パスワード回復手順Cisco Secure IDS（旧称NetRanger(R)）センサー

目次

概要

このドキュメントでは、すべてのバージョンの Cisco Secure Intrusion Detection System (IDS)（以前の NetRanger）アプライアンスおよびモジュールを回復する手順について説明します。

前提条件

要件

FTP サーバが必要な場合、パッシブ モードをサポートする必要があります。 リカバリ CD は、

Product Upgrade Tool（登録ユーザ専用）を使用して取得できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IDS アプライアンス バージョン 3 および 4
- IPS アプライアンス バージョン 5 および 6
- IDS モジュール（IDSM）バージョン 3 および IDSM-2 バージョン 4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IDS アプライアンス バージョン 3

バージョン 3 のアプライアンスでは、2 つのオプションが利用可能です。 パスワード回復プロセスを使用するか、またはバージョン 3 のリカバリ CD を使用して再イメージングすることができます。 再イメージングすると、すべての情報が失われることに注意してください。 パスワードの回復手順では、基本的に Solaris パスワードを回復します。 設定をコピーできる管理ステーション（Cisco Secure Policy Manager（CSPM）、VPN/Security Management Solution（VMS）、UNIX Director）がない場合は、このオプションのみ使用してください。

IDS アプライアンス バージョン 3 以前では、「netrangr」と「root」という 2 つのユーザ名を使用します。 デフォルト パスワードは、両方共「attack」です。

バージョン 3 を実行する IDS アプライアンスのパスワードの回復

パスワードを回復するために、以下のファイルが必要になります。

- Solaris デバイス コンフィギュレーション アシスタント ディスク（起動ディスク）。 このファイルは、Sun サポート Web サイト からダウンロードできます。**注:** このリンクが機能しない場合、Sun サポート Web サイトの最上位レベルに移動し、ドライバの下にある *デバイス コンフィギュレーション アシスタント起動ディスクの Solaris ドライバのダウンロード*を検索します。 シスコは、Sun サポート Web サイト を保守していないため、コンテンツの配置場所を管理しておりません。
- Solaris for Intel（x86）CD-ROM。
- ワークステーションへのコンソール アクセス。

パスワードを回復するには、以下の手順を実行します。

1. 起動ディスクを挿入します。
2. CD-ROM ドライブに CD を挿入します。
3. ワークステーションの電源を切り、10 秒間待ってから、再度電源を投入します。起動ディスクからシステムを起動します。 必要な設定を行うと、初期 [コンフィギュレーション アシ

スタント] 画面が表示されます。
4. F3 を押して、起動デバイスに対応するシステムの部分スキャンを実行します。スキャンが終了すると、デバイスのリストが表示されます。
5. CD-ROM デバイスがデバイスのリストに表示されていることを確認し、F2 を押して続行します。起動デバイスのリストが画面に表示されます。
6. **CD-ROM ドライブ**を選択し、Space キーを押します。CD-ROM デバイスの横に「X」が表示されます。
7. F2 を押して続行します。これで、ワークステーションが CD-ROM から起動します。
8. インストールのタイプの選択に使用する画面で、[Option 2 , Jumpstart] を選択します。システムの起動が続行します。
9. 言語を選択するプロンプトで、[Option 0] (英語の場合) を選択します。
10. 次の言語の画面で、もう一度 [Option 0] (英語 ANSI の場合) を選択します。システムの起動が続行し、[Solaris Installation] 画面が表示されます。
11. Ctrl キーを押しながら **C** を入力して、インストール スクリプトを停止すると、プロンプトへのアクセスが可能になります。
12. **mount -F ufs /dev/dsk/c0t0d0s0 /mnt** と入力します。これで、マウント ポイント「/mnt」に「/」パーティションがマウントされました。 ここから、「/etc/shadow」ファイルを編集し、root パスワードを削除できます。
13. **cd /mnt/etc** と入力します。
14. データを正しく読み取ることができるように、シェル環境を設定します。**TERM=ansi** と入力します。**export TERM** と入力します。
15. **vi shadow** と入力します。これでシャドウ ファイルに入り、パスワードを削除できるようになりました。 エントリは次のようになっている必要があります。
    `root:gNyqp8ohdfxPI:10598::::::` 「:」はフィールドの区切り記号であり、暗号化されたパスワードは 2 番目のフィールドです。
16. 2 番目のフィールドを削除します。 次に例を示します。`root:gNyqp8ohdfxPI:10598::::::`が次のようになります。
    `root::10598::::::`. これで root ユーザのパスワードが削除されました。
17. **Type: wq!** と入力し、 書き込みを行い、ファイルを終了します。
18. ドライブからディスクと CD-ROM を取り出します。
19. **init 6** と入力して、システムを再起動します。
20. login: プロンプトで、**root** と入力し、 Enter を押します。
21. パスワード プロンプトで Enter を押します。これで、Cisco Secure IDS センサーにログインしました。

バージョン 3 を実行する IDS アプライアンスの再イメージング

バージョン 3 を実行する IDS アプライアンスを再イメージングするには、以下の手順を実行します。

注: 続行する前に、マウスにセンサーが接続されていないことを確認してください。

1. バージョン 3 リカバリ CD を IDS アプライアンスに挿入し、再起動します。
2. リカバリが正常に完了するまで、セットアップに対応するプロンプトに従います。
3. デフォルトのユーザ名とパスワード「root/attack」を使用してログインします。
4. **sysconfig-sensor** を実行して、アプライアンスを再構成します。

IDS アプライアンス バージョン 4

管理者ユーザ名/パスワードが認識されている場合の回復手順

管理者アカウントのパスワードが認識されている場合、このユーザ アカウントを使用して、他のパスワードをリセットできます。

たとえば、IDS アプライアンスで、「cisco」と「adminuser」という 2 つユーザ名が設定されているとします。 ユーザ「cisco」のパスワードをリセットする必要がある場合、「adminuser」としてログインし、パスワードをリセットします。

```
sv8-4-ids4250 login: adminuserPassword:!--- Output is suppressed. idsm2-sv-rack#configure
terminal idsm2-sv-rack(config)#no username cisco idsm2-sv-rack(config)#username cisco priv admin
password 123cisco123 idsm2-sv-rack(config)#exit idsm2-sv-rack#exit sv8-4-ids4250 login: cisco
Password: !--- Output is suppressed. sv8-4-ids4250#
```

