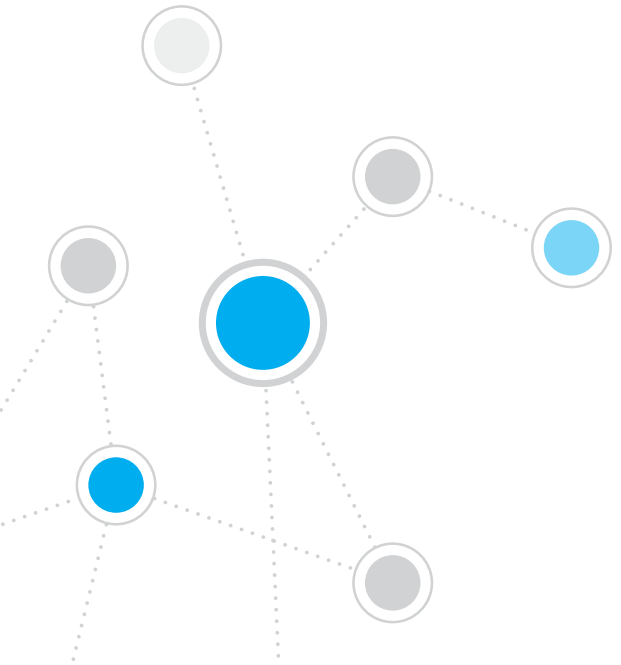
ForeScout

ForeScout CounterACT® 7

Samostatné zariadenie CounterACT

Stručný sprievodca inštaláciou



Obsah

Víta vás ForeScout CounterACT® verzia 7

ForeScout CounterACT je fyzické alebo virtuálne bezpečnostné zariadenie, ktoré dynamicky identifikuje a vyhodnocuje sieťové zariadenia a aplikácie vo chvíli pripojenia do siete. Pretože zariadenie CounterACT nevyžaduje agentov, pracuje s vašimi zariadeniami – spravovanými aj nespravovanými, známymi aj neznámymi, počítačmi aj mobilnými, vloženými aj virtuálnymi. Zariadenie CounterACT rýchlo určuje používateľa, vlastníka, operačný systém, konfiguráciu zariadenia, softvér, služby, stav cesty a prítomnosť agentov zabezpečenia. Následne poskytuje nápravu, kontrolu a nepretržité monitorovanie týchto zariadení pri ich pripájaní k sieti a odpájaní od siete. To všetko pri plynulej integrácii do existujúcej infraštruktúry IT.

Táto príručka opisuje inštaláciu jedného samostatného zariadenia CounterACT.

Podrobnejšie informácie alebo informácie o nasadení viacerých zariadení na ochranu celopodnikových sietí nájdete v *inštalačnej príručke CounterACT* a *návode na použitie konzoly*. Tieto dokumenty sa nachádzajú na CD pre CounterACT v priečinku /docs.

Okrem toho môžete prejsť na webovú stránku podpory na adrese: http://www.forescout.com/support, na ktorej nájdete najnovšiu dokumentáciu, články pre bázu znalostí a aktualizácie pre zariadenie.

Obsah balenia CounterACT

- Zariadenie CounterACT
- Stručný sprievodca inštaláciou
- CounterACT CD so softvérom Console, návod na použitie konzoly CounterACT a inštalačná príručka
- Záručný list
- Montážne svorky
- Napájací kábel
- Kábel na pripojenie konzoly DB9 (len pre sériové pripojenie)

Prehľad

Vykonaním nasledujúcich krokov nastavte CounterACT:

1. Vytvorte plán rozmiestnenia
2. Nastavte prepínač
3. Pripojte sieťové káble a napájanie
4. Nakonfigurujte zariadenie
5. Vzdialená správa
6. Overte pripojenie
7. Nastavte konzolu CounterACT

1. Vytvorte plán rozmiestnenia

Pred vykonaním inštalácie by ste sa mali rozhodnúť, kde chcete nasadiť zariadenie, a oboznámiť sa s informáciami o pripojeniach rozhraní zariadenia.

Rozhodnite sa, kde chcete nasadiť zariadenie

Zvolenie správneho umiestnenia siete pre zariadenie je rozhodujúce pre úspešné nasadenie a optimálny výkon CounterACT. Správne umiestnenie bude závisieť od požadovanej implementácie cieľov a politík prístupu k sieti. Zariadenie by malo byť schopné sledovať prevádzku, ktorá je relevantná pre požadovanú politiku. Napríklad ak vaša politika závisí od povolenia udalostí sledovania od koncových bodov až po overovanie firemných serverov, zariadenie musí byť inštalované tak, aby sledovalo tok od koncového bodu k autentizačnému serveru(-om).

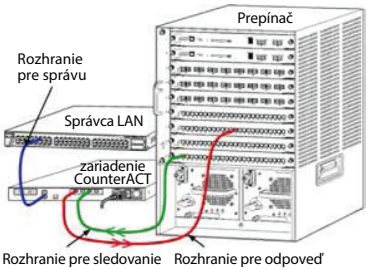
Ďalšie informácie o inštalácii a nasadení nájdete v inštalačnej príručke CounterACT, ktorá sa nachádza na CD CounterACT, ktorý sa dodáva v balení.

Pripojenie rozhraní zariadenia

Zariadenie je zvyčajne nakonfigurované s tromi pripojeniami k sieťovému prepínaču.

Rozhranie pre správu

Toto rozhranie umožňuje spravovať CounterACT a zadávať požiadavky a vykonávať dôkladnú kontrolu koncových bodov. Rozhranie musí byť pripojené k portu prepínača, ktorý má prístup ku všetkým koncovým sieťovým bodom.



