CHAPTER 13

センサーの管理タスク

この章では、センサーの管理面で役立つ手順について説明します。この章は、次の項で構成されています。

バナー ログインの作成

ユーザおよびパスワードのログイン プロンプトの前に表示されるバナー ログインを作成するには、**banner login** コマンドを使用します。メッセージの最大長は 2500 文字です。バナーを削除するには、**no banner login** コマンドを使用します。

バナー ログインを作成するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　バナー ログインを作成します。

```
sensor(config)# banner login
Banner[]:
```

ステップ 4　メッセージを入力します。

```
Banner[]: This message will be displayed on banner login. ^M Thank you
sensor(config)#
```

（注）　メッセージに ? または復帰を使用するには、**Ctrl+V+?** キーまたは **Ctrl+V+Enter** キーを押します。これらの記号は ^M で表されます。

完成したバナー ログインの例を次に示します。

```
This message will be displayed on login.
Thank you
login: cisco
Password:****
```

ステップ 5　バナー ログインを削除するには、次のように入力します。

```
sensor(config)# no banner login
```

バナーがログイン時に表示されなくなります。

CLI セッションの終了

別の CLI セッションを終了するには、**clear line** *cli-id* [**message**] コマンドを使用します。**message** キーワードを使用すると、受信ユーザに終了要求とともにメッセージを送信できます。メッセージの最大長は 2500 文字です。

次のオプションが適用されます。

- *cli-id*：ログイン セッションに関連付けられている CLI ID 番号。CLI ID 番号を見つけるには、**show users** コマンドを使用します。
- **message**：受信ユーザに送信するメッセージ。

注意　**clear line** コマンドでは、CLI ログイン セッションしかクリアできません。このコマンドでは、サービス ログインはクリアできません。

管理者がログインしようとしたときに最大セッション数に達していたときは、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, would you like to
terminate one of the open sessions? [no]
```

オペレータまたはビューアがログインしようとしたときに最大セッション数がオープンしていたときは、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

CLI セッションを終了するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　ログイン セッションに関連付けられている CLI ID 番号を見つけます。

```
sensor# show users
    CLI ID   User    Privilege
*   13533    jtaylor administrator
    15689    jsmith  operator
    20098    viewer  viewer
```

ステップ 3　jsmith の CLI セッションを終了します。

```
sensor# clear line cli_id message
Message[]:
```

例

```
sensor# clear line 15689 message
Message{}: Sorry! I need to terminate your session.
sensor#
```

ステップ 4　ユーザ jsmith は、管理者 jtaylor から次のメッセージを受信します。

```
sensor#
***
***
*** Termination request from jtaylor
***
Sorry! I need to terminate your session.
```

ターミナル プロパティの変更

ログイン セッションのターミナル プロパティを変更するには、**terminal [length]** *screen length* コマンドを使用します。*screen length* オプションを指定すると、画面に設定した行数が表示され、その後に --more-- プロンプトが表示されるようにすることができます。値が 0 の場合、出力は一時停止しません。デフォルト値は 24 行です。

（注）　ターミナル セッションの中には、画面の行数を指定する必要のないタイプがあります。これは、一部のリモート ホストでは、指定された画面の行数が分かるためです。

ターミナル プロパティを変更するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　複数画面の出力間で一時停止しないようにするには、*screen length* 値として 0 を使用します。

```
sensor# terminal length 0
```

（注）　画面の行数は、ログイン セッション間では保存されません。

ステップ 3　10 行ごとに CLI を一時停止して、--more-- プロンプトを表示するには、*screen length* 値として 10 を使用します。

