CHAPTER 11

HA のアカウンティング

この章では、Cisco Mobile Wireless Home Agent のアカウントに関するコンセプト、およびこの機能の設定方法について説明します。

この章の内容は、次のとおりです。

HA アカウンティングの概要

この機能は主として、CMX ソリューションにおいて、Home Agent（HA）と Service Selection Gateway（SSG）を相互運用する目的で開発されました。しかし、SSG と相互運用しない場合でも、この機能を使用できます。

このリリースは、次のアカウンティング機能をサポートしています。

- 冗長設定での HA アカウンティング
- アカウンティング レコードのパケット カウントおよびバイト カウント
- アカウンティング レコードの追加アトリビュート
- 追加のアカウンティング方式 — 暫定アカウンティングのサポート

バイトおよびパケットのカウントは HA 上で実行されるので、このアカウンティング機能では、完全なアカウンティング情報を生成するためにネットワーク上の SSG を使用する必要はありません。

HA のアカウンティング機能には、次のアクティビティが含まれます。

- HA は、モバイルの初回バインディングの作成時に、アカウンティング開始レコードを送信します。
- HA は、モバイルの最終バインディングの削除時に、アカウンティング停止レコードを送信します。
- HA は、ハンドオフの発生時にアカウンティング アップデートを送信します。
- スタートストップおよび中間アカウンティング方式がサポートされます。
- 認証済み Network Access Identifier（NAI）について、エラー コードを含むモバイル IP レジストレーション応答が送信されると（その NAI のバインディングが存在しない場合など）、アカウンティング停止レコードが送信されます。
- 既存バインディングの再レジストレーションに失敗すると、認証済み NAI について、対応する拒否コードを含むウォッチドッグ メッセージが送信されます。

次のアトリビュートが、アカウンティング レコードにより送信されます。

- Username アトリビュートの NAI（1）
- Framed IP Address アトリビュートの MN IP アドレス（8）
- HA IP アドレス（26/7、3gpp2 アトリビュート）
- トンネル エンド ポイントの Care-of Address（CoA; 気付アドレス）（66）
- Network Access Server（NAS）IP アドレス アトリビュート（4）
- Accounting Status Type アトリビュート（40）
- アカウンティング セッション ID（44）
- アカウンティング終了理由（49）— アカウンティング停止時のみ
- アカウンティング遅延時間（41）
- Acct-Input-Octets（42）
- Acct-Output-Octets（43）
- Acct-Input-Packets（47）
- Acct-Output-Packets（48）
- Acct-Input-Gigawords（52）
- Acct-Output-Gigawords（53）
- 「mobileip-mn-flags」cisco-avpair アトリビュートのレジストレーション フラグ
- 「mobileip:ip-vrf」cisco-avpair アトリビュートの Vrf 名
- 「mobileip:mn-reject-code」cisco-avpair アトリビュート（RRQ が拒否された場合のアカウンティング停止時およびアカウンティング アップデート時のみ）

HA 冗長設定でのアカウンティング カウンタの同期化

冗長設定で HA アカウンティングをイネーブルにし、定期アカウンティングを設定すると、次のコマンドが設定されている場合、アクティブとスタンバイの間でアカウンティング カウンタが定期的に同期化されます。

ip mobile home-agent *method* **redundancy [virtual-network address** *address*] **periodic-sync**

ip mobile home-agent *method* **redundancy periodic-sync** コマンドを設定すると、アカウンティング アップデート イベントにより、各バインディングのバイトおよびパケットのカウントがスタンバイに同期化されます。ただし、最後の同期化以降、バイト カウントが変更されている場合だけです。Time-of-the-day アカウンティングはサポートされません。

次に、例を示します。

aaa accounting update periodic *60* および **ip mobile home-agent** *method* **redundancy update-periodic** を設定して、バインディングを開くと、次のイベントが発生します。