サービス ユーザ名/パスワードが認識されている場合の回復手順

サービス アカウントのパスワードが認識されている場合、このユーザ アカウントを使用して、他のパスワードをリセットできます。

たとえば、IDS アプライアンスで、「cisco」、「adminuser」、「serviceuser」という 3 つのユーザ名が設定されているとします。 ユーザ「cisco」のパスワードをリセットする必要がある場合、「serviceuser」としてログインし、パスワードをリセットします。

```
sv8-4-ids4250 login: tacPassword:
!--- Output is suppressed. bash-2.05a$ su root Password: [root@sv8-4-ids4250 serviceuser]#passwd
cisco Changing password for user cisco. New password: Retype new password: passwd: all
authentication tokens updated successfully. [root@sv8-4-ids4250 serviceuser]#exit exit bash-
2.05a$ exit logout sv8-4-ids4250 login: cisco Password: !--- Output is suppressed. sv8-4-
ids4250#
```

注: ルート パスワードは、サービス アカウントのパスワードと同じです。

バージョン 4 を実行する IDS アプライアンスの再イメージング

IDS アプライアンスを再イメージングするには、以下の手順を実行します。

注: 続行する前に、マウスにセンサーが接続されていないことを確認してください。

1. バージョン 4 リカバリ CD を IDS アプライアンスに挿入し、再起動します。
2. リカバリが正常に完了するまで、セットアップに対応するプロンプトに従います。
3. 「デフォルトのユーザ名とパスワード「cisco/cisco」を使用してログインします。
4. セットアップを実行して、アプライアンスを再構成します。

IPS アプライアンス バージョン 5 およびバージョン 6

AIP-SSM のリロード、シャット ダウン、リセット、および回復

適応型セキュリティ アプライアンスから、Advanced Inspection and Prevention Security Services Module (AIP-SSM) のリロード、シャット ダウン、リセット、パスワードの回復、および回復を直接実行するには、以下のコマンドを使用します。

注: 特権 EXEC モードまたはグローバル コンフィギュレーション モードから、**hw-module** コマンドを入力できます。 シングル ルーテッド モードおよびシングル トランスペアレント モードでコ

マンドを入力できます。 マルチ モード (ルーテッドまたはトランスペアレント マルチ モード) で動作している適応型セキュリティ デバイスでは、 (管理者またはユーザ コンテキストからでなく) システム コンテキストからのみ **hw-module** コマンドを実行できます。

- **hw-module module slot_number reload**：このコマンドは、ハードウェアをリセットすることなく、AIP-SSM 上のソフトウェアをリロードします。 このコマンドは、AIP-SSM がアップ状態のときにのみ有効です。
- **hw-module module slot_number shutdown**：このコマンドは、AIP-SSM 上のソフトウェアをシャット ダウンします。 このコマンドは、AIP-SSM がアップ状態のときにのみ有効です。
- **hw-module module slot_number reset**：このコマンドは、AIP-SSM のハードウェア リセットを実行します。 カードがアップ/ダウン/無応答/回復状態のときに適用できます。
- **hw-module module slot_number password-reset** ：このコマンドは、Cisco ASA 5500 シリーズ Content Security and Control Security Services Module (CSC-SSM) または AIP-SSM 上のパスワードを回復します。デバイスを再イメージングする必要はありません。**注:** このコマンドは、IPS 6.0 (ASA 7.2 バージョン) からサポートを開始し、Cisco CLI アカウントのパスワードをデフォルトの **cisco** に復元するために使用されます。
- **hw-module module slot_number recover [boot | stop | configure]**：**recover** コマンドは、リカバリ パラメータを設定または変更するための一連のインタラクティブ オプションを表示します。 Enter を押して、パラメータを変更するか、または既存の設定を維持することができます。AIP-SSM の回復に使用する手順については、「AIP-SSM システム イメージのインストール」を参照してください。**hw-module module slot_number recover boot**：このコマンドは、AIP-SSM のリカバリを開始します。 このコマンドは、AIP-SSM がアップ状態のときにのみ適用できます。**hw-module module slot_number recover stop**：このコマンドは AIP-SSM のリカバリを停止します。 このコマンドは、AIP-SSM がリカバリ状態のときにのみ適用できます。**注:** AIP-SSM リカバリを停止する必要がある場合、AIP-SSM リカバリを開始してから 30 ~ 45 秒以内に **hw-module module 1 recover stop** コマンドを発行する必要があります。これ以上待機すると、予期しない結果をもたらす可能性があります。 たとえば、AIP-SSM が無応答状態になる可能性があります。**hw-module module 1 recover configure**：このコマンドを使用して、モジュール リカバリのパラメータを設定します。 必須パラメータは、IP アドレスおよびリカバリ イメージの TFTP URL の場所です。例：`aip-ssm#hardware-module module 1 recover configure Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-1.img]: Port IP Address [10.89.149.226]: VLAN ID [0]: Gateway IP Address [10.89.149.254]:`

AIP-SSM システム イメージの再イメージング

AIP-SSM のシステム イメージをインストールするには、以下の手順を実行します。

1. ASA にログインします。
2. イネーブル モードに入ります。`asa>enable`
3. AIP SSM 用のリカバリ設定を行います。`asa#hw-module module 1 recover configure` **注:** リカバリ設定に誤りがあった場合は、**hw-module module 1 recover stop** コマンドを使用してシステムの再イメージングを停止してから、設定を修正できます。
4. システム イメージの TFTP URL を指定します。`Image URL [tftp://0.0.0.0/]:` 例：`Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img`
5. AIP-SSM のコマンドおよび制御インターフェイスを指定します。`Port IP Address [0.0.0.0]:`例：`Port IP Address [0.0.0.0]: 10.89.149.231`
6. VLAN ID を 0 のままにします。 `VLAN ID [0]:`
7. AIP-SSM のデフォルト ゲートウェイを指定します。`Gateway IP Address [0.0.0.0]` :例

