



ForeScout CounterACT[®] 7

Appliance CounterACT unique

Guide d'installation rapide

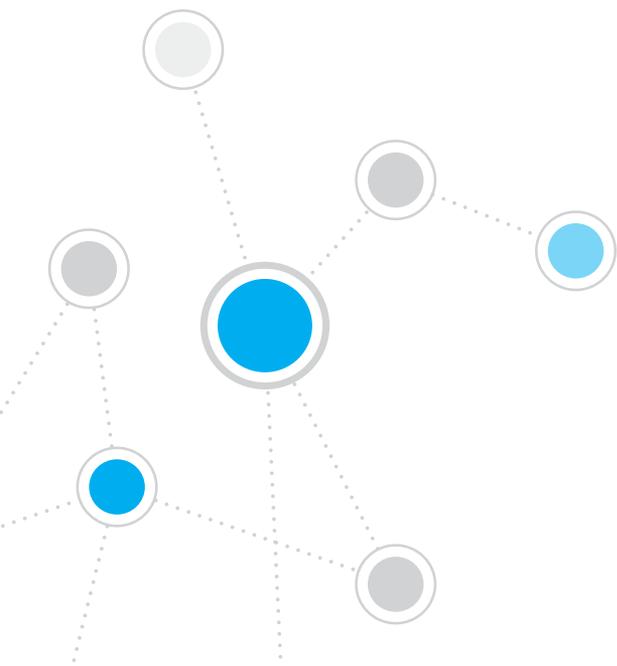


Table des Matières

Bienvenue dans ForeScout CounterACT® Version 7	3
Inclus dans votre paquet CounterACT	3
Présentation	4
1. Créer un plan de déploiement	5
Décider où déployer l'appliance	5
Connexions de l'interface de l'appliance	5
2. Configurer le Commutateur	8
A. Options de Connexion du Commutateur	8
B. Notes sur le réglage du commutateur	9
3. Brancher les câbles réseau et mettre sous tension	10
A. Déballer l'appliance et brancher les câbles	10
B. Enregistrer les affectations d'interface	11
C. Mettre l'appliance sous tension	11
4. Configurer l'appliance	12
Licence	14
Exigences liées à la connexion réseau	14
5. Gestion à distance	15
Configuration d'iDRAC	15
Connecter le module au réseau	18
Se connecter à iDRAC	18
6. Vérifier la connectivité	19
Vérifier la connexion de l'interface de gestion	19
Vérifier la connectivité du commutateur/appliance	19
Effectuer un test ping	20
7. Configurer la console CounterACT	21
Installer la console CounterACT	21
Se connecter	22
Exécuter la configuration initiale	22
Informations de contact	24

Bienvenue dans ForeScout CounterACT®

Version 7

ForeScout CounterACT est une appliance de sécurité physique ou virtuelle qui identifie et évalue de façon dynamique les périphériques réseau et les applications au moment où ils se connectent à votre réseau. Comme CounterACT n'a pas besoin d'agents, il fonctionne avec vos périphériques, qu'ils soient gérés ou non gérés, connus ou inconnus, PC ou mobiles, intégrés ou virtuels. CounterACT détermine rapidement l'utilisateur, le propriétaire, le système d'exploitation, la configuration du périphérique, les logiciels, les services, l'état du correctif et la présence d'agents de sécurité. Ensuite, il fournit une solution, un contrôle et une surveillance continue de ces périphériques lorsqu'ils accèdent au réseau. Il fait tout cela tout en s'intégrant de façon transparente à votre infrastructure informatique existante.



Ce guide décrit l'installation d'une appliance CounterACT autonome.

Pour plus d'informations sur le déploiement de plusieurs appliances afin de protéger un réseau d'entreprise, consultez le *Guide d'installation de CounterACT* et le *Manuel d'utilisateur de la console CounterACT*. Ces documents se trouvent sur le CD CounterACT dans le répertoire/docs.

De plus, vous pouvez accéder au site Web de support à l'adresse : <https://www.forescout.com/support> pour obtenir la documentation, les articles de base de connaissances et les mises à jour les plus récents concernant votre appliance.

Inclus dans votre paquet CounterACT

- Appliance CounterACT
- Guide d'installation rapide
- CD CounterACT avec logiciel de la console, Manuel d'utilisateur de la console CounterACT et Guide d'installation de CounterACT
- Document de garantie
- Supports de montage
- Câble d'alimentation
- Câble de connexion de console DB9 (pour les connexions série uniquement)

Présentation

Effectuez les étapes suivantes pour configurer CounterACT :

1. Créer un plan de déploiement
2. Configurer le commutateur
3. Brancher les câbles réseau et mettre sous tension
4. Configurer l'appliance
5. Gestion à distance
6. Vérifier la connectivité
7. Configurer la console CounterACT

1. Créer un plan de déploiement

Avant l'installation, vous devez décider où déployer l'appliance et connaître les connexions de l'interface de l'appliance.

Décider où déployer l'appliance

Il est essentiel de choisir le bon emplacement d'installation de l'appliance sur le réseau pour garantir la réussite du déploiement et les performances optimales de CounterACT. L'emplacement correct dépend de vos objectifs de mise en place et des politiques d'accès au réseau. L'appliance doit pouvoir surveiller le trafic pertinent pour la politique souhaitée. Par exemple, si votre politique dépend de la surveillance d'événements d'autorisation entre des points de terminaison et des serveurs d'authentification d'entreprise, l'appliance devra être installée de façon à ce qu'elle voie le trafic des points de terminaison se diriger vers le ou les serveurs d'authentification.

Pour plus d'informations sur l'installation et le déploiement, consultez le Guide d'installation de CounterACT, qui se trouve sur le CD CounterACT que vous avez reçu avec ce paquet.