```
sensor# terminal length 10
```

イベント

この項では、イベント ストアからイベントを表示およびクリアする方法について説明します。取り上げる事項は次のとおりです。

イベントの表示

イベント ストアからイベントを表示するには、**show events** [{[**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***]] | **error** [warning] [error] [fatal] | **log** | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用します。

開始時刻から、イベントが表示されます。開始時刻を指定しない場合は、現在時刻から、イベントが表示されます。イベント タイプを指定しない場合は、すべてのイベントが表示されます。

（注）　イベントは、Ctrl+C キーを押して要求をキャンセルするまで、ライブ フィードとして表示されます。

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であること、または攻撃が試みられたことを示している可能性のある不審なアクティビティを通知します。

  レベル（informational、low、medium、または high）が選択されていない場合は、すべてのアラート イベントが表示されます。
- **include-traits**：指定した特性を持つアラートを表示します。
- **exclude-traits**：指定した特性を持つアラートを表示しません。
- **traits**：10 進数（0 ～ 15）で表した特性ビットの位置。
- **error**：エラー イベントを表示します。エラー イベントは、エラー条件が発生したときにサービスによって生成されます。
- **log**：ログ イベントを表示します。ログ イベントは、トランザクションが受信され、アプリケーションの応答があったときに生成されます。トランザクションの要求、応答、および成功または失敗に関する情報が含まれています。
- **NAC**：ARC（ブロック）要求を表示します。

  （注）　ARC は、以前は Network Access Controller（NAC）と呼ばれていました。この名前の変更は、IDM および CLI for IPS 5.1 で完全には反映されていません。
- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、分数、秒数の間に開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注）　**show events** コマンドは、指定されたイベントが使用可能になるまで待機します。待機し、イベントを表示している状態は、Ctrl+C キーを押して終了するまで継続します。

イベント ストアからイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始されているすべてのイベントを表示します。

```
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

フィードは、**Ctrl+C** キーを押すまですべてのイベントを表示し続けます。

ステップ 3　2005 年 2 月 9 日の午前 10 時から、ブロック要求を表示します。

```
sensor#@ show events NAC 10:00:00 Feb 9 2005
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2005/02/09 10:33:31 2004/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

ステップ 4　2005 年 2 月 9 日の午前 10 時から、警告レベルのエラーを表示します。

```
sensor# show events error warning 10:00:00 Feb 9 2005
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2003/01/07 04:49:25 2003/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2005/03/02 14:15:59 2005/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　過去 30 秒間に始まったイベントを表示します。

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアからのイベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力してイベントをクリアします。

システム クロック

この項では、システム クロックを表示および手動で設定する方法について説明します。取り上げる事項は次のとおりです。

システム クロックの表示

システム クロックを表示するには、**show clock** [**detail**] コマンドを使用します。**detail** オプションを使用して、クロック ソース（NTP またはシステム）と現在のサマータイム設定（ある場合）を示すことができます。

システム クロックは、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックが NTP などの時刻源によって設定されている場合は、フラグが設定されます。

記号	説明
*	時刻は信頼できません。
（ブランク）	時刻は信頼できます。
.	時刻は信頼できますが、NTP は同期していません。

システム クロックを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
sensor# show clock
22:39:21 UTC Sat Jan 25 2003
```

ステップ 3　システム クロックを詳細に表示します。

```
sensor# show clock detail
22:39:21 CST Sat Jan 25 2003
Time source is NTP
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、センサーが NTP から時間を取得していることと、設定および同期されていることを示しています。

```
sensor# show clock detail
*12:19:22 CST Sat Dec 04 2004
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

これは、時刻源が設定されていないことを示しています。

手動によるクロック設定

アプライアンスのクロックを手動で設定するには、**clock set** *hh:mm [:ss] month day year* コマンドを使用します。その他の時刻源を使用できない場合は、このコマンドを使用します。

（注）　センサーが NTP クロック ソースなど有効な外部の時刻メカニズムと同期している場合、システム クロックを設定する必要はありません。

NTP の設定手順については、P.4-32 の「NTP の設定」を参照してください。センサーに有効な時刻源が必要であることの重要性の説明については、P.4-22 の「時刻源およびセンサー」を参照してください。クロックを誤って設定した場合の処置の説明については、P.4-24 の「センサー上の時刻の修正」を参照してください。

clock set コマンドは、次のプラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- AIP SSM 10
- AIP SSM 20

クロックをアプライアンスに手動で設定するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　クロックを手動で設定します。

