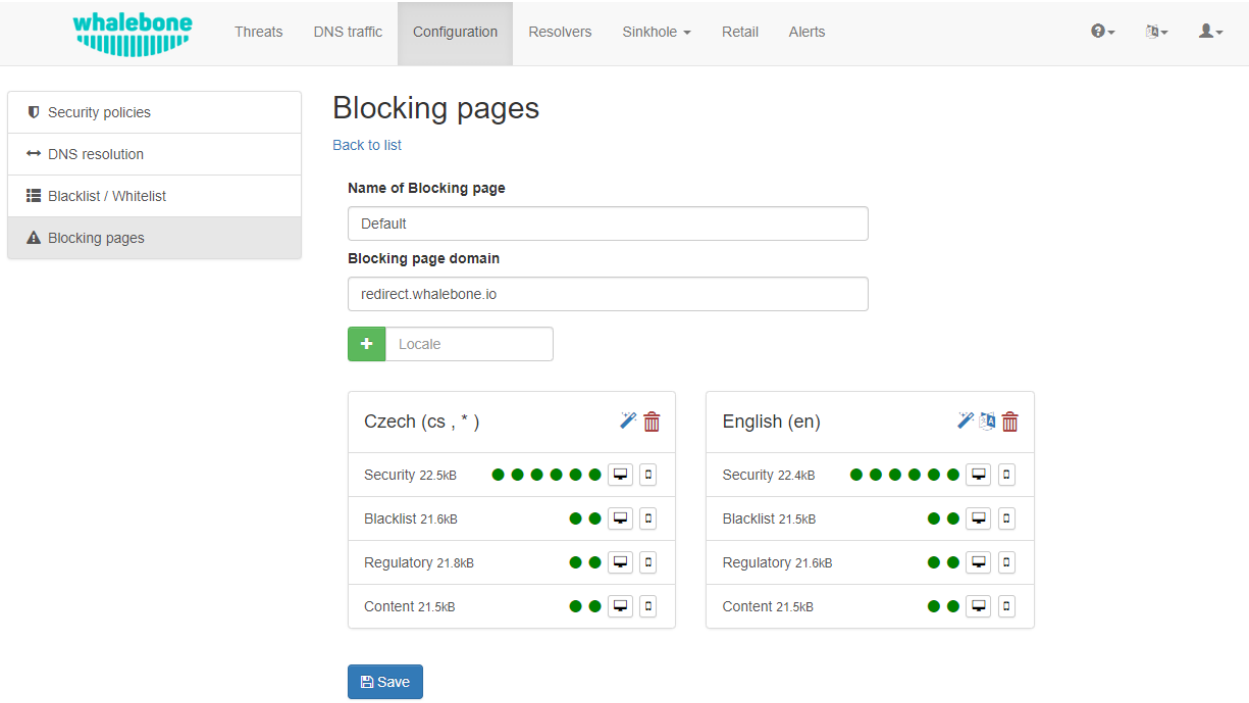


Figure2: Blocking Pages Menu

Pro každou lokalizaci je dostupné několik možností. V příkladu výše má anglická verze následující možnosti:

1. **Možnost** – Použití šablony:

   Při použití šablony jsou zadané informace vloženy přímo do kódu šablony. To je nejrychlejší a nejjednodušší způsob, jak přizpůsobit blokační stránku.

Poznámka: Nastavení blokovací stránky lze provést kliknutím na tlačítko **Kouzelná hůlka**. Při použití šablony dojde k přemázání předešlé konfigurace.

---

2. **Možnost** – Výchozí lokalizace blokační stránky:

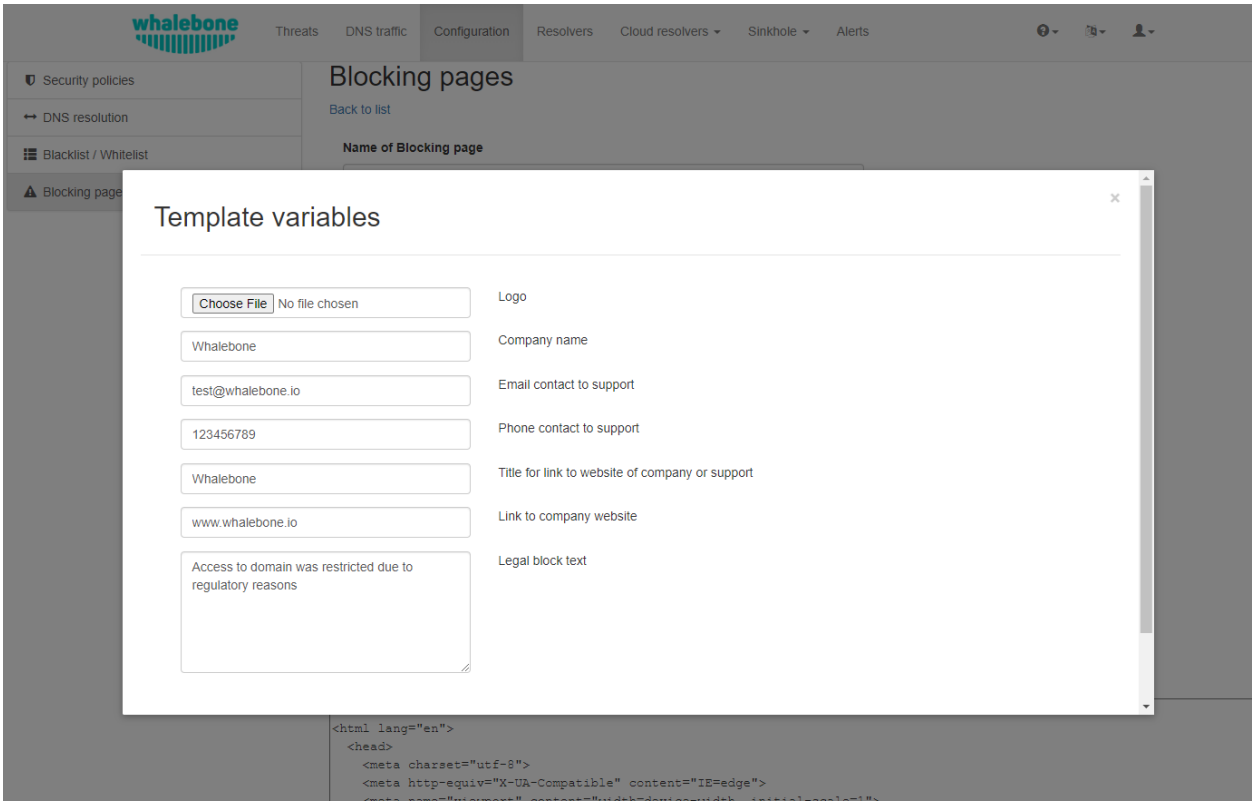
   Tato možnost umožňuje přizpůsobit výchozí jazyk blokační stránky. V případě, že některý prohlížeč neuvádí svůj preferovaný jazyk, funguje „Výchozí“ jazyk jako záložní mechanismus. Výchozí lokalita je označena pomocí symbolu hvězdičky (*) vedle typu jazyka.

3. **Možnost** – Odstranění lokalizace blokační stránky:

Lokalitu lze smazat kliknutím na ikonu **Koše**.

Každou z verzí blokační stránky (Bezpečnost, Blacklist, Právní, Obsah) lze detailněji přizpůsobit úpravou HTML kódu. Po kliknutí na každou verzi se zobrazí editor, který umožňuje provést jakékoli požadované změny.

Editor také exponuje rozhraní „Ověření“, které analyzuje konečný HTML kód a kontroluje povolené funkce. Kontrola



je založena na *id* konkrétních prvků. Více informací a požadavků pro každou funkci lze najít kliknutím na příslušné štítky.

Poznámka: Každá Verze blokační stránky má unikátní charakteristiky, které lze vybrat. Například, Blokovací Stránka pro **Bezpečnost** může zahrnovat tlačítko **Obejití blokace**, které není dostupné ve verzi stránky v případě **Regulace** a **Blacklist**.

Po editaci a uložení změn na blokačních stránkách je důležité, aby byly aplikovány na jednotlivé resolvery.

Tip: Blokovací Stránky jsou zobrazovány přímo z webového serveru na Resolveru. Stránky se očekávají jako jediný soubor, takže veškeré další zdroje (CSS, obrázky, skripty) musí být buď přímo vloženy do HTML kódu, nebo dostupné z veřejně přístupného webového serveru. Resolver neneposkytuje žádnou možnost vkládat jiný obsah.

10.1 Podpis blokačních stránek pomocí Certifikační Autority

Pro nasazení, kde máte kontrolu nad koncovými body (typicky firemní prostředí s Group Policy) a můžete do jejich úložišť vložit podepsané SSL certifikáty a díky tomu lze podepsat blokační stránku přímo za provozu. To vede k tomu, že prohlížeče přímo přecházejí na blokovací stránku bez zobrazení bezpečnostního varování, které je obvykle přítomno. Resolver v podstatě provádí MITM pokaždé, když provádí přesměrování na blokační stránku, takže je očekáváno varování prohlížeče.

Krok 1. – Vytvořte soubor „v3_cfg“ s následujícím obsahem:

```
[req]
req_extensions = v3_ca_extensions
distinguished_name = req_dn
[v3_ca_extensions]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
keyUsage = cRLSign, keyCertSign
subjectAltName = @alt_names
[alt_names]
DNS.1 = localhost
[req_dn]
countryName = Country Name (2 letter code)
countryName_default = US
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = New York
localityName = Locality Name (eg, city)
localityName_default = New York City
organizationName = Organization Name (eg, company)
organizationName_default = My Organization
commonName = Common Name (eg, your name or your server's hostname)
commonName_max = 64
```

Krok 2. – Vygenerujte klíč:

```
openssl genpkey -algorithm RSA -out /certs/ca.key
```

Krok 3. – Vytvořte a podepište certifikát:

```
openssl req -x509 -new -nodes -key /certs/ca.key -sha256 -days 1024 -out /certs/ca.crt -
↪config /certs/v3_cfg
```

Krok 4. – Exportujte .pfx soubor a uložte ho do /certs/ folder:

```
openssl pkcs12 -export -in ca.crt -inkey ca.key -out ca.pfx -certpbe PBE-SHA1-3DES -
↪keypbe PBE-SHA1-3DES -macal
```

Krok 5. – Pošlete název souboru a heslo na podporu Whalebone, aby byla konfigurace trvale uložena na backendu a zajistilo se, že nebude smazána při restartu VM nebo kontejneru.

CHAPTER 11

Resolver agent

11.1 Command line interface

Akce agenta lze vyvolat pomocí proxy bash skriptu, který se nachází v **/etc/whalebone/cli/cli.sh**. Tento skript volá python sccip, který se stará o provádění následujících akcí agenta:

- **sysinfo - vrací údaje o stavu systému ve formátu JSON.**
  - Parametry: Žádné
  - Výstup: testované kategorie na testovaném klíči mohou mít dvě hodnoty **OK** a **FAIL**.


```
{
   "hostname":"hostname",
   "system":"Linux",
   "platform":"CentOS Linux 7 (Core)",
   "cpu":{
      "count":4,
      "usage":28.6
   },
   "memory":{
      "total":7.6,
      "available":3.9,
      "usage":49.2
   },
   "hdd":{
      "total":50.0,
      "free":14.4,
      "usage":71.1
   },
   "swap":{
      "total":0.0,
      "free":0.0,
```


(continues on next page)

(pokračujte na předchozí stránce)


```
      "usage":0
   },
   "resolver":{
      "answer.nxdomain":3284,
      "answer.tc":35,
      "answer.ad":849,
      "answer.100ms":3983,
      "answer.cd":6,
      "answer.1500ms":74,
      "answer.slow":215,
      "answer.rd":224337,
      "answer.1ms":104683,
      "answer.servfail":215,
      "predict.epoch":24,
      "query.dnssec":6,
      "answer.250ms":14941,
      "query.edns":35498,
      "answer.cached":86713,
      "answer.nodata":3622,
      "answer.aa":2362,
      "answer.do":6,
      "answer.edns0":35498,
      "answer.ra":224337,
      "predict.queue":0,
      "answer.total":224337,
      "answer.10ms":35351,
      "answer.noerror":217216,
      "answer.50ms":59766,
      "answer.500ms":4642,
      "answer.1000ms":653,
      "predict.learned":80
   },
   "docker":{
      "Platform":{
         "Name":""
      },
      "Components":[
         {
            "Name":"Engine",
            "Version":"17.12.1-ce",
            "Details":{
               "ApiVersion":"1.35",
               "Arch":"amd64",
               "BuildTime":"2022-02-27T22:17:54.000000000+00:00",
               "Experimental":"false",
               "GitCommit":"88888fc6",
               "GoVersion":"go1.999.999",
               "KernelVersion":"3.22.66-693.21.1.el7.x86_64",
               "MinAPIVersion":"1.99",
               "Os":"linux"
            }
         }
```


(continues on next page)

(pokračujte na předchozí stránce)


```
      ],
      "Version":"19.32.1-ce",
      "ApiVersion":"1.98",
      "MinAPIVersion":"1.12",
      "GitCommit":"7390fc6",
      "GoVersion":"go1.9.4",
      "Os":"linux",
      "Arch":"amd64",
      "KernelVersion":"3.10.0-693.21.1.el7.x86_64",
      "BuildTime":"2018-02-27T22:17:54.000000000+00:00"
   },
   "check":{
      "resolve":"ok",
      "port":"ok"
   },
   "containers":{
      "lr-agent":"running",
      "passivedns":"running",
      "resolver":"running",
      "kresman":"running",
      "pcpy":"running",
      "logrotate":"running",
      "logstream":"running"
   },
   "images":{
      "lr-agent":"whalebone/agent:1.1.1",
      "passivedns":"whalebone/passivedns:1.1.1",
      "resolver":"whalebone/kres:1.1.1",
      "kresman":"whalebone/kresman:1.1.1",
      "logrotate":"whalebone/logrotate:1.1.1",
      "logstream":"whalebone/logstream:1.1.1"
   },
   "error_messages":{
   },
   "interfaces":[
      {
         "name":"lo",
         "addresses":[
            "127.0.0.1",
            "::1",
            "00:00:00:00:00:00"
         ]
      },
      {
         "name":"eth0",
         "addresses":[
            "1.1.1.1",
            "::c8",
            "fe80::",
            "00:00:00:00:00:00"
         ]
      },
```


(continues on next page)

(pokračujte na předchozí stránce)

```
      {
         "name":"docker0",
         "addresses":[
            "198.1.1.1",
            "00:00:00:00:00:00"
         ]
      }
   ]
}
```

- **stop - zastaví až tři kontejnery**
  - Parametry: kontejnery k zastavení (až 3), Příklad: ./cli.sh stop resolver lr-agent kresman

```
{
        'resolver': {'status': 'success'},
        'lr-agent': {'status': 'success'},
        'kresman': {'status': 'success'}
}
```

- **remove - odstraní až tři kontejnery**
  - Parametry: kontejnery k odstranění (až 3), Příklad: ./cli.sh remove resolver lr-agent kresman

```
{
        'resolver': {'status': 'success'},
        'lr-agent': {'status': 'success'},
        'kresman': {'status': 'success'}
}
```

- **upgrade - aktualizuje až tři kontejnery, konfigurace kontejneru je určena pomocí docker-compose v kontejneru agenta (lze také nalézt ve adresáři /etc/whalebone/agent).**
  - Parametry: kontejnery k upgradu (až 3), Příklad: ./cli.sh upgrade resolver lr-agent kresman

```
{
        'resolver': {'status': 'success'},
        'lr-agent': {'status': 'success'},
        'kresman': {'status': 'success'}
}
```

- **create - vytvoří kontejnery, kontejnery jsou zadány pomocí docker-compose v kontejneru agenta (lze také nalézt v adresáři /etc/whalebone/agent).**
  - Parametry: Žádné, Příklad: ./cli.sh create

```
{'resolver': {'status': 'success'}
```

- **updatecache - vynutí aktualizaci mezipaměti IoC resolveru (která se používá pro blokování), tato akce by měla být provedena, aby se ručně vynutila aktualizace a obnovení domén přítomných v mezipaměti škodlivých domén.**
  - Parametry: Žádné

```
{'status': 'success', 'message': 'Cache update successful'}
```

- **containers - seznam kontejnerů a jejich informací, které zahrnují: štítky, obrázek, název a stav.**

- Parametry: Žádné


```
[
   {
      "id":"b8f4489379",
      "image":{
         "id":"c893b4df5ca3",
         "tags":[
            "whalebone/agent:1.1.1"
         ]
      },
      "labels":{
         "lr-agent":"1.1.1"
      },
      "name":"lr-agent",
      "status":"running"
   },
   {
      "id":"e433d58f13",
      "image":{
         "id":"2c4b84a7daee",
         "tags":[
            "whalebone/passivedns:1.1.1"
         ]
      },
      "labels":{
         "passivedns":"1.1.1"
      },
      "name":"passivedns",
      "status":"running"
   },
   {
      "id":"2aeec00121",
      "image":{
         "id":"fc442e625539",
         "tags":[
            "whalebone/kres:1.1.1"
         ]
      },
      "labels":{
         "resolver":"1.1.1"
      },
      "name":"resolver",
      "status":"running"
   },
   {
      "id":"662dac2e6c",
      "image":{
         "id":"b37d0d1bd10b",
         "tags":[
            "whalebone/kresman:1.1.1"
         ]
      },
```


(continues on next page)

(pokračujte na předchozí stránce)


```
      "labels":{
         "kresman":"1.1.1"
      },
      "name":"kresman",
      "status":"running"
   },
   {
      "id":"05188ac1df",
      "image":{
         "id":"5b50cdc924fc",
         "tags":[
            "whalebone/logrotate:1.1.1"
         ]
      },
      "labels":{
         "logrotate":"1.1.1"
      },
      "name":"logrotate",
      "status":"running"
   },
   {
      "id":"01e64dd697",
      "image":{
         "id":"fffb52c2dadd",
         "tags":[
            "whalebone/logstream:1.1.1"
         ]
      },
      "labels":{
         "logstream":"1.1.1"
      },
      "name":"logstream",
      "status":"running"
   }
]
```


Každá z těchto akcí provede podobně pojmenovanou akci a vypíše stav, nebo výstup této akce. Akce **list** a **run** jsou určeny pro stav, kdy je vyžadováno potvrzení určité akce. Seznam akcí zobrazuje akci, která má být provedena, a změny, které by tato akce provedla u kontejnerů uvedených v této akci. Slouží jako příklad toho, co by se stalo, kdyby byla čekající akce provedena. Spuštěná akce pak provede akci čekající na spuštění.

Akce **upgrade** a **create** využívají šablonu docker-compose přítomnou v kontejneru agenta k vytvoření/upgradu požadovaného kontejneru. Tato šablona se nachází v **/etc/whalebone/agent**, pokud se ji uživatel rozhodne změnit. Tuto změnu je však třeba provést i v šabloně přítomné na **portal.whalebone.io**, pokud se tak nestane, budou lokální změny při příští aktualizaci přepsány z cloudu.

Bash skript by měl být vyvolán takto: `./cli.sh action param1 param2 param3`. **Action** je název akce a **parameters** jsou parametry akce. Používají je pouze akce pro zastavení, odebrání a upgrade kontejneru a určují, kterých kontejnerů se má příslušná akce týkat.

11.2 Přísný režim

Výchozí volbou agenta je okamžité provedení akcí ze správy cloudu. Je však možné povolit ruční potvrzování požadavků. To dává správci kontrolu nad tím, kdy a co bude provedeno. Chcete-li povolit Přísný režim resolveru, vytvořte prosím ticket na podporu Whalebone.

Pro vypsání změn, které požadavek zavádí, je třeba použít volbu cli **list**. Pro spuštění požadavku použijte volbu cli **run**. Ve frontě může být pouze jeden čekající požadavek. Nový požadavek z cloudu přepíše předchozí, ale nový požadavek stejně obsahuje celý požadovaný stav. Pro odstranění čekajícího požadavku použijte volbu cli **delete_request**. Akce, které mohou přetrvávat, jsou následující: **upgrade**, **create** a **suicide**. Viz příklady použití příkazů CLI.

- **list - vypíše čekající příkaz a změny, které by byly provedeny v kontejnerech zadaných v čekající akci, tato akce je určena pro lidskou kontrolu, proto je její formát**
  - Parametry: Žádné
  - Příklad: ./cli.sh list

```
------------------------------
Changes for resolver
New value for label: resolver-1.1.1

        Old value for label: resolver-1.0.0
------------------------------
```

- **run - provede čekající příkaz**
  - Parametry: žádné
  - Příklad: ./cli.sh run

```
{'resolver': {'status': 'success'}
```

- **delete_request - odstraní čekající požadavek.**
  - Parametry: žádné
  - Příklad: ./cli.sh delete_request

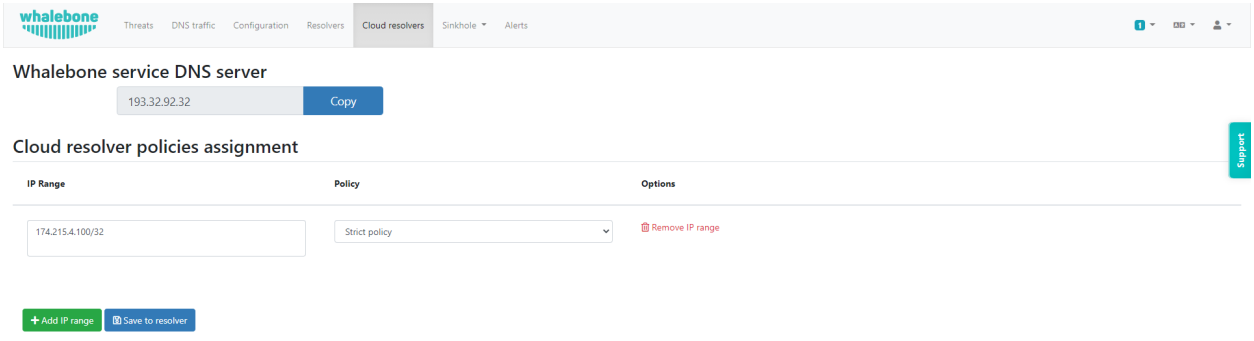
```
Pending configuration request deleted.
```

CHAPTER 12

Cloudové DNS resolvery

Videonávod krok za krokem si můžete prohlédnout zde. Whalebone Cloud DNS resolver je služba určená především pro malé nebo střední zákazníky, kteří mohou cloudové resolvery používat jako záložní resolver. Typicky je zaměřena na poskytovatele internetových služeb, kteří mají pouze jeden on-premise resolver a pro zajištění vysoké dostupnosti používají cloudové DNS resolvery jako sekundární rekurzivní resolver pro své zákazníky. Jedním z předpokladů je definování veřejné IP adresy nebo rozsahy pro přiřazení bezpečnostní politiky coudovému resolveru, aby mohl rozlišovat a poskytovat správné zásady filtrování, které jste nastavili pro svou síť.

Definice rozsahu veřejné sítě slouží k rozlišení jednotlivých zákazníků a jejich uživatelů. Je nutné zahrnout všechny rozsahy veřejné sítě, které bude resolver DNS používat, i uživatelé přistupující k internetu. Definice slouží k přizpůsobení vzhledu stránky blokování (popsáno později). Jeden zákazník může spravovat více síťových rozsahů, tyto rozsahy lze přiřadit lokalitám, aby bylo možné snadno rozlišit jednotlivé síťové zóny při investigaci provozu DNS a incidentech.