Každé zariadenie potrebuje samostatnú správu pripojenia k sieti. Toto pripojenie musí mať IP adresu na lokálnej sieti LAN a prístup cez port 13000/TCP z počítačov, na ktorých bude spustená aplikácia na správu konzoly CounterACT. Rozhranie pre správu musí mať prístup k nasledujúcim prvkom na sieti:

Port	Služba	Do alebo z CounterACT	Funkcia
22/TCP	SSH	Do	Umožňuje prístup k príkazovému riadku rozhrania CounterACT.
2222/TCP			(Vysoká dostupnosť) Umožňuje prístup k fyzickým zariadeniam CounterACT, ktoré sú súčasťou klastra s vysokou dostupnosťou. Použite 22/TCP na prístup k zdieľanej (virtuálnej) IP adrese klastra.

Port	Služba	Do alebo z CounterACT	Funkcia
25/TCP	SMTP	Z	Používa sa na odosielanie e-mailov zo zariadenia CounterACT
53/UDP	DNS	Z	Umožňuje zariadeniu CounterACT získať vnútorné IP adresy.
80/TCP	HTTP	Do	Umožňuje presmerovanie HTTP.
123/UDP	NTP	Z	Umožňuje zariadeniu CounterACT pristupovať k časovému serveru NTP. Predvolene používa CounterACT adresu ntp.foreScout.net.
135	WMI	Z	Umožňuje vzdialené vyšetrovanie koncových bodov s OS Windows.
139/TCP	SMB, MS-RPP	Z	Umožňuje vzdialené vyšetrovanie koncových bodov s OS Windows (pre koncové body s OS Windows 7 a starším).
445/TCP			Umožňuje vzdialené vyšetrovanie koncových bodov s OS Windows.
161/UDP	SNMP	Z	Umožňuje zariadeniu CounterACT komunikovať so zariadeniami v sieťovej infraštruktúre, ako sú prepínače a smerovače. Informácie o konfigurácii SNMP nájdete v *návode na použitie konzoly CounterACT*
162/UDP	SNMP	Do	Umožňuje zariadeniu CounterACT prijímať depeše SNMP od zariadení v sieťovej infraštruktúre, ako sú prepínače a smerovače. Informácie o konfigurácii SNMP nájdete v *návode na použitie konzoly CounterACT.*
443/TCP	HTTPS	Do	Umožňuje presmerovanie HTTP pomocou TLS.
2200/TCP	Secure Connector	Do	Umožňuje službe SecureConnector vytvoriť zabezpečené pripojenie (šifrované SSH) k zariadeniu z počítača s OS Macintosh/Linux. *SecureConnector* je skriptový agent, ktorý umožňuje správu koncových bodov s OS Macintosh a Linux, keď sú pripojené k sieti.
10003/TCP	Secure Connector for Windows	Do	Umožňuje službe SecureConnector vytvoriť zabezpečené pripojenie (šifrované TLS) k zariadeniu z počítača s OS Windows. *SecureConnector* je agent, ktorý umožňuje správu koncových bodov s OS Windows, keď sú pripojené k sieti. Viac informácií o službe SecureConnector nájdete v *návode na použitie konzoly CounterACT.*

			Keď sa služba SecureConnector pripojí k zariadeniu alebo k správcovi Enterprise Manager, je presmerovaná na zariadenie, ku ktorému je priradený jej hostiteľ. Dbajte na to, aby bol tento port otvorený pre všetky zariadenia a pre správcu Enterprise Manager, aby sa umožnila transparentná mobilita v rámci organizácie.
13000/TCP	CounterACT	Do	Umožňuje pripojenie k zariadeniu z konzoly. V prípade systémov s viacerými zariadeniami CounterACT umožňuje pripojenie od konzoly k správcovi Enterprise Manager a od správcu Enterprise Manager ku všetkým zariadeniam.

Rozhranie sledovania

Toto pripojenie umožňuje zariadeniu monitorovať a sledovať sieťovú prevádzku.

Prenos je zrkadlený do portu na prepínači a sledovaný zariadením. V závislosti od množstva zrkadlených sietí VLAN môže alebo nemusí byť prenos označený ako 802.1Q VLAN.

- **Samostatná sieť VLAN (neoznačená):** Keď je sledovaný prenos generovaný zo samostatnej siete VLAN, zrkadlový prenos nemusí byť označený ako VLAN.
- **Viac sietí VLAN (označené):** Ak je prenos sledovaný z viac ako jednej siete VLAN, zrkadlový prenos musí byť označený ako 802.1Q VLAN.

Ak sú dva prepínače pripojené ako redundantný pár, zariadenie musí sledovať prenosy z oboch prepínačov.

Rozhranie sledovania nevyžaduje IP adresu.

Rozhranie pre odpoveď

Zariadenie reaguje na prenosy pomocou tohto rozhrania. Prenosová odozva slúži na ochranu pred škodlivými činnosťami a vykonáva akcie politiky NAC. Tieto akcie môžu napríklad zahŕňať presmerovanie webových prehliadačov alebo vykonávanie blokovania brány firewall. Konfigurácia príslušného portu prepínača závisí od prenosu, ktorý je monitorovaný.

- **Samostatná sieť VLAN (neoznačená):** Keď je sledovaný prenos generovaný zo samostatnej siete VLAN, rozhranie odozvy musí byť nakonfigurované tak, aby bolo súčasťou tej istej siete VLAN. V tomto prípade zariadenie vyžaduje jednu IP adresu na tejto sieti VLAN.
- **Viac sietí VLAN (označené):** Ak je prenos sledovaný z viac ako jednej siete VLAN, rozhranie odozvy musí byť tiež nakonfigurované s označením 802.1Q na tej istej sieti VLAN. Zariadenie musí mať IP adresu pre každú chránenú sieť VLAN.

