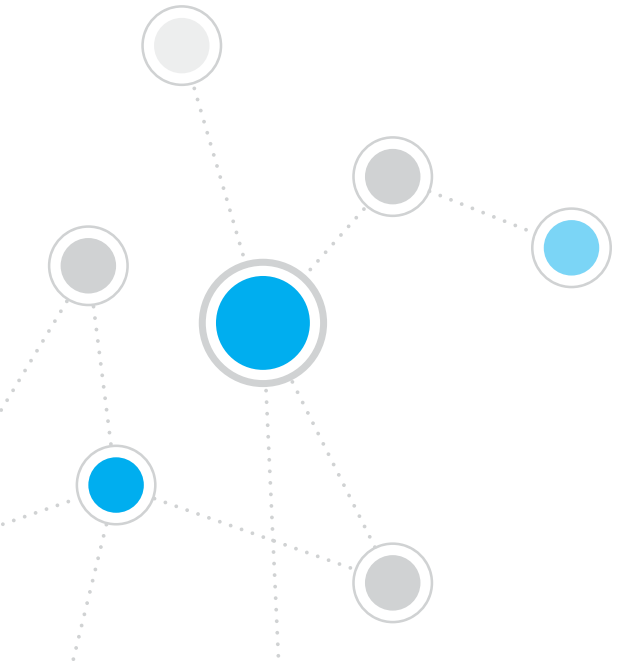
ForeScout

ForeScout CounterACT® 7

Samostatné zařízení CounterACT

Příručka pro rychlou instalaci



Obsah

Vítejte u ForeScout CounterACT® Verze 7

ForeScout CounterACT je fyzické nebo virtuální bezpečnostní zařízení, které dynamicky identifikuje a ohodnocuje síťová zařízení a aplikace v momentě jejich připojení k síti. Protože CounterACT nevyžaduje žádné agenty, funguje s Vašimi zařízeními – řízenými i neřízenými, známými i neznámými, PC i mobilními, vestavěnými i virtuálními. CounterACT rychle určí uživatele, vlastníka, operační systém, konfiguraci zařízení, software, služby, stav patche a přítomnost bezpečnostních agentů. Dále poskytuje nápravu, řízení a nepřetržité monitorování těchto zařízení při připojování a odpojování od sítě. Toto všechno zvládne při hladké integraci do Vaší existující IT infrastruktury.

Tato příručka popisuje instalaci jednoho samostatného zařízení CounterACT.

Podrobnější informace nebo informace o instalaci více těchto zařízení pro firemní sítě viz *Instalační příručka CounterACT a Příručka uživatele konzole*. Tyto dokumenty jsou umístěny na CounterACT CD ve složce /docs.

Kromě toho můžete také navštívit webové stránky podpory: https://www.forescout.com/support, kde naleznete aktuální dokumentaci, znalostní databázi a aktualizace pro své zařízení.

Obsah balíčku CounterACT

- Zařízení CounterACT
- Příručka pro rychlou instalaci
- CounterACT CD s konzolovým softwarem, Příručku uživatele konzole CounterACT a Instalační příručku
- Záruční list
- Montážní držáky
- Napájecí kabel
- DB9 kabel pro připojení konzole (pouze pro sériová zapojení)

Přehled

Postup nastavení zařízení CounterACT:

1. Vytvoření plánu instalace
2. Nastavení switche (přepínače)
3. Zapojení síťových kabelů a napájení
4. Konfigurace zařízení
5. Vzdálená správa
6. Ověření konektivity
7. Nastavení konzole CounterACT

1. Vytvoření plánu instalace

Před provedením instalace byste se měli rozhodnout, kam umístíte zařízení, a prostudovat prvky rozhraní.

Rozhodnutí o umístění zařízení

Výběr správného síťového umístění pro zařízení je klíčový pro úspěšnou instalaci a optimální výkon CounterACT. Správné umístění bude záviset na vámi požadovaných cílech implementace a zásadách síťového přístupu. Zařízení by mělo monitorovat síťový provoz, který je důležitý pro požadované zásady. Například pokud vaše zásady síťového přístupu závisí na monitorování autorizačních událostí z koncových bodů na firemní autorizační servery, zařízení bude třeba nainstalovat tak, aby vidělo provoz plynoucí z koncových bodů na autorizační servery.

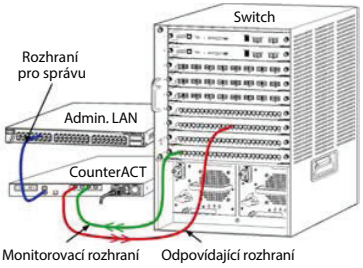
Více informací o instalaci naleznete v Instalační příručce CounterACT, která je na CounterACT CD přibaleném do tohoto balíčku.

Zapojení prvků rozhraní zařízení

Zařízení je běžně konfigurováno se třemi zapojeními do síťového switche.

Rozhraní pro správu

Toto rozhraní umožňuje spravovat CounterACT a provádět požadavky na koncové body a jejich hlubokou kontrolu. Rozhraní musí být připojeno k portu switche, který má přístup ke všem síťovým koncovým bodům.