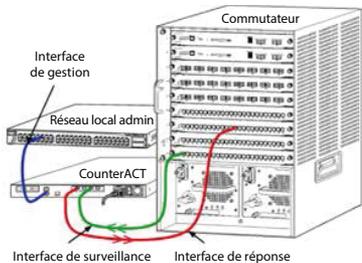
Connexions de l'interface de l'appliance

En général, l'appliance est configurée avec trois connexions vers le commutateur réseau.

Interface de gestion

Cette interface vous permet de gérer CounterACT et d'exécuter des requêtes et une inspection approfondie des points de terminaison. L'interface doit être connectée à un port de commutateur qui a accès à tous les points de terminaison du réseau.

Chaque appliance requiert une connexion de gestion unique vers le réseau. Cette connexion requiert une adresse IP sur le réseau local et un accès au port 13000/TCP depuis des machines qui exécuteront l'application de gestion de la console CounterACT. L'interface de gestion doit avoir accès aux éléments suivants sur votre réseau :



Port	Service	Vers ou Depuis CounterACT	Fonction
22/TCP	SSH	Vers	Permet d'accéder à l'interface de ligne de commande de CounterACT.
2222/TCP			(Haute disponibilité) Permet d'accéder aux périphériques CounterACT physiques qui font partie du cluster Haute disponibilité. Utilisez 22/TCP pour accéder à l'adresse IP partagée (virtuelle) du cluster.

Port	Service	Vers ou Depuis CounterACT	Fonction
25/TCP	SMTP	Depuis	Utilisé pour envoyer des messages depuis CounterACT
53/UDP	DNS	Depuis	Permet à CounterACT de résoudre des adresses IP internes.
80/TCP	HTTP	Vers	Autorise la redirection HTTP.
123/UDP	NTP	Depuis	Permet à CounterACT d'accéder à un serveur de temps NTP. Par défaut, CounterACT utilise ntp.foreScout.net.
135	WMI	Depuis	Permet à CounterACT d'exécuter une investigation approfondie et de contrôler les points de terminaison Windows à l'aide de WMI.
139/TCP	SMB, MS-RPP	Depuis	Permet l'inspection à distance des points de terminaison Windows (pour les points de terminaison exécutant Windows 7 et versions antérieures).
445/TCP			Permet l'inspection à distance des points de terminaison Windows.
161/UDP	SNMP	Depuis	Permet à CounterACT de communiquer avec le matériel d'infrastructure réseau, tel que des commutateurs et des routeurs. Pour plus d'informations sur la configuration de SNMP, consultez le <i>Manuel d'utilisateur de la console CounterACT</i> .
162/UDP	SNMP	Vers	Permet à CounterACT de recevoir des interruptions SNMP provenant du matériel d'infrastructure réseau, tel que des commutateurs et des routeurs. Pour plus d'informations sur la configuration de SNMP, consultez le <i>Manuel d'utilisateur de la console CounterACT</i> .
443/TCP	HTTPS	Vers	Autorise la redirection HTTP à l'aide de TLS.
2200/TCP	Secure Connector	Vers	Permet à SecureConnector de créer une connexion sécurisée (SSH chiffré) vers l'appliance depuis des ordinateurs Macintosh/Linux. <i>SecureConnector</i> est un agent basé sur un script qui permet de gérer des points de terminaison Macintosh et Linux lorsqu'ils sont connectés au réseau.

10003/TCP	Secure Connector pour Windows	Vers	<p>Permet à SecureConnector de créer une connexion sécurisée (SSL chiffré) vers l'appliance depuis des ordinateurs Windows. <i>SecureConnector</i> est un agent qui permet de gérer des points de terminaison Windows lorsqu'ils sont connectés au réseau. Reportez-vous au <i>Manuel d'utilisateur de la console CounterACT</i> pour obtenir plus d'informations sur SecureConnector.</p> <p>Lorsque SecureConnector se connecte à une appliance ou à Enterprise Manager, il est redirigé vers l'appliance à laquelle son hôte est affecté. Vérifiez que ce port est ouvert pour toutes les appliances et pour Enterprise Manager afin d'assurer la transparence de la mobilité dans toute l'entreprise.</p>
13000/TCP	CounterACT	Vers	<p>Autorise la connexion entre la console et l'appliance.</p> <p>Pour les systèmes avec plusieurs appliances CounterACT, autorise la connexion entre la console et Enterprise Manager et entre Enterprise Manager et chaque appliance.</p>

Interface de surveillance

Cette connexion permet à l'appliance de surveiller et de suivre le trafic réseau.

Le trafic est mis en miroir sur un port sur le commutateur et surveillé par l'appliance. En fonction du nombre de réseaux locaux virtuels (VLAN) mis en miroir, le trafic peut ou pas avoir une balise 802.1Q VLAN.

- **VLAN unique (sans balise) :** lorsque le trafic surveillé est généré depuis un VLAN unique, le trafic mis en miroir n'a pas besoin d'avoir la balise VLAN.
- **Plusieurs VLAN (avec balise) :** lorsque le trafic surveillé provient de plusieurs VLAN, le trafic mis en miroir doit avoir une balise 802.1Q VLAN.

Lorsque deux commutateurs sont connectés sous forme de paire redondante, l'appliance doit surveiller le trafic provenant des deux commutateurs.

L'interface de surveillance ne nécessite pas d'adresse IP.

Interface de réponse

L'appliance répond au trafic à l'aide de cette interface. Le trafic de réponse est utilisé pour se protéger contre les activités malveillantes et exécuter les actions de politique de CAR. Ces actions peuvent inclure, par exemple, la redirection de navigateurs Web ou l'exécution du blocage d'un pare-feu. La configuration du port de commutateur liée dépend du trafic surveillé.