：Gateway IP Address [0.0.0.0]:10.89.149.254

8. リカバリを実行します。asa#**hw-module module 1 recover boot**
9. リカバリが完了するまで、進行状態を定期的にチェックします。**注:** 状態は、リカバリ中に guest@localhost.localdomain を読み取り、再イメージング完了時に guest@localhost.localdomain を読み取ります。asa#**show module 1** Mod Card Type Model Serial No. --- ---------- 0 ASA 5540 Adaptive Security Appliance ASA5540 P2B00000019 1 ASA 5500 Series Security Services Module-20 ASA-SSM-20 P1D000004F4 Mod MAC Address Range Hw Version Fw Version Sw Version --- ---------- 0 000b.fcf8.7b1c to 000b.fcf8.7b20 0.2 1.0(7)2 7.0(0)82 1 000b.fcf8.011e to 000b.fcf8.011e 0.1 1.0(7)2 5.0(0.22)S129.0 Mod Status --- ---------- 0 Up Sys 1 Up asa# **注:** リカバリ プロセスで発生する可能性があるエラーをデバッグするには、**debug module-boot** コマンドを使用して、システム再イメージング プロセスのデバッグを有効にします。
10. AIP-SSM へのセッションでは、**setup** コマンドを使用して AIP-SSM を初期化します。

IDSM

設定が保持されている間、IDSM でパスワード リカバリを実行するために使用できる方式はありません。

注: この手順では、メンテナンス パーティションを使用する必要があります。 メンテナンス パーティションのパスワードが変更されたため口グインできない場合、IDSM を交換する必要があります。 このような場合は、シスコ テクニカル サポートに相談してください。

ネイティブ IOS (統合 IOS) コードを実行するスイッチによる IDSM の再イメージング

ネイティブ IOS (統合 IOS) コードを実行するスイッチにより ISDM を再イメージングするには、以下の手順を実行します。

1. スイッチ コマンド **hw-module module x reset hdd:2** (ここで、*x* はスロット番号を表します) を使用して、メンテナンス パーティションに IDSM を起動します。SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ---------- ---------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------- ------ ---------- ------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok SV9-1#**hw-module module 6 reset hdd:2** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output suppressed.*
2. スイッチ コマンド **show module x** を使用して、IDSM がオンラインになることを確認します。IDSM ソフトウェアのバージョンの先頭に 2 が表示され、現在 IDSM でメンテナンス パーティションが実行され、状態が正常であることを確認します。SV9-1#**show module 6** Mod Ports Card Type Model Serial No. --- ----- ---------- ---------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------- ------ ---------- ------ ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 2.5(0) Ok
3. スイッチ コマンド **session slot x processor 1** を使用して、IDSM のメンテナンス パーティションに接続します。ユーザ名/パスワードとして、**ciscoids/attack** を使用します。SV9-1#**session slot 6 proc 1** The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: ciscoidsPassword: maintenance#
4. キャッシュ イメージをインストールして、IDSM アプリケーション パーティションを再イ

メージングします。診断コマンド **ids-installer system /cache /show** を発行して、キャッシュ イメージが存在することを確認します。`maintenance#**diag** maintenance(diag)#**ids-installer system /cache /show** Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ---------- maintenance(diag)#` キャッシュ イメージが存在しないか、キャッシュされたバージョンがインストール対象のバージョンではない場合、手順 5 に進みます。キャッシュ イメージを使用する ISDM を再イメージングするには、診断コマンド **ids-installer system /cache /install** を使用します。
`maintenance(diag)#**ids-installer system /cache /install** Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E41E-3608 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\!` 再イメージングが完了したら、手順 12 に進みます。

5. IDSM が IP 接続されていることを確認します。 **ping ip_address** コマンドを発行します。
`maintenance#**diag** maintenance(diag)#**ping 10.66.84.1** Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. IDSM が IP 接続されている場合は、手順 11 に進みます。 IP 接続されていない場合は、手順 7 ~ 9 を続行します。
7. コマンドおよび制御インターフェイスがスイッチで正しく設定されていることを確認します。 **show run interface Gigx/2** コマンドを発行します。`SV9-1#**show run interface Gig6/2** Building configuration... Current configuration : 115 bytes ! interface GigabitEthernet6/2 no ip address switchport switchport access vlan 210 switchport mode access end SV9-1#`
8. 通信パラメータが IDSM のメンテナンス パーティションで正しく設定されていることを確認します。 診断コマンド **ids-installer netconfig /view** を発行します。`maintenance#**diag** maintenance(diag)#**ids-installer netconfig /view** IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack`
9. パラメータが何も設定されていない場合、または一部のパラメータを変更する必要がある場合は、診断コマンド **ids-installer netconfig /configure parameters** を使用します。
`maintenance(diag)#**ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack** STATUS: Network parameters for the config port have been configured ! NOTE: Reset the module for the changes to take effect!`
10. IDSM を変更を有効にするためにリセットした後 IP接続を再度チェックして下さい。 IP 接続に依然として問題がある場合は、通常の IP 接続の問題としてトラブルシュートし、手順 11 に進みます。
11. IDSM アプリケーション パーティションを再イメージングします。 診断コマンド **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** を使用して、イメージをダウンロードします。ここで、*ip_address* は、FTP サーバの IP アドレスです。*account* は、FTP サーバにログインするときに使用するユーザ名またはアカウント名です。*save* は、キャッシュ コピーとしてダウンロードされたイメージのコピーを保存するかどうかを決定します。 yes の場合、既存のキャッシュ イメージが上書きされます。 no の場合、ダウンロードされたイメージは非アクティブ パーティションにインストールされますが、キャッシュ コピーは保存されません。*ftp_path* は、イメージ ファイルが配置される FTP サーバのディレクトリを指定します。*file_prefix* は、ダウンロードされたイメージ内の .dat ファイルのファイル名です。 ダウンロードされたイメージは、.dat 拡張子が付いた 1 つのファイルと .cab 拡張子が付いた複数のファイルで構成されます。 file_prefix 値は、.dat サフィックスまで (ただし、.dat サフィックスを含まない) の DAT ファイルの名前である必要があります。`maintenance#**diag** maintenance(diag)#**ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia'** / prefix=IDSMk9-a-3.0-1-S4 Please enter login password: *****

```
Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded
successfully ! Validating integrity of the image... PASSED! Formatting drive C:\....
Verifying 4016M Format completed successfully. 4211310592 bytes total disk space.
4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the
image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive
C:\!
```