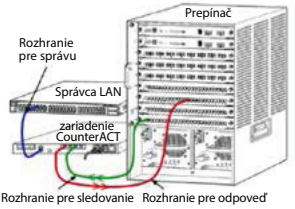
2. Nastavte prepínač

A. Možnosti pripojenia prepínača

Zariadenie bolo navrhnuté tak, aby sa jednoducho integrovalo do najrôznejších sieťových prostredí. Ak chcete úspešne integrovať zariadenie do svojej siete, skontrolujte, či je prepínač nastavený na sledovanie požadovaného prenosu.

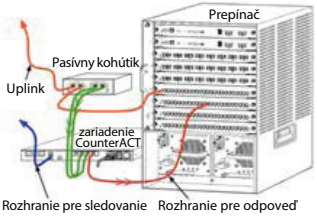
Na pripojenie zariadenia k prepínaču je dostupných viacero možností.

1. **Štandardné nasadenie (samostatné riadenie, monitorovanie a rozhranie odozvy)**
   Odporúčané nasadenie používa tri samostatné porty. Tieto porty sú opísané v časti *Pripojenie rozhraní zariadenia.*

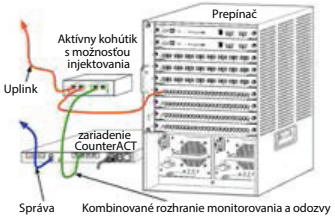


2. **Pasívny radový kohútik**
   Namiesto pripojenia k monitorovaciemu portu prepínača môže zariadenie používať pasívny radový kohútik.

   Pasívny kohútik vyžaduje dva monitorovacie porty s výnimkou prípadu „rekombinačných“ kohútikov, ktoré kombinujú dva duplexné prúdy do jedného portu. Prenosy na kohútikovom porte a rozhraní odozvy musia byť nakonfigurované rovnakým spôsobom. Napríklad v prípade, keď je prenos na kohútikovom porte označený ako VLAN (802.1Q), rozhranie odozvy musí byť tiež označené portom VLAN.



3. **Aktívny (s možnosťou injektovania) radový kohútik**
   Ak zariadenie používa radový kohútik s *možnosťou injektovania*, je možné kombinovať rozhrania monitorovania a odozvy. Na prepínači nie je potrebné nakonfigurovať samostatný port odozvy. Túto možnosť možno použiť pre ľubovoľný typ konfigurácie prepínača v smere alebo proti smeru.



4. **Odozva na vrstve IP (pre prepínače na vrstve 3)**
   Zariadenie môže používať svoje vlastné rozhranie správy odozvy na prevádzku. Napriek tomu, že táto možnosť môže byť použitá s akýmkoľvek monitorovaným prenosom, odporúča sa v prípade, keď zariadenie monitoruje porty, ktoré nie sú v žiadnej sieti VLAN, a preto zariadenie nemôže reagovať na monitorovaný prenos pomocou iného portu prepínača. To je typické pri monitorovaní spoja, ktorý prepája dva smerovače.

   Táto možnosť nedokáže reagovať na požiadavky protokolu rozlíšenia adresy (ARP), ktoré obmedzujú schopnosť zariadenia rozpoznať skenovania zamerané na IP adresy obsiahnuté v monitorovanej podsieti. Toto obmedzenie neplatí, ak je monitorovaná prevádzka medzi dvoma smerovačmi.

B. Poznámky k pripojeniu prepínača

Označenia VLAN (802.1Q)

- **Monitorovanie samostatnej siete VLAN (neoznačený prenos)**
  Ak je monitorovaný prenos zo samostatnej siete VLAN, prevádzka nevyžaduje označenia 802.1Q.
- **Monitorovanie viacerých sietí VLAN (označený prenos)**
  Ak je monitorovaný prenos z dvoch alebo viacerých sietí VLAN, tak obidve rozhrania (pre monitorovanie aj odozvu) musia mať povolené označovanie 802.1Q. Monitorovanie viacerých sietí VLAN je odporúčaná voľba, pretože poskytuje najlepšie celkové pokrytie a zároveň minimalizuje počet zrkadlených portov.
- Ak prepínač nedokáže používať značku 802.1Q VLAN na zrkadlenie portov, vykonajte jednu z nasledujúcich akcií:
  - Zrkadlite iba jednu sieť VLAN.
  - Zrkadlite jeden neoznačený uplinkový port.
  - Použite možnosť odozvy vrstvy IP.
- Ak prepínač dokáže zrkadliť iba jeden port, tak zrkadlite jeden uplinkový port. Ten môže byť označený. Všeobecne platí, že ak prepínač preberá označenia 802.1Q VLAN, budete musieť použiť možnosť odpovede vrstvy IP.

Ďalšie informácie

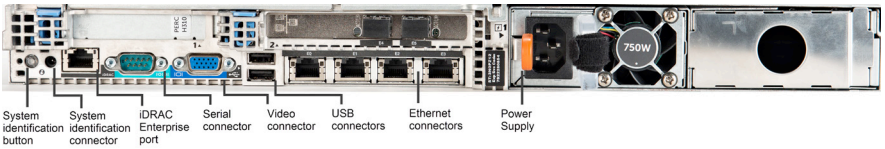
- Ak prepínač nedokáže zrkadliť prijímanú aj odosielanú prevádzku, monitorujte celý prepínač, kompletné siete VLAN (tie poskytujú odosielanie/prijímanie) alebo len jedno rozhranie (ktoré neumožňuje odosielanie/prijímanie). Uistite sa, že nepreťažujete zrkadlený port.
- Niektoré prepínače (napr. Cisco 6509) môžu vyžadovať úplné vyčistenie predchádzajúcej konfigurácie portov pred zadaním novej konfigurácie. Najčastejším následkom neodstránenia predchádzajúcich informácií o porte je, že prepínač preberá označenia 802.1Q.