```
sensor# clock set 13:21 July 29 2004
```

（注）　時刻形式は 24 時間です。

拒否された攻撃者のリストのクリア

拒否された攻撃者のリストを削除して、仮想センサーの統計情報をクリアするには、サービス イベント アクション ルール サブモードで **clear denied-attackers** コマンドを使用します。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。シグニチャを設定すると、インライン モードでパケット、接続、および攻撃者を拒否することができます。これは、センサーが単一パケット、接続、および特定の攻撃者を検出したときにそれらを拒否する、つまり送信しないことを意味します。

シグニチャが起動すると、攻撃者は拒否され、リストに入れられます。センサー管理の一環として、リストの削除やリスト内の統計情報のクリアを実行することもできます。

拒否された攻撃者のリストを削除して、統計情報をクリアするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　拒否された IP アドレスのリストを表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

今回 2 つの IP アドレスが拒否されたことが統計情報に示されています。

ステップ 3　拒否された攻撃者のリストを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of
attackers currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力してリストをクリアします。

ステップ 5　リストをクリアしたことを確認します。

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

`Denied Attackers and hit count for each` カテゴリの下には情報がなくなりました。

ステップ 6　統計情報だけをクリアするには、次の手順を実行します。

```
sensor# show statistics virtual-sensor clear
```

ステップ 7　統計情報をクリアしたことを確認します。

```
JWK-4255# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

統計情報は、Number of Active Denied Attackers カテゴリおよび Number of exec Clear commands during uptime カテゴリを除いて、すべてクリアされました。リストがクリアされたかどうかを認識していることが重要です。

統計情報の表示

仮想センサーの統計情報を表示するには、**show statistics virtual-sensor** [**clear**] コマンドを使用します。各センサー アプリケーションごとに統計情報を生成するには、**show statistics [analysis-engine** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **host** | **logger** | **network-access** | **notification** | **sdee-server** | **transaction-server** | **transaction-source** | **web-server] [clear]** コマンドを使用します。

（注）　**clear** オプションは、分析エンジン、ホスト、またはネットワーク アクセス アプリケーションには使用できません。

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　仮想センサーの統計情報を表示します。

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = fe0_1
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1675
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 241
         Total IP packets processed since reset = 12
         Total packets that were not IP processed since reset = 229
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 12
         Total packets that were not TCP, UDP, or ICMP processed since reset = 0
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 22513
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 13
         The average bytes per packet since reset = 93
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 0
      Denied Attackers and hit count for each.
      The Signature Database Statistics.
         The Number of each type of node active in the system (can not be reset)
            Total nodes active = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The number of each type of node inserted since reset
            Total nodes inserted = 28
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 6
         The rate of nodes per second for each time since reset
```

```
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraints
      TCP nodes keyed on both IP addresses and both ports = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
   Number of complete datagrams reassembled since last reset = 0
   Fragments hitting too many fragments condition since last reset = 0
   Number of overlapping fragments since last reset = 0
   Number of Datagrams too big since last reset = 0
   Number of overwriting fragments since last reset = 0
   Number of Initial fragment missing since last reset = 0
   Fragments hitting the max partial dgrams limit since last reset = 0
   Fragments too small since last reset = 0
   Too many fragments per dgram limit since last reset = 0
   Number of datagram reassembly timeout since last reset = 0
   Too many fragments claiming to be the last since last reset = 0
   Fragments with bad fragment flags since last reset = 0
TCP Normalizer stage statistics
   Packets Input = 0
   Packets Modified = 0
   Dropped packets from queue = 0
   Dropped packets due to deny-connection = 0
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
   Current Streams Denied = 0
Statistics for the TCP Stream Reassembly Unit
   Current Statistics for the TCP Stream Reassembly Unit
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   Cumulative Statistics for the TCP Stream Reassembly Unit since reset
      TCP streams that have been tracked since last reset = 0
      TCP streams that had a gap in the sequence jumped = 0
      TCP streams that was abandoned due to a gap in the sequence = 0
      TCP packets that arrived out of sequence order for their stream = 0
      TCP packets that arrived out of state order for their stream = 0
      The rate of TCP connections tracked per second since reset = 0
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 491
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 6
   Number of FireOnce Intermediate Alerts = 480
   Number of Summary First Alerts  = 0
   Number of Summary Intermediate Alerts  = 0
   Number of Regular Summary Final Alerts  = 0
   Number of Global Summary Final Alerts  = 0
   Number of Alerts Output for further processing = 491
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
```