12. スイッチ コマンド **hw-module module reset x hdd 1** を使用して、アプリケーション パーティションに IDSM を起動します。`SV9-1#hw-module module 6 reset hdd:1 Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y !--- Output is suppressed.` また、アプリケーション パーティションに IDSM を起動するようにスイッチが設定されていることも確認します。 これを確認するには、**show bootvar device module x** コマンドを使用します。`SV9-1#show bootvar device module 6 [mod:6 ]: SV9-1#` IDSM の起動デバイス変数を設定するには、スイッチ コンフィギュレーション コマンド **boot device module x hdd:1** を使用します。`SV9-1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#boot device module 6 hdd:1 Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#endSV9-1#show bootvar device module 6 [mod:6 ]: hdd:1 SV9-1#`
13. スイッチ コマンド **show module x** を使用して、IDSM がオンラインになることを確認します。IDSM ソフトウェアのバージョンがアプリケーション パーティションのバージョンである (たとえば、*3.0(1)S4*) ことと状態が正常であることを確認します。`SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ---------- -- ---------- ----------- 6 2 Intrusion Detection System WS-X6381-IDS SAD063000CE Mod MAC addresses Hw Fw Sw Status --- ---------- ------ ---------- ---------- ------- 6 0002.7e39.2b20 to 0002.7e39.2b21 1.2 4B4LZ0XA 3.0(1)S4 Ok`
14. アプリケーション パーティションに起動した IDSM に接続し、Director と通信できるように設定します。 **setup** コマンドを使用します。Director との通信が確立されると、IDSM に設定をダウンロードできます。ユーザ名/パスワードとして、**ciscoids/attack** を使用して口グインします。`SV9-1#session slot 6 proc 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.61 ... Open
login: ciscoids
Password:#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default settings are in square brackets '[]'. Current Configuration: Configuration last modified Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway:Host Name: Not Set Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask [255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port [45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100 Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director host id []: 249 Enter director host post office port [45000]: Enter director heart beat interval [5]: Enter director organization name []: cisco Enter director organization id []: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was entered: Configuration last modified Never Sensor:IP Address: 10.66.84.124 Netmask: 255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host Port: 45000 Organization Name: cisco Organization ID: 100 Director: IP Address: 10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5 Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled WARNING: Applying this configuration will cause all configuration files to be initialized and the card to be rebooted. Apply this configuation?: yes Configuration Saved. Resetting... !--- Output is suppressed.`

ハイブリッド (CatOS) コードを実行するスイッチによる IDSM の再イメージング

ハイブリッド (CatOS) コードを実行するスイッチにより ISDM を再イメージングするには、以下の手順を実行します。

注: アプリケーション パーティション上のすべての情報が失われます。 設定が保持されている間、IDSM でパスワード リカバリを実行するために使用できる方式はありません。

注: この手順では、メンテナンス パーティションを使用する必要があります。 メンテナンス パーティションのパスワードが変更されたため口グインできない場合、IDSM を交換する必要があります。 このような場合は、シスコ テクニカル サポートに相談してください。

1. スイッチ コマンド **reset x hdd:2** を使用して、メンテナンス パーティションに IDSM を起動します。`ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- --- - ----- ------------------------ ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ---- ------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------- -- ------ ---------- ---------------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(5)S23 ltd9-9> (enable)**reset 4 hdd:2** This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y Module 4 shut down in progress, please don't remove module until shutdown completed. *!--- Output is suppressed.*`
2. スイッチ コマンド **show module x** を使用して、IDSM がオンラインになることを確認します。IDSM ソフトウェアのバージョンの先頭に 2 が表示され、現在 IDSM でメンテナンス パーティションが実行され、状態が正常であることを確認します。`ltd9-9> (enable) **show module 4** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- -- ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ----------- 4 SAD 063000CEMod MAC-Address(es) Hw Fw Sw --- ---------- ------ ---------- -------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 2.5(0)`
3. スイッチ コマンド **session x** を使用してメンテナンス パーティションに起動した IDSM に接続します。ユーザ名/パスワードとして、**ciscoids/attack** を使用します。`ltd9-9> (enable)**session 4** Trying IDS-4... Connected to IDS-4. Escape character is '^]'. login: ciscoids Password: maintenance#`
4. キャッシュ イメージをインストールして、IDSM アプリケーション パーティションを再イメージングします。診断コマンド **ids-installer system /cache /show** を使用して、キャッシュ イメージが存在することを確認します。`maintenance#**diag** maintenance(diag)#**ids-installer system /cache /show** Details of the cached image: Package Name : IDSMk9-a-3.0-1-S4 Release Info : 3.0-1-S4 Total CAB Files in the package : 5 CAB Files present : 5 CAB Files missing : 0 List of CAB Files missing ---------- maintenance(diag)#` キャッシュ イメージが存在しないか、キャッシュされたバージョンがインストール対象のバージョンではない場合、手順 5 に進みます。キャッシュ イメージを使用する ISDM を再イメージングするには、診断コマンド **ids-installer system /cache /install** を使用します。`maintenance(diag)#**ids-installer system /cache /install** Validating integrity of the image... PASSED! Formatting drive C:\.... Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is E41E-3608 Extracting the image... *!--- Output is suppressed.* STATUS: Image has been successfully installed on drive C:\!` 再イメージングが完了したら、手順 12 に進みます。
5. **ping ip_address** コマンドを使用して、IDSM が IP 接続されていることを確認します。`maintenance#**diag** maintenance(diag)#**ping 10.66.84.1** Pinging 10.66.84.1 with 32 bytes of data: Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255 Reply from 10.66.84.1: bytes=32 time<10ms TTL=255`
6. IDSM が IP 接続されている場合は、手順 11 に進みます。 IP 接続されていない場合は、手順 7 ~ 9 を続行します。
7. **show port status x/2** コマンドを使用して、コマンドおよび制御インターフェイスがスイッチで正しく設定されていることを確認します。`ltd9-9> (enable)**show port status 4/2** Port Name`

```
Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ------ -----
------------ 4/2 connected 1 full 1000 Intrusion De
```