3. Pripojte sieťové káble a zapnite zariadenie

A. Odbaľte zariadenie a pripojte káble

1. Vyberte zariadenie a napájací kábel z prepravného kontajnera.
2. Vyberte súpravu koľajníc, ktorá sa dodáva so zariadením.
3. Pripevnite súpravu koľajníc k zariadeniu a namontujte zariadenie do stojana.
4. Pripojte sieťové káble medzi sieťovým rozhraním na zadnom paneli zariadenia a portami na prepínači.

Ukážka zadného panela — zariadenie CounterACT



B. Zaznamenajte si priradenia rozhraní

Po dokončení inštalácie zariadenia v dátovom centre a po inštalácií konzoly CounterACT budete vyzvaní k registrácii priradených rozhraní. Tieto priradenia, ktoré sa nazývajú *definície kanálov*, sa zadávajú v Sprievodcovi počiatočným nastavením, ktorý sa otvorí po prvom prihlásení ku konzole.

Zaznamenajte si do tabuľky uvedenej nižšie priradené fyzické rozhrania a použite ich pri dokončovaní nastavenia kanála na konzole.

Rozhranie Ethernet	Priradenie rozhraní (napr. správa, monitorovanie, odozva)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Zapnite zariadenie

1. Pripojte napájací kábel do napájacieho konektora na zadnom paneli zariadenia.
2. Druhý koniec napájacieho kábla zapojte do uzemnenej elektrickej zásuvky.
3. Pripojte klávesnicu a monitor k zariadeniu alebo nastavte zariadenie na sériové pripojenie. Pozri *inštalačnú príručku CounterACT* na CD CounterACT.
4. Na zadnom paneli zapnite zariadenie.

Dôležité: Pred odpojením vypnite zariadenie.

4. Nakonfigurujte zariadenie

Predtým ako budete konfigurovať zariadenie, pripravte si nasledujúce informácie.

☐ Hostiteľský názov zariadenia	
☐ Heslo správcu CounterACT	**Heslo si uschovajte na bezpečnom mieste**
☐ Rozhranie pre správu	
☐ IP adresa zariadenia	
☐ Maska siete	
☐ IP adresa predvolenej brány	
☐ Názov domény DNS	
☐ Adresy servera DNS	

Po zapnutí budete prostredníctvom nasledujúcej správy vyzvaní, aby ste spustili konfiguráciu:

```
CounterACT Appliance boot is complete.
  (Spustenie zariadenia CounterACT je dokončené).
Press <Enter> to continue. (Pokračujte stlačením
  klávesu <Enter>).
```

1. Stlačením klávesu **Enter** zobrazíte nasledujúce menu:

```
1) Configure CounterACT (Konfigurácia CounterACT)
2) Restore saved CounterACT configuration
   Obnoviť uloženú konfiguráciu CounterACT)
3) Identify and renumber network interfaces
   (Identifikovať a prečíslovať sieťové rozhrania)
4) Configure keyboard layout (Konfigurácia
   rozloženia klávesnice)
5) Turn machine off (Vypnutie zariadenia)
6) Reboot the machine (Reštartovanie zariadenia)
Choice (Voľba) (1-6) :1
```

2. Vyberte **1** – Configure CounterACT. Pri otázke:

   `Continue (Pokračovať): (yes/no) (áno/nie)?`

   Stlačením klávesu **Enter** spustite inštaláciu.

3. Otvorí sa menu **`High Availability Mode (Režim vysokej dostupnosti).`** Stlačením klávesu **Enter** vyberte Standard Installation (Štandardná inštalácia).
4. Zobrazí sa okno **`CounterACT Initial Setup (Úvodné nastavenie CounterACT).`** Pokračujte stlačením klávesu **Enter**.
5. Otvorí sa menu **`Select CounterACT Installation Type (Vyberte typ inštalácie CounterACT).`** Zadajte **1** a stlačením klávesu **Enter** nainštalujte štandardné zariadenie CounterACT. Inicializuje sa inštalácia. Môže to chvíľu trvať.

6. Na obrazovke **Enter Machine Description (Zadajte opis zariadenia)** zadajte krátky text identifikujúci toto zariadenie a stlačte **Enter**.
   Zobrazí sa nasledujúca informácia:

```
>>>>>> Nastavte heslo správcu <<<<<<

Toto heslo sa používa na prihlásenie ako „root“
do operačného systému zariadenia a ako „admin“
do konzoly CounterACT.
Heslo by malo byť v rozmedzí 6 až 15 znakov a
musí obsahovať aspoň jeden znak iný ako písmeno.

Heslo správcu:
```

7. V zobrazení **Set Administrator Password (Nastavte heslo správcu)** zadajte reťazec, ktorý má byť heslom (reťazec sa nezobrazuje na obrazovke), a stlačte **Enter**. Budete vyzvaní, aby ste potvrdili heslo. Heslo musí byť v rozmedzí 6 až 15 znakov a musí obsahovať aspoň jeden znak iný ako písmeno.
   Do zariadenia sa prihlasujte ako root a do konzoly ako admin.

8. Na obrazovke **Set Host Name (Zadajte názov hostiteľa)** zadajte názov hostiteľa a stlačte **Enter**. Názov hostiteľa môže byť použitý pri prihlásení do konzoly, je zobrazený na konzole a pomôže vám identifikovať zariadenie CounterACT, ktoré sledujete.

9. Pokyn na obrazovke **Configure Network Settings (Konfigurácia nastavení siete)** vás vyzve k sérii konfiguračných parametrov. Na každej obrazovke zadajte hodnotu a pokračujte stlačením klávesu **Enter**.
   - Komponenty CounterACT komunikujú cez rozhranie pre správu. Počet uvedených rozhraní pre správu závisí od modelu zariadenia.
   - **IP adresa správy** je adresa rozhrania, cez ktoré komunikujú komponenty zariadenia CounterACT. Pridajte VLAN ID pre toto rozhranie iba v prípade, že rozhranie pre komunikáciu medzi komponentmi CounterACT je pripojené k označenému portu.
   - Ak existuje viac ako jedna **adresa servera DNS**, oddeľte každú adresu medzerou — väčšina interných serverov DNS prekladá externé a interné adresy, ale možno budete musieť zahrnúť externý server DNS na prekladanie adries. Pretože takmer všetky požiadavky DNS vykonávané zariadením budú pre interné adresy, externý DNS server by mal byť uvedený ako posledný.