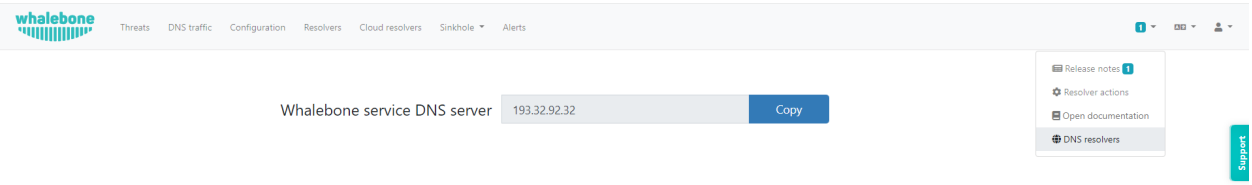
Varování: Pokud nevyplníte rozsahy veřejné sítě, budou cloudové resolvery sloužit jako jednoduché DNS resolvery **bez jakéhokoli filtrování**. Pokud používáte místní resolvery, musíte stále zadávat rozsahy sítě, aby se blokovaným uživatelům zobrazovala plně přizpůsobená blokační stránka.

- Do pole **Rozsah** vložte jeden nebo více síťových rozsahů pomocí zápisu <síťová adresa>/<maska>, např: **198.51.100.0/24**.

- Stisknutím tlačítka **Přidat rozsah IP** přidáte další segmenty sítě.
- Nezapomeňte nové nastavení uložit pomocí tlačítka **Uložit k resolveru**.

Tip: Při testování Whalebone (např. přidáním testovací domény na blacklist) nezapomeňte, že mnoho DNS záznamů může být uloženo v cache kdekoli mezi resolverem a uživatelem (včetně prohlížeče, operačního systému nebo forwarderů). Testování ihned po změně konfigurace by proto mohlo selhat a doba, než se ochrana stane aktivní, by se mohla lišit v závislosti na TTL konkrétního záznamu DNS (pokud by všechny mezipaměti po cestě skutečně dodržovaly hodnotu TTL).

Pokud je tato možnost nasazení preferována, měli byste provoz DNS přesměrovat na cloudové resolvery Whalebone. Cloudové resolvery jsou k dispozici anycast IP adrese **193.32.92.32** a **193.32.92.33**.



IP adresy resolverů jsou dostupné v části **Cloudové resolvery** a v nabídce **Nápověda** → **DNS překladače**.

CHAPTER 13

Odinstalování lokálního resolveru

Pro odinstalování resolveru a odstranění všech konfiguračních souborů Whalebone je třeba provést následující kroky:

Varování: Před zahájením procesu je třeba upozornit, že všechny jednotlivé komponenty, které podporují funkčnost resolveru, jsou spuštěny jako docker kontejnery. Kroky 1 a 2 platí pouze v případě, že je hostitelský server **dedikovaný** a **žádné další služby** nejsou spuštěny jako kontejnery. V případě jiné situace nás prosím kontaktujte a my vám poskytneme aktuální seznam kontejnerů, které by měly být odstraněny.

1. Krok – Zastavte a odstraňte všechny spuštěné kontejnery docker:

```
docker rm -f lr-agent && docker rm -f $(docker ps -q)
```

2. Krok – Odinstalujte docker:

Postupujte podle pokynů pro příslušný operační systém:

- CentOS
- Red Hat
- Debian
- Ubuntu

3. Krok – Odstranění všech konfiguračních souborů resolveru a souvisejících dat:

```
rm -rf /etc/whalebone
rm -rf /var/whalebone
rm -rf /var/lib/kres
```

4.Krok – Odstranění protokolů o provozu DNS a incidentech:

Pokud chcete resolver zcela odinstalovat včetně záznamů z přenosů a incidentů DNS, odstraňte také složku s záznamy. Pokud je vaším záměrem pouze přeinstalovat resolver, ale protokoly ponechat, můžete tento krok přeskočit.

CHAPTER 14

Analýza dat

Whalebone Portal (grafické uživatelské rozhraní) poskytuje uživateli řadu možností, jak analyzovat, co se děje na DNS resolverech a v síti.

14.1 Hrozby

Hrozby jsou zvláštní události, při kterých dochází k požadavku DNS na doménu která se nachází v Whalebone dazabázi. Existují dva typy akce při zjištění hrozby. První je **audit** události a zároveň druhým je její **Block**. Možnost **Audit** pouze zaznamená doménu, ale přístup je uživateli umožňěn.

Akce, která má být provedena, závisí na nastavení bezpečnostních politik, které jsou přiřazeny konkrétnímu resolveru. Více informací naleznete v sekci Bezpečnostní politiky.

Existují některé předkonfigurované filtry, které lze aplikovat na data. Ukázky některých dotazů jsou zobrazeny níže. Tyto dotazy zobrazují většinu případů použití, ale není zde žádné pevné omezení, protože dostupný vyhledávač je **full-textový** a lze sestavit **jakýkoli** dotaz.

Videoprůvodce krok za krokem si můžete prohlédnout zde.

14.1.1 Vyhledání událostí typu audit/block:

Existují dvě možnosti filtrování různých typů událostí. První možností je využití vizuálního filtru. V rámci grafu můžete kliknutím na jednu z akcí (audit, blokování, povolení) filtrovat a zobrazit pouze případy, ve kterých k dané události došlo. Druhou možností je kliknout vedle pole **Filtr výsledku** na tlačítko **Filtr** a vybrat požadovanou možnost filtrování.

14.1.2 Vyhledání domény:

Nejjednodušším způsobem vyhledání domény lze pomocí kliknutí na konkrétní doménu v hostorii logů. Druhou možností je pomocí zadání názvu domény do pole **Filtr výsledků**.

14.1.3 Vyhledání konkrétní IP adresy:

Vyfiltrování logů od konkrétní IP adresy je možné po vybrání konkrétní zdrojové IP adresy v historii logů. Druhou možností je pomocí zadání názvu domény do pole **Filtr výsledků**.

14.1.4 Vyhledání události na základě konkrétní kategorie hrozeb:

Existuje velké množství kategorií hrozeb.

Z nichž jmenujeme např.: *malware*, *c&c*, *blacklist*, *phishing*, *coinminer*, *spam*, and *compromised*.

Jednoduchým způsobem vyhledání útoků je možné vybráním konkrétní kategorie z koláčových grafů nebo v sezamu logů v sloupci **Kategorie hrozeb**. Další možností je kliknout vedle pole **Filtr výsledku** na tlačítko **Filtr** a vybrat požadovanou možnost filtrování.

14.1.5 Jak změnit časový rozsah událostí:

Rozsah data údajů, které lze zobrazit v náhledu na portálu, lze měnit několika způsoby. Mezi základní způsob výběru se řadí volba předdefinovaných časových oken (1,7, 14 nebo 30 dní) v rozbalovacím seznamu umístěném vedle **filtru výsledků**. V případě potřeby je možné specifikovat konkrétní časové rozmezí pomocí oken **Datum a čas začátku** a **Datum a čas konce**.

14.1.6 Analýza domény:

V případě, že se chcete dozvědět další informace o doméně, zejména jaké skóre Whalebone přiřazuje konkrétní doméně, kdy byla poprvé spatřena a zařazena do kategorie jako škodlivá, zda spadá do regulační kategorie nebo z jakých externích zdrojů. o ní víte, podívejte se na video zde.

14.2 DNS Provoz:

Záložka **DNS Provoz** obsahuje přehled o provozu, který byl byl zaznamenán na resolveru. Obsahuje všechny dotazy spolu s některými dalšími informacemi, jako je typ, odpověď a TTL (time to live) odpovědi.

Tip: Data podléhají de-duplikaci. To znamená, že resolver zaznamenává pouze jedinečné kombinace dotazu, typu dotazu a odpovědi za 24 hodin. hodin. Z tohoto důvodu se může stát, že dotaz nebude viditelný na portálu, i když byl vyřešen.

Videoprůvodce krok za krokem si můžete prohlédnout zde.

Níže budou popsány některé užitečné možnosti filtrace dostupných dat.

14.2.1 Zobrazení dotazů určitého typu:

Nejjednodušším způsobem, jak vybrat dotazy určitého typu je pomocí zakliknutí ikony **filtr** a zvolení požadovaného typu dotazu. Na výběr je několik možností, mezi které se řadí: `A`, `AAAA`, `CNAME`, `MX`, `NS`, `PTR`, `RRSIG`, `SPF`, `SRV` a `TXT`.

14.2.2 Zobrazení odpovědí podle typu:

V okně **Odpovědi** je možné zvolit požadovanou odpověď, nebo v seznamu logů ve sloupci **odpověď** nebo požadovanou odpověď zakliknout.

14.2.3 Vyhledání domény:

K vyhledání domén lze využít textové pole **Filtr výsledků** do kterého lze zadat název hledané domény. Mezi další možnosti, jak vyhledat doménu je zakliknutí domény v části **Domény 2. řádu** popř. přímo v seznamu logů ve stejnojmenném sloupci.

14.2.4 Jak změnit časový rozsah událostí:

Rozsah data údajů, které lze zobrazit v náhledu na portálu, lze měnit několika způsoby. Mezi základní způsob výběru se řadí volba předdefinovaných časových oken (1,7, 14 nebo 30 dní) v rozbalovacím seznamu umístěném vedle **filtru výsledků**. V případě potřeby je možné specifikovat konkrétní časové rozmezí pomocí oken **Datum a čas začátku** a **Datum a čas konce**.

14.2.5 How to view DGA (Domain Generation Algorithm) indications:

Indikace DGA lze vyfiltrovat podobným způsobem, jako v případě zobrazení dotazů určitého typu, v tomto případě stačí zvolit poslední záznam v seznamu - **DGA**

14.2.6 Fulltext filtering

Pro pokročilejší použití lze použít fulltextový filtr a sestavit složený dotaz. Fulltextové filtrování funguje pouze v panelu **Hrozby**.

> **Varování:** Panely **Obsah** a **DNS provoz** v tuto chvíli nepodporují fulltextové filtrování.

Tato pole lze spojovat pomocí logických operátorů. Podporovány jsou `AND`, `OR`, `NOT`, `<`, `>` a zástupný znak `*`. Řetězce nemusí být obaleny uvozovkami. Příklad syntaxe je následující: `action: block AND accu:>70 AND (client_ip: 10.20.30.41 OR 10.20.30.40 OR 192.168.*) a NOT geoip. country_name: Germany AND matched_iocs.classification.type: malware AND NOT phishing` Při spuštění fulltextového dotazu se aktualizuje obsah celého řídicího panelu.

Hrozby	Popis	Příklad hodnoty
timestamp	Přesný čas, kdy resolver zaregistroval požadavek / incident DNS	2022-10-14T12:28:01.000Z
client_ip	Zdrojová IP adresa, ze které byl odeslán požadavek / incident DNS	192.168.2.3
domain	Doména v dotazu DNS	whalebone.io OR whale*one.io
resolver_id	The id of ther resolver which handled the event	2404
device_id	ID resolveru, který událost zpracoval	MB2A1b4OTDin3Xz6DgftAip72v57e
geoip. continent_code	Kód kontinentu z php knihovny geoIP	AF | AN | AS | EU | NA | OC | SA
geoip. country_code3	Kód země z php knihovny geoIP	RU | CZ | US | CN | DE | ...
geoip. country_name	Jméno země z php knihovny geoIP	Russia
ip	IP adresa v odpovědi DNS nebo IP adresa odpovědi, kdyby ji resolver nezablokoval	174.85.249.36 OR SERVFAIL OR NXDOMAIN
action	Akce, kterou resolver provedl s daným dotazem	block | allow | audit
accu	Skóre domény v době události	0..100 < and > operators can be used too
matched_iocs. classification. type	Typ zranitelnosti	malware | c&c | phishing | coinminer | spam | compromised | blacklist

Tip: Filtrační operátory jsou umístěny staticky v URL. Proto si můžete vytvořit sadu filtrů předem (například zobrazení na jednotlivé IP adresy) a v případě potřeby je použít. Můžete je uložit do CRM a v případě řešení problémů k nim přistupovat okamžitě. To pomůže ušetřit váš čas, když zákazník požádá o podporu, protože můžete situaci okamžitě ověřit.

CHAPTER 15

Analýza překladu domén

Může se stát, že se správce setká se situací, kdy překlad DNS není úspěšný. Většinou to nesouvisí s resolverem Whalebone, ale pravděpodobně se jedná o problém s autoritativním serverem.

Poskytovatelé internetových služeb se často setkávají se stížnostmi, že uživatelé nemohou přistoupit k doméně, v mnoha případech to není chyba poskytovatele. Whalebone vám poskytne informace pro identifikaci problému.

15.1 Jednotlivé kroky k provedení analýzy

1. **Krok ** : Prozkoumejte doménu v záložce **Hrozby**.
   - Zkontrolujte, zda doména nebyla zablokována z důvodu bezpečnosti.
2. **Krok ** : Prozkoumejte doménu v záložce **DNS provoz**.
   - Pokud nebyla zablokována kvůli **hrozbám**, přejděte na stránku **DNS provoz** a zkontrolujte, zda se dotaz dostal až k resolveru.
   - Uživatelé často mění nastavení DNS serveru na veřejné a z nefunkčnosti viní poskytovatele připojení.

   Můžete se setkat s třemi možnostmi:
   - Překlad byl správny.
   - NXDOMAIN odpověď - autoritativní server odpověděl, ale subdoména neexistuje.
   - SERVFAIL odpověď - žádná odpověď ze strany serveru. Může se jednat o výpadek serveru nebo spojení.
3. **Krok ** – Prozkoumejte doménu pomocí **DNSVIZ.**
   - V seznamu domén lze pomocí šipky otevřít seznam nástrojů pro investigaci.
   - Nástroj **DNSVIZ** může v grafické podobně nastínit jestli byla DNSSEC validace úspěšná, nebo, že autoritativní server nebyl dosažitelný

Videoprůvodce krok za krokem si můžete prohlédnout zde.

Portál Whalebone poskytuje možnost trasovat doménu. Tato funkce je k dispozici v části **Resolvery** pod třemi tečkami každého resolveru. Tato funkce ukazuje, jaké informace jsou předávány resolveru při překladu konkrétní domény.

Videoprůvodce krok za krokem si můžete prohlédnout zde.

CHAPTER 16

Reporty

Možnosti zasílání repotů lze nakonfigurovat v rozevírací nabídce pod účtem uživatele. Mezi možnosti, které lze nastavit, patří četnost, s jakou jsou hlášení doručována, preferovaný den v týdnu, jazyk a příjemci.

Poznámka: Výchozím příjemcem je vlastník účtu a zprávy jsou doručovány na jeho příslušnou registrovanou e-mailovou adresu.

CHAPTER 17

Alerty

Alerting Whalebone poskytuje upozorňovat v reálném čase na klíčové informace, jako je stav resolveru, stav řešení, využití hardwaru, a také informuje o zásadních bezpečnostních incidentech a mnoha dalších. Všechny tyto informace lze předávat prostřednictvím několika kanálů, např. e-mailu, slacku, syslogu nebo webhooku. Nová upozornění lze vytvářet z předdefinovaných šablon a upozornění lze následně přizpůsobit úpravou jejich parametrů. Videoprůvodce krok za krokem si můžete prohlédnout zde.

Poznámka: Chcete-li zapnout upozornění, musíte mu nejprve přiřadit cíl. Kliknutím na název výstrahy ji podrobně rozbalíte a v rámečku vyberete cíl. Kliknutím na adresy lze vybrat více cílů.

Poznámka: Pokud je kanálem upozornění syslog, je ve výchozím nastavení jako protokol transportní vrstvy podporován protokol TCP nebo TLS.

Poznámka: Alerty přes Syslog nebo Webhook jsou odesílány z následujících IP adres: 159.100.247.142 a 159.100.247.58. Pokud vyberete jeden z těchto kanálů, ujistěte se, že jste na bráně firewall udělali výjimku pro příchozí provoz TCP, abyste mohli zprávu přijímat.

17.1 DNS provoz - Phishing na základě podobné domény (Homografický útok)

Toto upozornění je odesláno, když je zjištěn možný homografický útok pro zadanou doménu. Parametry:

- **DOMAIN**: Doména, která se má sledovat z hlediska možných útoků homografů (jedno upozornění může sledovat pouze jednu doménu).
- **DISTANCE**: Počet znaků, které se mohou lišit v doméně phishingu (výchozí=1)

- **DOMAIN_WILDCARD_IGNORE**: Tento seznam domén oddělených čárkou ve výstraze ignorujte. V případě, že je DISTANCE větší než 1, bude detekce probíhat u domén, které podporují globální i regionální formáty nejvyšší úrovně. Doporučujeme přidávat legitimní domény na bílé seznamy, abyste se vyhnuli zbytečným poplachům. (Výchozí hodnota=žádná)

17.2 DNS provoz - počet unikátních dotazů

Toto upozornění se odešle, když je dosaženo prahové hodnoty pro filtrované jedinečné protokoly DNS. Parametry:

- **MINUTES**: Časový rámec - časové okno (Výchozí=15)
- **TRESHOLD**: Prahová hodnota - počet událostí v časovém rámci pro spuštění výstrahy, jedná se o percentuální změnu (Výchozí=100).
- **QUERY_TYPE**: Filtrovat podle typu dotazu DNS (Výchozí=*)
- **RESPONSE_TYPE**: Filtrovat podle odpovědi DNS (Výchozí=*)

17.3 DNS provoz - počet unikátních požadavků z IP

Toto upozornění se spustí, když jedna zdrojová IP adresa dosáhne limitu jedinečných požadavků s definovanými atributy. Parametry:

- **MINUTES**: časové okno v minutách (výchozí=15)
- **TRESHOLD**: počet událostí v časovém rozmezí pro spuštění výstrahy, jedná se o percentuální změnu (výchozí=100).
- **QUERY_TYPE**: (Výchozí=*): filtruje podle typu dotazu DNS.
- **RESPONSE_TYPE**: Filtrovat podle odpovědi DNS (Výchozí=*)
- **IP_WILDCARD**: Zahrnout do výstrahy pouze tyto IP adresy oddělené čárkou (Výchozí=*)
- **IP_WILDCARD_IGNORE**: Ignorovat tyto domény oddělené čárkou ve výstraze (Výchozí=žádná)
- **DOMAIN_WILDCARD**: Do upozornění zahrne pouze tyto domény oddělené čárkou(Výchozí=*)
- **DOMAIN_WILDCARD_IGNORE**: Ignorovat tyto domény oddělené čárkou v upozornění (Výchozí=žádná)
- **DGA**: Filtrování podle algoritmu generování domén - pouze s DGA, pouze bez DGA nebo obojí (Výchozí=*)

17.4 DNS provoz - procentuální nárůst dotazů

Toto upozornění se odešle, pokud je počet záznamů o provozu DNS procentuálně vyšší za nastavené časové období. Parametry:

- **MINUTES**: Časový rámec - časové okno (výchozí=15)
- **PERCENT**: Procentuální nárůst (např. 200 %) - rozdíl mezi dvěma intervaly (Výchozí=50)
- **QUERY_TYPE**: (Výchozí=*): Filtruje podle typu dotazu DNS.
- **RESPONSE_TYPE**: Filtrovat podle odpovědi DNS (Výchozí=*)

17.5 Hrozby - nově blokovaná doména

Toto upozornění se odešle, pokud resolver v zadaném časovém období zjistí nově zablokovanou hrozbu. Parametry:

- **DAYS**: Počet dní ve kterých budou vyhledávány nově blokované domény (výchozí=30)
- **DOMAIN_WILDCARD**: Do upozornění zahrne pouze tyto domény oddělené čárkou(Výchozí=*)

17.6 Hrozby - počet za časový interval

Toto upozornění se odešle, pokud je procento záznamů o hrozbě vyšší za nastavené časové období. Parametry: * **MINUTES**: časové okno v minutách (výchozí=15)

- **TRESHOLD**: počet událostí v časovém rozmezí pro spuštění výstrahy, jedná se o percentuální změnu (výchozí=100).
- **LOG_TYPE**: (Výchozí=*): filtruje podle typu akce (audit/block)

17.7 Hrozby - událost detekce

Toto upozornění je odesláno v případě nové položky na stránce hrozeb podle zadaného typu hrozby a provedené akce. Parametry:

- **LOG_TYPE**: (Výchozí=*): filtruje podle typu akce (audit/block)
- **THREAT_TYPE**: (Výchozí=*): filtruje podle typu detekované hrozby

17.8 Resolver - Nedostatek systémových požadavků

Toto upozornění je odesláno, když místní agent resolveru zjistí, že využití hardwaru vzrostlo nad definovanou mezní hodnotu. Parametry jsou vyjádřeny v procentech využití v porovnání s celkovými prostředky. Jako příklad lze uvést, že chcete být upozorněni, když hostitel využívá 80 % celkového diskového prostoru, nastavte hodnotu THRESHOLD_HDD na 80. Parameters:

- **THRESHOLD_CPU**: (Výchozí hodnota=80): Využití procesoru.
- **THRESHOLD_MEMORY**: Využití paměti RAM (výchozí=90)
- **THRESHOLD_HDD**: Využití pevného disku (výchozí=80)

17.9 Resolver - Výpadek komunikace s cloudem

Toto upozornění je odesláno, když backend neobdrží žádnou zprávu od místního agenta resolveru po dobu delší než 20 minut.

17.10 Resolver - Výpadek překladu

Resolver pravidelně provádí kontroly, aby otestoval funkčnost překladu známých domén. Google.com, facebook.com, microsoft.com a apple.com jsou kontrolovány každou minutu. Výchozí nastavení parametrů je velmi přísné, takže i když se rozlišení jedné ze čtyř domén během desetiminutového intervalu nezdaří, je odesláno upozornění. Parametry:

- **TRESHOLD**: počet událostí, které musí nastat během časového intervalu, aby se výstraha spustila (výchozí=1)
- **MINUTY**: časový rámec v minutách (Výchozí=10)

CHAPTER 18

Integrace API

Whalebone API je jednoduchý a praktický způsob, jak přistupovat ke všem datům, která jsou shromažďována Whalebone resolvery a integrovat je do externích systémů. Dokumentace API má dvě oddělené schémata. Jedno pro získávání událostí od Whalebone a druhé pro získávání a konfiguraci nastavení.

- Pokud chcete získávat incidenty, data DNS provozu a metriky resolveru, použijte toto schéma.
- Pokud chcete konfigurovat resolver, aktualizovat politiky, přidávat domény na seznamy povolených/zakázaných nebo získat nastavení, použijte toto schéma.

Pro autentizaci k API potřebuje každý uživatel sadu klíčů **Access Key** a **Secret Key**. Tyto lze spravovat v nabídce **API keys** v rozbalovacím menu pod účtem uživatele.

Video návod krok za krokem můžete shlédnout zde.

- **Generování API klíče**

Generování API klíče lze provést kliknutím na tlačítko **Generate new key**.

Poznámka: Nezapomeňte si zkopírovat *Key secret*, protože jej nelze získat opětovně.

- **Deaktivace API klíče**

V případě, že se API klíč ztratí nebo bude kompromitován, jeho zrušení lze provést ve stejném menu kliknutím na ikonu červeného koše. Každý klíč je úzce spojen s ID uživatele a neexistuje centrální správa klíčů. Aby bylo možné zneplatnit klíč, ke kterému nemáte přístup, musí příslušný uživatel klíč sám smazat, nebo musí být smazán celý uživatelský účet.