```
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
          SigEvent Action Filter Stage Statistics
             Number of Alerts received to Action Filter Processor = 0
             Number of Alerts where an action was filtered = 0
             Number of Filter Line matches = 0
             Actions Filtered
                deny-attacker-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
          SigEvent Action Handling Stage Statistics.
             Number of Alerts received to Action Handling Processor = 491
             Number of Alerts where produceAlert was forced = 0
             Number of Alerts where produceAlert was off = 0
             Actions Performed
                deny-attacker-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 11
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 5
                request-snmp-trap = 0
                reset-tcp-connection = 0
             Deny Actions Requested in Promiscuous Mode
                deny-packet not performed = 0
                deny-connection not performed = 0
                deny-attacker not performed = 0
                modify-packet not performed = 0
             Number of Alerts where deny-connection was forced for deny-packet action = 0
             Number of Alerts where deny-packet was forced for non-TCP deny-connection
action = 0
          Per-Signature SigEvent count since reset
             Sig 2004 = 5
             Sig 2156 = 486
sensor#
```

ステップ 3　分析エンジンの統計情報を表示します。

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1999
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 13
   Receiver Statistics
      Total number of packets processed since reset = 290
      Total number of IP packets processed since reset = 12
   Transmitter Statistics
      Total number of packets transmitted = 290
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 491
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 11
sensor#
```

ステップ 4　認証の統計情報を表示します。

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 2
   failedAuthenticationAttempts = 0
sensor#
```

ステップ 5　システム内で拒否された攻撃者の統計情報を表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
sensor#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

ステップ 8　ホストの統計情報を表示します。

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05  Thu Feb 10 2005
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet  HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185  Bcast:10.89.149.255  Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 MiB)  TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
sensor#
```

ステップ 9　ロギング アプリケーションの統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
sensor#
```

ステップ 10　ARC の統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 10.89.150.138
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
```

```
            InterfacePreBlock = Pre_Acl_Test
         BlockInterface
            InterfaceName = 507
            InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

ステップ 11　通知アプリケーションの統計情報を表示します。

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

ステップ 12 SDEE サーバの統計情報を表示します。

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

ステップ 13 トランザクション サーバの統計情報を表示します。

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

ステップ 14 トランザクション ソースの統計情報を表示します。

```
sensor# show statistics transaction-source
General
   totalControlTransactions = 0
   failedControlTransactions = 0
sensor#
```

ステップ 15 Web サーバの統計情報を表示します。

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

ステップ 16 ロギング アプリケーションなどのアプリケーションの統計情報をクリアするには、次の手順を実行します。

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

統計情報が検出され、クリアされました。

ステップ 17 統計情報がクリアされたことを確認します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

統計情報はすべて 0 から始まります。

テクニカル サポート情報の表示

システム情報を画面に表示するか、または特定の URL に送信するには、**show tech-support** [**page**] [**password**] [**destination-url** *destination-url*] コマンドを使用します。この情報は、TAC でトラブルシューティング ツールとして使用できます。

次のパラメータはオプションです。

- **page**：一度に 1 ページずつ、情報の出力を表示します。
  次の出力行を表示するには **Enter** キーを押し、次のページの情報を表示するには Space キーを押します。
- **password**：パスワードとその他のセキュリティ情報を出力に残します。
- **destination-url**：情報を HTML としてフォーマットし、このコマンドの後に続く宛先に送信するよう指示します。このキーワードを使用した場合、出力は画面に表示されません。
- *destination-url*：情報を HTML としてフォーマットすることを示します。URL は、情報の送信先を指定します。このキーワードを使用しない場合は、情報が画面に表示されます。

テクニカル サポート情報を表示するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　画面に出力を表示します。

```
sensor# show tech-support page
```

システム情報が、一度に 1 ページずつ画面に表示されます。次のページを表示するには Space キーを押し、プロンプトへ戻るには **Ctrl+C** キーを押します。

ステップ 3　ファイルへ出力を送信する（HTML 形式で）には、次の手順を実行します。

a. 次のコマンドを入力し、その後に有効な宛先を入力します。