Každé zařízení vyžaduje jedno připojení pro správu k síti. Toto připojení vyžaduje IP adresu na lokální síti LAN a přístup k portu 13000/TCP z počítačů, na kterých poběží aplikace pro správu konzole CounterACT. Rozhraní pro správu musí mít přístup k následujícím portům vaší sítě:

Port	Služba	Z nebo do CounterACT	Funkce
22/TCP	SSH	do	Umožňuje přístup k rozhraní příkazové řádky CounterACT.
2222/TCP			(Vysoká dostupnost) Umožňuje přístup k fyzickým zařízením CounterACT, která jsou součástí clusteru s vysokou dostupností. Použijte 22/TCP pro přístup ke sdíleným (virtuálním) IP adresám na clusteru.

Port	Služba	Z nebo do CounterACT	Funkce
25/TCP	SMTP	z	Slouží pro posílání pošty ze zařízení CounterACT
53/UDP	DNS	z	Umožňuje zařízení CounterACT rozlišovat interní IP adresy.
80/TCP	HTTP	do	Umožňuje přesměrování HTTP.
123/UDP	NTP	z	Umožňuje zařízení CounterACT přístup k časovému serveru NTP. Ve výchozím nastavení používá CounterACT server ntp.foreScout.net.
135/TCP	MS-WMI	z	Umožňuje vzdálenou kontrolu koncových bodů Windows.
139/TCP	SMB, MS-RPP	z	Umožňuje vzdálenou kontrolu koncových bodů Windows (koncové body pod Windows verze 7 a nižší).
445/TCP			Umožňuje vzdálenou kontrolu koncových bodů Windows.
161/UDP	SNMP	z	Umožňuje CounterACT komunikovat se síťovou infrastrukturou, např. switchi a routery. Informace ohledně konfigurace SNMP naleznete v *Příručce uživatele konzole CounterACT*.
162/UDP	SNMP	do	Umožňuje CounterACT přijímat zprávy (trap) ze síťové infrastruktury, např. switchů a routerů. Informace ohledně konfigurace SNMP naleznete v *Příručce uživatele konzole CounterACT*.
443/TCP	HTTPS	do	Umožňuje přesměrování HTTP pomocí TLS.
2200/TCP	Secure Connector	do	Umožňuje funkci SecureConnector vytvořit bezpečné připojení (kódované pomocí SSH) k zařízení z počítačů se systémem MacOS/Linux. *SecureConnector* je skriptovací agent, který umožňuje správu koncových bodů MacOS a Linux při jejich připojení k síti.
10003/TCP	Secure Connector pro Windows	do	Umožňuje funkci SecureConnector vytvořit bezpečné připojení (kódované pomocí TLS) k zařízení z počítačů se systémem Windows. *SecureConnector* je agent umožňující správu koncových bodů Windows při jejich připojení k síti. Pro více informací o funkci SecureConnector se prosím odkažte do Uživatelského manuálu zařízení CounterACT.

			Při připojení agenta SecureConnector k zařízení nebo firemnímu správci (Enterprise Manager) je přesměrován na zařízení, ke kterému je přiřazen jeho host. Zajistěte, aby byl tento port otevřený pro všechna zařízení a pro Enterprise Managera pro transparentní pohyb v rámci organizace.
13000/TCP	CounterACT	do	Umožňuje propojení konzole a zařízení. U systémů s více zařízeními CounterACT umožňuje propojení konzole a firemního manažeru (Enterprise Manager) a propojení firemního manažeru s každým zařízením.

Monitorovací rozhraní

Toto zapojení umožňuje zařízení monitorovat a sledovat provoz sítě.

Provoz je zrcadlen na port na switchi a monitorován zařízením. Podle počtu monitorovaných sítí VLAN může nebo nemusí být provoz označen značkou 802.1Q VLAN.

- **Jedna VLAN (bez značky):** Když je monitorovaný provoz vytvářen z jediné VLAN, zrcadlený provoz není třeba označit jako VLAN.
- **Více VLAN (se značkou):** Když je monitorovaný provoz z více než jedné sítě VLAN, zrcadlený provoz *musí* být označen jako 802.1Q VLAN.

Když jsou dva switche připojeny jako redundantní pár, musí zařízení monitorovat provoz z obou switchů.

Monitorovací rozhraní nevyžaduje IP adresu.

Odpovídací rozhraní

Zařízení odpovídá na provoz pomocí tohoto rozhraní. Odpovídací provoz slouží k ochraně proti škodlivým aktivitám a provádění akcí dle zásad NAC. Mezi takové akce může patřit například přesměrování webových prohlížečů nebo provedení blokace pomocí firewallu. Konfigurace portů switche závisí na monitorovaném provozu.

- **Jedna VLAN (bez značky):** Když je monitorovaný provoz vytvářen z jediné VLAN, odpovídající rozhraní musí být konfigurováno jako součást té samé VLAN. V tomto případě zařízení vyžaduje jednu IP adresu na této VLAN.
- **Více VLAN (se značkou):** If Je-li monitorovaný provoz z více než jedné VLAN, odpovídající rozhraní musí být konfigurováno se značkami 802.1Q pro dané sítě VLAN. Zařízení vyžaduje IP adresu pro každou chráněnou VLAN.

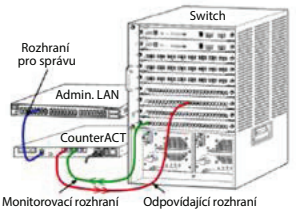
2. Nastavení switche

A. Možnosti zapojení switche

Zařízení bylo navrženo tak, aby se hladce integrovalo do širokého spektra síťových prostředí. Chcete-li úspěšně integrovat toto zařízení do své sítě, ověřte si, že je váš switch nastaven tak, aby monitoroval požadovaný provoz.