- バインディングを開いたあと、バインディングを通過したデータがない場合、AAA サーバに暫定アカウンティング レコードが送信されていても、スタンバイ装置にバイトカウントは同期化されません。
- 次の暫定レコードが送信される前に、バインディングの各方向に 500 バイトのデータが通過したとします。この場合、アクティブ装置から暫定レコードがトリガーされた時点で、スタンバイにカウンタが同期化されます。
- 次の暫定インターバルでは、フローを通過するデータが存在しなかったとします。この場合、アクティブ装置から前提レコードがトリガーされても、新たにレポートする内容はないので、スタンバイ装置には何も同期化されません。
- この時点でスイッチオーバーが発生した場合、新しいアクティブ装置が保持しているバインディング カウントは、入出力バイト数が 500、入出力パケット数が 5 （各 100 バイトの 5 パケットが通過したと想定した場合）になります。前のアクティブ装置が回復してスタンバイ装置になると、これらのカウンタがスタンバイ装置にバルク同期化されます。

HA は、RADIUS サーバに対して、HA のフェールオーバーを通知できます。この通知には、RADIUS アカウンティング レコードの cisco-avpair radius アトリビュート「mobileip-rfswat=1」が含まれます。このアトリビュートが含まれるのは、フェールオーバー前に作成されていたバインディングで、フェールオーバー後に生成されたそのバインディングの最初のアカウンティング レコードだけです。

たとえば、バインディングが作成され、そのバインディングのアカウンティング開始が送信されます。しばらくして、アクティブに障害が発生し、スタンバイに引き継がれたとします。ここで、スタンバイは RADIUS サーバに、このバインディングのアカウンティング アップデートを送信します。HA は、このアカウンティング レコードに、Cisco-avpair radius アトリビュート「mobileip-rfswat=1」を付加します。

この機能をイネーブルにするには、次のコマンドを使用します。

ip mobile home-agent redundancy *group* **virtual-network address** *HA address* **swact-notification**

基本的なアカウンティング メッセージ

Home Agent Release 2.1 以上は、Cisco Service Selection Gateway（SSG）をサポートしています。このリリースで HA が送信するのは、統計情報を含まない 3 つのアカウンティング メッセージだけです。SSG は、すべてのネットワーク トラフィックが SSG を通過するように設計され、配置されます。

すべてのトラフィックが通過するので、SSG はすべての統計情報を保持しますが、モバイル IP セッション情報は保持しません。HA は、モバイル IP セッション情報を保持しているので、この情報を SSG に送信します。

HA は、SSG/AAA サーバに次のメッセージを送信します。

- アカウンティング開始 : HA は、次の場合に、このメッセージを SSG/AAA サーバに送信します。
  - MN が初回レジストレーションに成功した場合。これは、MN の新規モバイル IP セッションの開始を示しています。
  - 冗長設定の HA の場合、スタンバイ HA は、アクティブになった時点で以前のバインディングが存在しない場合にのみ、アカウンティング開始メッセージを送信します。これにより、SSG で、障害 HA 上の MN のホスト オブジェクトが保持されます。ただし、Phase-1 では、冗長性はサポートされません。
- アカウンティング アップデート : HA は、定期的なアカウンティング アップデート メッセージが設定され、モバイル ノードの Point of Attachment（POA）が変更されると、アカウンティング アップデート メッセージを生成します。モバイル IP セッションの場合、これは、モバイル ノードが CoA 変更後の再レジストレーションに成功したことを意味します。CoA は、外部ネットワーク上のモバイル ノードの現在位置です。また、既存バインディングの再レジストレーションに失敗した場合、HA は適正な拒否コードを含むアカウンティング アップデート メッセージを送信します。
- アカウンティング停止 : HA は、認証済み NAI について、その NAI にバインディングが存在しないという理由で、エラー コードを含む RRP が送信された場合、アカウンティング停止メッセージを送信します。

すべてのメッセージに、次の情報が含まれます。

- **Network Access Identifier（NAI）**：MN の名前です。abc@service_provider1.com のような名前になります。
- **Network Access Server（NAS）IP**：アカウンティング ノードの IP アドレスです。HA はアカウンティング ノードなので、このフィールドには HA のアドレスが含まれます。
- **フレーム化された IP アドレス**：MN の IP アドレスです。通常、レジストレーションに成功すると、HA により MN に IP アドレスが割り当てられます。
- **Point Of Attachment（POA）**：ネットワーク上の MN の接続ポイントです。モバイル IP セッションの場合、MN の COA になります。