- **VLAN unique (sans balise) :** lorsque le trafic surveillé est généré depuis un VLAN unique, l'interface de réponse doit être configurée pour faire partie du même VLAN. Dans ce cas, l'appliance nécessite une adresse IP unique sur ce VLAN.
- **Plusieurs VLAN (avec balise) :** si le trafic surveillé provient de plusieurs VLAN, l'interface de réponse doit également être configurée avec le balisage 802.1Q pour les mêmes VLAN. L'appliance nécessite une adresse IP pour chaque VLAN protégé.

2. Configurer votre Commutateur

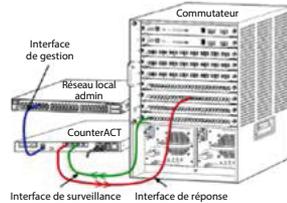
A. Options de Connexion du Commutateur

L'appliance a été conçue pour s'intégrer de façon transparente à une grande variété d'environnements réseau. Pour intégrer correctement l'appliance dans votre réseau, vérifiez que votre commutateur est configuré pour surveiller le trafic requis.

Plusieurs options sont disponibles pour connecter l'appliance à votre commutateur.

1. Déploiement standard (interfaces de gestion, de surveillance et de réponse séparées)

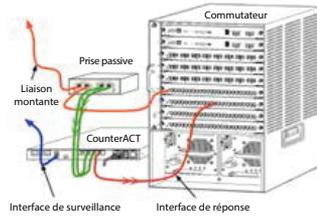
Le déploiement recommandé utilise trois ports séparés. Ces ports sont décrits dans *Connexions de l'interface de l'appliance*.



2. Prise de signal passive

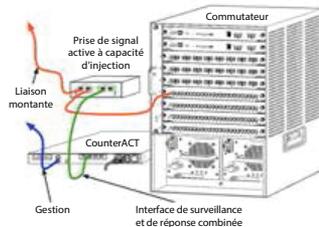
Au lieu de se connecter à un port de surveillance de commutateur, l'appliance peut utiliser une prise de signal passive.

Une prise passive requiert deux ports de surveillance, sauf dans le cas de prises de « recombinaison », qui combinent les deux flux duplex en un seul port. Le trafic sur le port de prise et l'interface de réponse doit être configuré de la même façon. Par exemple, si le trafic sur le port de prise a une balise VLAN (802.1Q), l'interface de réponse doit également être un port avec une balise VLAN.



3. Prise de signal active (à capacité d'injection)

Lorsque l'appliance utilise une prise de signal qui est à *capacité d'injection*, les interfaces de surveillance et de réponse peuvent être combinées. Il n'est pas nécessaire de configurer un port de réponse séparé sur le commutateur. Cette option peut être utilisée pour tout type de configuration de commutateur en amont ou en aval.



4. Réponse de couche IP (pour les installations de commutateur de couche 3)

L'appliance peut utiliser sa propre interface de gestion pour répondre au trafic. Bien que cette option puisse être utilisée avec n'importe quel trafic surveillé, elle est recommandée lorsque l'appliance surveille des ports qui ne font partie d'aucun VLAN et que, par conséquent, elle ne peut pas répondre au trafic surveillé à l'aide d'un autre port de commutateur. Ceci est typique lors de la surveillance d'une liaison connectant deux routeurs.

Cette option ne peut pas répondre aux demandes de protocole ARP (Address Resolution Protocol), ce qui limite la capacité de l'appliance à détecter les analyses destinées aux adresses IP incluses dans le sous-réseau surveillé. Cette limite ne s'applique pas lorsque le trafic entre deux routeurs est surveillé.

B. Notes sur le réglage du commutateur

Balises VLAN (802.1Q)

- **Surveillance d'un VLAN unique (trafic sans balise)** Si le trafic surveillé provient d'un VLAN unique, le trafic n'a pas besoin de balises 802.1Q.
- **Surveillance de plusieurs VLAN (trafic avec balise)** Si le trafic surveillé provient de deux VLAN ou plus, l'interface de surveillance et l'interface de réponse doivent accepter les balises 802.1Q. La surveillance de plusieurs VLAN est l'option recommandée car elle offre la meilleure couverture globale tout en minimisant le nombre de ports de mise en miroir.
- Si le commutateur ne peut pas utiliser de balise 802.1Q VLAN sur les ports de mise en miroir, effectuez l'une des actions suivantes :
 - Mettre en miroir un seul VLAN
 - Mettre en miroir un seul port de liaison montante sans balise
 - Utiliser l'option de réponse de couche IP
- Si le commutateur ne peut mettre en miroir qu'un seul port, alors mettez en miroir un port de liaison montante unique. Il peut comporter une balise. En général, si le commutateur supprime les balises 802.1Q VLAN, vous devez utiliser l'option de réponse de couche IP.

Informations supplémentaires

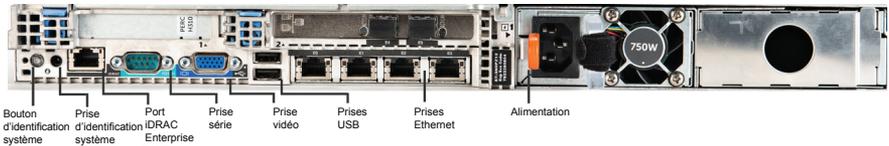
- Si le commutateur ne peut pas mettre en miroir le trafic transmis et le trafic reçu, surveillez tout le commutateur, les VLAN complets (cela fournit le trafic transmis/reçu) ou simplement une interface (ce qui n'autorise pas le trafic transmis/reçu). Vérifiez que vous ne surchargez pas le port de mise en miroir.
- Pour certains commutateurs (tels que Cisco 6509), il peut être nécessaire de supprimer complètement les anciennes configurations de port avant d'entrer de nouvelles configurations. Si vous ne procédez pas à la suppression des anciennes informations sur le port, le commutateur supprime les balises 802.1Q.