CHAPTER 19

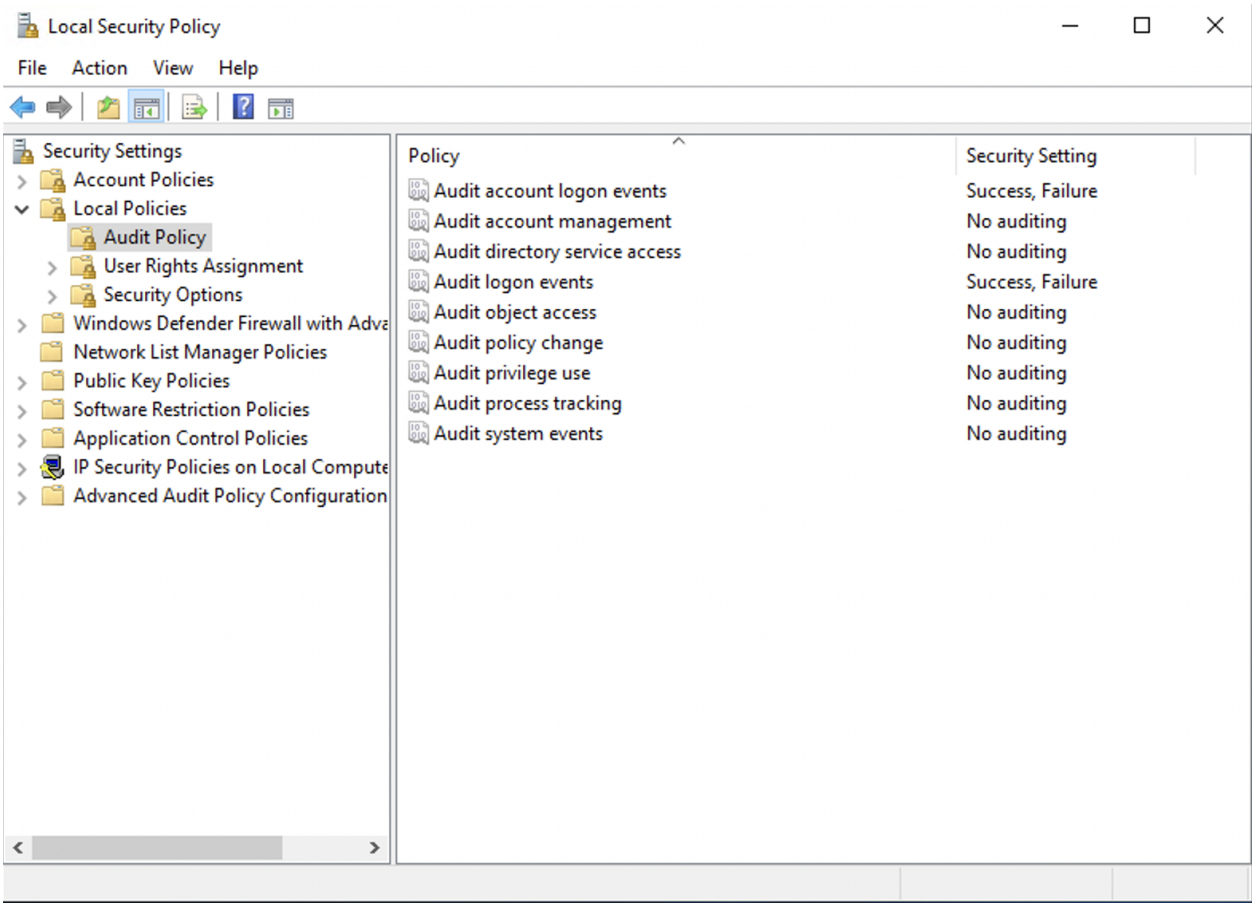
Integrace s Active Directory

19.1 Požadavky pro instalaci

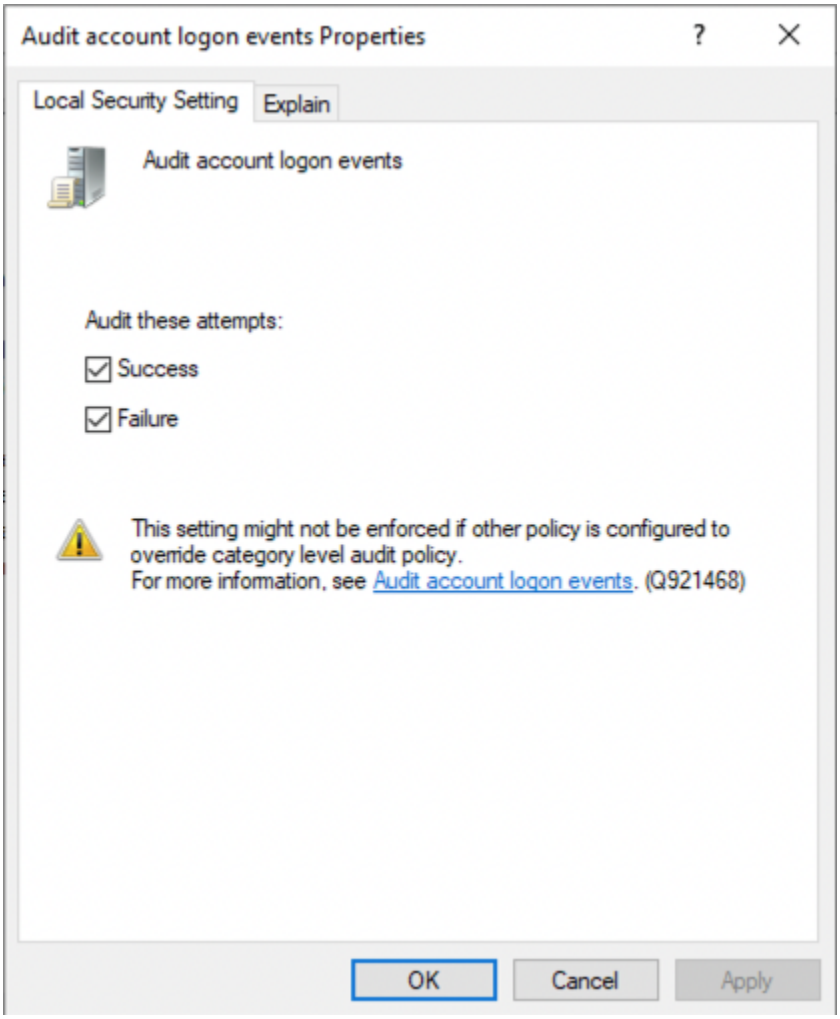
Před instalací Event Log Forwarderu (ELF) na jedno nebo více vašich zařízení se ujistěte, že máte povolený audit událostí.

Na každém vašem řadiči domény (DC) přejděte do: `Windows Administrative Tools` → `Local Security Policy`, poté do `Security Settings` → `Local Policies` → `Audit Policy`, a zde najdete `Audit account logon events`, `Audit account sign-in events` a `Audit logon events`.

Některá nastavení se mohou lišit názvem nebo mohou chybět, v závislosti na verzi Windows.



Zaškrtněte **Úspěch** a **Selhání**.



Možná bude potřeba znovu načíst nakonfigurovanou politiku. Pro znovunačtení politiky, prosím, spusťte následující příkaz:

```
gpupdate /force
```

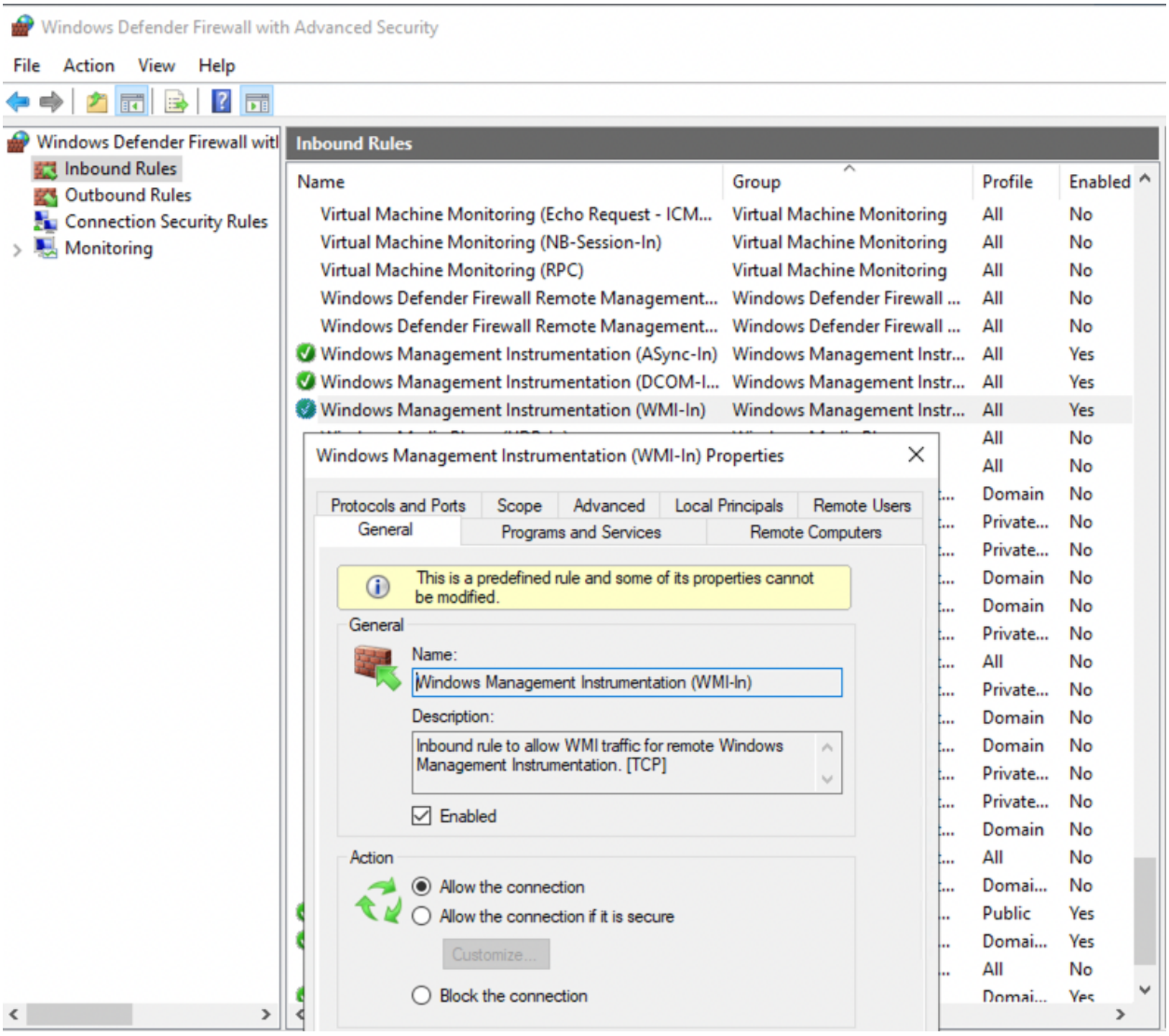
19.2 Konfigurace řadiče domény (Domain Controleru)

19.2.1 DC Firewall pro Windows

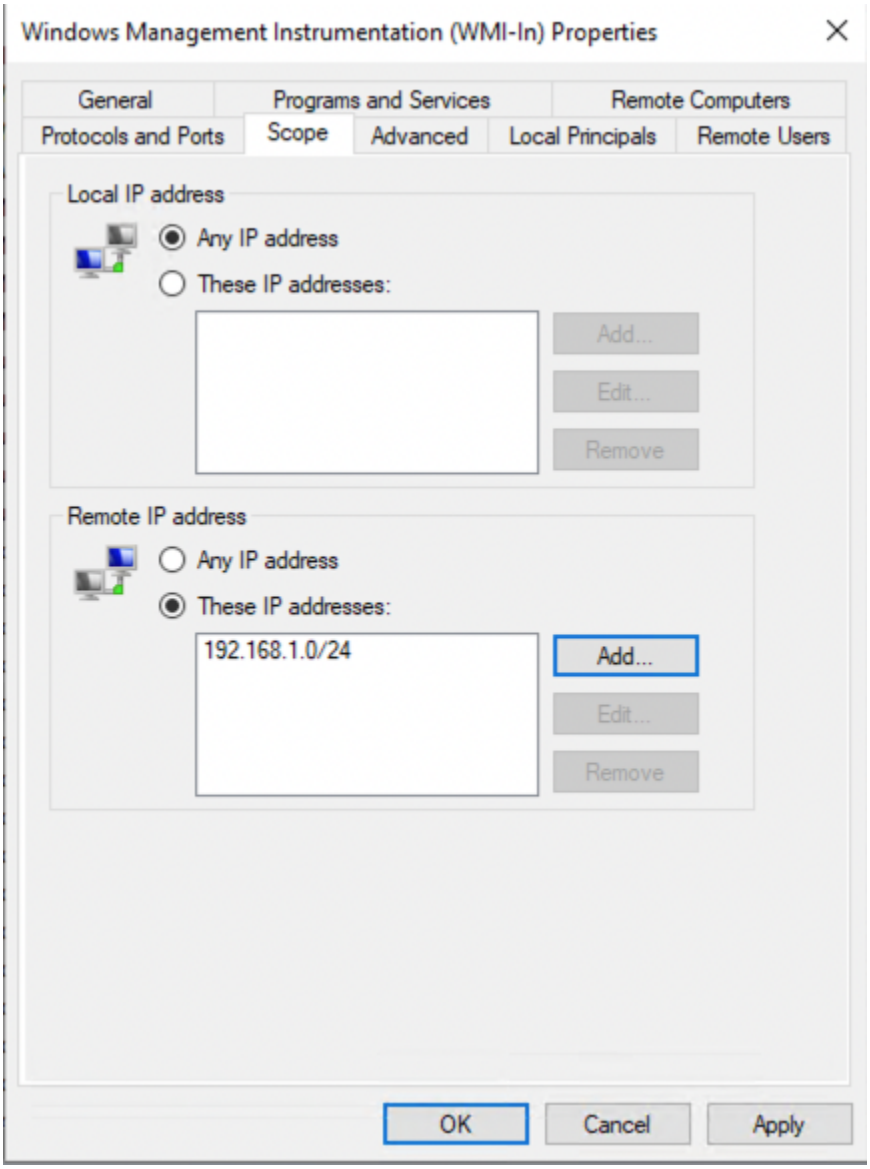
Ujistěte se, že Event Log lze přistupovat skrze konfiguraci Firewallu pomocí WMI.

Na každém vašem řadiči domény přejděte do: `Windows Defender Firewall` → `Windows Defender Firewall with Advanced Security on Local Computer` `Inbound Rules` → `Windows Management Instrumentation (WMI-In)`

Ujistěte se, že pravidlo umožňuje připojení.



Nastavte rozsah povolených adres, které se mohou připojit. V tomto příkladu je povolena vzdálená adresa **192.168.1.0/24.**



Nebo, alternativně, můžete použít příkazový řádek:

```
netsh firewall set service RemoteAdmin enable
```

19.2.2 DC Firewall Rules

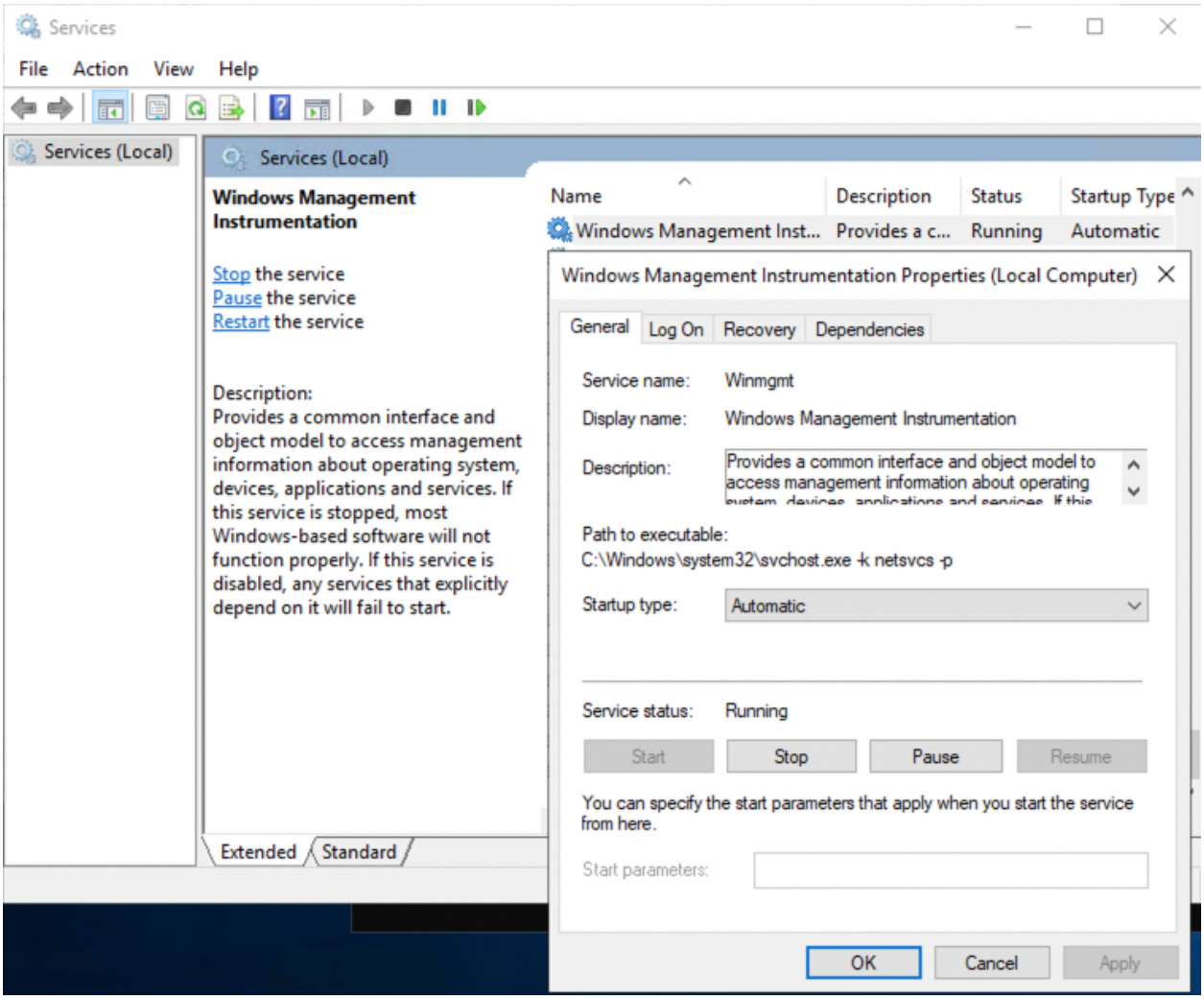
Zdroj	Směr	Cíl	Port	Protokol	Důvod
DC	—>	local netwk	135	TCP/UDP	Microsoft RPC
DC	—>	local netwk	445	TCP	Microsoft MQ
DC	—>	local netwk		ICMP	

19.2.3 Služba Windows

Ujistěte se, že služba `Windows Management Instrumentation` běží.

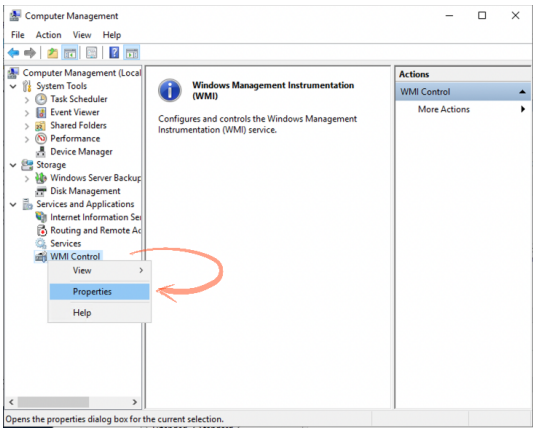
```
C:\Users\Administrator>sc query Winmgmt

SERVICE_NAME: Winmgmt
      TYPE               : 30  WIN32
      STATE              : 4  RUNNING
                              (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
      WIN32_EXIT_CODE    : 0  (0x0)
      SERVICE_EXIT_CODE  : 0  (0x0)
      CHECKPOINT         : 0x0
      WAIT_HINT          : 0x0
```

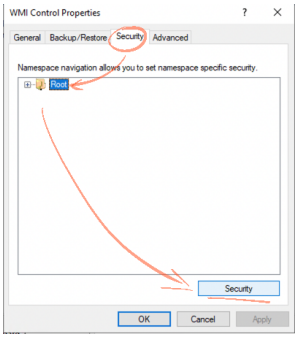


19.2.4 Vzdálená konfigurace WMI

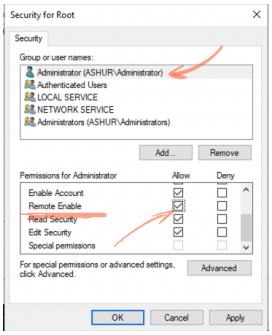
Pokud se rozhodnete nainstalovat ELF na jiném počítači s Windows, ujistěte se, že může používat WMI na dálku. Pro povolení vzdáleného WMI pro účet, který bude použit pro připojení k řadiči domény, přejděte do: `Computer Management` → `Services and Applications` → `WMI Control` Klikněte pravým tlačítkem a vyberte `Properties`.



Vyberte kartu `Security`, poté vyberte jmenný prostor `Root` a klikněte na tlačítko `Security`.



Přidejte uživatele do seznamu nebo vyberte skupinu, ke které patří, zaškrtněte povolení `Remote Enable`.