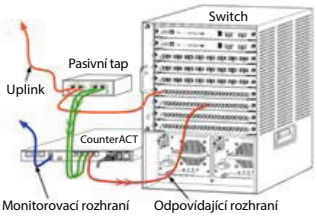
Pro připojení zařízení ke switchi existuje několik možností.

1. **Standardní instalace (oddělená rozhraní pro správu, monitorování a odpovídání)**
   Doporučená instalace využívá tří oddělených portů. Tyto porty jsou popsány v části *Zapojení prvků rozhraní zařízení*.

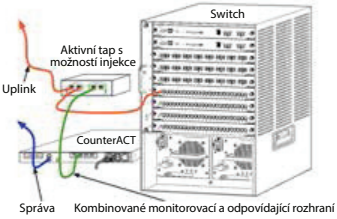


2. **Pasivní inline tap**
   Namísto připojení k monitorovacímu portu switche může zařízení používat pasivní inline tap.

   Pasivní tap vyžaduje dva monitorovací porty, kromě případů tzv. rekombinačních tapů, které kombinují dva duplexní streamy do jediného portu. Provoz na tapovaném portu a odpovídající rozhraní musí být nakonfigurovány stejně. Je-li například provoz na tapovaném portu označen jako VLAN (802.1Q), odpovídající rozhraní musí být také port se značkou VLAN.



3. **Aktivní inline tap (s možností injekce)**
   Když zařízení používá inline tap s *možností injekce*, monitorovací a odpovídající rozhraní lze kombinovat. Není potřeba konfigurovat samostatný odpovídající portu na switchi. Tuto možnost lze používat pro jakýkoliv typ upstreamové či downstreamové konfigurace switche.



4. **Odpověď IP vrstvy (pro instalace switche Layer-3)**
   Zařízení může používat vlastní rozhraní správy pro odpovídání na provoz. Přestože lze tuto možnost používat u jakéhokoliv monitorovaného provozu, doporučujeme ji používat pro případy, kdy zařízení monitoruje porty, které nejsou součástí žádné VLAN, a proto zařízení nemůže odpovídat na monitorovaný provoz pomocí nějakého dalšího portu switche. Typickým příkladem je monitorování spojení dvou routerů.

   Tato možnost nemůže odpovídat na požadavky protokolu ARP, což omezuje schopnost zařízení detekovat skenování IP adres obsažených v monitorované podsíti. Toto omezení neplatí pro případy, kdy je monitorován provoz mezi dvěma routery.

B. Poznámky k nastavení switche

Značky VLAN (802.1Q)

- **Monitorování jediné VLAN (neoznačený provoz)** Jestliže je provoz z jediné VLAN, není potřeba značek 802.1Q.
- **Monitorování více VLAN (označený provoz)** Jestliže je provoz z více sítí VLAN, monitorovací i odpovídající rozhraní musí mít zapnuté značky 802.1Q. Monitorování více VLAN je doporučenou možností, protože poskytuje celkově lepší pokrytí a zároveň minimalizuje počet zrcadlových portů.
- Jestliže switch nemůže používat značky 802.1Q VLAN na zrcadlových portech, proveďte jednu z následujících akcí:
  - Zrcadlete pouze jedinou síť VLAN
  - Zrcadlete jeden neoznačený uplink port
  - Použijte možnost odpovědi IP vrstvy
- Jestliže může switch zrcadlit pouze jediný port, zrcadlete jeden uplink port. Může být označen. Obecně platí, že pokud switch odstraňuje značky 802.1Q VLAN, musíte použít možnost odpovědi IP vrstvy.

Další informace

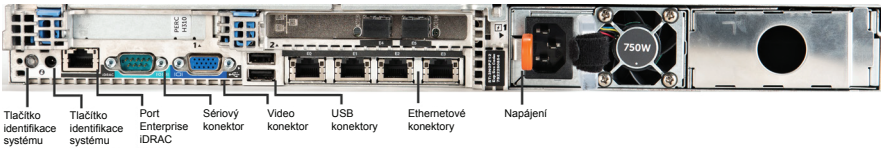
- Jestliže switch nedokáže zrcadlit vysílací i přijímací síťový provoz, je monitorován celý switch, kompletní sítě VLAN (poskytují vysílání/přijímání) nebo pouze jedno rozhraní (které poskytuje vysílání/přijímání). Ověřte, zda není zrcadlový port přetížen.
- U některých switchů (např. Cisco 6509) bude před zadáním nových konfigurací potřeba zcela vymazat předchozí konfigurace portů. Nejčastějším následkem nevymazání starých informací o portech je to, že switch začne odstraňovat značky 802.1Q.

3. Zapojení síťových kabelů a napájení

A. Rozbalení zařízení a připojení kabelů

1. Vyjměte zařízení a napájecí kabel z balení.
2. Vyjměte sadu vodicích lišt dodanou se zařízením.
3. Přimontujte vodicí lišty na zařízení a poté přimontujte zařízení do racku.
4. Zapojte síťové kabely mezi síťová rozhraní na zadním panelu zařízení a porty switche.

Příklad zadního panelu — zařízení CounterACT



B. Záznam přiřazení prvků rozhraní

Po dokončení instalace zařízení v datovém centru a instalace konzole CounterACT budete požádáni, abyste registrovali přiřazení prvků rozhraní. Tato přiřazení, kterým se říká *definice kanálů*, jsou zadávána v průvodci úvodním nastavením, který se otevře při prvním přihlášení ke konzoli.