3. Brancher les câbles réseau et mettre sous tension

A. Déballez l'apppliance et branchez les câbles

1. Sortez l'apppliance et le câble d'alimentation de l'emballage de transport.
2. Sortez le kit de rails que vous avez reçu avec l'apppliance.
3. Montez le kit de rails sur l'apppliance et fixez l'apppliance sur le support.
4. Branchez les câbles réseau entre les interfaces réseau sur le panneau arrière de l'apppliance et les ports de commutateur.

Exemple de panneau arrière — Périphérique CounterACT



B. Enregistrer les affectations d'interface

Après avoir terminé l'installation de l'appliance sur le centre de données et installé la console CounterACT, vous êtes invité à enregistrer les affectations d'interface. Ces affectations, appelées *définitions de canal*, sont entrées dans l'assistant Configuration initiale qui s'ouvre lors de votre première connexion à la console.

Enregistrez les affectations d'interface physique ci-dessous et utilisez-les lorsque vous avez terminé la configuration de canal sur la console.

Interface Ethernet	Affectation d'interface (p. ex. Gestion, Surveillance, Réponse)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Mettre l'appliance sous tension

1. Branchez le câble d'alimentation à la prise d'alimentation sur le panneau arrière de l'appliance.
2. Branchez l'autre extrémité du câble d'alimentation à une prise secteur mise à la terre.
3. Branchez le clavier et l'écran à l'appliance ou configurez l'appliance pour une connexion série. Consultez le *Guide d'installation de CounterACT* qui se trouve sur le CD CounterACT.
4. Mettez l'appliance sous tension depuis le panneau avant.

Important : mettez la machine hors tension avant de la débrancher.

4. Configurer l'apppliance

Préparez les informations suivantes avant de configurer l'apppliance.

<input type="checkbox"/> Nom d'hôte de l'apppliance	
<input type="checkbox"/> Mot de passe d'administrateur de CounterACT	Conserver le mot de passe dans un endroit sûr
<input type="checkbox"/> Interface de gestion	
<input type="checkbox"/> Adresse IP de l'apppliance	
<input type="checkbox"/> Masque de réseau	
<input type="checkbox"/> Adresse IP de la passerelle par défaut	
<input type="checkbox"/> Nom de domaine DNS	
<input type="checkbox"/> Adresses de serveur DNS	

Après la mise sous tension, vous êtes invité à démarrer la configuration avec le message suivant :

```
Le démarrage de l'apppliance CounterACT est
terminé.
Appuyez sur <Entrée> pour continuer.
```

1. Appuyez sur **Entrée** pour afficher le menu suivant :

```
1) Configurer CounterACT
2) Restaurer la configuration CounterACT
   enregistrée
3) Identifier et renuméroter les interfaces réseau
4) Configurer la disposition du clavier
5) Mettre la machine hors tension
6) Redémarrer la machine
Choix (1-6) :1
```

2. Sélectionnez **1** - Configurer CounterACT. À l'invite :

```
Continuer : (oui/non) ?
```

Appuyez sur **Entrée** pour lancer la configuration.

3. Le menu **Mode Haute disponibilité** s'ouvre. Appuyez sur **Entrée** pour sélectionner Installation standard.
4. L'invite **Configuration initiale de CounterACT** est affichée. Appuyez sur **Entrée** pour continuer.
5. Le menu **Sélectionner le type d'installation de CounterACT** s'ouvre. Saisissez **1** et appuyez sur **Entrée** pour installer une appliance CounterACT standard. La configuration est initialisée. Cela peut prendre du temps.

6. À l'invite **Entrer la description de la machine**, entrez un court texte identifiant ce périphérique, puis appuyez sur **Entrée**.
Voici ce qui s'affiche :

```
>>>>> Définir le mot de passe
      d'administrateur <<<<<<

Ce mot de passe est utilisé pour se connecter
en tant qu'utilisateur « racine » au système
d'exploitation de la machine et en tant
qu'utilisateur « admin » à la console CounterACT.
Le mot de passe doit contenir entre 6 et 15
caractères dont au moins un caractère non
alphabétique.

Mot de passe d'administrateur :
```

7. À l'invite **Définir le mot de passe d'administrateur**, saisissez la chaîne qui sera votre mot de passe (la chaîne n'apparaît pas à l'écran) et appuyez sur **Entrée**. Vous êtes invité à confirmer le mot de passe. Le mot de passe doit contenir entre 6 et 15 caractères dont au moins un caractère non alphabétique.
-  *Connectez-vous à l'appliance en tant qu'utilisateur racine et connectez-vous à la console en tant qu'utilisateur admin.*
8. À l'invite **Définir le nom d'hôte**, saisissez un nom d'hôte et appuyez sur **Entrée**. Le nom d'hôte peut être utilisé lors de la connexion à la console. Il est affiché sur la console pour vous aider à identifier l'appliance CounterACT que vous voyez.
9. L'écran **Configurer les paramètres réseau** vous invite à entrer une série de paramètres de configuration. Saisissez une valeur à chaque invite et appuyez sur **Entrée** pour continuer.
- Les composants de CounterACT communiquent via des interfaces de gestion. Le nombre d'interfaces de gestion répertoriées dépend du modèle de l'appliance.
 - L'**adresse IP de gestion** est l'adresse de l'interface via laquelle les composants de CounterACT communiquent. Ajoutez un ID de VLAN pour cette interface uniquement si l'interface utilisée pour communiquer entre les composants de CounterACT est connectée à un port avec balise.
 - S'il y a plusieurs **adresses de serveur DNS**, séparez-les avec un espace. La plupart des serveurs DNS internes résolvent les adresses externes et internes, mais il est possible que vous deviez inclure un serveur DNS résolvant en externe. Comme presque toutes les requêtes DNS exécutées par l'appliance sont destinées à des adresses internes, le serveur DNS externe doit être répertorié en dernier.
10. L'écran **Résumé de la configuration** est affiché. Vous êtes invité à effectuer des tests de connectivité générale, à reconfigurer des paramètres ou à terminer la configuration. Saisissez **D** pour terminer la configuration.