8. 診断コマンド **ids-installer netconfig /view** を使用して、通信パラメータが IDSM のメンテナンス パーティションで正しく設定されていることを確認します。`maintenance#diag maintenance(diag)#ids-installer netconfig /view IP Configuration for Control Port: IP Address : 10.66.84.124 Subnet Mask : 255.255.255.128 Default Gateway : 10.66.84.1 Domain Name Server : 1.1.1.1 Domain Name : cisco Host Name : idsm-sv-rack`
9. パラメータが何も設定されていない場合、または一部のパラメータを変更する必要がある場合は、診断コマンド **ids-installer netconfig /configure parameters** を使用します。`maintenance(diag)# ids-installer netconfig /configure / ip=10.66.84.124 /subnet=255.255.255.128 /gw=10.66.84.1 / dns=1.1.1.1/domain=cisco /hostname=idsm-sv-rack`
10. IDSM をリセットして変更を有効にしたら、再度 IP 接続を確認します。IP 接続に依然として問題がある場合は、通常の IP 接続の問題としてトラブルシュートし、手順 11 に進みます。
11. IDSM アプリケーション パーティションを再イメージングします。 診断コマンド **ids-installer system /nw /install /server=ip_address /user=account /save={yes/no} /dir=ftp_path /prefix=file_prefix** を使用して、イメージをダウンロードします。ここで、*ip_address* は、FTP サーバの IP アドレスです。*account* は、FTP サーバにログインするときに使用するユーザ名またはアカウント名です。*save* は、キャッシュ コピーとしてダウンロードされたイメージのコピーを保存するかどうかを決定します。 yes の場合、既存のキャッシュ イメージが上書きされます。 no の場合、ダウンロードされたイメージは非アクティブ パーティションにインストールされますが、キャッシュ コピーは保存されません。*ftp_path* は、イメージ ファイルが配置される FTP サーバのディレクトリを指定します。*file_prefix* は、ダウンロードされたイメージ内の .dat ファイルのファイル名です。 ダウンロードされたイメージは、.dat 拡張子が付いた 1 つのファイルと .cab 拡張子が付いた複数のファイルで構成されます。 file_prefix 値は、.dat サフィックスまで (ただし、.dat サフィックスを含まない) の DAT ファイルの名前である必要があります。`maintenance#diag maintenance(diag)#ids-installer system /nw /install /server=10.66.64.10 /user=cisco /save=yes /dir='/tftpboot/georgia' /prefix=IDSMk9-a-3.0-1-S4 Please enter login password: ***** Downloading the image.. File 05 of 05 FTP STATUS: Installation files have been downloaded successfully! Validating integrity of the image... PASSED! Formatting drive C:\....Verifying 4016M Format completed successfully. 4211310592 bytes total disk space. 4206780416 bytes available on disk. Volume Serial Number is 2407-F686 Extracting the image... !--- Output is suppressed. STATUS: Image has been successfully installed on drive C:\!`
12. スイッチ コマンド **reset x hdd:1** を使用して、アプリケーション パーティションに IDSM を起動します。`ltd9-9> (enable)reset 4 hdd:1 This command will reset module 4. Unsaved configuration on module 4 will be lost Do you want to continue (y/n) [n]? y !--- Output is suppressed.` また、アプリケーション パーティションに IDSM を起動するようにスイッチが設定されていることも確認します。 これを確認するには、**show boot device x** コマンドを使用します。`ltd9-9> (enable)show boot device 4 Device BOOT variable =` IDSM の起動デバイス変数を設定するには、スイッチ コンフィギュレーション コマンド **set boot device hdd:1 x** を使用します。`ltd9-9> (enable)set boot device hdd:1 4 Device BOOT variable = hdd:1 Warning: Device list is not verified but still set in the boot string. ltd9-9> (enable)show boot device 4 Device BOOT variable = hdd:1`
13. スイッチ コマンド **show module x** を使用して、IDSM がオンラインになることを確認します。IDSM ソフトウェアのバージョンがアプリケーション パーティションのバージョンである (たとえば、*3.0(1)S4*) ことと状態が正常であることを確認します。`ltd9-9> (enable)show module 4 Mod Slot Ports Module-Type Model Sub Status --- ---- ----- --------- ---------- ------------------ --- -------- 4 4 2 Intrusion Detection Syste WS-X6381-IDS no ok Mod Module-Name Serial-Num --- ------------------- ----------- 4 SAD063000CE Mod MAC-Address(es) Hw Fw Sw --- ---------------------------------- ------ ---------- ---------- ---------- 4 00-02-7e-39-2b-20 to 00-02-7e-39-2b-21 1.2 4B4LZ0XA 3.0(1)S4`