```
sensor# show tech-support destination-url destination-url
```

次の宛先タイプを指定できます。

- **ftp:**：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`ftp:[[//username@location]/relativeDirectory]/filename` または `ftp:[[//username@location]//absoluteDirectory]/filename` です。
- **scp:**：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`scp:[[//username@]location]/relativeDirectory]/filename` または `scp:[[//username@]location]//absoluteDirectory]/filename` です。

たとえば、ファイル `/absolute/reports/sensor1Report.html` へテクニカル サポート出力を送信するには、次の手順を実行します。

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

`password:` プロンプトが表示されます。

b. このユーザ アカウントのパスワードを入力します。

`Generating report:` メッセージが表示されます。

バージョン情報の表示

インストール済みのすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで動作中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体のコンフィギュレーションを表示するには、**more current-config** コマンドを使用します。

バージョンおよびコンフィギュレーションを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　バージョン情報を表示します。

```
sensor# show version
```

次の例に、アプライアンスと NM-CIDS のバージョン出力のサンプルを示します。

アプライアンスのバージョン出力のサンプル

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.1(0.16)S185.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 5 days.
Using 722145280 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.3M out of 166.8M bytes of available disk space (23%
usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


Upgrade History:

  IDS-K9-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005

Recovery Partition Version 1.1 - 5.1(0.16)

sensor#
```

NM-CIDS のバージョン出力のサンプル

```
nm-cids# show version
Application Partition:
Cisco Intrusion Prevention System, Version 5.1(0.16)S185.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: NM-CIDS
Serial Number: JAD06490681
No license present
Sensor up-time is 1 day.
Using 485675008 out of 509448192 bytes of available memory (95% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
```

```
application-data is using 31.1M out of 166.8M bytes of available disk space (20%
usage)
boot is using 39.5M out of 68.6M bytes of available disk space (61% usage)
application-log is using 529.6M out of 2.8G bytes of available disk space (20% usage)


MainApp          2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
AnalysisEngine   2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
CLI              2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600


Upgrade History:

  IDS-K9-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005

Recovery Partition Version 1.1 - 5.1(0.16)

nm-cids#
```

（注） --MORE-- プロンプトが表示されたら、Space キーを押して次の情報を表示するか、**Ctrl+C** キーを押して出力をキャンセルし、CLI プロンプトに戻ります。

ステップ 3　コンフィギュレーション情報を表示します。

（注） **more current-config** コマンドまたは **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Version 5.1(0.16)
! Current configuration last modified Wed Oct 31 03:20:54 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on banner login.
exit
time-zone-settings
--MORE--
```

シリアル接続への出力の転送

シリアル接続にすべての出力を転送するには、**display-serial** コマンドを使用します。このコマンドを使用すると、ブート処理中でも、リモート コンソール（シリアル ポートを使用）にシステム メッセージを表示できます。この選択が有効である限り、ローカル コンソールは使用できません。出力をローカル ターミナルにリセットするには、**no display-serial** コマンドを使用します。

注意　シリアル ポートに接続している場合は、Linux が完全にブートされてシリアル接続のサポートがイネーブルになるまで、フィードバックは取得できません。

display-serial コマンドは、次の IPS プラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- IDS-4215
- IPS-4240
- IPS-4255
- AIP SSM 10
- AIP SSM 20

シリアル ポートに出力を転送するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　シリアル ポートへの出力を指示します。

```
sensor# configure terminal
sensor(config)# display-serial
```

デフォルトでは、出力はシリアル接続に転送されません。

ステップ 3　リセットして、ローカル コンソールへ出力するようにします。

```
sensor(config)# no display-serial
```

ネットワーク接続性の診断

基本的なネットワーク接続性を診断するには、**ping** ip-*address* [**count**] コマンドを使用します。

注意　このコマンドには、コマンド割り込みは使用できません。最後まで実行する必要があります。

基本的なネットワーク接続性を診断するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　対象のアドレスを ping します。

```
sensor# ping ip-address count
```

count は、送信するエコー要求の数です。数を指定しない場合は、要求が 4 回送信されます。範囲は 1 ～ 10,000 です。

正常な ping の例

```
sensor# ping 10.89.146.110 6
PING 10.89.146.110 (10.89.146.110): 56 data bytes
64 bytes from 10.89.146.110: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 10.89.146.110: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=5 ttl=61 time=0.2 ms