10. Zobrazí sa obrazovka **Setup Summary (Zhrnutie inštalácie).** Budete vyzvaní, aby ste vykonali všeobecné testy pripojenia, konfiguráciu nastavenia a dokončenie inštalácie. Zadaním **D** dokončite inštaláciu.

Licencia

Po inštalácii musíte nainštalovať úvodnú demo licenciu, ktorú vám poskytne zástupca CounterACT. Licencia je nainštalovaná počas úvodného nastavenia konzoly. Táto úvodná demo licencia je platná počas určitého počtu dní. Pred vypršaním tejto lehoty musíte nainštalovať trvalú licenciu. Budete kontaktovaní prostredníctvom e-mailu, v ktorom bude uvedený dátum vypršania platnosti. Okrem toho sa informácie o dátume vypršania platnosti a stave licencie zobrazujú v konzole v paneli Spotrebiče/Zariadenia.

Keď dostanete trvalú licenciu, licencia sa bude každodenne overovať prostredníctvom licenčného servera ForeScout. V paneli Device Details (Podrobnosti o zariadení) sa zobrazia licenčné upozornenia a porušenia.

Licencie, ktoré nemôžu byť overené počas jedného mesiaca, budú zrušené. Ďalšie podrobnosti o licenciách nájdete v inštalačnej príručke CounterACT.

Požiadavky na pripojenie k sieti

Aspoň jedno zariadenie CounterACT (zariadenie alebo správca podniku) musí mať prístup k internetu. Toto pripojenie sa používa na overenie licencie pomocou licenčného servera ForeScout.

Licencie, ktoré nemôžu byť overené počas jedného mesiaca, budú zrušené. CounterACT raz denne odošle varovný e-mail, ktorý označuje chybu komunikácie so serverom.

5. Vzdialená správa

Nastavenie iDRAC

Integrovaný ovládač vzdialeného prístupu Dell Remote Access Controller (iDRAC) je integrované riešenie serverového systému, ktoré poskytuje správcom zariadenia/podniku vzdialený prístup nezávislý od umiestnenia/nezávislý od OS cez LAN alebo internet. Použite modul na vykonávanie prístupu KVM, zapnutie/vypnutie/resetovanie a ktorý vykonáva úlohy, riešenie problémov a údržbu.

Vykonajte nasledujúce práce pomocou modulu iDRAC:

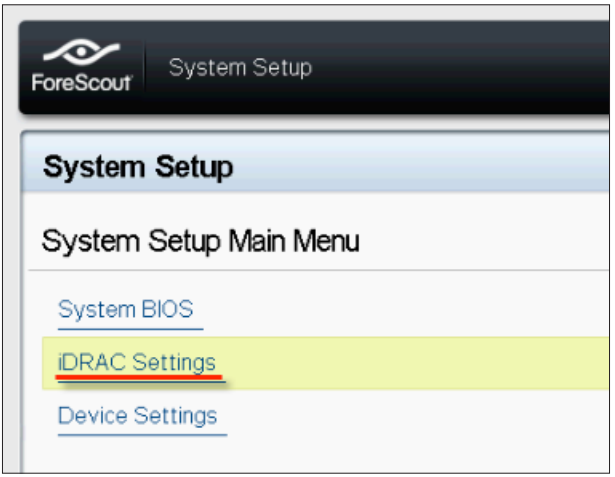
- *Povoľte a nakonfigurujte modul iDRAC.*
- *Pripojte modul k sieti.*
- *Prihláste sa do iDRAC.*

Povoľte a nakonfigurujte modul iDRAC

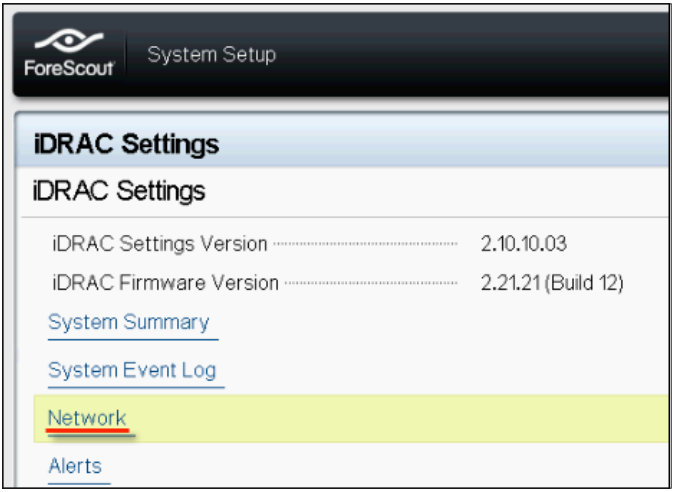
Zmeňte nastavenie iDRAC pre povolenie vzdialeného prístupu k zariadeniu CounterACT. Táto časť opisuje základné integračné nastavenia potrebné na prácu s CounterACT.