14. アプリケーション パーティションに起動した IDSM に接続し、Director と通信できるように設定します。 **setup** コマンドを使用します。ユーザ名/パスワードとして、**ciscoids/attack** を使用してログインします。

```
ltd9-9> (enable)session 4
Trying IDS-4...
Connected to IDS-4.
Escape character is '^]'.
login: ciscoids
Password:#setup --- System Configuration Dialog --- At any point you may enter a question
mark '?' for help. User ctrl-c to abort configuration diaglog at any prompt. Default
settings are in square brackets '[]'. Current Configuration: Configuration last modified
Never Sensor: IP Address: 10.0.0.1 Netmask: 255.0.0.0 Default Gateway: Host Name: Not Set
Host ID: Not Set Host Port: 45000 Organization Name: Not Set Organization ID: Not Set
Director: IP Address: Not Set Host Name: Not Set Host ID: Not Set Host Port: 45000 Heart
Beat Interval (secs): 5 Organization Name: Not Set Organization ID: Not Set Direct Telnet
access to IDSM: disabled Continue with configuration dialog? [yes]: Enter virtual terminal
password[]: Enter sensor IP address[10.0.0.1]: 10.66.84.124 Enter sensor netmask
[255.0.0.0]: 255.255.255.128 Enter sensor default gateway []: 10.66.84.1 Enter sensor host
name []: idsm-sv-rack Enter sensor host id []: 124 Enter sensor host post office port
[45000]: Enter sensor organization name []: cisco Enter sensor organization id []: 100
Enter director IP address[]: 10.66.79.249 Enter director host name []: vms1 Enter director
host id []: 249 Enter director host post office port [45000]: Enter director heart beat
interval [5]: Enter director organization name []: cisco Enter director organization id
[]: 100 Enable direct Telnet access to IDSM? [no]: The following configuration was
entered: Configuration last modified Never Sensor: IP Address: 10.66.84.124 Netmask:
255.255.255.128 Default Gateway: 10.66.84.1 Host Name: idsm-sv-rack Host ID: 124 Host
Port: 45000 Organization Name: cisco Organization ID: 100 Director:IP Address:
10.66.79.249 Host Name: vms1 Host ID: 249 Host Port: 45000 Heart Beat Interval (secs): 5
Organization Name: cisco Organization ID: 100 Direct Telnet access to IDSM: disabled
WARNING: Applying this configuration will cause all configuration files to be initialized
and the card to be rebooted. Apply this configuation?: yes Configuration Saved.
Resetting... !--- Output is suppressed.
```

ISDM-2

管理者ユーザ名/パスワードが認識されている場合の回復手順

管理者アカウントのパスワードが認識されている場合、このユーザ アカウントを使用して、他のパスワードをリセットできます。

たとえば、IDSM-2 で、「cisco」と「adminuser」という 2 つユーザ名が設定されているとします。 ユーザ「cisco」のパスワードをリセットする必要がある場合、「adminuser」としてログインし、パスワードをリセットします。

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: adminuser
Password: !--- Output is suppressed. idsm2-sv-rack#configure terminal idsm2-sv-rack(config)#no
username cisco idsm2-sv-rack(config)#username cisco priv admin password 123cisco123 idsm2-sv-
rack(config)#exit idsm2-sv-rack#exit [Connection to 127.0.0.61 closed by foreign host] SV9-
1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit'
at the remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !---
Output is suppressed. idsm2-sv-rack#
```

サービス ユーザ名/パスワードが認識されている場合の回復手順

サービス アカウントのパスワードが認識されている場合、このユーザ アカウントを使用して、他のパスワードをリセットできます。

たとえば、IDSM-2 で、「cisco」、「adminuser」、「serviceuser」という 3 つのユーザ名が設

定されているとします。 ユーザ「cisco」のパスワードをリセットする必要がある場合、「serviceuser」としてログインし、パスワードをリセットします。