19.3 Event Log Forwarder

ELF můžete nainstalovat lokálně na DC nebo na jiném počítači s Windows. ELF využívá následující spojení:

19.3.1 ELF Firewall Rules

Zdroj	Směr	Cíl	Port	Protokol	Důvod
ELF	—>	DC	135	TCP/UDP	
ELF	—>	resolver	4222	TCP	NATS Message Queue

19.3.2 Instrukce pro instalaci

Instalace nebo aktualizace:

```
msiexec /i "Whalebone.Event.Log.Forwarder.Installer.msi" ui="true"
```

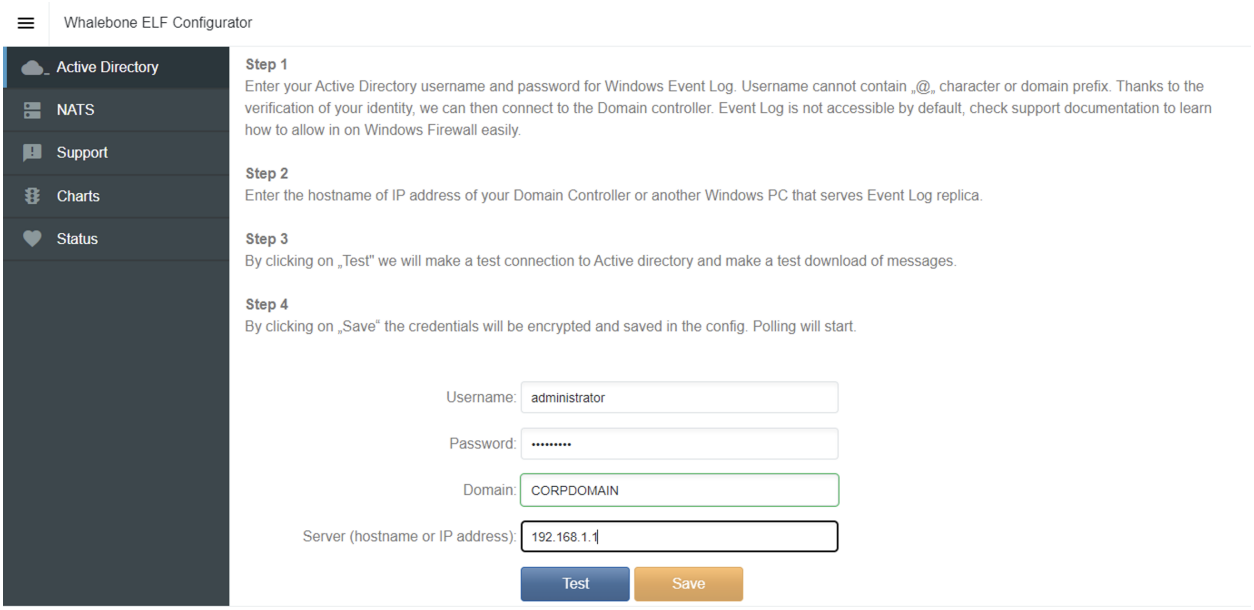
Odinstalace:

```
msiexec /x "Whalebone.Event.Log.Forwarder.Installer.msi
```

19.3.3 Konfigurace

Instalátor by měl automaticky otevřít okno konfigurace. Konfiguraci můžete přistupovat z oblíbeného webového prohlížeče pomocí příkazu:

```
start http://localhost:55225/Configure/AD
```



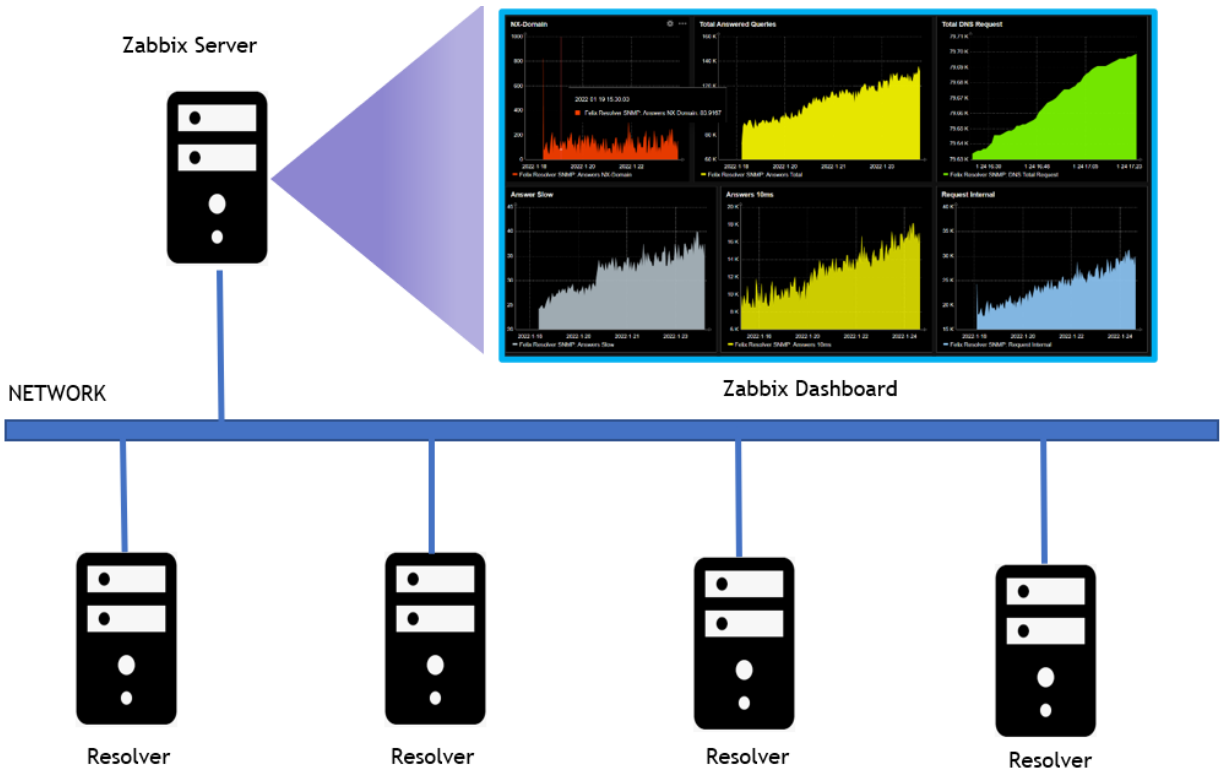
19.3.4 Logy služby

Protokoly služby lze najít v `c:\ProgramData\Whalebone\Event Log Forwarder\`, které obsahují podrobné informace o stavu služby. V případě, že narazíte na neočekávané chování služby, prosím, zahrňte obsah této složky k požadavku na podporu.

CHAPTER 20

SNMP Monitorování

20.1 High Level Síťové schéma



Agent SNMP Whalebone je v resolverech povolen k aktivnímu sledování místních zdrojů, požadavků a statistik.

20.2 SNMP OID

SNMP OID je zkratka pro identifikátory objektů pro vytvoření šablony SNMP pro nástroj monitorování sítě. V následující tabulce jsou uvedeny identifikátory OID SNMP Whalebone.

Property	ID	SNMP OID
Hostname	1	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.1
Check Port	2	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.2
Check Resolve	4	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.3
CPU Count	6	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.4
Memory Available	7	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.6
Memory Total	8	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.7
Memory Usage	9	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.8
HDD Free	10	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.9
HDD Total	11	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.10
HDD Usage	12	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.11
Swap Free	13	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.12
Swap Total	14	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.13
Swap Usage	15	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.14
Timestamp	16	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.15
Requests Total	17	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.16
equests Internal	18	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.17
Requests UDP	19	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.18
Requests TCP	20	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.19
Requests DoT	21	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.20
Requests DoH	22	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.21
Requests XDP	23	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.22
Answers Total	24	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.23
Answers cached	25	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.24
Answers No error	26	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.25
Answers No data	27	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.26
Answers NX-Domain	28	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.27
Answers SERVFAIL	29	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.28
Answers 1ms	30	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.29
Answers 10ms	31	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.30
Answers 50ms	32	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.31
Answers 100ms	33	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.32
Answers 250ms	34	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.33
Answers 500ms	35	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.34
Answers 1000ms	36	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.35
Answers 1500ms	37	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.36
Answers slow	38	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.37
Answers AA	39	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.38
Answers TC	39	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.39
Answers RA	40	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.40
Answers RD	41	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.41
Answers AD	42	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.42
Answers CD	43	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.43
Answers DO	44	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.44
Answers ENDS0	45	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.45

continues on next page

Table 1 – pokračujte na předchozí stránce

Property	ID	SNMP OID
Queries EDNS	46	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.46
Queries DNSSEC	47	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.47
Predict Epoch	48	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.48
Predict learned	49	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.49
Predict Queue	50	.1.3.6.1.4.1.8072.1.3.2.4.1.2.9.119.104.97.108.101.98.111.110.101.50

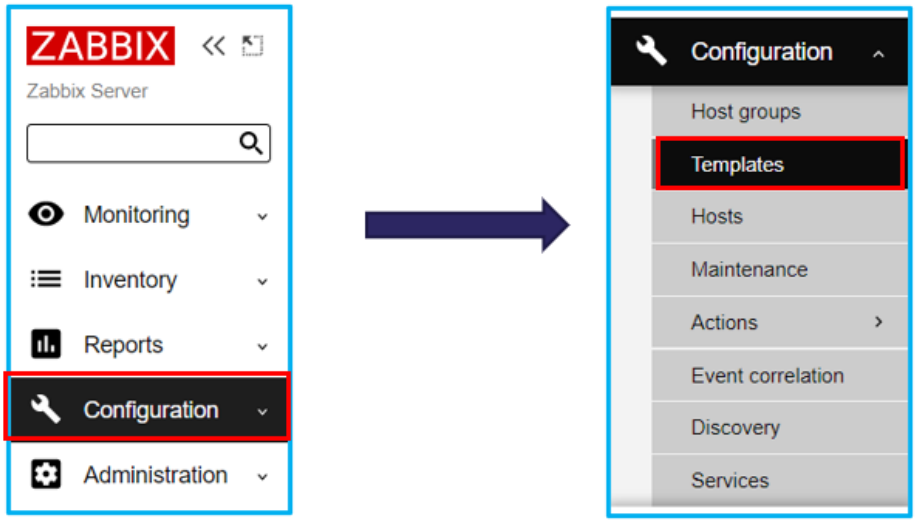
20.2.1 Integrace Zabbix

Agent shromažďuje provozní informace lokálně a posílá data na server Zabbix ke zpracování. Kromě toho Zabbix nabízí funkce pro reportování a vizualizace dat na základě uložených dat z resolveru.

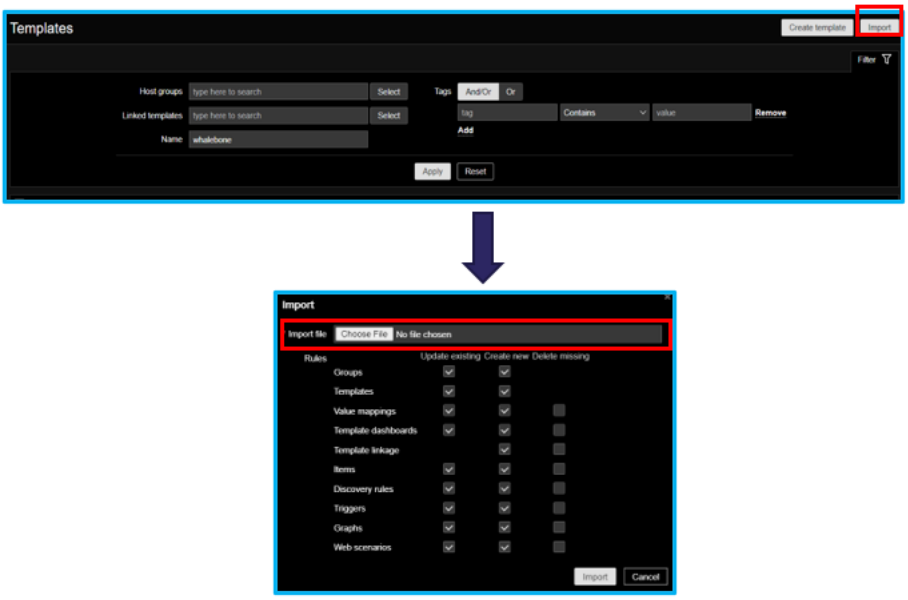
Zabbix je monitorovací nástroj, který poskytuje výkonnostní metriky, jako je využití sítě, využití procesoru a paměti. Monitoruje také síť odpojování a nedostupnost serveru.

20.3 Jak importovat šablonu Whalebone

- Chcete-li importovat šablonu Whalebone, přejděte na stránku **Configuration**. V části Konfigurace přejděte na položku **Šablony**.



- V záložce **Šablony** zvolte **Import** a zvolte soubor šablony.



20.4 Jak přidat resolver v nástroji Zabbix

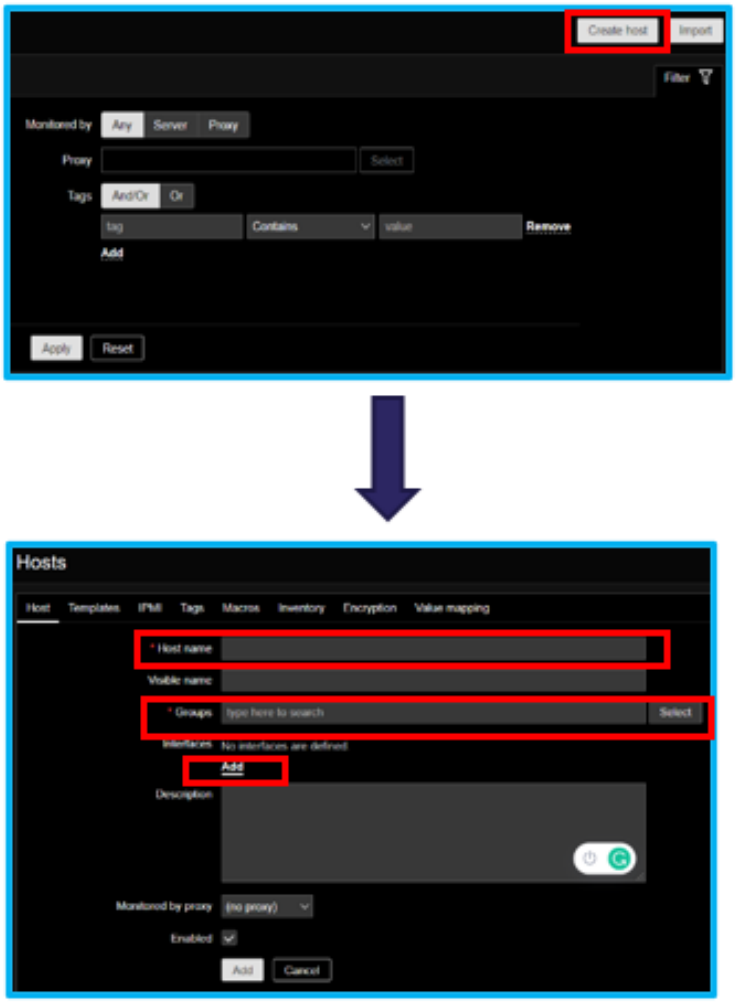
- Chcete-li přidat hosta, přejděte do části Konfigurace a klikněte na položku **hosts**. Klikněte na tlačítko **create host** a zadejte název hostitele, skupiny. Poté přidejte ip adresu resolveru.

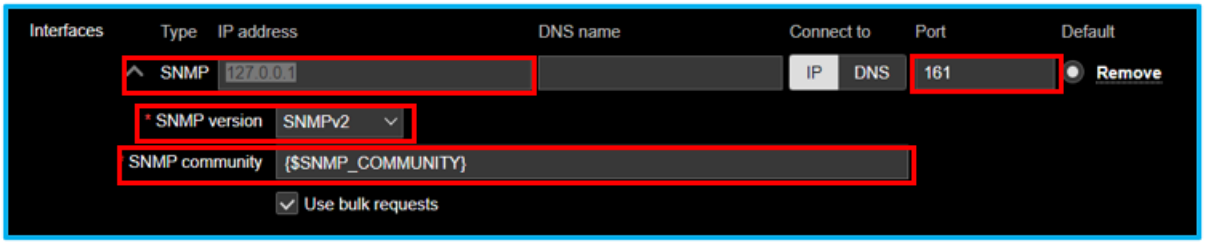
- Pod rozhraním vyberte **SNMP** → Zadejte SNMP **IP adresu** → Port **161** → SNMP verzi SNMPv2 a poté přidejte **SNMP community**.

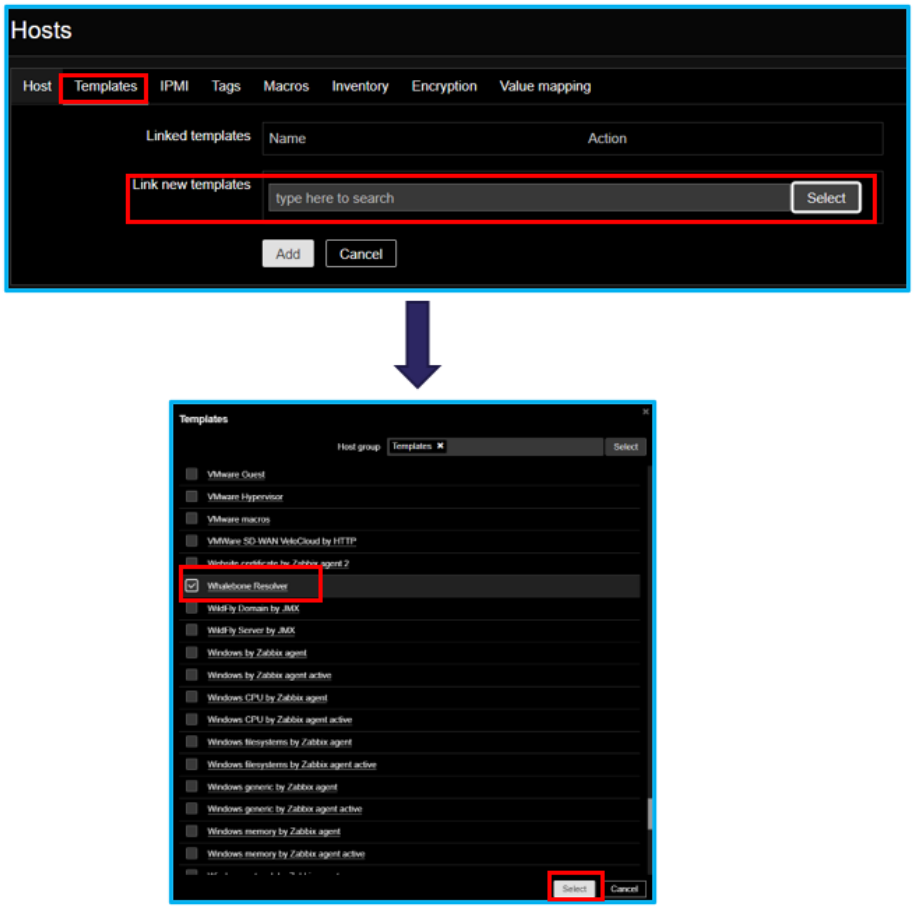
- Po přidání hosta přejděte na kartu **Templates** → Vyberte šablonu Whalebone. Klikněte na tlačítko **Select** a **Add**.

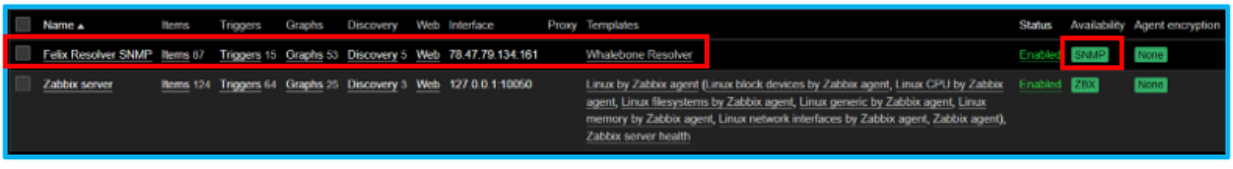
- Po výběru šablony Whalebone se vraťte do **Host** a klikněte na tlačítko **add**. Na kartě vidíme, že resolver byl přidán do monitoringu Zabbix.

Poznámka: SNMP data from the resolver to Zabbix will take time to initialized. Wait the Zabbix to gather data from the server. Always observe the availability on the right corner to see if it's green. Green means its already connected to the whalebone resolver.


Create host
Import
Filter
Monitored by
Any
Server
Proxy
Proxy
Select
Tags
And/Or
Or
tag
Contains
value
Remove
Add
Apply
Reset
Hosts
Host
Templates
IPMI
Tags
Macros
Inventory
Encryption
Value mapping
* Host name
Visible name
* Groups
type here to search
Select
Interfaces
No interfaces are defined.
Add
Description
Monitored by proxy
(no proxy)
Enabled
Add
Cancel

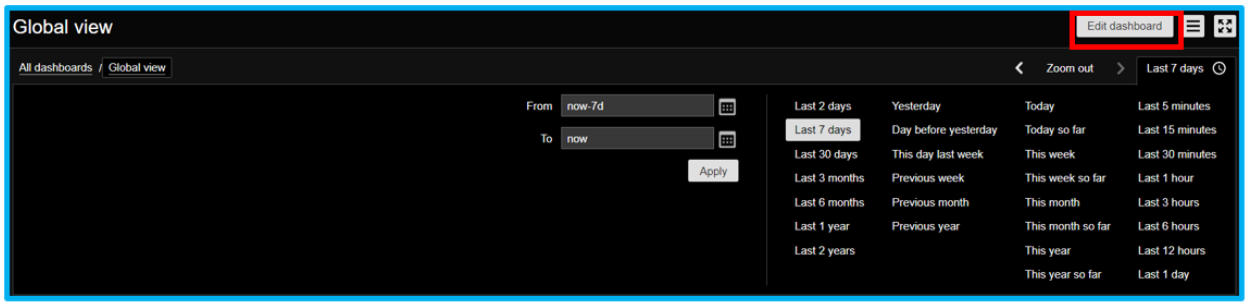

Interfaces
Type
IP address
DNS name
Connect to
Port
Default
SNMP
127.0.0.1
IP
DNS
161
Remove
* SNMP version
SNMPv2
* SNMP community
{$SNMP_COMMUNITY}
Use bulk requests


Hosts
Host
Templates
IPMI
Tags
Macros
Inventory
Encryption
Value mapping
Linked templates
Name
Action
Link new templates
type here to search
Select
Add
Cancel
Templates
Host group
Templates
Select
VMware Guest
VMware Hypervisor
VMware macros
VMWare SD-WAN VeloCloud by HTTP
Whalebone Resolver
WildFly Domain by JMX
WildFly Server by JMX
Windows by Zabbix agent
Windows by Zabbix agent active
Windows CPU by Zabbix agent
Windows CPU by Zabbix agent active
Windows filesystems by Zabbix agent
Windows filesystems by Zabbix agent active
Windows generic by Zabbix agent
Windows generic by Zabbix agent active
Windows memory by Zabbix agent
Windows memory by Zabbix agent active
Select
Cancel


Name
Items
Triggers
Graphs
Discovery
Web
Interface
Proxy
Templates
Status
Availability
Agent encryption
Felix Resolver SNMP
Items 87
Triggers 15
Graphs 53
Discovery 5
Web
78.47.79.134:161
Whalebone Resolver
Enabled
SNMP
None
Zabbix server
Items 124
Triggers 64
Graphs 25
Discovery 3
Web
127.0.0.1:10050
Linux by Zabbix agent (Linux block devices by Zabbix agent, Linux CPU by Zabbix agent, Linux filesystems by Zabbix agent, Linux generic by Zabbix agent, Linux memory by Zabbix agent, Linux network interfaces by Zabbix agent, Zabbix agent), Zabbix server health
Enabled
ZBX
None

20.5 Jak přidat widget Whalebone na dashboard Zabbix

- Chcete-li přidat dahboard, přejděte do části **Monitoring** a poté do části **Dashboard**. V globálním zobrazení dashboardu vidíme možnost **Edit dahboard**. Klepnutím na tlačítko přidáte nové grafy.

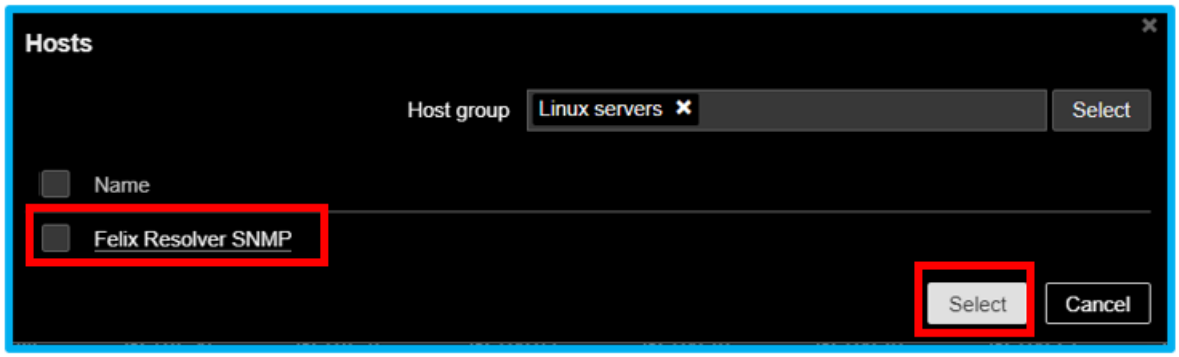


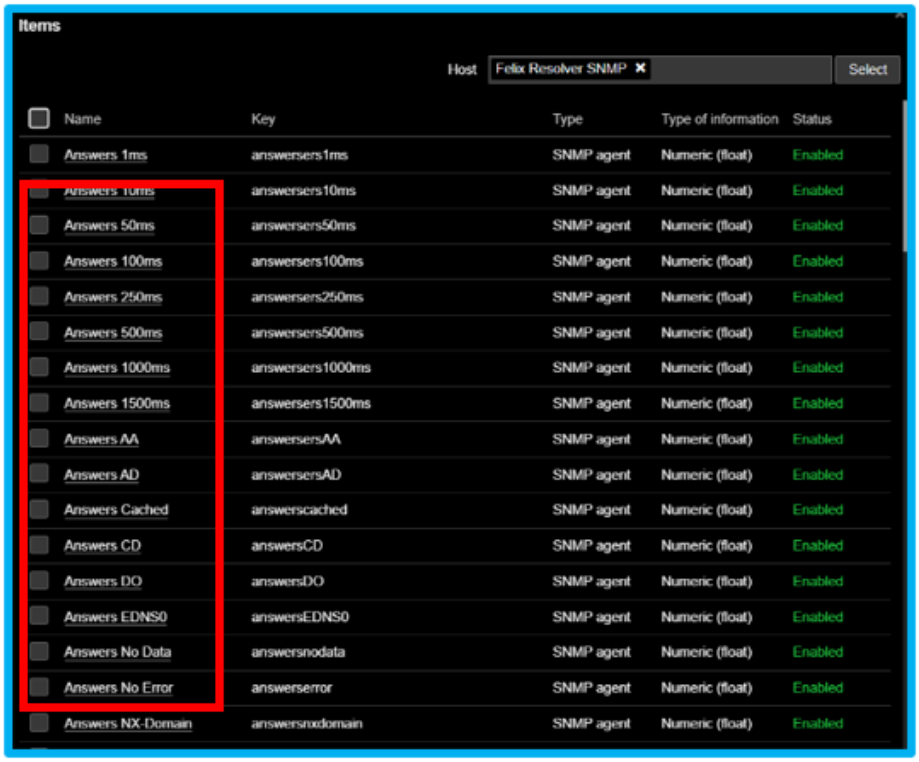
Poznámka: Před přidáním grafů na dashboard se ujistěte, že host již grafy detekoval. Grafy najdete v části **Configuration** → **Hosts** → **Graphs**.