HA のシステム アカウンティング

HA のサービス開始時点（つまり、ボックスのリロード後の初期化時点）で、アクティブな HA が存在しない場合、accounting-on が送信されます。

accounting-off は、アクティブ HA のサービスが停止（グレースフルその他）し、HA サービスを提供するスタンバイ HA が存在しない場合には、送信されるはずです。accounting-off は、常に送信されるとは限りません。

スタンバイ HA のサービス停止（グレースフルその他）の場合、accounting-off は送信されません。

モバイル IP HA から送信されないメッセージ

次のメッセージは、モバイル IP HA から送信されません。

- HA ボックスがオンラインになった時点、またはブートアップ時の Accounting On メッセージ（Acct-Status-Type=Accounting-On）：このメッセージは、モバイル IP コンフィギュレーションに関係のない、プラットフォームのグローバル エンティティです。このメッセージは通常、モバイル IP などのサービスではなく、プラットフォームのコードによって初期化中に実装されます。
- HA ボックスのシャットダウン時の Accounting Off メッセージ（Acct-Status-Type=Accounting-Off）：このメッセージは、モバイル IP コンフィギュレーションに関係のない、プラットフォームのグローバル エンティティです。このメッセージは通常、モバイル IP などのサービスではなく、プラットフォームのコードによってリブート中に実装されます。

HA アカウンティングの設定

モバイル IP では現在、AAA コマンドを使用して認証パラメータを設定しています。次のすべてのコマンドが必要です。デフォルトでは、HA アカウンティング機能はディセーブルです。設定しない場合、HA は AAA サーバにアカウンティング メッセージを送信しません。HA アカウンティング機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent accounting list`	HA アカウンティングをイネーブルにし、HA の定義済みアカウンティング方式リストを適用します。*list* は、HA アカウンティング レコードの生成に使用する AAA アカウンティング方式です。
ステップ 2	`Router(config)# ip mobile home-agent method redundancy [virtual-network address address] periodic-sync`	アカウンティング アップデート イベントを使用して、各バインディングのバイトとパケットのカウントをスタンバイ装置に同期化します。同期が実行されるのは、最後の同期以降、バイト カウントが変更された場合だけです。
ステップ 3	`Router(config)# aaa accounting network method list name start-stop group group name`	処理の開始時にアカウンティング「開始」通知、処理の終了時にアカウンティング「停止」通知を送信します。アカウンティング「開始」レコードは、バックグラウンドで送信されます。要求したユーザ プロセスは、アカウンティング サーバがアカウンティング「開始」通知を受信したかどうかに関係なく、開始されます。
ステップ 4	`Router(config)# aaa accounting update newinfo`	対象ユーザに関する新しいアカウンティング情報が発生するごとに、アカウンティング サーバに暫定アカウンティング レコードを送信します。
ステップ 5	`Router(config)# aaa accounting system default start-stop group radius`	HA によるシステム メッセージの送信をイネーブルにします。
ステップ 6	`Router# debug aaa accounting`	HA アカウンティング メッセージのデバッグをイネーブルにします。
ステップ 7	`Router# debug radius` `Router# debug tacacs`	セキュリティ プロトコル特定メッセージのデバッグをイネーブルにします。
ステップ 8	`Router# debug ip mobile`	モバイル IP 関連デバッグ メッセージをイネーブルにします。アカウンティングでは、デバッグ メッセージが出力されるのはエラー発生時だけです。

HA アカウンティングの設定例

最初のコマンド ブロックは、AAA の設定です。ネットワーク アカウンティング用に、アカウンティング方式リスト（mylist）が作成されています。Start-Stop キーワードは、HA から 開始および終了レコードを送信することを意味します。詳細については、『*IOS Security Configuration Guide*』を参照してください。