```
SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type
'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: serviceuser
Password: !--- Output is suppressed. bash-2.05a$ su root Password: [root@idsm2-sv-rack
serviceuser]#passwd cisco Changing password for user cisco. New password: Retype new password:
passwd: all authentication tokens updated successfully. [root@idsm2-sv-rack serviceuser]# exit
exit bash-2.05a$ exit logout [Connection to 127.0.0.61 closed by foreign host] SV9-1#session
slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the
remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: !--- Output
is suppressed. idsm2-sv-rack#
```

注: ルート パスワードはサービス アカウントのパスワードと同じです。

ネイティブ IOS (統合 IOS) コードを実行するスイッチによる IDSM-2 の再イメージング

ネイティブ IOS (統合 IOS) コードを実行するスイッチにより ISDM-2 を再イメージングするには、以下の手順を実行します。

注: アプリケーション パーティション上のすべての情報が失われます。 設定が保持されている間、ISDM-2 でパスワード リカバリを実行するために使用できる方式はありません。

1. スイッチ コマンド **hw-module module x reset cf:1** (ここで、*x* はスロット番号を表し、cf は「コンパクト フラッシュ」を表します) を使用して、メンテナンス パーティションに IDSM-2 を起動します。**注:** cf:1 を使用して問題が発生した場合、代わりに hdd:2 を使用してみてください。
```
SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ---------
---------------------------- ----------------- ----------- 6 8 Intrusion Detection System
WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ----------------------------
------ ------ ------------ ------------ ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102
7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- --------------------------- -
-------------- --------------- ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG
0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass SV9-1#hw-module
module 6 reset cf:1 Device BOOT variable for reset = Warning: Device list is not verified.
Proceed with reload of module? [confirm]y % reset issued for module 6 !--- Output is
suppressed.
```
2. スイッチ コマンド **show module x** を使用して、IDSM-2 がオンラインになることを確認します。IDSM-2 ソフトウェアのバージョンの末尾に「m」があり、状態が正であることを確認します。
```
SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ---------------
----------------------- ----------------- ----------- 6 8 Intrusion Detection System (MP)
WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ----------------------------
------ ------ ------------ ------------ ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102
7.2(1) 1.3(2)m Ok Mod Sub-Module Model Serial Hw Status --- --------------------------- ---
------------ --------------- ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG
0347FDB6B8 2.0 Ok Mod Online Diag Status --- ------------------- 6 Pass
```
3. メンテナンス パーティションに起動した IDSM-2 に接続します。 スイッチ コマンド **session slot x processor 1** を使用します。ユーザ名/パスワードとして、**guest/cisco** を使用します。
```
SV9-1#session slot 6 processor 1 The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open
Cisco Maintenance image login: guest Password: Maintenance image version: 1.3(2)
guest@idsm2-sv-rack.localdomain#
```
4. IDSM-2 が IP 接続されていることを確認します。 **ping ip_address** コマンドを使用します。
```
guest@idsm2-sv-rack.localdomain#ping 10.66.79.193 guest@idsm2-sv-rack.localdomain#ping
10.66.79.193 PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64
bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=2.188 msec 64 bytes from 10.66.79.193:
icmp_seq=1 ttl=255 time=1.014 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=991
```

usec 64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.011 msec 64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.019 msec --- 10.66.79.193 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev = 0.991/1.244/2.188/0.473 ms guest@idsm2-sv-rack.localdomain#

5. IDSM-2 が IP 接続されている場合は、手順 14 に進みます。
6. コマンドおよび制御インターフェイスがスイッチで正しく設定されていることを確認します。 **show run | inc intrusion-detection** コマンドを使用します。SV9-1#**show run | inc intrusion-detection** intrusion-detection module 6 management-port access-vlan 210
7. 通信パラメータが IDSM-2 のメンテナンス パーティションで正しく設定されていることを確認します。 **show ip** コマンドを使用します。guest@idsm2-sv-rack.local domain#**show ip** IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.66.79.223 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193Nameserver(s) :
8. パラメータが何も設定されていない場合、または一部のパラメータを変更する必要がある場合は、すべてクリアします。 **clear ip** コマンドを使用します。guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0 Nameserver(s) :
9. IDSM-2 メンテナンス パーティションの IP アドレスとマスク情報を設定します。 **ip address ip_address netmask** コマンドを使用します。guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224**
10. IDSM-2 メンテナンス パーティションのデフォルト ゲートウェイを設定します。 **ip gateway gateway-address** コマンドを使用します。guest@localhost.localdomain#**ip gateway 10.66.79.193**
11. IDSM-2 メンテナンス パーティションのホスト名を設定します。 **ip host hostname** コマンドを使用します。これは必ずしも必要ではありませんが、プロンプトも設定するので、デバイスを特定するのに便利です。guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-sv-rack.localdomain#
12. ブロードキャスト アドレスを明示的に設定するために必要になる場合があります。 **ip broadcast broadcast-address** コマンドを使用します。通常はデフォルト設定で十分です。guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. 再度 IP 接続を確認します。 IP 接続に依然として問題がある場合は、通常の IP 接続の問題としてトラブルシュートし、手順 14 に進みます。
14. IDSM-2 アプリケーション パーティションを再イメージングします。 **upgrade ftp-url ---- install** コマンドを使用します。guest@idsm2-sv-rack.localdomain#**upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install** Downloading the image. This may take several minutes... Password for cisco@10.66.64.10: 500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood. ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.40 sec (913.99k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is downloaded. Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing it [y|N]: y Proceeding with upgrade. Please do not interrupt. If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade. Creating IDS application image file... Initializing the hard disk... Applying the image, this process may take several minutes... Performing post install, please wait... Application image upgrade complete. You can boot the image now.
15. アプリケーション パーティションに IDSM-2 を起動します。 スイッチ コマンド **hw-module module x reset hdd:1** を使用します。SV9-1#**hw-module module 6 reset hdd:1** Device BOOT variable for reset = Warning: Device list is not verified. Proceed with reload of module? [confirm]y % reset issued for module 6 *!--- Output is suppressed.* または、起動デバイス変数が正しく設定されている限り、IDSM-2 で **reset** コマンドを使用できます。IDSM-2 の起動デバイス変数の設定を確認するには、スイッチ コマンド **show bootvar device module x** を使用します。SV9-1#**show bootvar device module 6** [mod:6]: SV9-1# IDSM-2 の起動デバイス変数を設定するには、スイッチ コンフィギュレーション コマンド **boot**

device module x hdd:1 を使用します。`SV9-1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SV9-1(config)#boot device module 6 hdd:1 Device BOOT variable = hdd:1 Warning: Device list is not verified. SV9-1(config)#exitSV9-1#show bootvar device module 6 [mod:6 ]: hdd:1` メンテナンス パーティションの CLI を使用して IDSM-2 をリセットするには、**reset** コマンドを使用します。`guest@idsm2-sv-rack.localdomain#reset !--- Output is suppressed.`