--- 10.89.146.110 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

正常でない ping の例

```
sensor# ping 172.21.172.1 3
PING 172.21.172.1 (172.21.172.1): 56 data bytes

--- 172.21.172.1 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

アプライアンスのリセット

アプライアンスで動作中のアプリケーションを適切にシャットダウンしてアプライアンスをリブートするには、**reset [powerdown]** コマンドを使用します。**powerdown** オプションを指定すると、アプライアンスの電源を切るか（可能な場合）、またはアプライアンスを、電源を切ることができる状態にしておくことができます。

（注）　モジュールのリセットについては、P.15-31 の「IDSM-2 のリセット」、P.16-9 の「NM-CIDS のシャットダウン、リロード、およびリセット」、および P.14-7 の「AIP SSM のリロード、シャットダウン、リセット、および復旧」にあるそれぞれの手順を参照してください。

コマンドを実行すると、即座にシャットダウン（アプライアンスの停止）が開始されます。シャットダウンには少し時間がかかることがあり、この間に CLI コマンドにアクセスできますが、セッションは警告なしに終了します。

アプライアンスをリセットするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して CLI にログインします。

ステップ 2　すべてのアプリケーションを停止してアプライアンスをリブートするには、次のステップを実行します。あるいは、アプライアンスの電源を切って、ステップ 4 に進みます。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 3　**yes** を入力してリセットを続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

ステップ 4　すべてのアプライアンスを停止して、アプライアンスの電源を切るには、次のように入力します。

```
sensor# reset powerdown
Warning: Executing this command will stop all applications and power off the node if
possible. If the node can not be powered off it will be left in a state that is safe
to manually power down.
Continue with reset? []:
```

ステップ 5　**yes** を入力して、リセットおよび電源切断を続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

コマンド履歴の表示

現在のメニューに入力したコマンドのリストを表示するには、**show history** コマンドを使用します。リスト内の最大コマンド数は 50 です。

最近使用したコマンドのリストを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　EXEC モードで使用したコマンドの履歴を表示します。

```
sensor# show history
clear line
configure terminal
show history
```

ステップ 3　ネットワーク アクセス モードで使用したコマンドの履歴を表示します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show history
show settings
show settings terse
show settings | include profile-name|ip-address
exit
show history
sensor (config-net)#
```

ハードウェア インベントリの表示

PEP 情報を表示するには、**show inventory** コマンドを使用します。このコマンドは、センサーの PID、VID、および SN から構成される UDI 情報を表示します。

PEP 情報によって、CLI を使用してハードウェア バージョンおよびシリアル番号を容易に知ることができるようになります。

show inventory コマンドは、次のプラットフォームには適用されません。

- IDSM-2
- NM-CIDS
- IDS-4210
- IDS-4215
- IDS-4235
- IDS-4250

PEP 情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　PEP 情報を表示します。

```
sensor# show inventory

Name: "Chassis", DESCR: "IPS 4255 Intrusion Prevention Sensor"
PID: IPS-4255-K9, VID: V01 , SN: JAB0815R017

Name: "Power Supply", DESCR: ""
PID: ASA-180W-PWR-AC, VID: V01 , SN: 123456789AB
sensor#

sensor# show inventory

Name: "Module", DESCR: "ASA 5500 Series Security Services Module-20"
PID: ASA-SSM-20, VID: V01 , SN: JAB0815R036
sensor#

sensor-4240# show inventory

Name: "Chassis", DESCR: "IPS 4240 Appliance Sensor"
PID: IPS-4240-K9, VID: V01 , SN: P3000000653
sensor-4240#
```

TAC とやり取りする際に、この情報が使用できます。

IP パケットのルートのトレース

宛先までの IP パケットのルートを表示するには、**trace** *ip_address count* コマンドを使用します。*ip_address* オプションは、ルートをトレースする宛先のシステムのアドレスです。*count* オプションに、使用するホップ数を定義できます。デフォルトは 4 です。有効な値は 1 ～ 256 です。