Licence

Après l'installation, vous devez installer la licence de démo initiale fournie par votre représentant CounterACT. La licence est installée au cours de la configuration initiale de la console. Cette licence de démo initiale est valide pendant un certain nombre de jours. Vous devez installer une licence permanente avant la fin de cette période. Vous serez contacté par e-mail concernant la date d'expiration. De plus, des informations sur la date d'expiration et la licence d'état sont affichées sur le panneau Appliances/périphériques de la console.

Lorsque vous recevez une licence permanente, elle est validée quotidiennement par le serveur de licences de ForeScout. Des alertes et des violations de licence sont affichées dans le volet Détails du périphérique.

Les licences ne pouvant pas être validées pendant un mois seront révoquées. Consultez le Guide d'installation de CounterACT pour plus de détails sur les licences.

Exigences liées à la connexion réseau

Au moins un périphérique CounterACT (Appliance ou Enterprise Manager) doit pouvoir accéder à Internet. Cette connexion est utilisée pour valider les licences CounterACT par rapport au serveur de licences ForeScout.

Les licences ne pouvant pas être authentifiées pendant un mois seront révoquées. CounterACT envoie un e-mail d'avertissement une fois par jour indiquant qu'il existe une erreur de communication avec le serveur.

5. Gestion à distance

Configuration d'iDRAC

iDRAC (Integrated Dell Remote Access Controller) est une solution de système de serveur intégrée qui vous donne un accès à distance indépendant de l'emplacement / indépendant de l'OS sur le réseau local ou Internet à des Appliances / Enterprise Managers CounterACT. Utilisez le module pour gérer l'accès KVM, mettre sous tension / hors tension / réinitialiser et effectuer des tâches de dépannage et de maintenance.

Effectuez les étapes suivantes pour utiliser le module iDRAC :

- Activer et configurer le module iDRAC
- Connecter le module au réseau
- Se connecter à iDRAC

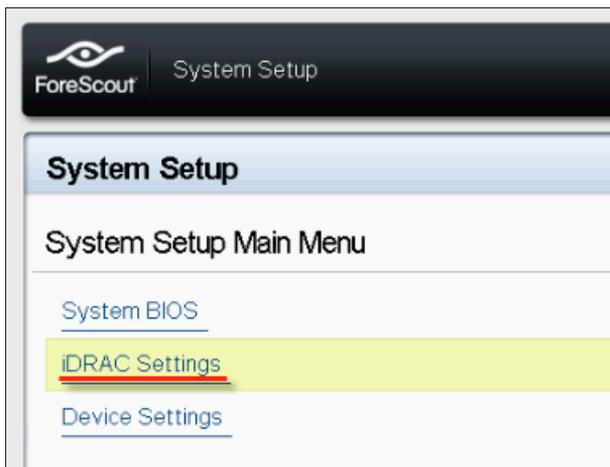
Activer et configurer le module iDRAC

Modifiez les paramètres iDRAC pour activer l'accès à distance sur le périphérique CounterACT. Cette section décrit les paramètres d'intégration de base requis pour utiliser CounterACT.

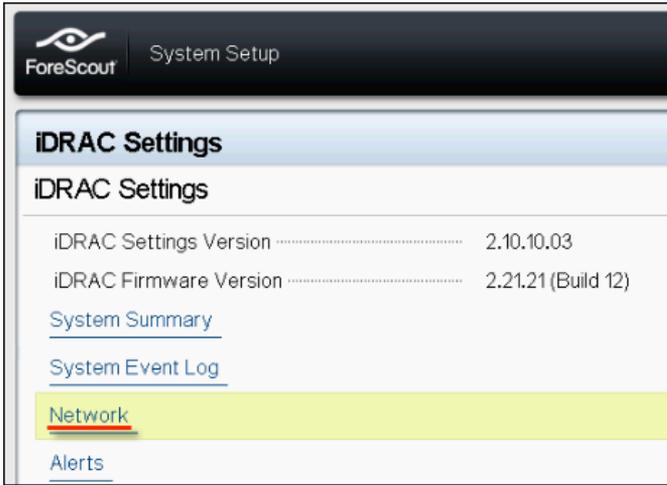
Pour configurer iDRAC :

1. Mettez le système géré sous tension.
2. Sélectionnez F2 lors de l'autotest de mise sous tension (POST).
3. Sur la page Menu principal de configuration du système, sélectionnez

Paramètres iDRAC.