Zaznamenejte přiřazení fyzických prvků rozhraní níže a použijte je při nastavování kanálů v konzoli.

Ethernetové rozhraní	Přiřazení prvku rozhraní (např. správa, monitorování, odpovídání)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Zapnutí zařízení

1. Připojte napájecí kabel do napájecího konektoru na zadním panelu zařízení.
2. Připojte druhý konec napájecího kabelu do uzemněné elektrické zásuvky.
3. Připojte klávesnici a monitor k zařízení nebo nastavte zařízení pro sériové zapojení. Viz *Instalační příručka CounterACT* umístěná na CounterACT CD.
4. Zapněte zařízení pomocí prvku na předním panelu.

Důležité: Před odpojením zařízení ze zásuvky jej vypněte.

4. Konfigurace zařízení

Před konfigurací zařízení si připravte následující informace.

☐ Hostitelský název zařízení	
☐ CounterACT heslo administrátora	**Uložte heslo na bezpečné místo**
☐ Rozhraní pro správu	
☐ IP adresa zařízení	
☐ Maska sítě	
☐ IP adresa výchozí brány	
☐ Doménové jméno DNS	
☐ Adresy DNS serveru	

Po zapnutí budete požádáni, abyste začali s konfigurací, následující zprávou:

```
Bootování zařízení CounterACT je dokončeno.
Stisknutím klávesy <Enter> pokračujte.
```

1. Stisknutím klávesy **Enter** se zobrazí následující nabídka:

```
1) Konfigurovat CounterACT
2) Obnovit uloženou konfiguraci CounterACT
3) Identifikovat a přečíslovat síťová rozhraní
4) Konfigurovat rozvržení klávesnice
5) Vypnout zařízení
6) Rebootovat zařízení
Výběr (1-6) :1
```

2. Vyberte **1** – Konfigurovat CounterACT. Při dotazu:

   `Pokračovat: (ano/ne)?`

   Stiskněte klávesu **Enter** a spustí se nastavování.

3. Otevře se nabídka **`Režim vysoké dostupnosti.`** Stiskněte klávesu **Enter** a vyberte standardní instalaci.
4. Zobrazí se dotaz **`Úvodní nastavení CounterACT.`** Stisknutím klávesy **Enter** pokračujte.
5. Otevře se nabídka **`Výběr typu instalace CounterACT.`** Zadejte **1** a stiskněte klávesu **Enter**, čímž se provede standardní instalace zařízení CounterACT. Spustí se průvodce nastavením. Může to chvilku trvat.

6. Při dotazu **`Zadejte popis zařízení`** zadejte krátký popis tohoto zařízení a poté stiskněte klávesu **Enter**.
   Zobrazí se toto:

```
>>>>>> Nastavení hesla administrátora <<<<<<

Toto heslo slouží pro přihlášení se jako tzv.
root k operačnímu systému zařízení a jako
administrátor (admin) ke konzoli CounterACT.
Heslo musí mít délku mezi 6 až 15 znaky a musí
obsahovat alespoň jeden neabecední znak.

Heslo administrátora:
```

7. U dotazu **`Nastavení hesla administrátora`** zadejte řetězec textu, který bude vaším heslem (řetězec se nezobrazuje na obrazovce) a stiskněte klávesu **Enter**. Budete požádáni o potvrzení hesla. Heslo musí mít délku 6 až 15 znaků a musí obsahovat alespoň jeden neabecední znak.

   Přihlaste se k zařízení jako root *a přihlaste se ke konzoli jako* admin.

8. U dotazu **`Nastavení názvu hostitele`** zadejte název hostitele a stiskněte klávesu **Enter**. Název hostitele lze použít při přihlašování ke konzoli a je zobrazen na konzoli, aby vám pomohl identifikovat zařízení CounterACT, které se právě zobrazuje.

9. Obrazovka **`Konfigurace nastavení sítě`** vás požádá o zadání několika konfiguračních parametrů. U každého dotazu zadejte hodnotu a stiskněte **Enter** pro pokračování.
   - Součásti zařízení CounterACT komunikují skrze rozhraní pro správu. Počet uvedených rozhraní pro správu závisí na modelu zařízení.
   - **IP adresa správy** je adresa rozhraní, skrze které komunikují součásti zařízení CounterACT. VLAN ID pro toto rozhraní přidejte pouze tehdy, jestliže rozhraní sloužící ke komunikaci součástí zařízení CounterACT je připojeno k označenému portu.
   - Jestliže existuje více než jedna **adresa serveru DNS**, oddělte každou adresu pomocí mezery—Většina interních serverů DNS rozlišuje externí a interní adresy, ale možná bude třeba zahrnout externí rozlišovací server DNS. Protože skoro všechny DNS dotazy prováděné zařízením budou pro interní adresy, externí server DNS by měl být uveden jako poslední.

10. Zobrazí se obrazovka **`Souhrn nastavení.`** Budete požádáni, abyste provedli obecné testy konektivity, překonfigurovali nastavení nebo jej dokončili. Zadejte **D** a dokončete nastavení.