- Klikněte na **Edit dashboard** a přidejte widget v **Add widget** → **Type** → **Graph** a zadejte název widgetu.

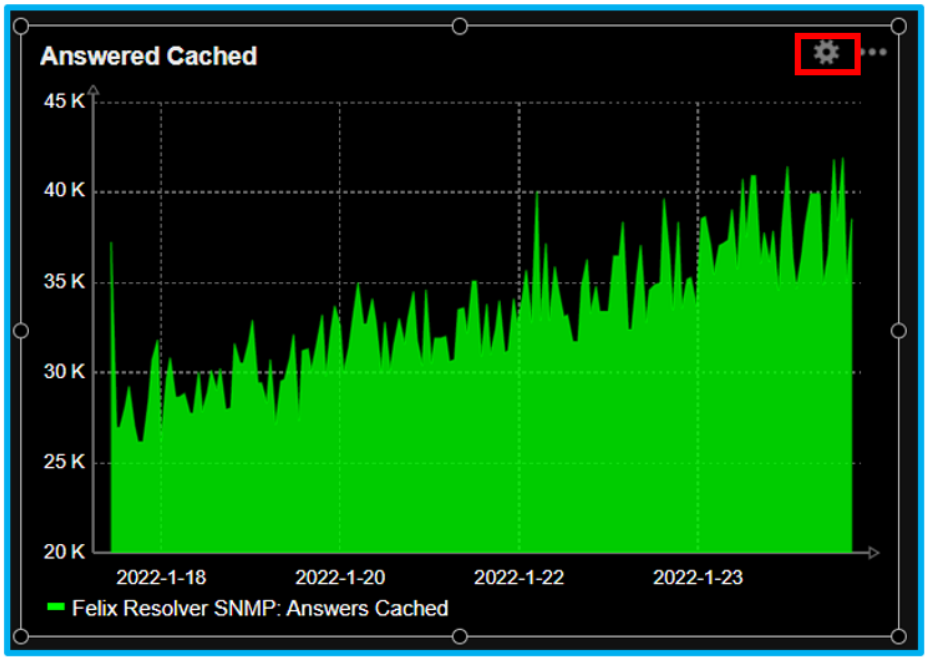
- Vyberte **Data set**, kterým je název hosta, a vyberte **Item pattern**, kde můžeme najít šablonu Whalebone.

- Vyberte položky, které chcete přidat na widget pro grafickou vizualizaci. Po přidání **Items** vyberte základní barvu pro grafy, poté můžete upravit šířku, velikost bodu, průhlednost a výplň.


Hosts
Host group
Linux servers
Select
Name
Felix Resolver SNMP
Select
Cancel


Items
Host
Felix Resolver SNMP
Select
Name
Key
Type
Type of information
Status
Answers 1ms answersers1ms SNMP agent Numeric (float) Enabled
Answers 10ms answersers10ms SNMP agent Numeric (float) Enabled
Answers 50ms answersers50ms SNMP agent Numeric (float) Enabled
Answers 100ms answersers100ms SNMP agent Numeric (float) Enabled
Answers 250ms answersers250ms SNMP agent Numeric (float) Enabled
Answers 500ms answersers500ms SNMP agent Numeric (float) Enabled
Answers 1000ms answersers1000ms SNMP agent Numeric (float) Enabled
Answers 1500ms answersers1500ms SNMP agent Numeric (float) Enabled
Answers AA answersersAA SNMP agent Numeric (float) Enabled
Answers AD answersersAD SNMP agent Numeric (float) Enabled
Answers Cached answerscached SNMP agent Numeric (float) Enabled
Answers CD answersCD SNMP agent Numeric (float) Enabled
Answers DO answersDO SNMP agent Numeric (float) Enabled
Answers EDNS0 answersEDNS0 SNMP agent Numeric (float) Enabled
Answers No Data answersnodata SNMP agent Numeric (float) Enabled
Answers No Error answerserror SNMP agent Numeric (float) Enabled
Answers NX-Domain answersnxdomain SNMP agent Numeric (float) Enabled

- Widget byl úspěšně přidán na dahboard. Chcete-li widget upravit nebo změnit, klikněte na ikonu ozubeného kola.

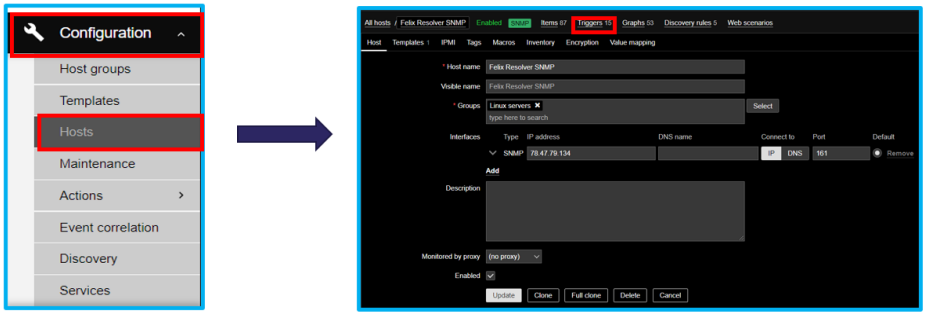


- Nezapomeňte kliknout na tlačítko uložit vpravo nahoře, abyste widget uložili na dashboard.

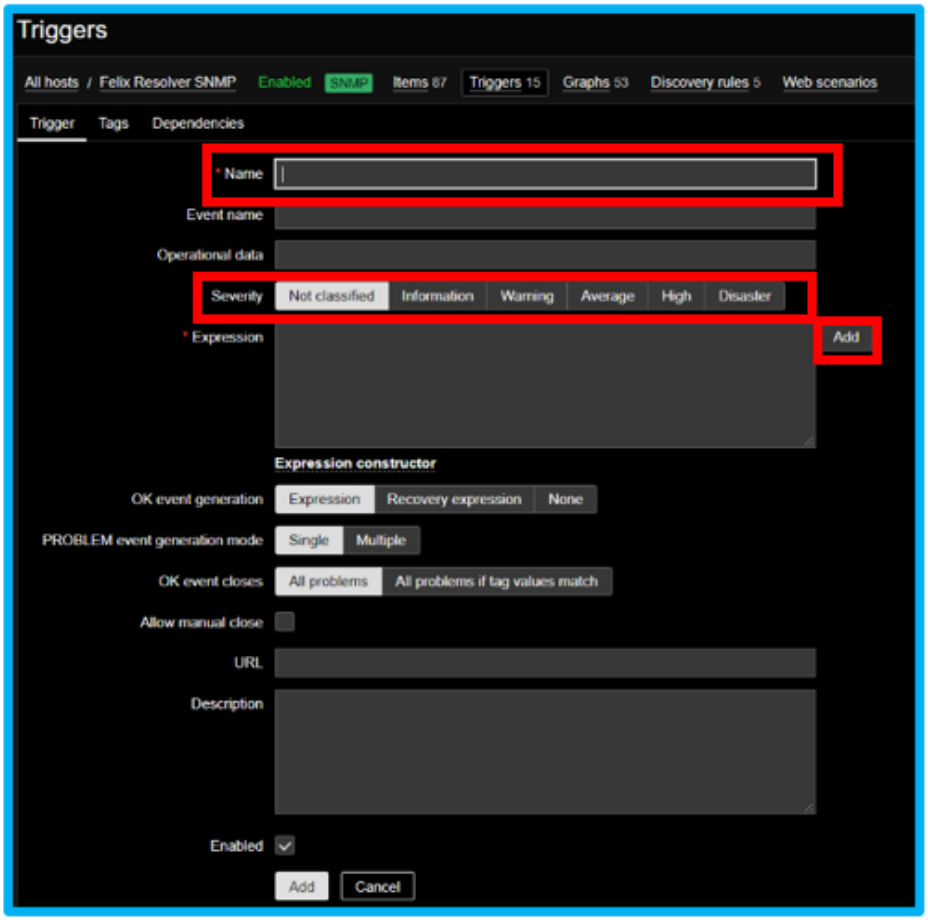
20.6 Jak přidat spouštěče (triggers) v systému Zabbix

Spouštěče jsou logické výrazy, které „vyhodnocují“ data shromážděná položkami a představují aktuální stav systému. Nastavení spouštěče umožňuje definovat hranici toho, jaký stav je přijatelný. Pokud tedy příchozí data překročí přijatelný stav, je spouštěč „spuštěn“ - neboli změní stav na **PROBLEM**. Příklad: Pokud by Whalebone resolver narazil na 1000 NXDOMAIN odpovědí, spouštěč bude mít hodnotu inicializován, aby upozornil, že data překročila nastavené prahové hodnoty.

- Chcete-li konfigurovat spouštěč, přejděte do části **Configuration** → **Hosts**. Klikněte na kartu **Triggers**.

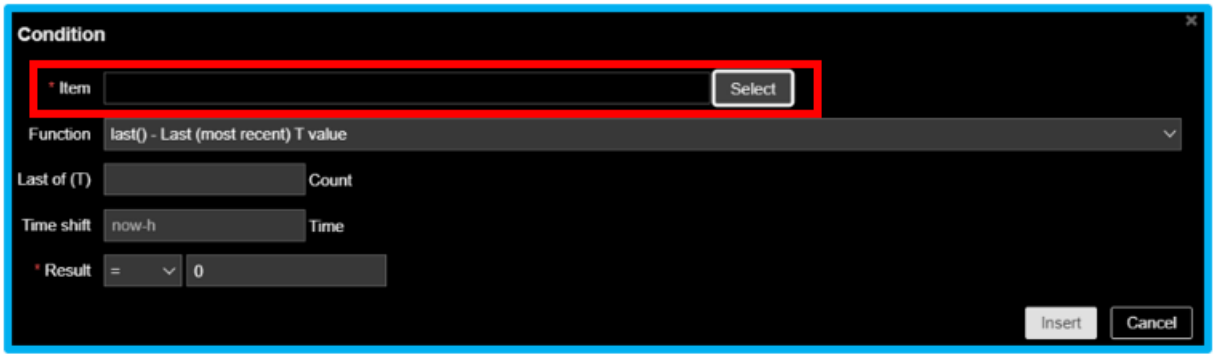


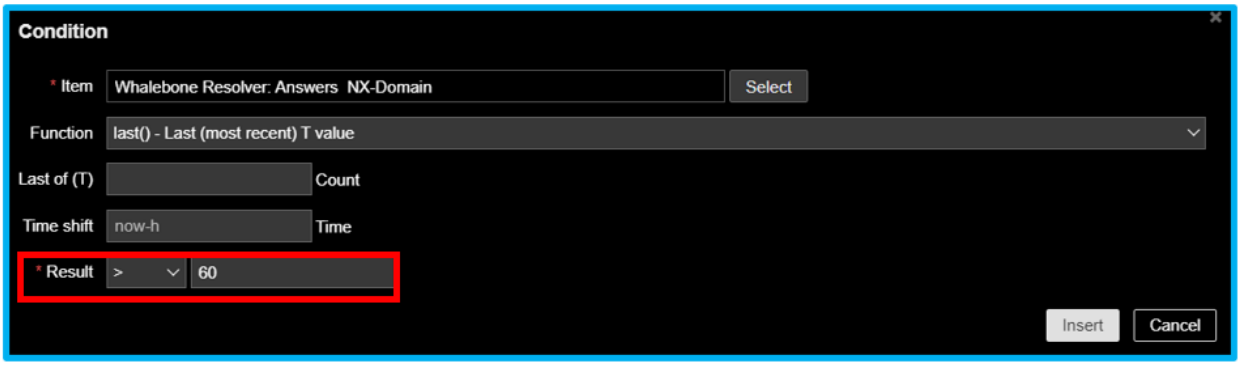
- Vytvořit **spouštěč** → Zadejte **název** a přidejte výraz. Řekněme, že chceme spouštět, pokud hodnota NXDOMAIN resolveru překročí hodnotu 60. Pro tento spouštěč vyberte závažnost - **Severity**.



- Klikněte na tlačítko **Add** → Na kartě **Condition** → **Item** → **Select**. Zde vybereme položku **NXDOMAIN**.

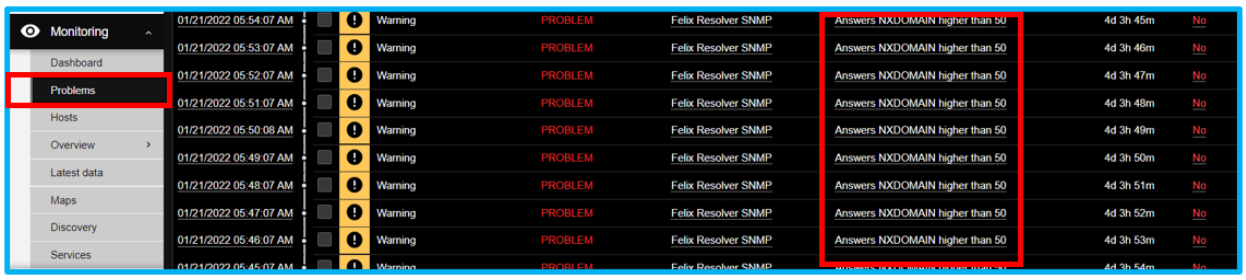
- **Na kartě Condition nastavte Count → Time shift - now-h → Result. Pro pole Result vyberte operand a poté nastavte hodnotu na 60. Tato podmínka se spustí, pokud NXDOMAIN překročí hodnotu 60.**
- Klikněte na tlačítko **Insert** a uložte spouštěče. Ujistěte se, že je spouštěč v šabloně povolen.


Condition
* Item
Select
Function
last() - Last (most recent) T value
Last of (T)
Count
Time shift
now-h
Time
* Result
=
0
Insert
Cancel

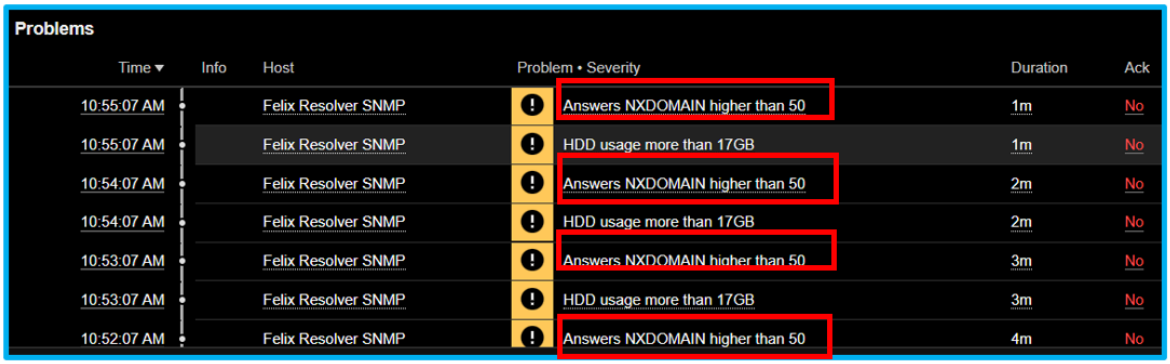

Condition
* Item
Whalebone Resolver: Answers NX-Domain
Select
Function
last() - Last (most recent) T value
Last of (T)
Count
Time shift
now-h
Time
* Result
>
60
Insert
Cancel


Severity
Name ▲
Operational data
Expression
Status
Tags
Warning
Answers 1ms less than 40000
last(/Whalebone Resolver/answersers1ms)<40000
Enabled
Warning
Answers 100ms higher than 5000
last(/Whalebone Resolver/answersers100ms)>5000
Enabled
Warning
Answers NXDOMAIN higher than 50
last(/Whalebone Resolver/answersnxdomain)>50
Enabled
Warning
HDD usage more than 17GB
last(/Whalebone Resolver/hddusage)>18
Enabled

- Na kartě **Problems** zkontrolujte položku **NXDOMAIN**, která překračuje prahovou hodnotu.



- Na dashboardu lze identifikovat NXDOMAIN, který překračuje prahovou hodnotu.



20.7 Jak nakonfigurovat akce spouštěče

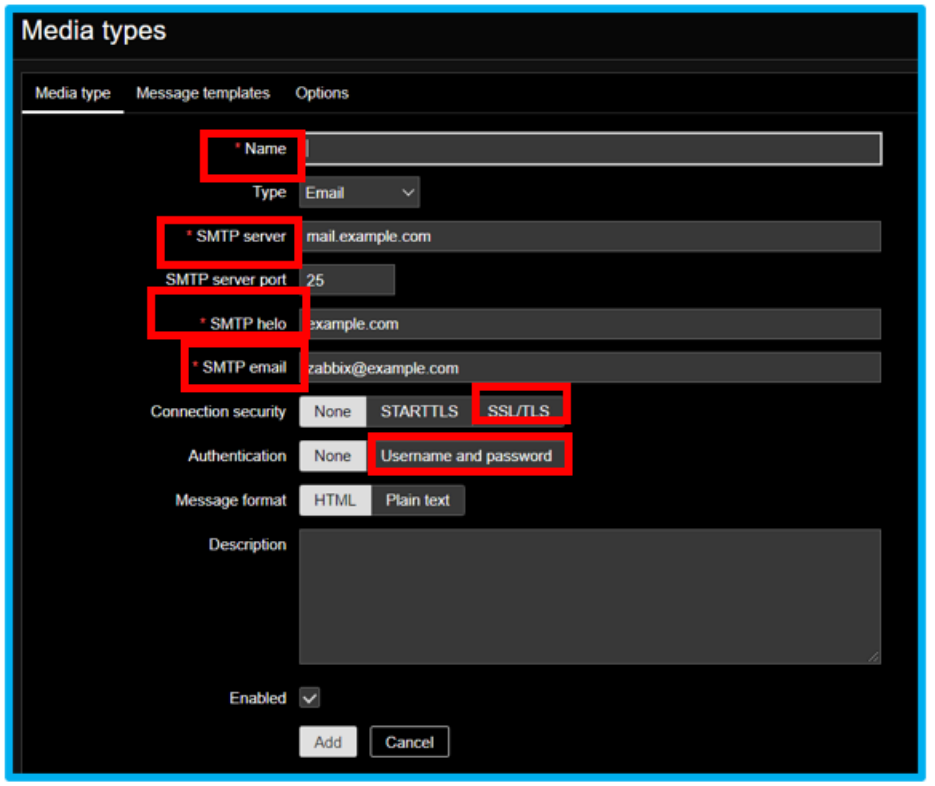
Akční spouštěče jsou logické výrazy, které „vyhodnocují“ data shromážděná položkami a představují aktuální stav systému. Výraz spouštěče umožňuje definovat hranici, kdy jsou data „přijatelná“. Proto, pokud příchozí data překročí přijatelný stav, je spouštěč „spuštěn“ nebo změní stav na PROBLÉM. Pro tento příklad řekněme, že NXDOMAIN překročí hodnotu 60. Spouštěč pošle e-mail správci nebo vytoří oznámení.

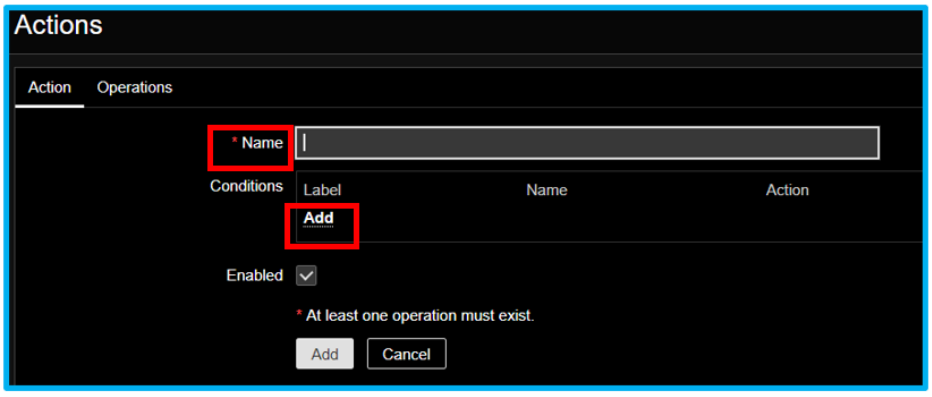
- Prvním krokem je nastavení spouštěcí akce pomocí e-mailu. Přejděte do **Administration** a zde do **Media types**. Vytvořte nový a zadejte název. Dále zadejte název SMTP serveru a e-mail na který budou oznámení zasílána. Autentikaci volte metodou jména a hesla.

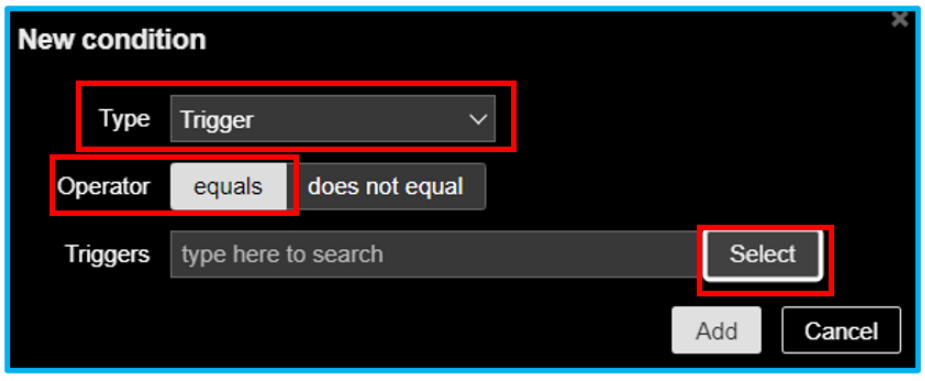
- Po nastavení e-mailu → Přejděte do **Configuration** → **Actions** → **Spouštěče akcí**. Na spouštěči **Akce** → **Vytvořit akci** → Zadejte název → Přidejte podmínku **New condition**.

- V okně **New condition** vyberte Typ: **Trigger**, Operátor : **equals**: a jako spouštěč Zvolte **NXDOMAIN**.

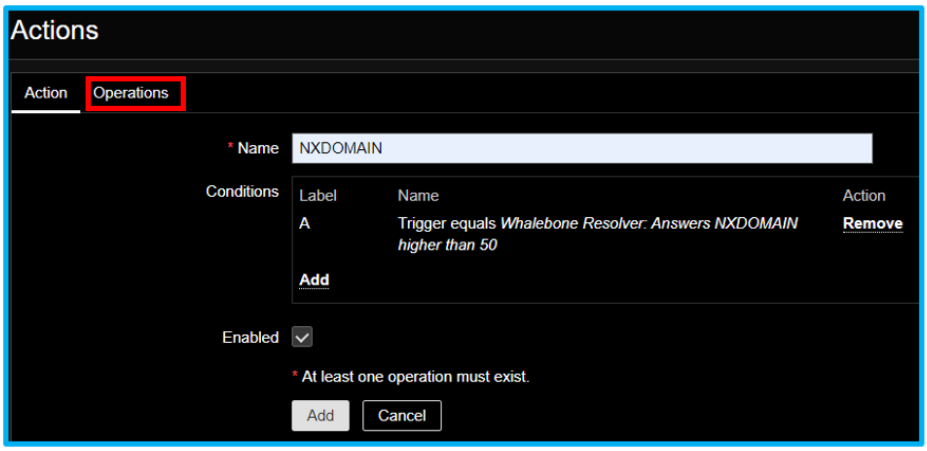
- Vyberte položku NXDOMAIN pro spouštěče akcí. Klikněte na tlačítko **Add**.