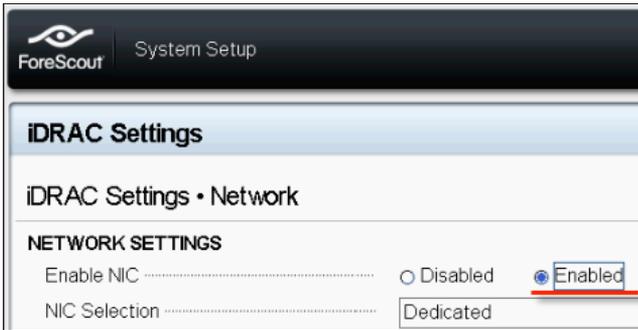


4. Sur la page Paramètres iDRAC, sélectionnez **Réseau**.



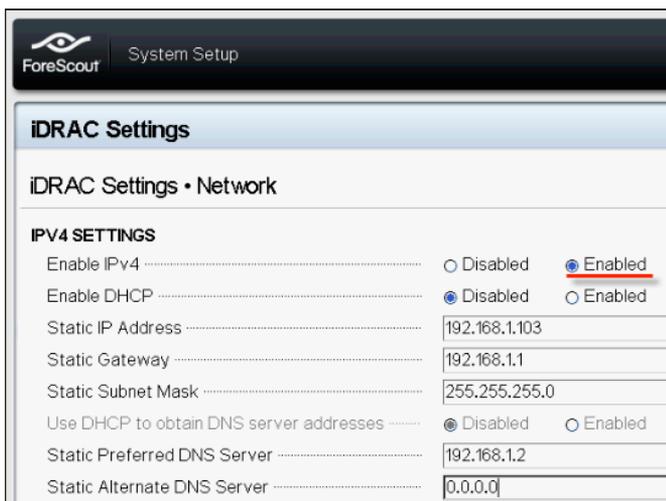
5. Configurez les paramètres réseau suivants :

- **Paramètres réseau.** Vérifiez que le champ **Activer la carte réseau** est réglé sur **Activé**.



- **Paramètres communs.** Dans le champ Nom DRAC DNS, vous pouvez mettre à jour un DNS dynamique (facultatif).

- **Paramètres IPv4.** Vérifiez que le champ **Activer IPv4** est réglé sur **Activé**. Réglez le champ **Activer DHCP** sur **Activé** pour utiliser l'adressage IP dynamique ou sur **Désactivé** pour utiliser l'adressage IP statique. S'il est activé, DHCP affecte automatiquement les adresses IP, la passerelle et le masque de sous-réseau à iDRAC. S'il est désactivé, entrez des valeurs dans les champs **Adresse IP statique**, **Passerelle statique** et **Masque de sous-réseau statique**.



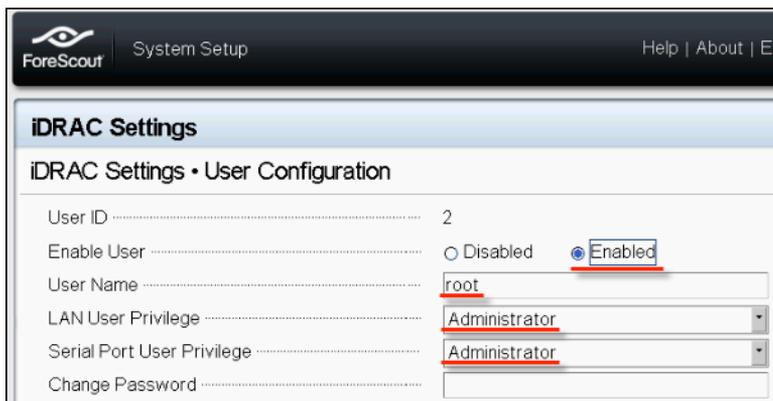
iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> <u>Enabled</u>
Enable DHCP	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static IP Address	<input type="text" value="192.168.1.103"/>	
Static Gateway	<input type="text" value="192.168.1.1"/>	
Static Subnet Mask	<input type="text" value="255.255.255.0"/>	
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static Preferred DNS Server	<input type="text" value="192.168.1.2"/>	
Static Alternate DNS Server	<input type="text" value="0.0.0.0"/>	

6. Sélectionnez **Retour**.
7. Sélectionnez **Configuration utilisateur**.
8. Configurez les champs Configuration utilisateur suivants :
 - **Activer l'utilisateur.** Vérifiez que ce champ est réglé sur **Activé**.
 - **Nom d'utilisateur.** Entrez un nom d'utilisateur.
 - **Privilèges d'utilisateur du réseau local et du port série.** Définissez les niveaux de privilège sur **Administrateur**.
 - **Modifier le mot de passe.** Définissez un mot de passe pour la connexion utilisateur.



iDRAC Settings

iDRAC Settings • User Configuration

User ID	2
Enable User	<input type="radio"/> Disabled <input checked="" type="radio"/> <u>Enabled</u>
User Name	<input type="text" value="root"/>
LAN User Privilege	<input type="text" value="Administrator"/>
Serial Port User Privilege	<input type="text" value="Administrator"/>
Change Password	<input type="text"/>

9. Sélectionnez **Retour** et **Terminer**. Confirmez les paramètres modifiés. Les paramètres réseau sont enregistrés et le système redémarre.

Connecter le module au réseau

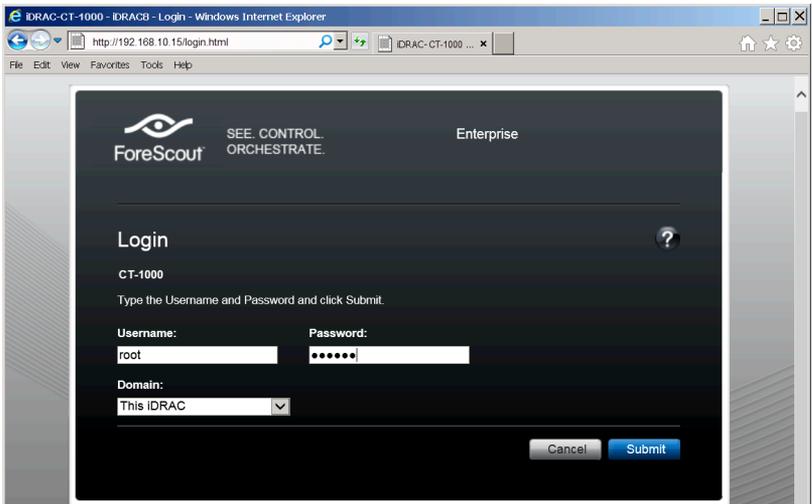
Le module iDRAC se connecte à un réseau Ethernet. Il est habituel de le connecter à un réseau de gestion. L'image suivante montre l'emplacement du port iDRAC sur le panneau arrière de l'apppliance CT-1000 :