Konfigurácia iDRAC:

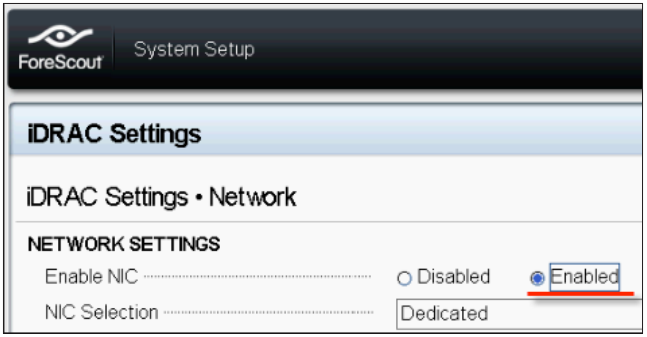
1. Zapnite riadený systém.
2. Počas samotestovania pri zapnutí (POST) stlačte F2.
3. Na stránke hlavného menu nastavenia systému vyberte **iDRAC Settings (Nastavenia iDRAC)**.



4. Na stránke nastavenia iDRAC vyberte **Network (Sieť)**.

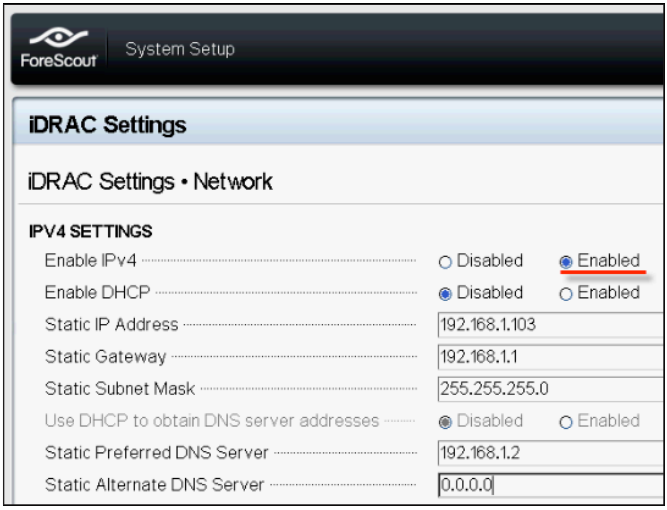


5. Nakonfigurujte nasledujúce nastavenia siete:
   - ***Nastavenia siete.*** Skontrolujte, či je pole **Enable NIC (Povoliť NIC)** nastavené na **Enabled (Povolené)**.

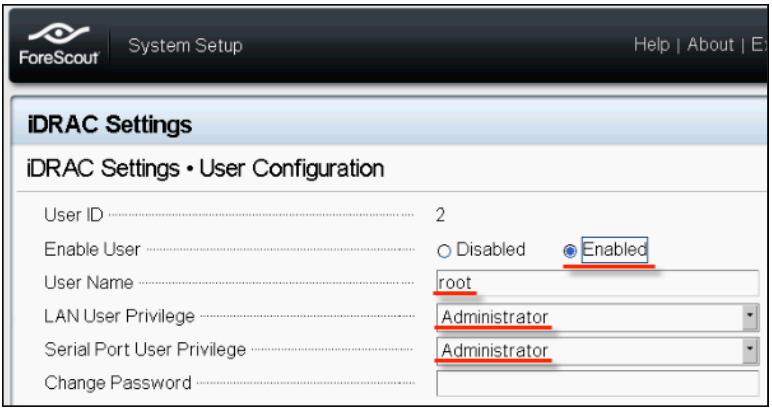


   - ***Bežné nastavenia.*** V poli s názvom DNS DRAC môžete aktualizovať dynamický server DNS (voliteľné).

- ***Nastavenia IPV4.*** Skontrolujte, či je pole **Enable IPv4 (Povoliť IPv4)** nastavené na **Enabled (Povolené)**. Nastavte pole **Enable DHCP (Povoliť DHCP)** na **Enabled (Povolené)** pre používanie dynamického adresovania IP alebo na Disabled (Zakázané) pre použitie statického adresovania IP. Ak je možnosť povolená, DHCP bude zariadeniu iDRAC automaticky priraďovať IP adresu, bránu a masku podsiete. Ak je možnosť zakázaná, zadajte hodnoty do polí pre **statickú IP adresu, statickú bránu a statickú masku podsiete**.



6. Vyberte možnosť **Back (Späť)**.
7. Vyberte **User Configuration (Konfigurácia používateľa)**.
8. Nakonfigurujte nasledujúce polia konfigurácie používateľa:
   - ***Enable User (Povoliť používateľa).*** Skontrolujte, či je toto pole nastavené na Enabled (Povolené).
   - ***User Name (Používateľské meno).*** Zadajte meno používateľa.
   - ***LAN and Serial Port User Privileges (Používateľské práva LAN and sériového portu).*** Nastavenie úrovne povolení pre správcu.
   - **Change Password (Zmeniť heslo).** Nastavte heslo pre prihlásenie používateľa login.



9. Vyberte možnosť **Back (Späť)** a potom **Finish (Dokončiť)**. Potvrďte zmenené nastavenia. Sieťové nastavenia sa uložia a systém sa reštartuje.

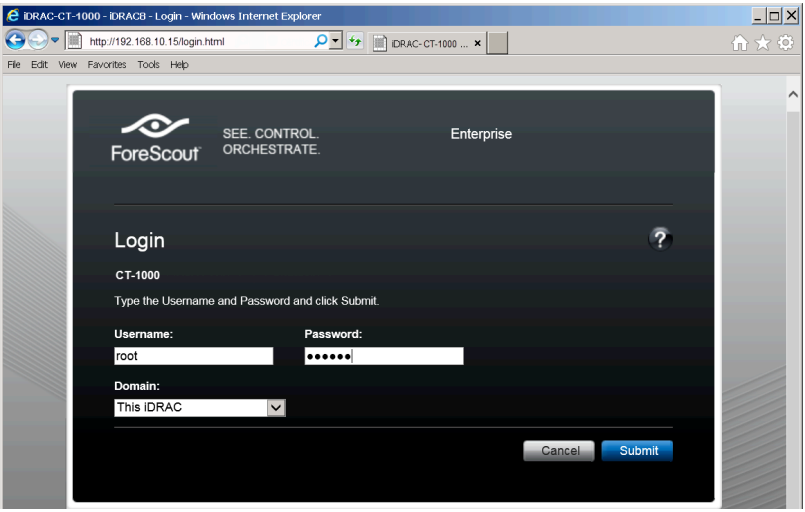
Pripojte modul k sieti

iDRAC sa pripája k sieti Ethernet. Obvykle sa pripája k sieti pre správu. Nasledujúci obrázok ukazuje umiestnenie portu iDRAC na zadnom paneli zariadenia CT-1000:

Prihláste sa do iDRAC

Prihlásenie do iDRAC:

1. Prejdite na IP adresu alebo doménové meno nakonfigurované v **iDRAC Settings (Nastavenia iDRAC) > Network (Sieť).**



2. Zadajte používateľské meno a heslo nakonfigurované na stránke pre konfiguráciu používateľa v nastavení systému iDRAC.
3. Vyberte **Submit (Potvrdiť)**.

Ďalšie informácie o iDRAC nájdete v používateľskej príručke iDRAC.

Je veľmi dôležité aktualizovať predvolené povolenia.

6. Overte pripojenie

Overte pripojenie správy rozhraní

Ak chcete otestovať pripojenie k rozhraniu pre správu, prihláste sa do zariadenia a spustite nasledujúci príkaz:

```
fstool linktest
```

Zobrazí sa nasledujúca informácia:

```
Management Interface status (Stav rozhrania
  pre správu)
Pinging default gateway information (Príkaz
  ping pre informácie o predvolenej bráne)
Ping statistics (Štatistika ping)
Performing Name Resolution Test (Vykonanie
  testu rozlíšenia názvu)
Test summary (Zhrnutie testu)
```

Overte pripojenie prepínača/zariadenia

Pred opustením dátového centra overte, či je prepínač správne pripojený k zariadeniu. Ak to chcete vykonať, spustite príkaz fstool ifcount na zariadení pre každé rozpoznané rozhranie.

```
fstool ifcount eth0 eth1 eth2
```

(Každé rozhranie oddeľte medzerou.)

Tento nástroj priebežne zobrazuje sieťovú prevádzku na uvedených rozhraniach. Pracuje v dvoch režimoch: na rozhranie alebo na VLAN. Režim je možné meniť na displeji. Zobrazí sa celkový počet bitov za sekundu a percentuálny podiel každej z nasledujúcich kategórií prevádzky:

- Monitorovacie rozhranie by malo v prvom rade vidieť zrkadlenú prevádzku — nad 90 %.
- Rozhranie pre odpoveď by malo v prvom rade vidieť širokopásmové prenosy.
- Rozhranie pre monitorovanie a odozvu by malo vidieť očakávané siete VLAN.

Možnosti príkazov:

```
v – zobrazenie v režime VLAN
I – zobrazenie v režime rozhrania
P – zobraziť predchádzajúce
N – zobraziť ďalšie
q – ukončenie zobrazenia
```

Režim VLAN:

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth3.untagged   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%
Show [v]lans [i]nterfaces <-[p]rev [n]ext->     [q]uit
```

Režim rozhrania:

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interface       Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth0            3Kbps   42.3%      0.0%      14.1%       43.7%
eth1            475bps  0.0%       100.0%    0.0%        0.0%
```

*To my MAC (Na moju MAC) — Cieľová adresa MAC je adresa MAC zariadenia.

*From my MAC (Z mojej MAC) — Prenos odoslaný týmto zariadením (Zdrojová adresa MAC je adresa MAC zariadenia. Cieľ môže byť typu broadcast alebo unicast).

Ak nevidíte žiadny prenos, skontrolujte, či je rozhranie v prevádzke. Použite nasledujúci príkaz na zariadení:

`ifconfig [názov rozhrania] up`

Vykonajte test príkazom Ping

Spustite test ping zo zariadenia do sieťového počítača na overenie pripojenia.

Ak chcete spustiť test:

1. Prihláste sa do zariadenia.
2. Spustite nasledujúci príkaz: **`Ping [IP adresa sieťového zariadenia]`** V predvolenom nastavení zariadenie samotné neodpovedá na ping.

7. Nastavte konzolu CounterACT

Nainštalujte konzolu CounterACT

Konzola CounterACT je aplikácia na centrálne riadenie, ktorá slúži na zobrazenie, sledovanie a analýzu aktivity rozpoznanej zariadením. Pomocou konzoly môžete definovať NAC, ochranu pred hrozbami, bránu Firewall a iné politiky. Ďalšie informácie nájdete v *návode na použitie konzoly CounterACT*.

Musíte určiť počítač na hosťovanie aplikačného softvéru konzoly CounterACT. Minimálne hardvérové požiadavky sú:

- Nevyhradený počítač s OS:
  - Windows XP, Windows Vista alebo Windows 7
  - Windows Server 2003 alebo Server 2008
  - Linux
- Pentium 3, 1 GHz
- 2 GB pamäte
- 1 GB miesta na disku

Na vykonanie inštalácie konzoly sú k dispozícii dve metódy:

Použite inštalačný softvér zabudovaný v zariadení.

1. Otvorte okno prehliadača z konzolového počítača.
2. Zadajte nasledujúci príkaz do adresného riadku prehliadača **`http://<Appliance ip>/install`**
   <Appliance ip> je IP adresa tohto zariadenia. Prehliadač zobrazí inštalačné okno konzoly.
3. Riaďte sa pokynmi na obrazovke.

Inštalácia z disku CounterACT CD-ROM

1. Vložte disk CounterACT CD ROM do jednotky DVD.
2. Otvorte súbor **`ManagementSetup.htm`** na disku CD ROM pomocou prehliadača.
3. Riaďte sa pokynmi na obrazovke.