Media types
Media type
Message templates
Options
* Name
Type
Email
* SMTP server
mail.example.com
SMTP server port
25
* SMTP helo
example.com
* SMTP email
zabbix@example.com
Connection security
None
STARTTLS
SSL/TLS
Authentication
None
Username and password
Message format
HTML
Plain text
Description
Enabled
Add
Cancel


Actions
Action
Operations
* Name
Conditions
Label
Name
Action
Add
Enabled
* At least one operation must exist.
Add
Cancel


New condition
Type
Trigger
Operator
equals
does not equal
Triggers
type here to search
Select
Add
Cancel

- V okně **Actions** → Klikněte na **Operations** → Zvolte výchozí na 1 min a klikněte na tlačítko **Add**



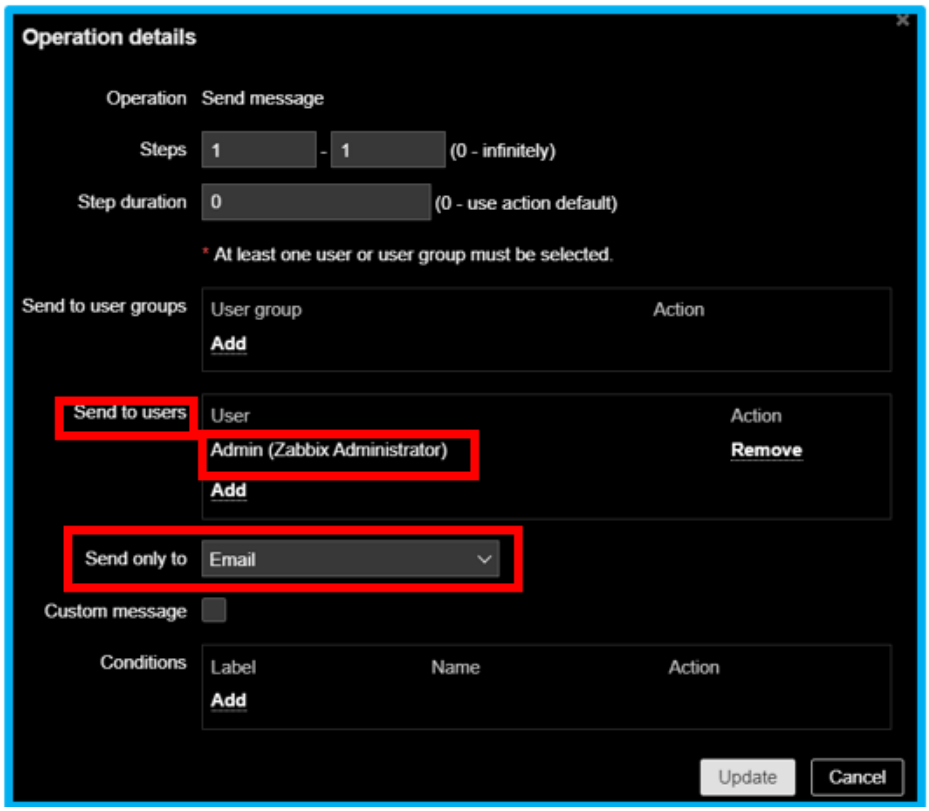
- Zvolte dobu trvání kroku (steps) na 1 minutu. Na operaci klikněte na **add** → **Send to users** → **Admin (Jméno administrátora)** → Send only to: **E-mail**.

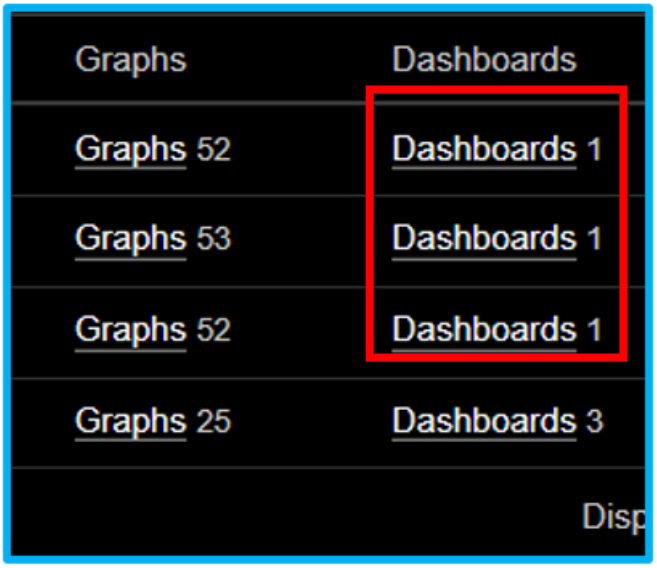
20.8 Jak zobrazit předdefinovaný dashboard Whalebone

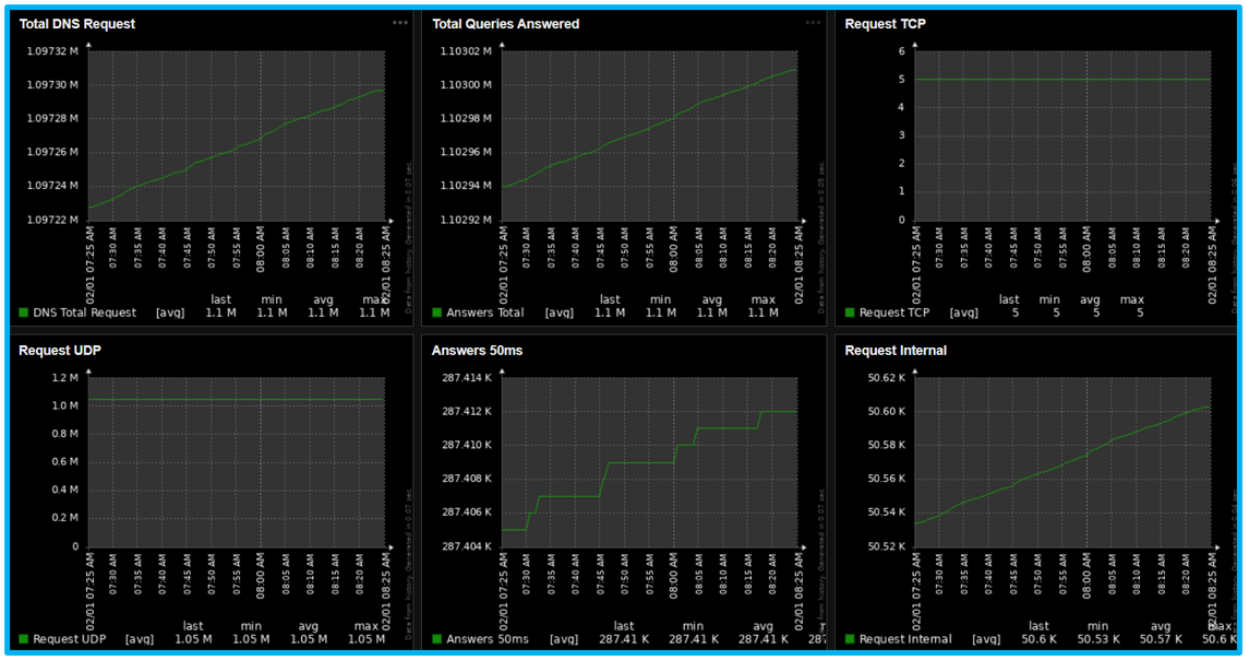
Pro příkalad, šablona Whalebone má ukázkový dashboard, který obsahuje přehled dat z resolveru.

- Chcete-li tento panel zobrazit, přejděte do části **Monitoring** → **hosts**. Poté v **hosts** klikněte na dasboard.

Toto je přehled předdefinovaného Whalebone dashboardu.


Operation details
Operation
Send message
Steps
1
1
(0 - infinitely)
Step duration
0
(0 - use action default)
* At least one user or user group must be selected.
Send to user groups
User group
Action
Add
Send to users
User
Action
Admin (Zabbix Administrator)
Remove
Add
Send only to
Email
Custom message
Conditions
Label
Name
Action
Add
Update
Cancel


Graphs
Dashboards
Graphs 52
Dashboards 1
Graphs 53
Dashboards 1
Graphs 52
Dashboards 1
Graphs 25
Dashboards 3
Disp


Total DNS Request
1.09732 M
1.09730 M
1.09728 M
1.09726 M
1.09724 M
1.09722 M
DNS Total Request [avg] last 1.1 M min 1.1 M avg 1.1 M max 1.1 M
Total Queries Answered
1.10302 M
1.10300 M
1.10298 M
1.10296 M
1.10294 M
1.10292 M
Answers Total [avg] last 1.1 M min 1.1 M avg 1.1 M max 1.1 M
Request TCP
6
5
4
3
2
1
0
Request TCP [avg] last 5 min 5 avg 5 max 5
Request UDP
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0
Request UDP [avg] last 1.05 M min 1.05 M avg 1.05 M max 1.05 M
Answers 50ms
287.414 K
287.412 K
287.410 K
287.408 K
287.406 K
287.404 K
Answers 50ms [avg] last 287.41 K min 287.41 K avg 287.41 K
Request Internal
50.62 K
50.60 K
50.58 K
50.56 K
50.54 K
50.52 K
Request Internal [avg] last 50.6 K min 50.53 K avg 50.57 K max 50.6 K

CHAPTER 21

Správa uživatelů/organizací

21.1 Správa uživatelů

Uživatele lze spravovat na příslušné kartě v nabídce **Uživatelé** nacházejícím se pod ikonou panáčka.

V této nabídce může správce spravovat uživatelské účty. Může přidávat, odebírat nebo zakazovat jejich používání. Kromě toho jsou mu k dispozici informace o posledním přihlášení a poslední změně hesla pro každý účet.

Tip: Když je uživatel pozván do organizace portálu a ještě nemá účet Whalebone, je pro něj vytvořen nový účet a na jeho registrovanou e-mailovou adresu je zaslán aktivační odkaz.

Podporovány jsou dva typy uživatelů:

Uživatelé:

- uživatelé, kteří mají svůj primární účet zaregistrovaný pod identifikátorem konkrétní organizace.

Externí uživatelé: (pokud jsou k dispozici)

- uživatelé, kteří patří pod jinou organizaci.
- mohou mít přiřazenou roli pod jinou organizací Whalebone.
- např. prodejci

Tip: Každému uživateli lze přiřadit jednu nebo více rolí, které lze kombinovat a vytvořit tak jeho konečnou roli. Oprávnění jsou aditivní (stohovatelná).¨

Níže jsou popsány jednotlivé role a činnosti, které mohou vykonávat.

Akce	Data o provozu	Data hrozeb	Úprava seznamů	Správce bezpečnostních politik	API tokeny	Pouze čtení	Resolver operátor	DNS Admin	Správce Home-Office Security	Správce uživatelů	Administrátor
View Threat Data											
View DNS Traffic											
View Whitelists/Blacklists											
Edit Whitelists/Blacklists											
View Security Policies											
Edit Security Policies											
View Resolver Configuration											
Edit Resolver Configuration											
View API Tokens											
Generate API Tokens											
View Network Configuration											
Edit Network Configuration											
View Alerts											
Edit Alerts											
View Reports											
Edit Reports											
HOS device management and policy settings											
Manage user accounts											

21.2 Nastavení organizace

Nastavení organizace najdete v nabídce **Nastavení organizace**.

21.2.1 Politika přístupu

Zásady přístupu k portálu definují bezpečnostní mechanismus pro uživatele přistupující k portálu. Whalebone Portal. Lze nakonfigurovat následující nastavení:

Povolené rozsahy IP: Rozsahy IPv4 nebo IPv6 v notaci CIDR, např. 10.0.0.0/24, které mají povolen přístup k portálu Whalebone.

Zamykání účtu: Pokud je povoleno, může omezit počet neúspěšných pokusů o přihlášení.

K dispozici jsou tyto možnosti:

- **Limit nesprávných pokusů**:

Počet neúspěšných pokusů o přihlášení před zablokováním účtu. Výchozí hodnota je 5.

- **Doba trvání uzamčení (minuty)**:

Doba v minutách, po kterou je zákázán další pokus o přihlášení.

- **Reset počítadla (minuty)**:

Doba trvání v minutách před resetováním počítadla neúspěšných pokusů.

- **Limit CAPTCHA**:

Počet neúspěšných pokusů o přihlášení před zapnutím ověření CAPTCHA.

Vyžadovat vícefaktorovou autentizaci: Vyžadujte, aby uživatelé používali aplikaci dvoufaktorového ověřování (2FA) a při přihlášení k portálu zadávali další tokeny.

21.2.2 Politika hesel

Lze nakonfigurovat následující nastavení hesla:

Expirace hesla (ve dnech): Doba platnosti hesla: Počet dní, než je třeba heslo změnit.

Historie hesla: Počet starých hesel, která nelze znovu použít při nastavování nových hesel.

Atributy hesla: Heslo, které se má změnit: Atributy, které by mělo nové heslo mít.

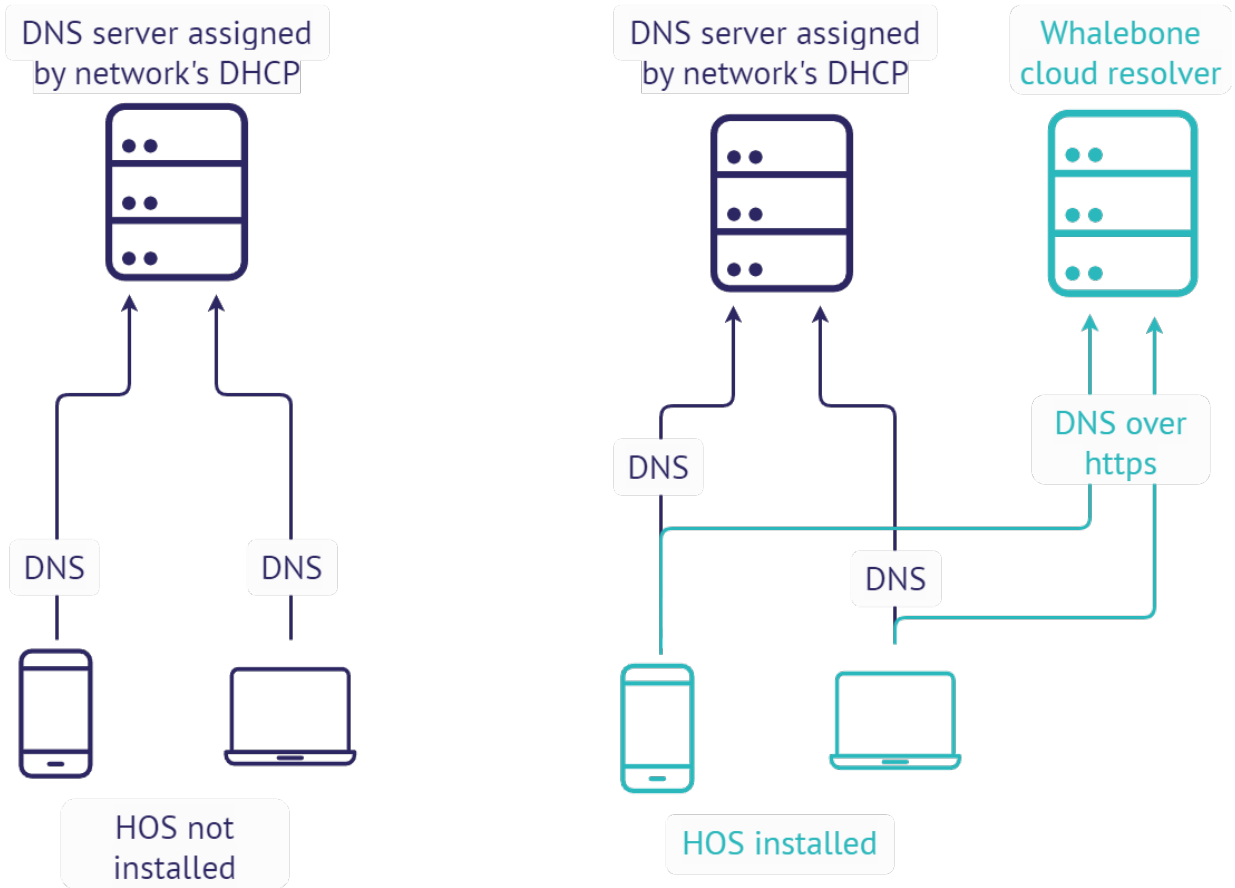
Atributy, které může mít nové heslo, jsou následující:

- Minimální délka
- Počet číslic
- Počet malých písmen
- Počet velkých písmen
- Počet speciálních znaků

CHAPTER 22

Přehled Home Office Security

Whalebone Home Office Security (HOS) poskytuje funkci filtrování DNS mimo síť pro stolní počítače a mobilní zařízení. Zachycuje provoz DNS a mění adresu DNS serveru. Chrání zařízení před síťovými hrozbami tím, že kontroluje každý paket DNS. V současné době jsou podporována zařízení se systémy Windows, Android a iOS. Podrobné informace o podpoře verzí operačních systémů naleznete níže.



HOS se dodává s instalátorem systému Windows pro nasazení. K provedení instalace není nutná žádná interakce uživatele, instalační program však vyžaduje `token`.

Výchozí cílový adresář je:

```
C:\Program Files (x86)\Whalebone\Home Office Security\
```

Pro Android, výchozí cílový adresář je:

```
/storage/emulated/0/Android/io.whalebone.securedns.corp/
```

22.1 Porporované operační systémy

Windows Desktop	Windows 7 nebo vyšší
Windows Server	Windows Server 2012 nebo vyšší
Android	Android 5 nebo vyšší
iOS	Všechny verze
MacOS	Není podporován
Linux	Není podporován

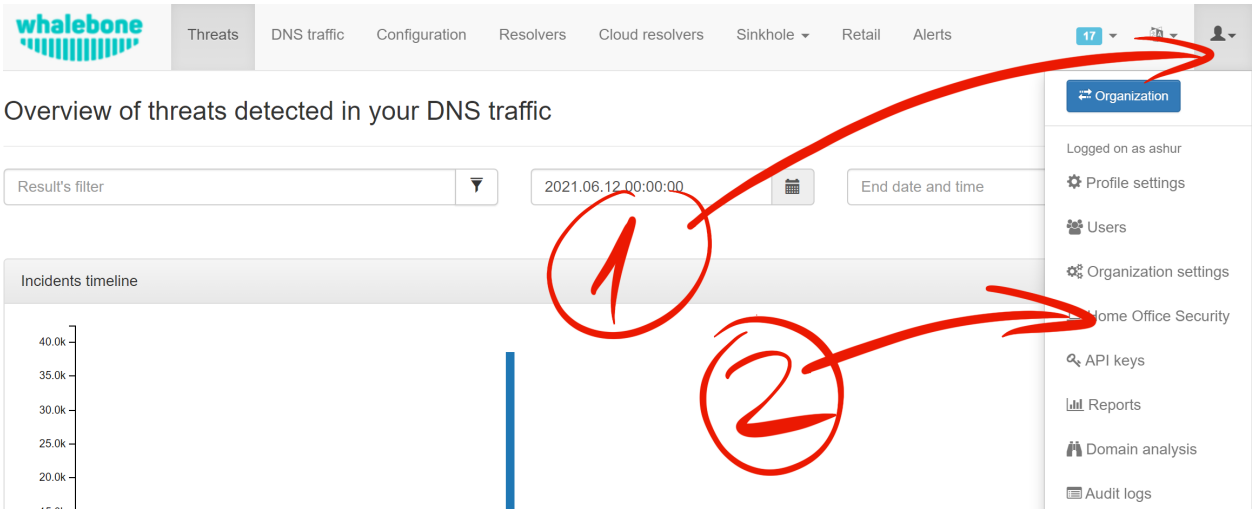
Systémy se operačním systémem Windows 7 musí být aktuální nebo musí mít nainstalovanou alespoň verzi KB3033929.

Systémy se operačním systémem Windows Server 2016 musí mít vypnuté zabezpečené spouštění (secure boot).

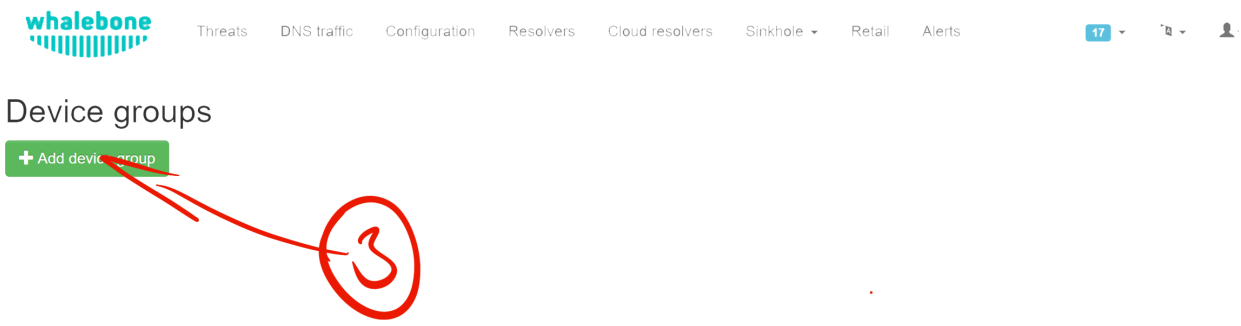
CHAPTER 23

Instalace krok za krokem

Chcete-li nainstalovat HOS do zařízení, musíte jej nejprve nakonfigurovat. Přejděte do **Whalebone Portalu**, přejděte do (1) **Uživatelského menu** a zde na (2) **Home Office Security**.



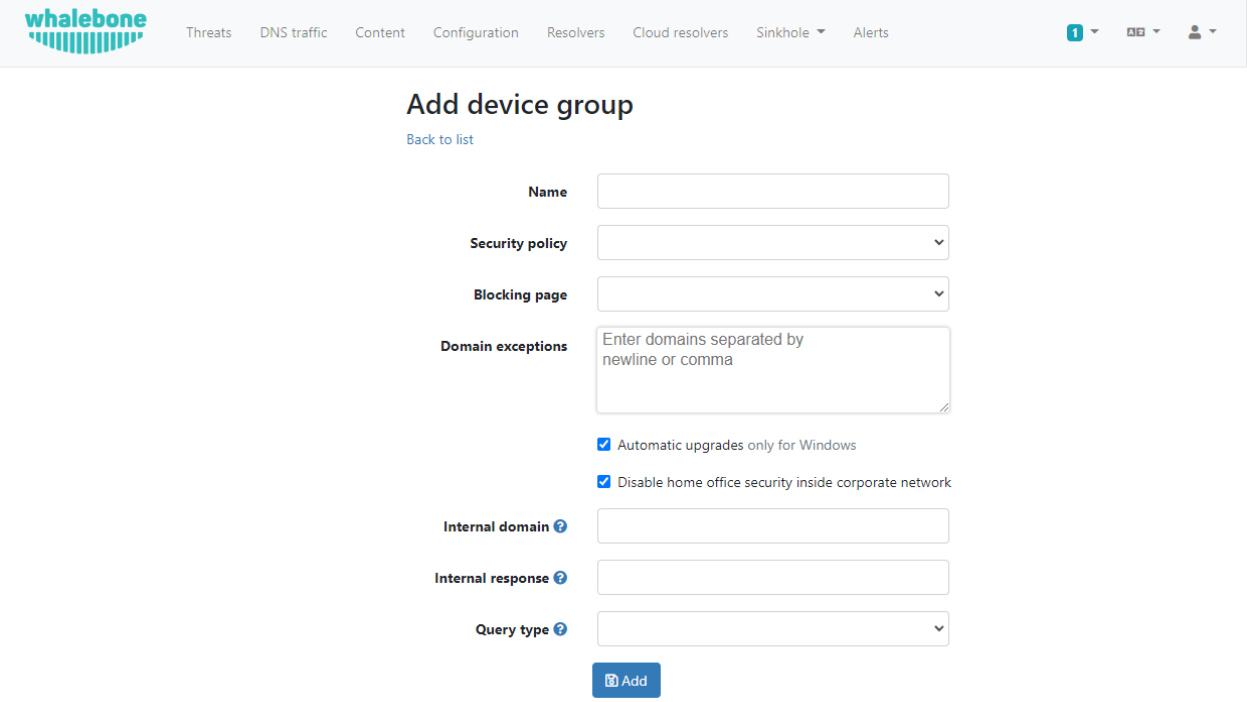
Skupina **Default** by již měla existovat. Pokud ne, vytvořte ji kliknutím na tlačítko (3) a **+ Vytvořit skupinu**.