Licence

Po instalaci budete muset nainstalovat úvodní demo licenci poskytnutou zástupcem pro značku CounterACT. Licence je instalována během úvodního nastavení konzole. Tato úvodní demo licence je platná několik dnů. Před jejím vypršením musíte nainstalovat permanentní licenci. Datum vypršení vám bude zasláno e-mailem. Kromě toho se informace o datu vypršení a stavu licence zobrazují v konzoli, v části Zařízení.

Jakmile dostanete permanentní licenci, bude licence každý den ověřována pomocí licenčního serveru ForeScout. Upozornění a porušení licence se zobrazují v části Podrobnosti o zařízení.

Licence, které nelze ověřit na jeden měsíc, budou zrušeny. Viz Instalační příručka CounterACT, kde naleznete další podrobnosti o licencích.

Požadavky připojení sítě

Minimálně jedno zařízení CounterACT (zařízení či firemní manažer) musí mít přístup k internetu. Toto připojení slouží k ověření licencí CounterACT na licenčním serveru ForeScout.

Licence, které nelze ověřit na jeden měsíc, budou zrušeny. CounterACT zašle varovnou e-mailovou zprávu jednou denně, ve které upozorní na případnou komunikační chybu se serverem.

5. Vzdálená správa

Nastavení iDRAC

Integrovaný ovladač vzdálené správy Dell Remote Access Controller (iDRAC) je integrovaným serverovým systémovým řešením, které vám poskytuje na místě či operačním systému nezávislý vzdálený přístup pomocí LAN nebo internetu k zařízením/firemním manažerům CounterACT. Pomocí tohoto modulu můžete provádět přístup KVM, zapínání/vypínání/restart a řešení problémů a údržbu.

Chcete-li pracovat s modulem iDRAC, proveďte toto:

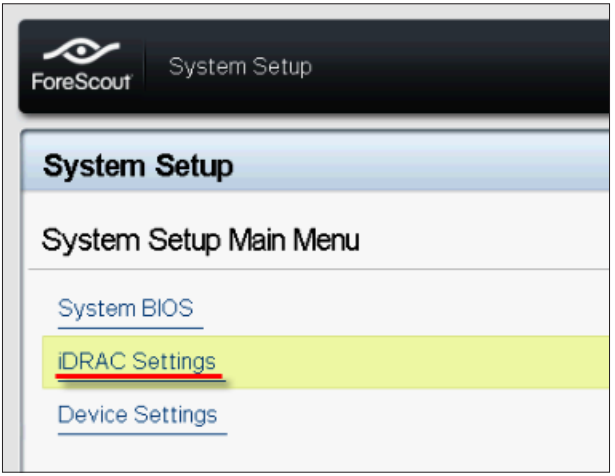
- *Zapněte a nakonfigurujte modul iDRAC*
- *Připojte modul k síti*
- *Přihlaste se k iDRAC*

Zapněte a nakonfigurujte modul iDRAC

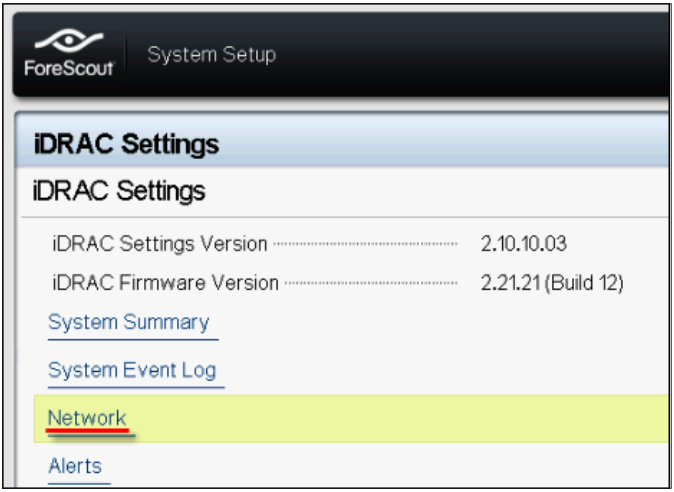
Změňte nastavení modulu iDRAC, aby byl zapnut vzdálený přístup k zařízení CounterACT. Tato část popisuje základní integrační nastavení vyžadovaná pro práci se zařízením CounterACT.

Postup konfigurace modulu iDRAC:

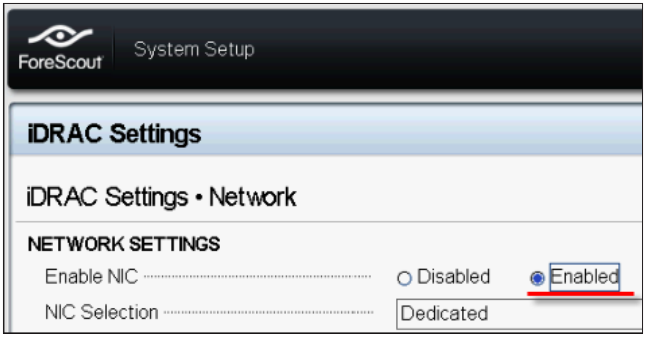
1. Zapněte spravovaný systém.
2. Během vlastní diagnostiky při startu (POST) stiskněte F2.
3. Na stránce Hlavní nabídka nastavení systému vyberte možnost **Nastavení iDRAC**.