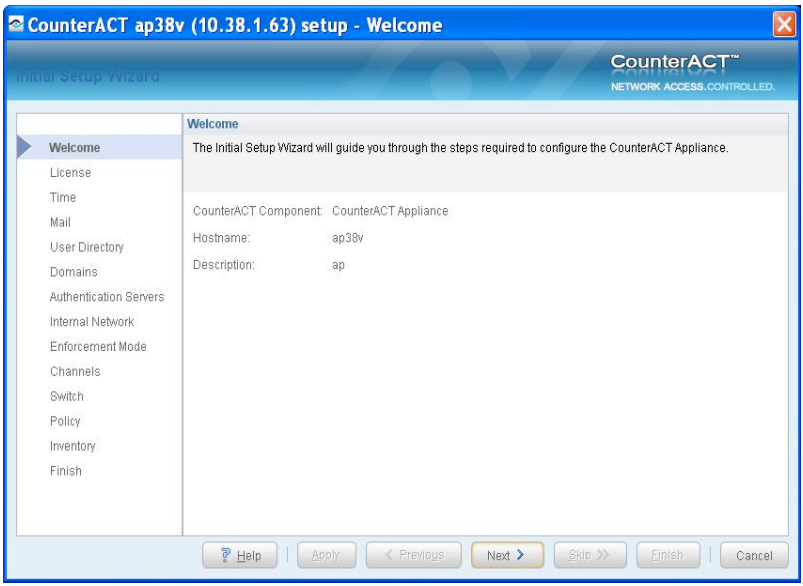
Prihlásenie

Po dokončení inštalácie sa môžete prihlásiť ku konzole CounterACT.

1. Vyberte ikonu CounterACT z umiestnenia pre zástupcu, ktoré ste vytvorili.
2. Zadajte IP adresu alebo hostiteľský názov zariadenia v poli **IP/Name (IP/názov)**.
3. Do poľa **User Name (Meno používateľa)** zadajte **admin**.
4. Do poľa **Password (Heslo)** zadajte heslo, ktoré ste vytvorili počas inštalácie zariadenia.
5. Zvolením **Login (Prihlásiť)** spustite konzolu.

Vykonajte úvodné nastavenie

Po prvom prihlásení sa zobrazí Sprievodca počiatočným nastavením. Tento sprievodca vás prevedie základnými konfiguračnými krokmi, ktoré zabezpečia, že zariadenie CounterACT bude pripravené na použitie rýchlo a efektívne.



Pred spustením úvodného nastavenia

Predtým ako budete pracovať so sprievodcom, pripravte si nasledujúce informácie:

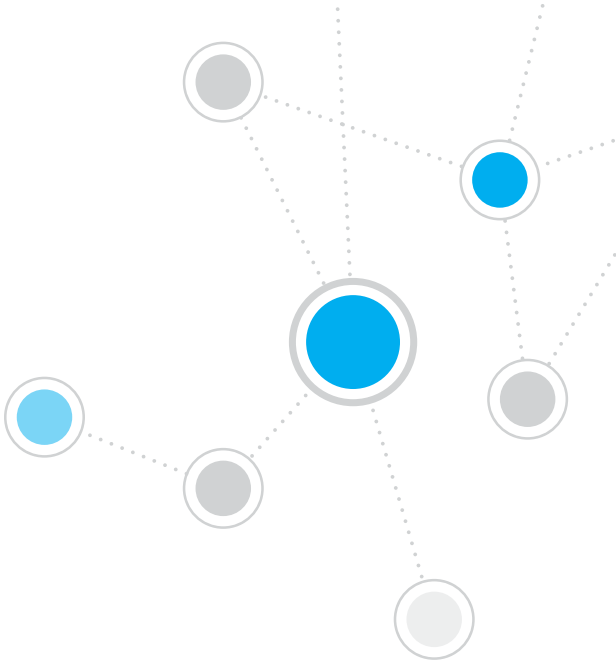
Informácie	Hodnoty
☐ Adresa servera NTP používaná vo vašej organizácii (voliteľné).	
☐ Interná poštová IP adresa. Táto adresa umožňuje doručovanie e-mailov zo zariadenia CounterACT, ak nie je povolený prenos SMTP zo zariadenia (voliteľné).	
☐ E-mailová adresa správcu CounterACT.	
☐ Rozhranie monitorovania a odozvy je definované v dátovom centre.	
☐ Segmenty alebo siete VLAN bez DHCP, segment siete alebo sieť VLAN, ku ktorej je priamo pripojené monitorovacie rozhranie a trvalé IP adresy, ktoré majú byť použité zariadením CounterACT pre každú takúto sieť VLAN. Táto informácia nie je nutná na inštaláciu správcu Enterprise Manager.	
☐ Rozsahy IP adries, ktoré bude zariadenie chrániť (všetky interné adresy vrátane nepoužívaných adries).	
☐ Informácie o účte používateľského priečinka a IP adresa servera s priečinkom používateľa.	
☐ Údaje pre doménu vrátane názvu a hesla účtu na správu domény.	
☐ Autentizačné servery, aby zariadenie CounterACT mohlo analyzovať, ktorí hostitelia siete sú úspešne overení.	
☐ Hlavná IP adresa prepínača, predajcu a parametre SNMP.	

Informácie o používaní správcu nájdete v *návode na použitie konzoly CounterACT* alebo v online pomocníkovi.

Kontaktné informácie

Pre technickú podporu ForeScout odošlite e-mail na support@forescout.com alebo zavolajte na:

- Bezplatná linka (USA): +1/866 377 8771
- Telefón (medzinárodný): +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 (USA): +1/866 377 8771
Telefón (medzinárodný): +1/408 213 3191
Podpora: +1/708 237 6591
Fax: +1/408 371 2284

400-00020-01