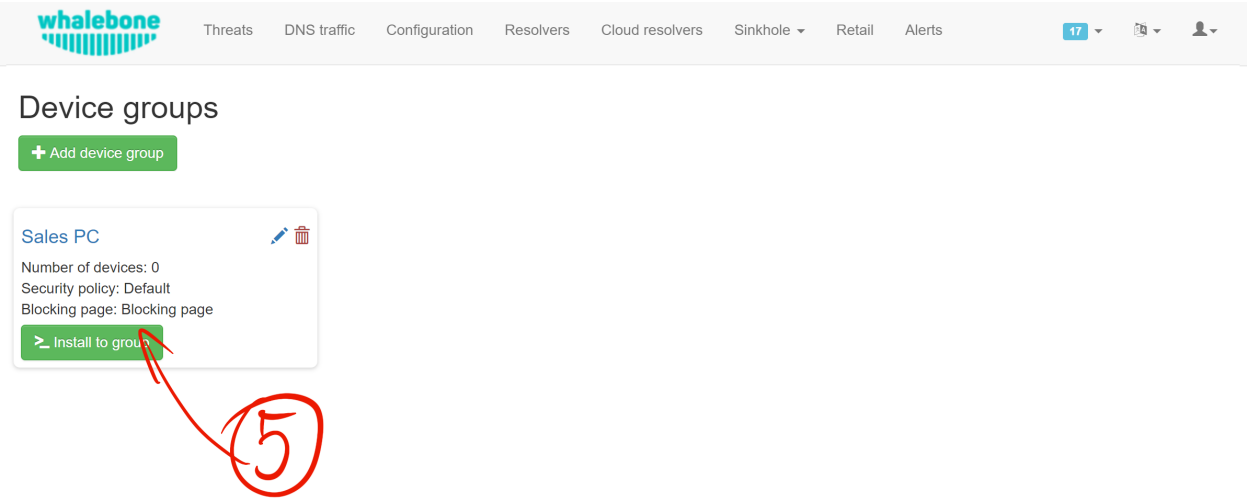
- **Název**: Tento údaj by měl jasně identifikovat skupinu zařízení, aby se odlišila od ostatních. Pokud používáte pouze jednu, můžete jeho název ponechat jako Default Group (Výchozí skupina).
- **Bezpečnostní politika**: Odpovídá zásadám, které vytvoříte v nabídce Konfigurace. Jedná se o soubor pravidel. Na základě zásad se zařízení nebo místní/cloudový resolver rozhoduje, co má při překladu DNS dělat. Tato sada pravidel zůstává v zařízení a je zpočátku aktualizována a později synchronizována. Z tohoto důvodu portál zajišťuje monitorování těchto zařízení.
- **Blokační stránka**: odpovídá stránkám blokování, které vytvoříte v nabídce Konfigurace.
- **Výjimky na domény**: Služba HOS nebude přesměrovávat žádné dotazy DNS, které obsahují dotaz na doménu na seznamu výjimek. Např. při zadání `example.com` bude dotaz DNS vyřešen jako obvykle na resolveru nakonfigurovaném operačním systémem. Stejné pravidlo platí pro dotaz `subdomena.example.com`.
- **Automatická aktualizace**: Pokud je tato konfigurační možnost zaškrtnuta, aplikace HOS v systému Windows se aktualizuje na nejnovější produkční verzi, jakmile je k dispozici ke stažení novější verze. Tato volba se projeví pouze v systému Windows, v mobilních zařízeních provádí aktualizace ekosystém výrobce.
- **Vypnout HOS uvnitř podnikové sítě: Po zaškrtnutí této možnosti se zobrazí další 3 textová pole. Konfigurace umožňuje, aby došlo k vypnutí HOS v podnikové sítě na základě procesu dotaz-odpověď.**
  - **Interní doména**: Specifikuje na jakou interní doménu se bude HOS periodicky dotazovat.
  - **Interní odpověď**: HOS po odelsání dotazu na interní doménu očekává odpověď specifikovanou v tomto poli.
  - **Typ dotazu**: Dle zvoleného typu dotazu (A, AAAA a MX) musí být korektně nakonfigurován záznam na interním domain controlleru.

> **Varování:** Dvě výše uvedená nastavení (Automatická aktualizace a Výjimka pro doménu) jsou k dispozici pouze ve verzi 2.10.0 pro Windows a vyšší. Pokud používáte starší verzi, je nutné provést update manuálně.

Po dokončení klikněte na tlačítko **Přidat** a vytvořte tuto skupinu.



Kliknutím na tlačítko (5) **Install to group** se zobrazí pokyny k instalaci a/nebo můžete použít odkaz ke stažení instalačního programu HOS.



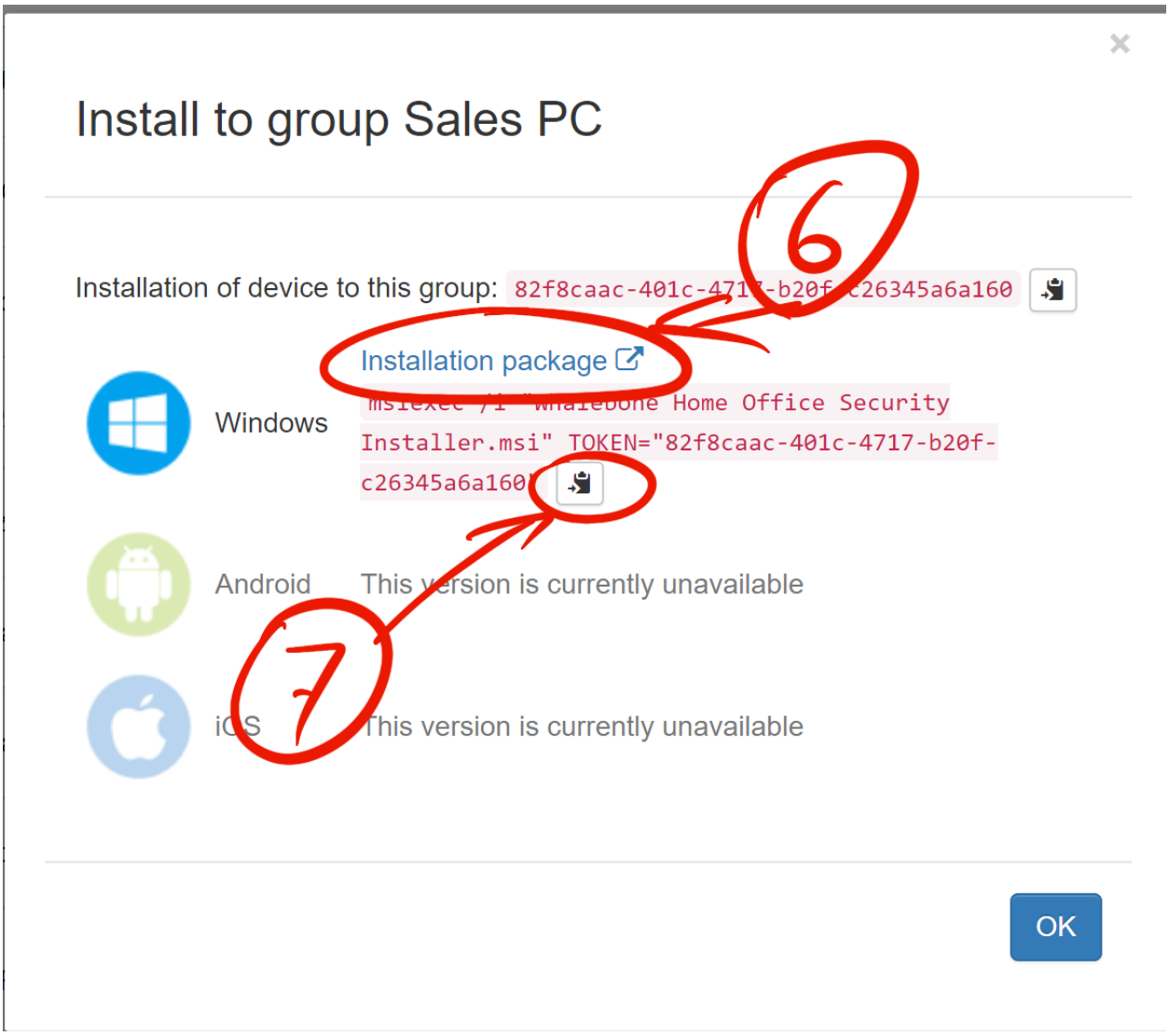
Pokud jste si ještě nestáhli instalační program (6). Během stahování instalačního programu zkopírujte instalační příkaz do schránky (7).

Instalace nebo aktualizace:

```
msiexec /i "Whalebone.Home.Office.Security.Installer.msi" TOKEN="60d5806e-07fe-432a-a4ad-
↪7797d82782b3"
```

Odinstalace:

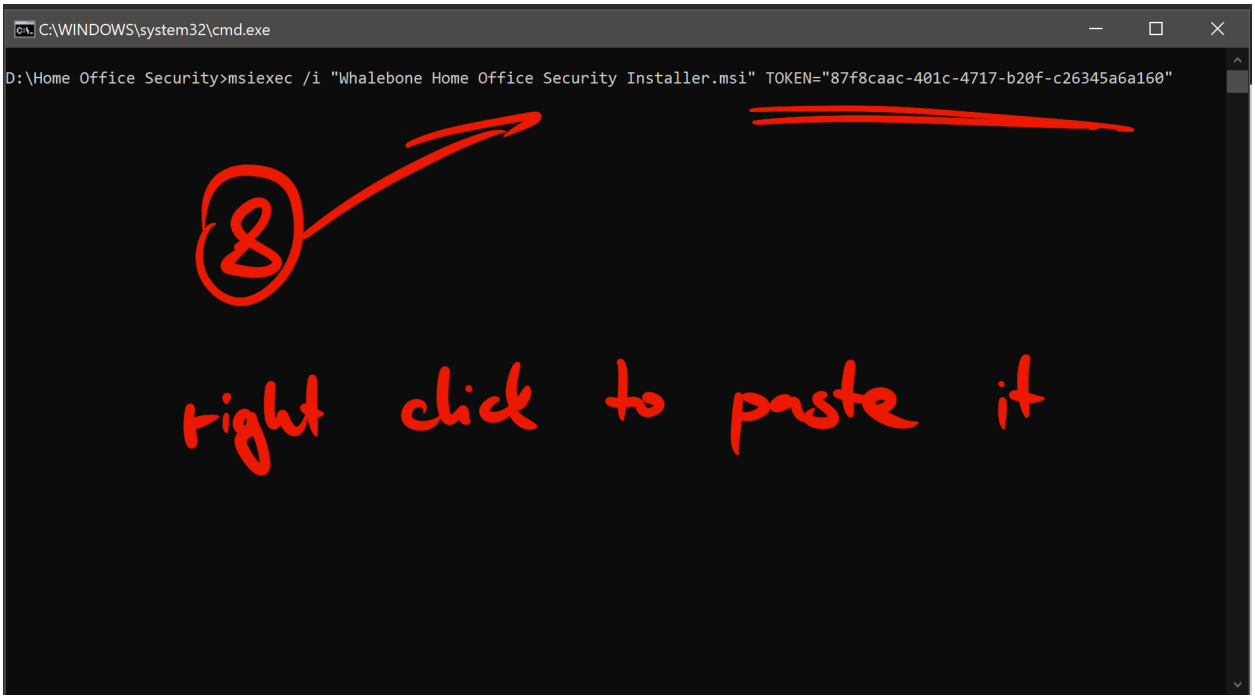
```
msiexec /x "Whalebone.Home.Office.Security.Installer.msi
```



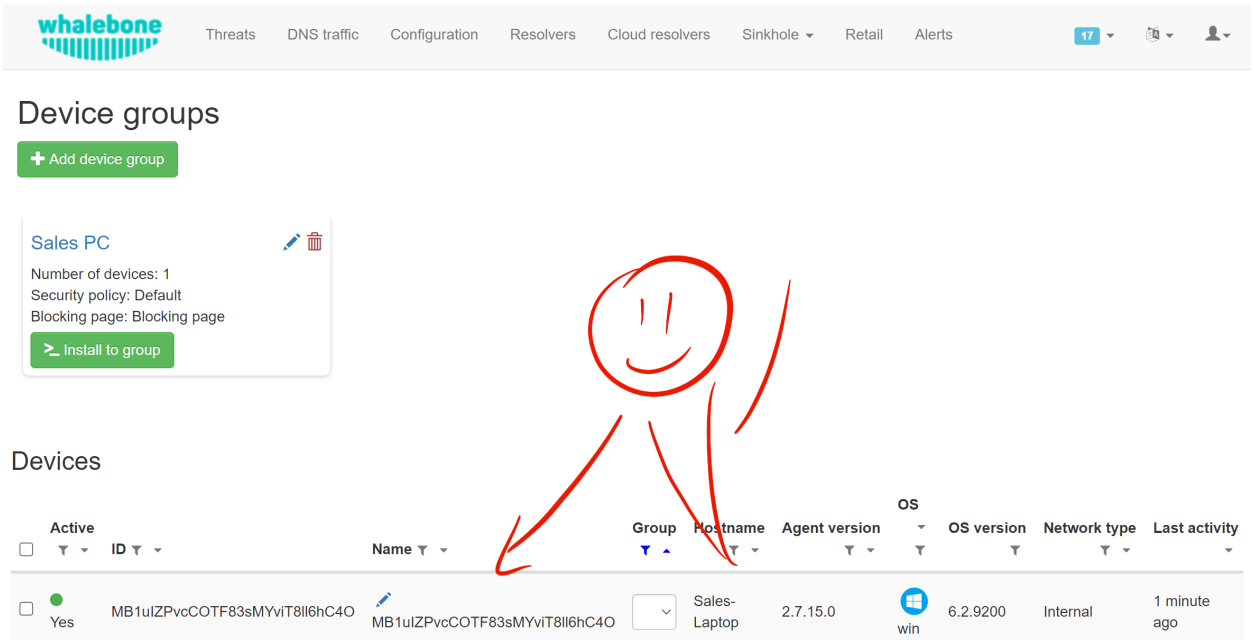
Najděte složku, ve které je instalátor umístěn. Měl by to být soubor s názvem **Whalebone.Home.Office.Security.Installer.msi**.

Otevřete příkazový řádek, změňte adresář na složku, kde je instalátor, a vložte (8) příkaz myší (klikněte pravým tlačítkem myši). Spusťte příkaz. To vyžaduje oprávnění správce.

Instalační program má minimální uživatelské rozhraní.



Tip: The installer has very minimal UI. If there was no error message, consider the installation successful.



Zařízení je nyní viditelné na Whalebone Portálu.

CHAPTER 24

Operace HOS

24.1 Zařízení

Vaše organizace může zařízení rozdělit do jedné nebo více skupin. Každé zařízení může patřit pouze do jedné z nich. Každé zařízení musí být členem **skupiny zařízení**, aby mohlo být monitorováno. Každá skupina poskytuje **Bezpečnostní politiku**, které jsou na ně později podmíněně aplikovány. Podle toho, zda je zařízení přítomno v **interní** nebo **externí** síti, je **aktivní** nebo **neaktivní**.

Rozděluje umístění v síti na **interní** nebo **externí** a největší roli zde má nastavení **interní domény**, které musí být definováno ve **Skupině Zařízení**. Pokud HOS detekuje správnou odpověď na **Interní doménu**, je síťové umístění určeno jako **interní**. Detekce se provádí spuštěním dotazu DNS na nakonfigurovanou interní doménu a obdržením nakonfigurované odpovědi.

24.2 Stavy

HOS neustále sleduje změny na síťových rozhraních a na základě podmínek mění své stavy.

`Aktivní`
: Veškerý provoz DNS je přesměrován na server DoH. HOS se stává **Aktivním**, když je připojen k veřejné síti, ale **Interní doména** je nedostupná. Tento stav se používá pro nebezpečné zóny, jako je veřejná wi-fi.

`Neaktivní`
: DNS trafic zůstává nedotčen. Tento stav se používá, když se zařízení nemůže připojit k internetu nebo když je připojeno přes vnitřní síť.

24.3 Bezpečnost

Na pozadí HOS používá **DNS-over-HTTPs** neboli **DoH**. Název **Hostname** z **Resolveru** není nikdy přesměrován a je uložen v mezipaměti. Identifikace a autentizace je ponechána na protokolu TLS. Pokud zařízení patří k libovolné **Doméně**, pak je všem doménovým jménům a jejich subdoménám umožněno přistoupit k serverům DNS, na které jsou směrovány. HOS používá k získání informací tabulku `Win32_NetworkAdapterConfiguration` WMI.

24.4 Systémové požadavky

24.4.1 Windows

Protože služba HOS musí zachytávat síťový provoz, musí být spuštěna jako **SYSTEM**. Můžete se dotázat na služby podle názvu **hos** a zjistit, zda se správně spustila. Pokud není zadán žádný nebo je zadán neplatný instalační token, služba se zastaví.

```
C:\Users\admin>sc query "Whalebone Home Office Security"

SERVICE_NAME: HOS
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Při prvním spuštění HOS nainstaluje také systémový ovladač `windivert`.

```
C:\Users\admin>sc query windivert type=kernel

SERVICE_NAME: windivert
        TYPE               : 1  KERNEL_DRIVER
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Služba je nakonfigurována tak, aby se po pádu třikrát pokusila o opětovné spuštění a poté zůstala zastavena.

24.4.2 Android

Aplikace pro systém Android má přístup k:

- Poloha
  - K přesné poloze (GPS a síťové)
- Fotoaparát
  - K pořizování snímků a videí (skenování QR kódu skupiny zařízení z portálu)

- Informace o připojení Wi-Fi
  - Zobrazení připojení Wi-Fi
- Ostatní
  - Zobrazení síťových připojení
  - Připojení a odpojení od sítě Wi-Fi
  - Úplný přístup k síti (pro vytvoření tunelu VPN k resolverům Whalebone Cloud)
  - Spustit při spuštění

24.5 Nastavení brány firewall pro aplikace

V aplikační bráně firewall povolte port TCP 443 pro **Whalebone Home Office Security.exe**. Chcete-li jej povolit pro všechny síťové profily v systému Windows, upravte následující příkaz tak, aby se služba HOS mohla připojit k vašemu serveru DoH (např. 185.150.10.71):

Pokud služba HOS nefunguje, zajistěte, aby se služba HOS mohla připojit k **hos.whalebone.io** a **mobileapi.whalebone.io**.

```
netsh advfirewall firewall add rule name="Whalebone Home Office Security" dir=out␣
↪action=allow program="C:\Program Files (x86)\Whalebone\Home Office Security\Whalebone␣
↪Home Office Security.exe" enable=yes remoteip=185.150.10.71,LocalSubnet
```

Není nutné, aby služba naslouchala na portu 53. Kromě toho služba naslouchá na **TCP endpointu localhost:9000**, aby poskytla datový endpoint pro aplikaci UI, a server aplikace UI **whosui.exe** naslouchá na **TCP endpointu localhost:55221**, aby vykresloval grafické komponenty. I když tyto porty nejsou pro provoz HOS kritické, jsou důležité pro aplikaci UI **AdminUI.exe**. Zajistěte, aby služby měly povoleno naslouchat na těchto místních portech, protože to umožňuje uživateli nahlédnout do provozu aplikace.

24.6 Aplikační Logy

Nacházejí se na adrese `c:\ProgramData\Whalebone\Home Office Security\Logs\`, obsahují podrobné informace o stavech a provozu aplikace. V případě, že se setkáte s neočekávaným chováním služby, zašlete obsah složky Log a/nebo složly Config spolu se svým dotazem na podporu. Aplikace poskytuje další informace pro sledování provozu, v aplikaci AdminUI.exe, karta Události vám může poskytnout lepší přehled o provozu HOS.

24.7 Odinstalování aplikace

Chcete-li aplikaci zcela odstranit, odinstalujte službu a odstraňte veškerý obsah z `c:\ProgramData\Whalebone\Home Office Security\`.

CHAPTER 25

Nasazení

25.1 Nasazení lokálního resolveru

Na rozdíl od jiných podobných služeb lze Whalebone nasadit jako plnohodnotný lokální resolver DNS. Tento typ nasazení doporučujeme. Instalace je poměrně jednoduchá. Potřebujete pouze přístup k portálu Whalebone Portal a virtuální nebo fyzický server, který je z hlediska hardwaru poměrně nenáročný. Z hlediska systémových požadavků Whalebone podporuje nejnovější verze nejpoužívanějších linuxových distribucí Debian, Ubuntu, CentOS a Red hat Enterprise Linux. Minimální velikost hardwaru jsou 2 jádra CPU, 4 GB RAM a 40 GB pevný disk. Takový stroj zvládne až 20 000 uživatelů.

Před nastavením serveru se ujistěte, jestli splňujete síťové požadavky a nebráníte přístupu na server zvenčí. Jakmile je server připraven, přejděte na portál Whalebone a vytvořte nový resolver. Vymyslete vhodný název, který můžete později změnit. Jakmile iniciujete přidání nového resolveru, zobrazí se jednořádkový příkaz instalačního skriptu. Zkopírujte jej do schránky. V tomto okamžiku přistupte k terminálu serveru vytvořeného pro tento resolver. Zbývá jen spustit instalační skript dříve zkopírovaný do schránky. Instalace by neměla trvat déle než několik minut. Skript vás bude informovat o jejím průběhu. Pokud instalace neproběhla úspěšně, zašlete nám protokol o instalaci a my se na to podíváme. Zanedlouho se stav resolveru změní. Jakmile se resolver stane aktivním, můžete na něj směrovat provoz a začít chránit svou síť.

25.2 Cloudové resolvery

Whalebone nabízí také cloudové resolvery s ochranou proti malwaru a blokováním obsahu. Jejich adresy najdete v portálu Whalebone na kartě Cloudový resolver. Můžete je používat přímo jako primární nebo sekundární resolvery nebo jako zálohu ke stávajícímu lokálnímu resolveru.

Pro konfiguraci zadejte své veřejné rozsahy IP, které chcete nasměrovat na cloudové resolvery. Poté stačí nastavit adresu cloudového resolveru Whalebone jako adresu serveru DNS ve vaší síti. Stejně jako u místních resolverů můžete vytvořit různé zásady a přiřadit je jednotlivým IP adresám nebo rozsahům. To vám umožní nabízet službu Whalebone institucím, například školám, které nutně nezískávají konektivitu od vás, ale vy spravujete jejich síť. Po uložení a nasměrování provozu stačí počkat, až se změny rozšíří mezi vaše klienty.