2 行めは、COA が変更された場合、アカウンティング アップレード レコードを送信するように HA に指示しています。

```
ip mobile home-agent accounting mylist address 10.3.3.1
ip mobile host 10.3.3.2 3.3.3.5 interface Ethernet2/2
ip mobile secure host 10.3.3.2 spi 1000 key ascii test algorithm md5 mode
prefix-suffix
!
```

これらは、モバイル IP コマンドです。1 行めで、アカウンティング方式リスト mylist を HA に適用し、HA のアカウンティングをイネーブルに設定しています。

```
!
!
radius-server host 172.16.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
!
```

これらは、RADIUS コマンドです。1 行めで、RADIUS サーバのアドレスを指定します。HA が AAA サーバにアクセスでき、適切なアクセス権限があることを確認してください。

次に、HA アカウンティングの設定例を示します。

アクティブ HA：

```
router#
router#show run
Building configuration...

Current configuration : 4927 bytes
!
! Last configuration change at 05:12:03 UTC Thu Oct 13 2005
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco7600
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
no ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
ip dhcp-server 99.107.0.13
```

```
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
!
username cisco7600 password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 description "LINK TO HAAA.................!"
 ip address 150.2.13.40 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 4 ip 150.2.0.252
 standby 4 priority 110
 standby 4 preempt delay reload 300
 standby 4 name cisco1
!
interface FastEthernet1/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.10 255.0.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby 2 ip 7.0.0.2
 standby 2 priority 110
 standby 2 preempt delay reload 300
 standby 2 name cisco
!
interface FastEthernet3/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
 bridge-group 4
 bridge-group 4 spanning-disabled
!
interface Ethernet6/0
 description ""LINK TO REFLECTOR...."
 ip address 99.107.0.19 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 99.107.89.67
```

```
 standby 3 priority 110
 standby 3 preempt delay reload 300
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.10 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/4
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/5
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/6
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/7
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Virtual-Template1
 no ip address
```

```
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent redundancy cisco virtual-network address 7.0.0.2 periodic-sync
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.67 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
access-list 120 deny   ip 40.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255
access-list 120 permit ip any any
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 password 7 0507070D
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end

router#
```

スタンバイ HA：

```
router#
router#show run
Building configuration...

Current configuration : 3995 bytes
!
! No configuration change since last restart
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname cisco7600
!
boot-start-marker
boot system tftp /auto/tftpboot-users/tennis/c7600-h1is-mz.123-3.8.PI2 171.69.1.129
boot-end-marker
!
enable password 7 00445566
!
no spd enable
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
ip subnet-zero
!
!
no ip cef
ip ftp username pdsn-team
ip ftp password 7 pdsneng
ip host PAGENT-SECURITY-V3 32.68.10.4 38.90.0.0
ip name-server 11.69.2.133
no ip dhcp use vrf connected
!
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
username mwt13-7600b password 0 cisco
!
```

```
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
 no ip route-cache
!
interface FastEthernet0/0
 ip address 4.0.10.2 255.0.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 no ip address
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO HAAA.................!"
 ip address 15.2.13.20 255.255.0.0
 no ip route-cache
 duplex full
 no cdp enable
 standby 4 ip 15.2.0.252
 standby 4 name cisco1
!
interface FastEthernet5/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.67 255.0.0.0
 no ip route-cache
 duplex full
 standby 2 ip 7.0.0.2
 standby 2 name cisco
!
interface Ethernet6/0
 description "LINK TO REFLECTOR....!"
 ip address 22.107.0.12 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 22.107.89.67
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.2 255.255.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
```

```
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent redundancy cisco virtual-network address 7.0.0.2 periodic-sync
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.10 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane

!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end
```

HA アカウンティングの設定の確認

HA アカウンティングのステータスを確認するには、**show ip mobile global** コマンドを使用します。現在のアカウンティング ステータスが、次のように表示されます。

```
router# sh ip mobile global
IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm disabled
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist
    NAT UDP Tunneling support enabled
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Standby groups
        cisco (virtual network - address 7.0.0.2)
    Virtual networks
        40.0.0.0 /8

Foreign Agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
Radius Disconnect Capability disabled


router#
```