4. Na stránce Nastavení iDRAC vyberte možnost **Síť**.

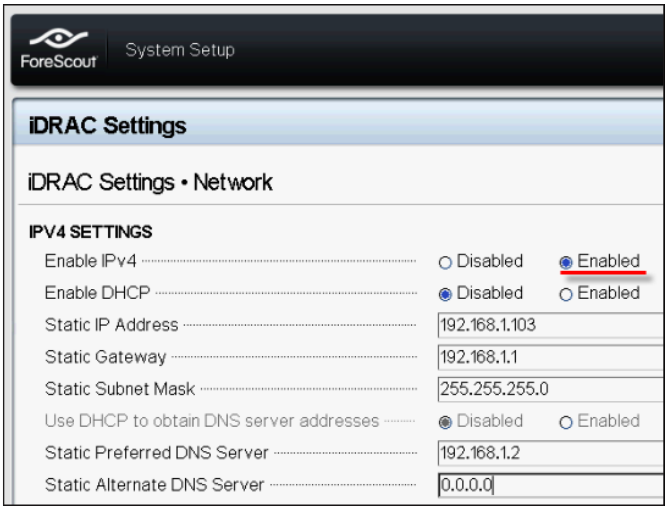


5. Nakonfigurujte následující nastavení sítě:
   - ***Nastavení sítě.*** Ověřte, že je pole **Zapnout NIC** nastaveno na **Zapnuto**.

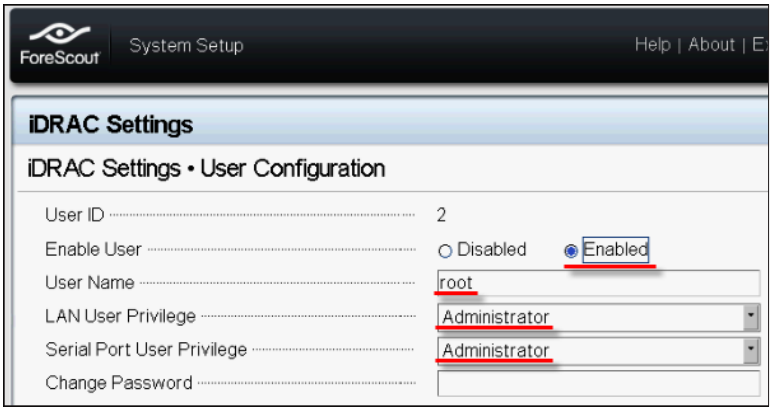


   - ***Běžná nastavení.*** V políčku Název DNS DRAC můžete aktualizovat dynamické DNS (Volitelné).

- ***Nastavení IPV4.*** Ověřte, že je pole **Zapnout IPv4** nastaveno na **Zapnuto**. Nastavte políčko **Zapnout DHCP** na hodnotu **Zapnuto**, čímž bude používáno dynamické adresování IP, nebo na Vypnuto, čímž bude používáno statické adresování IP. Je-li položka zapnutá, DHCP bude modulu iDRAC7 automaticky přiřazovat adresu IP, bránu a masku podsítě. Je-li položka vypnutá, zadejte hodnoty do políček **Statická adresa IP, Statická brána** a **Statická maska podsítě**.



6. Vyberte možnost **Zpět**.
7. Vyberte možnost **Konfigurace uživatele**.
8. Nastavte následující políčka Konfigurace uživatele:
   - ***Zapnout uživatele.*** Ověřte, že je toto políčko nastaveno na Zapnuto.
   - ***Jméno uživatele.*** Zadejte jméno uživatele.
   - ***Uživatelská práva pro LAN a sériový port.*** Nastavte úroveň práv na Administrátor.
   - **Změna hesla.** Nastavte heslo pro přihlášení uživatele.



9. Vyberte možnost **Zpět** a poté možnost **Dokončit**. Potvrďte změněná nastavení. Nastavení sítě se uloží a systém se rebootuje.

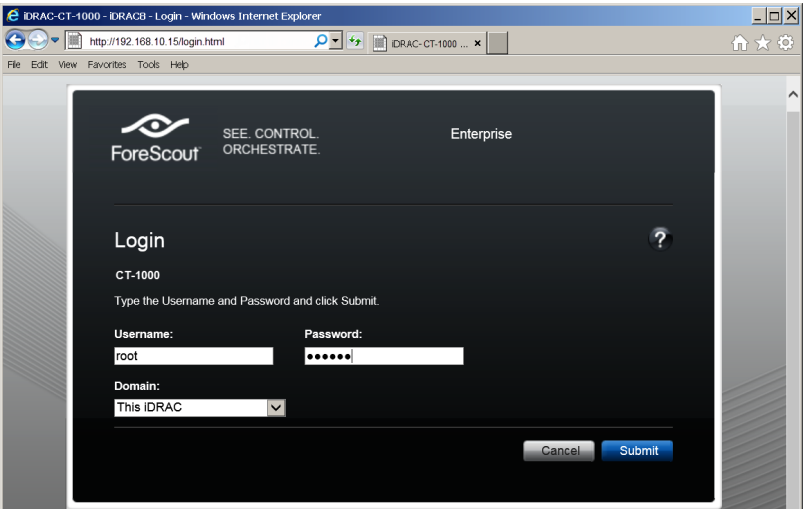
Připojte modul k síti

Modul iDRAC se připojuje k síti Ethernet. Je zvykem jej připojit k síti pro správu. Následující obrázek ukazuje umístění portu iDRAC na zadním panelu zařízení CT-1000:

Přihlaste se k iDRAC

Postup přihlášení k iDRAC:

1. Najděte adresu IP nebo název domény konfigurované v **Nastavení iDRAC > Síť.**



2. Zadejte jméno uživatele a heslo, která jste zadali na stránce Konfigurace uživatele u nastavení systému iDRAC.
3. Vyberte možnost **Potvrdit**.