Se connecter à iDRAC

Pour se connecter à iDRAC :

1. Accédez à l'adresse IP ou au nom de domaine configuré dans **Paramètres iDRAC > Réseau**.



2. Entrez le nom d'utilisateur et le mot de passe configurés sur la page Configuration utilisateur de la configuration du système iDRAC.
3. Sélectionnez **Envoyer**.

Pour plus d'informations sur iDRAC, consultez le [Guide d'utilisateur du module iDRAC](#).

Il est très important de mettre à jour les informations d'identification par défaut.

6. Vérifier la connectivité

Vérifier la connexion de l'interface de gestion

Pour tester la connexion de l'interface de gestion, connectez-vous à l'appliance et exécutez la commande suivante :

```
fstool linktest
```

Les informations suivantes sont affichées :

```
État de l'interface de gestion
Test ping des informations de passerelle par
défaut
Statistiques ping
Exécution d'un test de résolution de nom
Résumé du test
```

Vérifier la connectivité du commutateur/appliance

Vérifiez que le commutateur est bien connecté à l'appliance avant de quitter le centre de données. Pour cela, exécutez la commande `fstool ifcount` sur l'appliance pour chaque interface détectée.

```
fstool ifcount eth0 eth1 eth2  
(Séparez chaque interface par un espace.)
```

Cet outil affiche en continu le trafic réseau sur les interfaces spécifiées. Il fonctionne en deux modes : par interface ou par VLAN. Il est possible de modifier le mode sur l'écran. Le nombre total de bits par seconde et le pourcentage de chacune des catégories de trafic suivantes sont affichés :

- L'interface de surveillance doit principalement voir le trafic mis en miroir — au-dessus de 90 %.
- L'interface de réponse doit principalement voir le trafic de diffusion.
- Les interfaces de surveillance et de réponse doivent voir les VLAN attendus.

Options de commande :

```
v - affichage en mode VLAN  
I - affichage en mode interface  
P - afficher le précédent  
N - afficher le suivant  
q - quitter l'affichage
```

Mode 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
```

Mode interface :

```
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 — L'adresse MAC de destination est l'adresse MAC de l'apppliance.

* From my MAC — Trafic envoyé par cette appliance (L'adresse MAC source est l'adresse MAC de l'apppliance. La destination peut être de diffusion ou de monodiffusion).

Si vous ne voyez aucun trafic, vérifiez que l'interface est active. Utilisez la commande suivante sur l'apppliance :

```
ifconfig [interface name] up
```

Effectuer un test ping

Exécutez un test ping entre l'apppliance et un poste de travail réseau pour vérifier la connectivité.

Pour exécuter le test :

1. Connectez-vous à l'apppliance.
2. Exécutez la commande suivante : **Ping [network desktop IP]**
Par défaut, l'apppliance elle-même ne répond pas au test ping.

7. Configurer la console CounterACT

Installer la console CounterACT

La console CounterACT est une application de gestion centrale utilisée pour afficher, suivre et analyser l'activité détectée par l'appliance. Le contrôle d'accès au réseau, la protection contre les menaces, un pare-feu et d'autres politiques peuvent être définis à partir de la console. Consultez le *Manuel d'utilisateur de la console CounterACT* pour plus d'informations.

Vous devez fournir une machine pour héberger le logiciel d'application de la console CounterACT. Voici les exigences matérielles minimales :

- Machine non dédiée, exécutant :
 - Windows XP, Windows Vista ou Windows 7
 - Windows Server 2003 ou Server 2008
 - Linux
- Pentium 3,1 GHz
- 2 Go de mémoire
- 1 Go d'espace disque

Deux méthodes sont disponibles pour effectuer l'installation de la console :

Utilisez le logiciel d'installation intégré à votre appliance.

1. Ouvrez une fenêtre de navigateur sur l'ordinateur de la console.
2. Saisissez ce qui suit dans la ligne d'adresse du navigateur
[http://<Appliance ip>/install](http://<Appliance_ip>/install)
Où <Appliance ip> est l'adresse IP de cette appliance. Le navigateur affiche la fenêtre d'installation de la console.
3. Suivez les instructions à l'écran.

Installer à partir du CD-ROM CounterACT

1. Insérez le CD-ROM CounterACT dans le lecteur DVD.
2. Ouvrez le fichier **ManagementSetup.htm** sur le CD ROM avec un navigateur.
3. Suivez les instructions à l'écran.