注意　このコマンドには、コマンド割り込みは使用できません。最後まで実行する必要があります。

IP パケットのルートをトレースするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　対象の IP パケットのルートを表示します。

```
sensor# trace 10.1.1.1
traceroute to 10.1.1.1 (10.1.1.1), 4 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.267 ms  0.262 ms  0.236 ms
 2  10.89.128.17 (10.89.128.17)  0.24 ms *  0.399 ms
 3  * 10.89.128.17 (10.89.128.17)  0.424 ms *
 4  10.89.128.17 (10.89.128.17)  0.408 ms *  0.406 ms
sensor#
```

ステップ 3　ルートでデフォルトの 4 より多くのホップを使用するようにするには、*count* オプションを使用します。

```
sensor# trace 10.1.1.1 8
traceroute to 10.1.1.1 (10.1.1.1), 8 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.35 ms  0.261 ms  0.238 ms
 2  10.89.128.17 (10.89.128.17)  0.36 ms *  0.344 ms
 3  * 10.89.128.17 (10.89.128.17)  0.465 ms *
 4  10.89.128.17 (10.89.128.17)  0.319 ms *  0.442 ms
 5  * 10.89.128.17 (10.89.128.17)  0.304 ms *
 6  10.89.128.17 (10.89.128.17)  0.527 ms *  0.402 ms
 7  * 10.89.128.17 (10.89.128.17)  0.39 ms *
 8  10.89.128.17 (10.89.128.17)  0.37 ms *  0.486 ms
sensor#
```

サブモード設定の表示

現在のコンフィギュレーションの内容を表示するには、サブモードで **show settings** [**terse**] コマンドを使用します。

サブモードの現在のコンフィギュレーション設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC サブモードの現在のコンフィギュレーションを表示します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ------------------------------------------------
      profile-name: 2admin
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
      profile-name: insidePix
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      ------------------------------------------------
      profile-name: qatest
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      ------------------------------------------------
```

```
      profile-name: fwsm
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      -----------------------------------------------
      profile-name: outsidePix
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      -----------------------------------------------
      profile-name: cat
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      -----------------------------------------------
      profile-name: rcat
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: cisco default:
      -----------------------------------------------
      profile-name: nopass
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      -----------------------------------------------
      profile-name: test
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      -----------------------------------------------
      profile-name: sshswitch
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: cisco default:
      -----------------------------------------------
   -----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   -----------------------------------------------
      ip-address: 10.89.147.61
      -----------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: cat
         block-vlans (min: 0, max: 100, current: 1)
         -----------------------------------------------
            vlan: 1
            -----------------------------------------------
               pre-vacl-name:  <defaulted>
               post-vacl-name:  <defaulted>
            -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   -----------------------------------------------
      ip-address: 10.89.147.54
      -----------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         -----------------------------------------------
```

```
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name:  <defaulted>
               post-acl-name:  <defaulted>
            ------------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
      firewall-devices (min: 0, max: 250, current: 2)
      ---------------------------------------------
         ip-address: 10.89.147.10
         ---------------------------------------------
            communication: telnet default: ssh-3des
            nat-address: 0.0.0.0 <defaulted>
            profile-name: insidePix
         ---------------------------------------------
         ip-address: 10.89.147.82
         ---------------------------------------------
            communication: ssh-3des <defaulted>
            nat-address: 0.0.0.0 <defaulted>
            profile-name: f1
         ---------------------------------------------
      ---------------------------------------------
sensor (config-net)#
```

ステップ 3　ARC 設定を簡略モードで表示します。

```
sensor(config-net)# show settings terse
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ------------------------------------------------
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
```

```
   -----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   -----------------------------------------------
      ip-address: 10.89.147.61
   -----------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   -----------------------------------------------
      ip-address: 10.89.147.54
   -----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   -----------------------------------------------
      ip-address: 10.89.147.10
      ip-address: 10.89.147.82
   -----------------------------------------------
sensor(config-net)#
```

ステップ 4　**include**　キーワードを使用すると、フィルタリングされた出力で設定が表示できます。たとえば、ARC コンフィギュレーション内のプロファイル名および IP アドレスのみが表示できます。

```
sensor(config-net)# show settings | include profile-name|ip-address
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
      ip-address: 10.89.147.61
         profile-name: cat
      ip-address: 10.89.147.54
         profile-name: r7200
      ip-address: 10.89.147.10
         profile-name: insidePix
      ip-address: 10.89.147.82
         profile-name: test
sensor(config-net)#
```