Další informace o modulu iDRAC naleznete v Uživatelské příručce modulu iDRAC.

Je velmi důležité aktualizovat výchozí údaje.

6. Ověření konektivity

Ověření zapojení rozhraní pro správu

Pro testování připojení rozhraní pro správu se přihlaste k zařízení a zadejte následující příkaz:

```
fstool linktest
```

Zobrazí se následující informace:

```
Stav rozhraní pro správu
Informace o pingu výchozí brány
Statistiky pingu
Provedení testu rozlišení názvu
Výsledek testu
```

Ověření zapojení switche/zařízení

Před opuštěním datového centra ověřte, zda je switch správně zapojen k zařízení. To provedete tak, že na zařízení spoustíte příkaz fstool ifcount pro každé detekované rozhraní.

```
fstool ifcount eth0 eth1 eth2
```

(Každé rozhraní oddělte mezerou.)

Tento nástroj neustále zobrazuje síťový provoz na zadaných rozhraních. Funguje ve dvou režimech: podle rozhraní nebo podle VLAN. Režim lze změnit z displeje. Zobrazují se celkové bity za sekundu a procento každé z následujících kategorií provozu:

- Monitorovací rozhraní by mělo primárně vidět zrcadlený provoz — nad 90 %.
- Odpovídající rozhraní by mělo primárně vidět vysílaný provoz.
- Monitorovací i odpovídající rozhraní by měla vidět očekávané sítě VLAN.

Možnosti příkazu:

```
v – zobrazit v režimu VLAN
I – zobrazit v režimu rozhraní
P – ukázat předcházející
N – ukázat další
q – přestat zobrazovat
```

Režim VLAN:

```
aktualizace=[4] [eth3: 14 vlans]
Celkové    zrcadlené vysílání  rozhraní/Vlan  *Na moji MAC  *Z mé MAC
eth3.
neoznačen  4Mbps     0.2%      99.8%          0.0%          0.0%
eth3.1     9Mbps     0.0%      100.0%         0.0%          0.0%
eth3.2     3Mbps     0.1%      99.9%          0.0%          0.0%
eth3.4     542bps    100.0%    0.0%           0.0%          0.0%
eth3.20    1Kbps     100.0%    0.0%           0.0%          0.0%
Zobrazit sítě [v]lan a rozhraní[i] <-[p]ředch. [n]ásl.-> opustit[q]
```

Režim rozhraní:

```
aktualizace=[31]       [eth0: 32 vlans] [eth1: 1 vlans]
Celkové    zrcadlené vysílání  rozhraní       *Na moji MAC  *Z mé MAC
eth0       3Kbps     42.3%     0.0%           14.1%         43.7%
eth1       475bps    0.0%      100.0%         0.0%          0.0%
```

*Na moji MAC — Cílová MAC je MAC adresou zařízení.

*Z mojí MAC — Provoz zaslaný z tohoto zařízení (zdrojová MAC je MAC adresou zařízení). Cíl může být typu broadcast nebo unicast).

Pokud nevidíte žádný provoz, ověřte, zda je rozhraní zapnuté. Na zařízení zadejte následující příkaz:

`ifconfig [interface name] up`

Provedení testu pingu

Pro ověření konektivity proveďte test pingu mezi zařízením a desktopem na síti.

Postup provedení testu:

1. Přihlaste se k zařízení.
2. Spusťte následující příkaz: **`Ping [IP adresa desktopu]`**
   Ve výchozím stavu zařízení samotné nereaguje na ping.

7. Nastavení konzole CounterACT

Instalace konzole CounterACT

Konzole CounterACT je centrální řídicí aplikace sloužící k zobrazování, sledování a analyzování aktivity detekované zařízením. Z této konzole lze nastavit NAC, ochranu před hrozbami, firewall a další zásady. Více informací naleznete v *Příručce uživatele konzole CounterACT*.

Je nutné dodat zařízení pro hostování aplikačního softwaru konzole CounterACT. Minimální požadavky na hardware jsou následující:

- Nededikované PC se systémem:
  - Windows XP, Windows Vista nebo Windows 7
  - Windows Server 2003 nebo Server 2008
  - Linux
- Pentium 3, 1GHz
- 2 GB RAM
- 1GB volného místa na disku

Instalaci konzole lze provádět dvěma způsoby:

Použití instalačního softwaru zabudovaného do zařízení.

1. Otevřete okno prohlížeče na počítači s konzolí.
2. Do adresové řádky prohlížeče zadejte
   `http://<Appliance ip>/install`
   Kde <Appliance ip> je adresa IP zařízení. Prohlížeč zobrazí instalační okno konzole.
3. Postupujte podle pokynů na obrazovce.

Instalace z CounterACT CD-ROM

1. Vložte CounterACT CD-ROM do DVD mechaniky.
2. Otevřete soubor **`ManagementSetup.htm`** na CD-ROMu pomocí prohlížeče.
3. Postupujte podle pokynů na obrazovce.