CHAPTER 26

Konfigurace

26.1 Základní konfigurace

Každá síť má své specifické potřeby. Whalebone se dokáže přizpůsobit každé z nich a přizpůsobí se jí. Jednou z klíčových součástí, které je třeba při implementaci systému Whalebone nakonfigurovat, je nastavení „bezpečnostních politik“. Tato část konfigurace umožňuje upravit výchozí nastavení. Můžete například snížit práh blokování nebo blokování zcela deaktivovat, čímž vám zůstane režim auditu. V tomto režimu Whalebone sleduje incidenty, aniž by jim bránil. Základem konfigurace auditu a blokování je takzvané „skóre“, které jednotlivým doménám přiřazuje náš algoritmus. Čím vyšší je skóre, tím je doména nebezpečnější. Je na vás, zda si vyberete z přednastavených úrovní citlivosti, nebo se rozhodnete nastavit práh ručně. Sítím poskytovatelů internetových služeb doporučujeme „Blokovat opatrně“. Čím nižší je prahová hodnota, tím citlivější je blokování. Mějte však na paměti, že nastavení nízkého prahu zvyšuje riziko falešných pozitivních výsledků.

Můžete si také vybrat různé typy hrozeb, které mají být blokovány. V případě potřeby si můžete snadno vytvořit vlastní blokační seznamy nebo definovat domény, které mají být vždy přístupné. Našim zákazníkům se líbí, že Whalebone dokáže splnit zákonné požadavky na blokování jejich vlády za ně. Pokud nenajdete svou zemi na našem seznamu, dejte nám vědět a my se postaráme, aby se tam dostala. Pokud jste si aktivovali doplněk pro filtrování obsahu, můžete jej nakonfigurovat také zde. Vytvořte si libovolný počet jedinečných zásad zabezpečení. Poté můžete přejít do konfigurace daného resolveru a přiřadit tyto zásady různým IP adresám nebo rozsahům. Stačí, když v podrobnostech o resolveru přejdete do části „Přiřazení zásad“. a přiřadit zásady konkrétní IP adrese nebo rozsahu. Nezapomeňte nastavení uložit.

26.2 Bezpečnostní politiky

Jednou z klíčových součástí, které je třeba při implementaci systému Whalebone nakonfigurovat, je nastavení bezpečnostních politik. Tato část konfigurace umožňuje upravit výchozí nastavení. Můžete například snížit práh blokování nebo blokování zcela deaktivovat. což vám ponechá režim jen auditu. V tomto režimu Whalebone sleduje incidenty, aniž by jim bránil. Jádrem konfigurace auditu a blokování je tzv. skóre. které je jednotlivým doménám přiřazeno naším algoritmem. Čím vyšší je skóre, tím je doména nebezpečnější. Je na vás, zda si vyberete z přednastavených úrovní citlivosti, nebo se rozhodnete nastavit práh ručně.

Síti ISP doporučujeme **blokovat opatrně** Čím nižší je prahová hodnota, tím citlivější je blokování. Mějte však na paměti, že nastavení nízké prahové hodnoty zvyšuje riziko falešných pozitivních výsledků. Můžete také zvolit různé typy hrozeb, které mají být blokovány.

V případě potřeby si můžete snadno vytvořit vlastní seznam blokování nebo definovat domény, které mají být vždy přístupné. Našim zákazníkům se líbí, že Whalebone za ně dokáže splnit zákonné požadavky na blokování ze strany jejich vlády. Pokud v našem seznamu nenajdete svou zemi, dejte nám vědět a my se postaráme o nápravu.

Pokud jste si aktivovali doplněk pro filtrování obsahu, můžete jej nakonfigurovat také zde. Vytvořte si libovolný počet jedinečných zásad zabezpečení. Poté můžete přejít do konfigurace daného řešení a přiřadit tyto zásady různým IP adresám nebo rozsahům. Stačí, když v detailu resolveru přejdete do části **Přiřazení zásad**. a přiřadit zásady konkrétní IP adrese nebo rozsahu. Nezapomeňte nastavení uložit.

26.3 Konfigurace bokační stránky

Pomocí Whalebone portálu můžete plně přizpůsobit blokáční stránky, které se zobrazí v případě, že se někdo pokusí ve svém prohlížeči přistoupit na nebezpečnou webovou stránku. Tento nástroj potřebuje místní resolver, u kterého můžete blokovací stránku přepnout z cloudu na lokální. Chcete-li nakonfigurovat blokační stránky, přejděte do části **Konfigurace** a poté do části **Blokační stránky**. Můžete upravit ty stávající nebo vytvořit zcela nové. Při vytváření nové blokující stránky můžete definovat její název, doménu a jazyk stránky. Poté vyplňte všechny potřebné údaje včetně názvu společnosti, jejího loga a kontaktních informací. Tyto informace můžete samozřejmě později změnit. Pokud tak chcete učinit, použijte kouzelnou hůlku nebo upravujte přímo v kódu HTML. Design i obsah blokační stránky můžete upravit podle svého uvážení. Stačí, když zachováte potřebné proměnné zobrazené nad blokovacím polem.

Jakmile uložíte upravenou blokační stránku, přejděte do části **Resolvery** a vyberte resolver, na kterého chcete blokační stránku použít. Přejděte na **Přiřazení politik** a přiřaďte blokační stránku na daný resolver. Případně ji můžete přiřadit konkrétní IP adrese nebo rozsahu. Když už jste u toho, můžete také aktivovat **bypass**, který uživateli přesto umožní přístup k blokované doméně. .. raw:: html

<iframe width="560" height="315" src="https://www.youtube.com/embed/K0p2l-qxHtk" title="YouTube video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture" allowfullscreen></iframe>

26.4 Alerty

Nastavte si alerty a získávejte živě aktualizace o tom, co se děje s Vašimi resolvery, jak je vaše síť zabezpečená a jak dobře funguje překlad DNS. Základní nastavení je jednoduché: stačí si vybrat, jaký typ informací chcete dostávat a jak často chcete být upozorňováni. Upozornění můžete dostávat prostřednictvím e-mailu, nebo služby Slack. Upozornění Whalebone můžete také integrovat do svých systémů prostřednictvím Webhooku nebo syslogu. Velmi doporučujeme alespoň základní nastavení alertů pro monitorování překladu a funkčnost serveru na kterém resolver běží.

Určitě začněte nastavením výstrah pro selhání překladu. Poté nastavte výstrahy pro selhání hardwarových prostředků, například nedostatek místa místa na disku, RAM nebo CPU. Můžete také sledovat selhání komunikace mezi resolverem a Whalebone cloudem, kdy rozlišení funguje v pořádku, ale resolver není synchronizován s datovými centry Whalebone.

Můžete dokonce vytvářet pokročilá upozornění na provoz DNS a bezpečnostní incidenty. S nastavením pokročilých výstrah vám rádi pomůžeme, ať už během úvodní technické konzultace, na konci zkušební verze nebo kdykoli se rozhodnete kontaktovat podporu společnosti Whalebone.

CHAPTER 27

Analýza

27.1 Analýza domény

Existují dva způsoby, jak ručně provést analýzu domény v databázi Whalebone. Jedním ze způsobů je pomocí nástroje **Analýza domény** z uživatelské nabídky. Druhou možností je zkontrolovat konkrétní doménu přímo z kontextové nabídky v přehledech **Hrozby** nebo **DNS provoz**. Poté se zobrazí všechny informace které společnost Whalebone o dané doméně shromáždila. Jako příklad jsme použili stránku **kidos-bank.ru**. Vidíme, že s doménou jsou spojeny různé typy hrozeb. Její skóre je 80-100 a v březnu 2021 byla označena jako nebezpečná. V následujících grafech můžete vidět vývoj detekcí, respektive DNS požadavků na překlad domény v síti. Výsledek analýzy také ukazuje, že doméně není přiřazena kategorie obsahu a její blokování nebylo provedeno nařízena ze zákona. Takto se můžete dotázat na jakoukoli doménu. Stačí ji zadat do textového pole **Doména ke kontrole**. Vidíme, že doména **facebook.com** není považována za bezpečnostní hrozbu, probíhá na ní poměrně velký provoz a Whalebone ji kategorizuje jako **sociální síť**. Pokud zadáme **porn.com**, vidíme, že se kategorie změnila na **Sexuální obsah**.

27.2 Provoz DNS

V protokolu „DNS traffic“ si můžete prohlédnout časovou osu požadavků a odpovědí DNS za posledních 1, 7 nebo 14 dní. V dashboardu je zobrazen první překlad domény danou IP adresou za posledních 24 hodin, typ dotazu, výsledek řešení, zdrojovou a cílovou IP adresu. Vyhledávání je možné pomocí zakliknutí konrkrétních hodnot a také pomocí fulltextu.

Souhrnné grafy pod hlavní časovou osou zobrazují přehled nejčastějších odpovědí, domén druhé úrovně a IP adres s největším provozem. Všechna data jsou přístupná také ve formátu tabulky a můžete je dokonce exportovat do souboru CSV s maximálním počtem 1 000 000 řádků. Protokoly o provozu DNS jsou dočasně uloženy na serveru resolveru. Odtud k nim můžete přistupovat pro vlastní zpracování. Jednou z největších výhod sledování dat o provozu DNS je

možnost filtrování chyb v odpovědích, jako jsou NXDOMAIN a SERVFAIL. To umožňuje zobrazit škodlivý provoz na zařízeních připojených k síti. Toto video ukazuje zahashovanou IP adresu s téměř 240 000 překlady různých domén, které vedou k chybám NXDOMAIN a SERVFAIL. Můžete zde vidět veřejné i soukromé IP adresy.

Toto zobrazení je obzvláště užitečné, pokud do filtru přidáte další dotazy, například **MX**. Takové nastavení filtru vám ukáže IP adresy ve vaší síti, které rozesílají spam, a hrozí tedy, že se dostanou na černou listinu a následně ohrozí i ostatní zákazníky, pokud jsou za NAT. Podobně můžete zvolit například dotazy **A**. Specializujeme se na detekci škodlivé komunikace DGA. Klienti, kteří jsou takto infikováni, se připojují ke kvazi náhodně generovaným doménám, které se snaží komunikovat s řídicím centrem malwaru.

27.3 Hrozby

Whalebone se zaměřuje na ochranu vaší sítě. Proto máte přístup ke kompletnímu přehledu incidentů, které se staly za posledních 90 dní. Přehled nabízí nejen informace, ale také možnost filtrace a analýzy dat. Výsledky jsou rozděleny do tří kategorií: události, které byly zablokovány, auditovány a povoleny. Auditované domény představují domény, které jsou poněkud podezřelé. Jejich skóre je dostatečně vysoké na to, aby byly uvedeny v protokolu, ale nižší, než je práh blokování. Pokud jde o blokované domény, resolver vrací plně přizpůsobenou stránku blokování s volitelným tlačítkem pro obejití.

Data můžete také filtrovat podle typu incidentu. Podívejme se na příklad komunikace s řídicím centrem malwaru. Vidíme konkrétní blokované domény a také místní nebo veřejné IP adresy, které se k nim pokoušely přistupovat. Toto je příklad aktivního intenzivního provozu z konkrétní IP adresy a komunikace s malwarem Necurs. Takto infikovaný klient by ovlivnil i kvalitu připojení ostatních klientů. Pro každý jednotlivý záznam můžete v kontextové nabídce zvolit různé typy kontroly domény. Velmi praktické je zahájit analýzu vygooglováním domény. Nejčastěji vám však výsledky pouze sdělí, že doména je nebezpečná.

Dalším způsobem kontroly domény je použití různých bezpečnostních zdrojů. Příkladem takové služby je velmi užitečná webová stránka **Virustotal**. Pokud ani po analýze nejste přesvědčeni, že k zablokování byl dobrý důvod, neváhejte nám takovou doménu **nahlásit**. Případ prověříme a ozveme se vám. V případě, že se skutečně ukáže, že se jedná o falešně pozitivní blokaci, globálně povolíme přístup k doméně všem zákazníkům Whalebone zákazníkům.

27.4 Analýza dat

Portál Whalebone umožňuje podrobnou fulltextovou filtraci a související analýzu dat. Důkladný manuál naleznete v technické dokumentaci dostupné na adrese docs.whalebone.io. v části Analýza dat. Najdete zde seznam různých operátorů, příklady jejich použití a odkazy na možné rozdíly mezi přehledem provozu DNS a hrozeb. Můžete používat zástupné nebo logické operátory. Při použití fulltextové filtrace, je třeba všechny parametry zadat přímo do adresy URL. Tímto způsobem můžete snadno vytvářet filtry pro budoucí použití.

27.5 API

Pomocí rozhraní Whalebone API můžete integrovat Whalebone do svých vlastních systémů. Nejprve je třeba vytvořit nový klíč. Přejděte do konfigurace klíčů API z kontextové nabídky kliknutím na ikonu panáčka. Po vytvoření nového klíče API se zobrazí všechny potřebné údaje. Secret API klče nebude nikdy znovu zobrazen, proto se ujistěte, že jste si jej skutečně a správně zkopírovali. Klíč API můžete kdykoli zneplatnit. Stačí kliknout na příslušnou ikonu. K dispozici máme podrobnou interaktivní dokumentaci pro rozhraní Whalebone API dostupnou na apidocs.whalebone.io/public, nebo pomocí kliknutí na ikonu otazníku. Dokumentace vás provede různými kategoriemi informací a nastavení s konkrétními příklady. Část „Event“ obsahuje veškeré informace o hrozbách, například typy hrozeb a domény. Můžete dokonce modelovat API volání přímo v dokumentaci a ihned je používat. Kromě toho rozhraní API obsahuje určité informace, které zatím nejsou k dispozici na portálu Whalebone, například podrobnosti o ověřování DNSSEC. Samozřejmě můžete přistupovat k informacím o resolverech, jako je latence, stav resolverů nebo využití systémových prostředků. Než začnete modelovat volání API v dokumentaci, doporučujeme ji autorizovat pomocí klíčů API. To vám umožní přímo pracovat s vaším účtem v dokumentaci.

27.6 Řešení problémů s překladem domény

Když uživatelé internetu nemají přístup k doméně, často si myslí, že je to chyba poskytovatele internetu. Nejčastěji se však nejedná o problém poskytovatele, ale samotné domény. Bez ohledu na to musíte zákazníkovi stejně odpovědět a vysvětlit mu situaci. Pojďme se podívat, jak Whalebone tento proces zjednoduší.

Nejprve prozkoumejte potenciální zablokování domény vyhledáním domény v části **Hrozby**. Doporučujeme používat vyhledávací operátory a dotazovat se na subdomény. Ukázalo se, že doména **sufr.cz** nebyla zablokována jako hrozba. Druhým krokem je přejít do **DNS provozu** a zkontrolovat, zda k doméně vůbec někdo přistupoval. Pokud ano, podívejte se, jak se Whalebone vypořádává s překladem. Ukazuje se, že k pokusům o přístup k doméně došlo. V takovém případě musíme zkontrolovat výsledky. Vidíme, že odpověď pro tuto doménu byla **SERVFAIL**. Pro další postup řešení problémů můžeme analyzovat doménu prostřednictvím kontextové nabídky.

Doporučujeme použít nástroj **DNS Viz**. Nástroj DNS Viz je určen k úplné kontrole chování překladu DNS. Přímé prokliknutí vede k výsledkům ověření DNSSEC. Ukazuje se, že problém této konkrétní domény spočívá v tom, že má problémy s **prošlými kryptografickými podpisy**. Pokud máte pocit, že stále nevíte, co se s doménou děje, neváhejte nás kontaktovat e-mailem na adrese support@whalebone.io. Rádi se na Váš problém podíváme.

27.7 Sledování domén

Pro funkční připojení k internetu je nezbytné dobře fungující DNS překlad. Proto se můžete v portálu pro správu ujistit, že jednotlivé resolvery fungují v pořádku. Stačí vybrat příslušný místní resolver, otevřít kontextovou nabídku a kliknout na tlačítko **Trace domény**. V tomto okamžiku zadejte doménu, kterou chcete zkoumat. Řekněme, že je to whalebone.io.

Vyberte jeden z typů dotazů, například **A**, a doménu vytrasujte. Výsledek řešení si můžete prohlédnout zde. V horní části je zobrazen výsledek dotazu. Zelená barva vám říká, že s překladem DNS není nic v nepořádku. Pokud se vyskytne nějaký problém, budou informace o konkrétním problému uvedeny oranžovou nebo červenou barvou. Například pokud doména neexistuje, bude výsledkem **NXDOMAIN** V případě, že je s rozlišením problém, zobrazí se odpověď **SERVFAIL**. Pokud narazíte na nějaké problémy, pošlete protokol na adresu **support@whalebone.io** a my Vám pomůžeme s investigací.

CHAPTER 28

Odmítnutí odpovědnosti za licenci

Resolver Whalebone využívá ve svém řešení následující technologie:

28.1 variantu CRC64 s Jonesovým koeficientem

```
Copyright (c) 2012, Salvatore Sanfilippo <antirez at gmail dot com>.
Všechna práva vyhrazena.

Šíření a používání ve zdrojové i binární podobě, s nebo bez
úpravami, jsou povolena za předpokladu, že jsou splněny následující podmínky:

* Redistribuce zdrojového kódu musí zachovat výše uvedené upozornění na autorská práva,
  tento seznam podmínek a následující prohlášení o vyloučení odpovědnosti.
* Redistribuce v binární podobě musí obsahovat výše uvedené informace o autorských␣
↪právech.
  a tento seznam podmínek a následující prohlášení o vyloučení odpovědnosti.
  dokumentaci a/nebo v dalších materiálech dodávaných s distribucí.
* Nesmí být použito jméno Redis ani jména jeho přispěvatelů.
  k podpoře nebo propagaci produktů odvozených z tohoto softwaru, aniž by bylo prokázáno,
↪ že se jedná o produkty, které
  předchozího písemného souhlasu.

TENTO SOFTWARE JE POSKYTOVÁN DRŽITELI AUTORSKÝCH PRÁV A PŘISPĚVATELI "TAK, JAK JE".
A JAKÉKOLI VÝSLOVNÉ NEBO PŘEDPOKLÁDANÉ ZÁRUKY, VČETNĚ, ALE NEOMEZUJÍCÍ SE NA
PŘEDPOKLÁDANÝCH ZÁRUK PRODEJNOSTI A VHODNOSTI PRO URČITÝ ÚČEL.
JSOU VYLOUČENY. V ŽÁDNÉM PŘÍPADĚ NEJSOU VLASTNÍCI AUTORSKÝCH PRÁV ANI PŘISPĚVATELÉ
ODPOVĚDNÍ ZA JAKÉKOLI PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, ZVLÁŠTNÍ, EXEMPLÁRNÍ NEBO JINÉ ŠKODY,␣
↪KTERÉ BY MOHLY VZNIKNOUT V SOUVISLOSTI S JEJICH
NÁSLEDNÉ ŠKODY (VČETNĚ, ALE BEZ OMEZENÍ NA, OBSTARÁVÁNÍ
NÁHRADNÍHO ZBOŽÍ NEBO SLUŽEB, ZTRÁTY UŽITÍ, DAT NEBO ZISKŮ NEBO ZTRÁTY OBCHODNÍCH␣
↪PŘÍLEŽITOSTÍ.
```

(continues on next page)

(pokračujte na předchozí stránce)

```
PŘERUŠENÍ PROVOZU), AŤ UŽ BYLY ZPŮSOBENY JAKÝMKOLI ZPŮSOBEM A NA ZÁKLADĚ JAKÉKOLI TEORIE␣
↪ODPOVĚDNOSTI, AŤ UŽ V RÁMCI
SMLOUVĚ, PŘÍSNÉ ODPOVĚDNOSTI NEBO DELIKTU (VČETNĚ NEDBALOSTI NEBO JINÉHO).
VZNIKLÉ JAKÝMKOLI ZPŮSOBEM V SOUVISLOSTI S POUŽÍVÁNÍM TOHOTO SOFTWARU, A TO I V PŘÍPADĚ,␣
↪ŽE JSTE BYLI NA TYTO SKUTEČNOSTI UPOZORNĚNI.
MOŽNOST VZNIKU TAKOVÉ ŠKODY.
```

28.2 Knihovna Lightning.NET

```
Veřejná licence OpenLDAP
Verze 2.8, 17. srpna 2003

Šíření a používání tohoto softwaru a související dokumentace
(dále jen "software"), s úpravami nebo bez nich, je povoleno za předpokladu, že
pokud jsou splněny následující podmínky:

1. Redistribuce ve formě zdrojových kódů musí zachovat prohlášení o autorských právech.
a upozornění,

2. Redistribuce v binární podobě musí obsahovat příslušné záznamy o autorských právech.
prohlášení a upozornění, tento seznam podmínek a následující údaje
zřeknutí se odpovědnosti v dokumentaci a/nebo v dalších poskytnutých materiálech
s distribucí, a

3. Redistribuce musí obsahovat doslovnou kopii tohoto dokumentu.

Nadace OpenLDAP může tuto licenci čas od času revidovat.
Každá revize je označena číslem verze.  Můžete používat
tento software za podmínek této revize licence nebo za podmínek této revize licence.
podmínek jakékoli následující revize licence.

TENTO SOFTWARE POSKYTUJE NADACE OPENLDAP A JEJÍ
"TAK, JAK JE", A JAKÉKOLIV VÝSLOVNÉ NEBO PŘEDPOKLÁDANÉ ZÁRUKY,
VČETNĚ, ALE NIKOLIV VÝLUČNĚ, PŘEDPOKLÁDANÝCH ZÁRUK PRODEJNOSTI. A VHODNOSTI PRO URČITÝ␣
↪ÚČEL JSOU VYLOUČENY.  V ŽÁDNÉM PŘÍPADĚNADACE OPENLDAP, JEJÍ PŘISPĚVATELÉ NEBO␣
↪AUTOR(É)NEBO VLASTNÍK(CI) SOFTWARU NENESOU ODPOVĚDNOST ZA JAKÉKOLI PŘÍMÉ, NEPŘÍMÉ,
NÁHODNÉ, ZVLÁŠTNÍ, EXEMPLÁRNÍ NEBO NÁSLEDNÉ ŠKODY (VČETNĚ,
MIMO JINÉ ZA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ NEBO SLUŽEB;ZTRÁTU POUŽÍVÁNÍ, DAT NEBO ZISKU␣
↪NEBO PŘERUŠENÍ PROVOZU), AŤ UŽ SE JEDNÁ O JAKOUKOLI ŠKODU.
ZPŮSOBENÉ A NA ZÁKLADĚ JAKÉKOLIV TEORIE ODPOVĚDNOSTI, AŤ UŽ SMLUVNÍ, PŘÍSNÉ, NEBO␣
↪NEPŘÍMÉ.
ODPOVĚDNOSTI NEBO DELIKTNÍ ODPOVĚDNOSTI (VČETNĚ NEDBALOSTI NEBO JINÉ), KTERÁ VZNIKLA V␣
↪DŮSLEDKUJAKÝMKOLI ZPŮSOBEM V SOUVISLOSTI S POUŽÍVÁNÍM TOHOTO SOFTWARU, A TO I V␣
↪PŘÍPADĚ, ŽE JSTE BYLI UPOZORNĚNI NA TYTO SKUTEČNOSTIMOŽNOST VZNIKU TAKOVÉ ŠKODY.

Jména autorů a držitelů autorských práv nesmí být použita v.
v reklamě nebo jinak propagovat prodej, používání nebo jiné nakládání s autorskými právy.
s tímto softwarem bez předchozího písemného souhlasu.  Název
k autorským právům k tomuto softwaru zůstává po celou dobu u autorských práv
držitelům autorských práv.
```

(continues on next page)

(pokračujte na předchozí stránce)

```
OpenLDAP je registrovaná ochranná známka nadace OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA.  Všechna práva vyhrazena.  Povolení ke kopírování a
šířit doslovné kopie tohoto dokumentu.
```