Se connecter

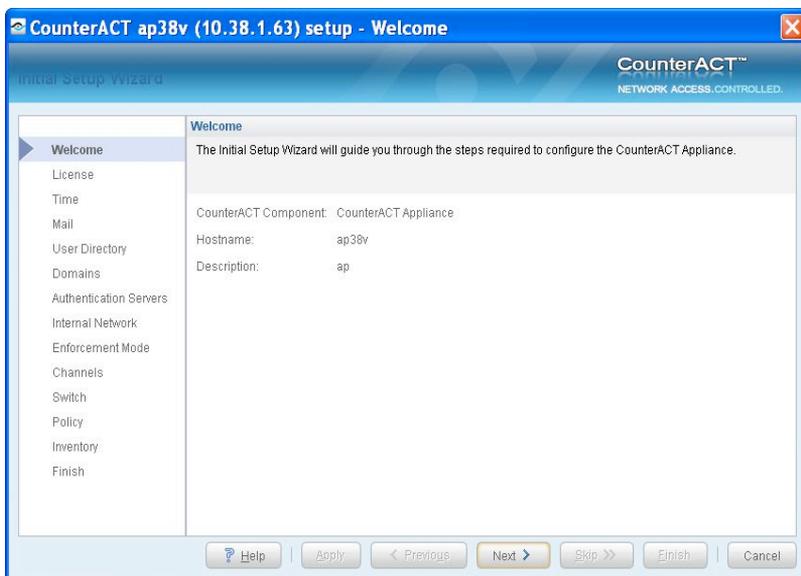
Une fois l'installation terminée, vous pouvez vous connecter à la console CounterACT.

1. Sélectionnez l'icône CounterACT depuis l'emplacement de raccourci que vous avez créé.
2. Entrez l'adresse IP ou le nom d'hôte de l'appliance dans le champ **IP/Nom**.
3. Dans le champ **Nom d'utilisateur**, entrez **admin**.
4. Dans le champ **Mot de passe**, entrez le mot de passe que vous avez créé lors de l'installation de l'appliance.
5. Sélectionnez **Se connecter** pour lancer la console.



Exécuter la configuration initiale

Lors de la première connexion, l'assistant Configuration initiale apparaît. L'assistant vous guide lors des étapes de configuration essentielles pour s'assurer que CounterACT est opérationnel rapidement et efficacement.



Avant de commencer la configuration initiale

Préparez les informations suivantes avant d'utiliser l'assistant :

Informations	Valeurs
<input type="checkbox"/> Adresse de serveur NTP utilisée par votre entreprise (facultatif).	
<input type="checkbox"/> Adresse IP de relais de messagerie interne. Cela permet de remettre les e-mails de CounterACT si le trafic SMTP n'est pas autorisé depuis l'appliance (facultatif).	
<input type="checkbox"/> Adresse e-mail de l'administrateur de CounterACT.	
<input type="checkbox"/> Affectations d'interfaces de surveillance et de réponse définies sur le centre de données.	
<input type="checkbox"/> Pour les segments ou les VLAN sans DHCP, le segment réseau ou les VLAN auxquels l'interface de surveillance est directement connectée et une adresse IP permanente à utiliser par CounterACT sur chaque VLAN. Ces informations ne sont pas requises pour la configuration d'Enterprise Manager.	
<input type="checkbox"/> Plages d'adresses IP que l'appliance protégera (toutes les adresses internes, y compris les adresses inutilisées).	
<input type="checkbox"/> Informations du compte Répertoire utilisateur et adresse IP du serveur Répertoire utilisateur.	
<input type="checkbox"/> Informations d'identification de domaine, y compris le nom et le mot de passe du compte administratif de domaine.	
<input type="checkbox"/> Serveurs d'authentification pour que CounterACT puisse analyser quels hôtes réseau se sont correctement authentifiés.	
<input type="checkbox"/> Adresse IP, fournisseur et paramètres SNMP du commutateur principal.	

Consultez le *Manuel d'utilisateur de la console CounterACT* ou l'aide en ligne pour plus d'informations sur l'utilisation de l'assistant.

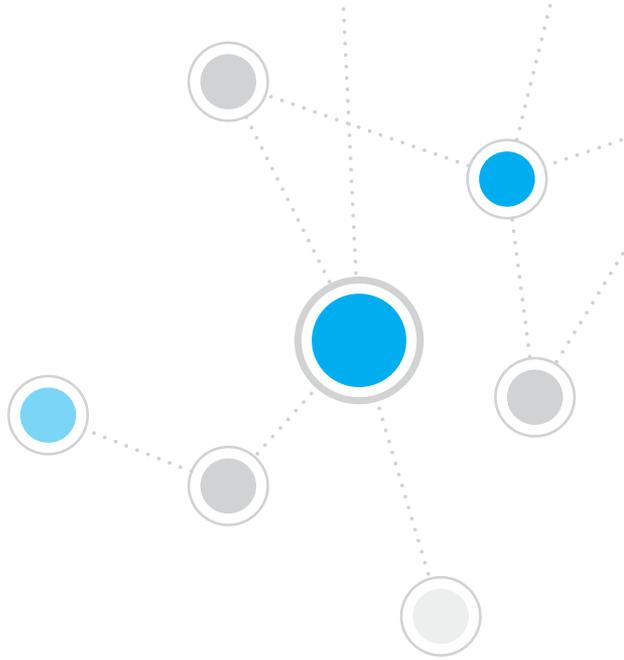
Informations de contact

Pour contacter le support technique de ForeScout, envoyez un e-mail à l'adresse support@forescout.com ou appelez l'un des numéros suivants :

- Numéro gratuit (US) : +1.866.377.8771
- Téléphone (Intl) : +1.408.213.3191
- Support : +1.708.237.6591
- Fax : +1.408.371.2284

©2016 ForeScout Technologies, Inc. Produits protégés par les brevets US #6,363,489, #8,254,286, #8,590,004 et #8,639,800. Tous droits réservés. ForeScout Technologies et le logo ForeScout sont des marques commerciales de ForeScout Technologies, Inc. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

L'utilisation de tout produit ForeScout est soumise aux conditions du Contrat de licence d'utilisateur final de ForeScout disponible à l'adresse www.forescout.com/eula.



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 États-Unis

Numéro gratuit (US) : +1.866.377.8771

Téléphone (Intl) : +1.408.213.3191

Support : +1.708.237.6591

Fax : +1.408.371.2284

400-00020-01