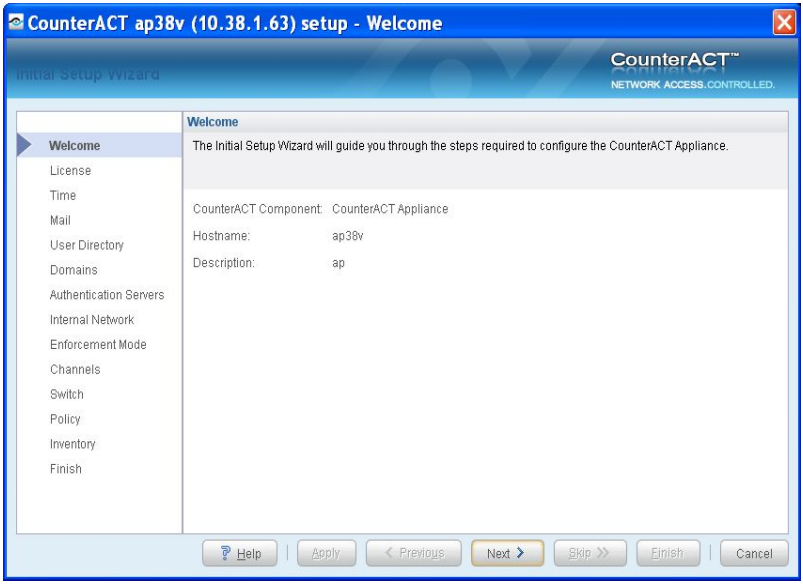
Přihlášení

Po dokončení instalace se můžete přihlásit ke konzoli CounterACT.

1. Vyberte ikonu CounterACT vytvořeného zástupce.
2. Zadejte adresu IP nebo název hostitele zařízení do políčka **IP/Název**.
3. Do políčka **Jméno uživatele** zadejte **admin**.
4. Do políčka **Heslo** zadejte heslo, které jste vytvořili během instalace zařízení.
5. Vyberte možnost **Přihlášení** a spustí se konzole.

Provedení úvodního nastavení

Po prvním přihlášení se zobrazí Průvodce úvodním nastavením. Ten vás provede základními kroky konfigurace, aby bylo zařízení CounterACT spuštěno a mohlo rychle a efektivně běžet.



Před úvodním nastavením

Před prací s průvodcem si připravte následující informace:

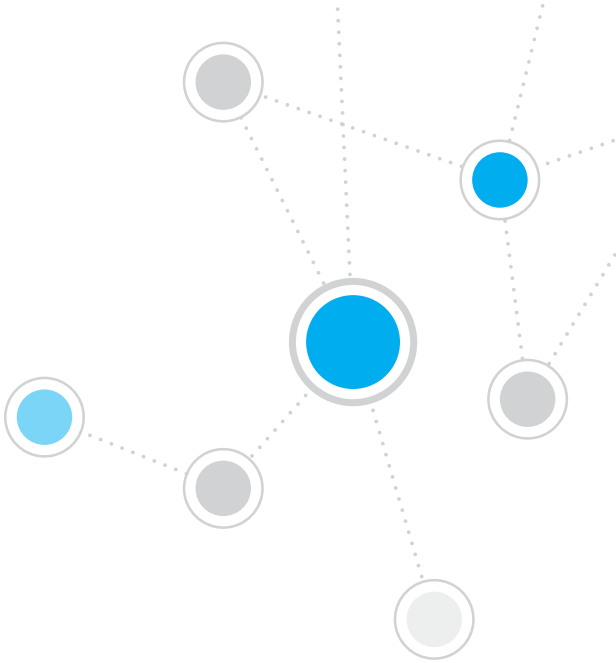
Informace	Hodnoty
☐ Adresa NTP serveru používaného vaší organizací (volitelné).	
☐ Interní mailová relay adresa IP. Umožňuje přenos e-mailových zpráv ze zařízení CounterACT, jestliže je provoz SMTP ze zařízení zakázán (volitelné).	
☐ E-mailová adresa administrátora zařízení CounterACT.	
☐ Přiřazení monitorovacího a odpovídajícího rozhraní definovaná v datovém centru.	
☐ Pro segmenty nebo sítě VLAN bez DHCP, síťové segmenty nebo sítě VLAN, ke kterým je monitorovací rozhraní přímo připojeno, a permanentní adresa IP používaná zařízením CounterACT u každé takové sítě VLAN. Tyto informace nejsou potřebné pro nastavení firemního manažera.	
☐ Rozsah adres IP, které bude zařízení chránit (všechny interní adresy, včetně nepoužívaných adres).	
☐ Informace o účtu User Directory a adrese IP serveru pro User Directory.	
☐ Údaje o doméně, včetně názvu a hesla administrativního účtu domény.	
☐ Autorizační servery, aby mohlo zařízení CounterACT analyzovat, kteří síťoví hostitelé jsou úspěšně autorizováni.	
☐ Adresa IP jádrového switche, značka a SNMP parametry.	

Informace o práci s průvodcem naleznete v *Příručce uživatele konzole CounterACT* nebo na online nápovědě.

Kontaktní informace

Pro technickou podporu pište na e-mail support@forescout.com nebo volejte na:

- Bezplatná linka (USA): 1.866.377.8771
- Telefon (mezinárodní): 1.408.213.3191
- Podpora: 1.708.237.6591
- Fax: 1.408.371.2284



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Bezplatná linka: 1.866.377.8771
Telefon (mezinárodní): 1.408.213.3191
Podpora: 1.708.237.6591
Fax: 1.408.371.2284

400-00020-01