16. IDSM-2 がオンラインになることを確認します。 スイッチ コマンド **show module x** を使用します。IDSM-2 ソフトウェアのバージョンがアプリケーション パーティションのバージョンである (たとえば、*4.1(1)S47*) ことと状態が正常であることを確認します。`SV9-1#show module 6 Mod Ports Card Type Model Serial No. --- ----- ---------- ---------- ----------- ------------------ ----------- 6 8 Intrusion Detection System WS-SVC-IDSM2 SAD0645010J Mod MAC addresses Hw Fw Sw Status --- ---------- ---------- ---------- ------- ---------- ---------- ------- 6 0030.f271.e3fd to 0030.f271.e404 0.102 7.2(1) 4.1(1)S47 Ok Mod Sub-Module Model Serial Hw Status --- ---------- ---------- ---------- ------- ---------- ---------- ------- ------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0 Ok Mod Online Diag Status --- ---------- ---------- ---------- 6 Pass`
17. アプリケーション パーティションに起動した IDSM-2 に接続します。 スイッチ コマンド **session slot x processor 1** を使用します。ユーザ名/パスワードとして、**cisco/cisco** を使用します。`SV9-1#session slot 6 proc 1 The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote prompt to end the session Trying 127.0.0.61 ... Open login: cisco Password: You are required to change your password immediately (password aged) Changing password for cisco (current) UNIX password: New password: Retype new password: !--- Output is suppressed.`
18. IDSM-2 を設定します。 **setup** コマンドを使用します。`sensor#setup --- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration:networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnet Option disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 23:34:53 2003 Setup Configuration last modified: Sat Sep 20 23:32:38 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask 255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit [0] Go to the command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration and exit setup.Enter your selection [2]:Configuration Saved. sensor#`

ハイブリッド (CatOS) コードを実行するスイッチによる IDSM-2 の再イメージング

ハイブリッド (CatOS) コードを実行するスイッチにより ISDM-2 を再イメージングするには、以下の手順を実行します。

1. メンテナンス パーティションに IDSM-2 を起動します。 スイッチ コマンド **reset x hdd:2** を使用します。**注:** hdd:2 を使用して問題が発生した場合、代わりに cf:1 を使用してみてください。`SV9-1> (enable)show module 6 Mod Slot Ports Module-Type Model Sub Status --- ---- -- --- ---------- ---------- ---------- --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ---------- ---------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------- ---------- ---------- ------ ---------- ---------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------- ---------- ---------- ------ ---------- ---------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8`

2.0 SV9-1> (enable)**reset 6 hdd:2** This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed. *!--- Output is suppressed.*

2. IDSM-2 がオンラインになることを確認します。 スイッチ コマンド **show module x** を使用します。IDSM-2 ソフトウェアのバージョンの先頭に「m」が表示され、現在メンテナンス パーティションが実行され、状態が正常であることを確認します。SV9-1> (enable)**show module 6** Mod Slot Ports Module-Type Model Sub Status --- ---- ----- ---------- ---------- -- ------------------ --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ------------------- ----------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------- ---------- ------ ---------- ---------- -------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 1.3(2)m Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------- ---------- ---------- ---------- ------ ------ 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0
3. メンテナンス パーティションに起動した IDSM-2 に接続します。 スイッチ コマンド **session x** を使用します。ユーザ名/パスワードとして、**guest/cisco** を使用します。SV9-1> (enable)**session 6** Trying IDS-6... Connected to IDS-6. Escape character is '^]'. Cisco Maintenance image login: guest Password: Maintenance image version: 1.3(2) guest@idsm2-sv-rack.localdomain#
4. IDSM-2 が IP 接続されていることを確認します。 **ping ip_address** コマンドを使用します。guest@idsm2-sv-rack.localdomain#**ping 10.66.79.193** PING 10.66.79.193 (10.66.79.193) from 10.66.79.210 : 56(84) bytes of data. 64 bytes from 10.66.79.193: icmp_seq=0 ttl=255 time=1.035 msec 64 bytes from 10.66.79.193: icmp_seq=1 ttl=255 time=1.041 msec 64 bytes from 10.66.79.193: icmp_seq=2 ttl=255 time=1.066 msec 64 bytes from 10.66.79.193: icmp_seq=3 ttl=255 time=1.074 msec 64 bytes from 10.66.79.193: icmp_seq=4 ttl=255 time=1.026 msec --- 10.66.79.193 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/mdev = 1.026/1.048/1.074/0.034 ms
5. IDSM-2 が IP 接続されている場合は、手順 14 に進みます。
6. コマンドおよび制御インターフェイスがスイッチで正しく設定されていることを確認します。 **show port status x/2** コマンドを使用します。SV9-1> (enable)**show port status 6/2** Port Name Status Vlan Duplex Speed Type ----- ------------------- ---------- ---------- ------ ----- ------------ 6/2 connected 210 full 1000 Intrusion De
7. 通信パラメータが IDSM-2 のメンテナンス パーティションで正しく設定されていることを確認します。 **show ip** コマンドを使用します。guest@idsm2-sv-rack.localdomain#**show ip** IP address : 10.66.79.210 Subnet Mask : 255.255.255.224 IP Broadcast : 10.255.255.255 DNS Name : idsm2-sv-rack.localdomain Default Gateway : 10.66.79.193 Nameserver(s) :
8. パラメータが何も設定されていない場合、または一部のパラメータを変更する必要がある場合は、**clear ip** コマンドを使用してすべてクリアします。guest@idsm2-sv-rack.localdomain#**clear ip** guest@localhost.localdomain#**show ip** IP address : 0.0.0.0 Subnet Mask : 0.0.0.0 IP Broadcast : 0.0.0.0 DNS Name : localhost.localdomain Default Gateway : 0.0.0.0
9. IDSM-2 メンテナンス パーティションの IP アドレスとマスク情報を設定します。 **ip address ip_address netmask** コマンドを使用します。guest@localhost.localdomain#**ip address 10.66.79.210 255.255.255.224** guest@localhost.localdomain#
10. IDSM-2 メンテナンス パーティションのデフォルト ゲートウェイを設定します。 **ip gateway gateway-address** コマンドを使用します。guest@localhost.localdomain#**ip gateway 10.66.79.193** guest@localhost.localdomain#
11. IDSM-2 メンテナンス パーティションのホスト名を設定します。 **ip host hostname** コマンドを使用します。これは必ずしも必要ではありませんが、プロンプトも設定するので、デバイスを特定するのに便利です。guest@localhost.localdomain#**ip host idsm2-sv-rack** guest@idsm2-sv-rack.localdomain#
12. ブロードキャスト アドレスを明示的に設定するために必要になる場合があります。 **ip broadcast broadcast-address** コマンドを使用します。通常はデフォルト設定で十分です。guest@idsm2-sv-rack.localdomain#**ip broadcast 10.66.79.223**
13. 再度 IP 接続を確認します。 IP 接続に依然として問題がある場合は、通常の IP 接続の問題としてトラブルシュートし、手順 14 に進みます。

14. IDSM-2 アプリケーション パーティションを再イメージングします。 **upgrade ftp-url ---- install** コマンドを使用します。`guest@idsm2-sv-rack.localdomain#`**`upgrade ftp://cisco@10.66.64.10// tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz --install`**
`Downloading the image. This may take several minutes... Password for cisco@10.66.64.10:500 'SIZE WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz': command not understood.ftp://cisco@10.66.64.10//tftpboot/WS-SVC-IDSM2-K9-a-4.1-1-S47.bin. gz (unknown size)/tmp/upgrade.gz [|] 65259K 66825226 bytes transferred in 71.37 sec (914.35k/sec) Upgrade file ftp://cisco@10.66.64.10//tftpboot/ WS-SVC-IDSM2-K9-a-4.1-1-S47.bin.gz is downloaded. Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing it [y|N]: y Proceeding with upgrade. Please do not interrupt. If the upgrade is interrupted or fails, boot into Maintenance image again and restart upgrade. Creating IDS application image file... Initializing the hard disk...Applying the image, this process may take several minutes...Performing post install, please wait...Application image upgrade complete. You can boot the image now.`
15. アプリケーション パーティションに IDSM-2 を起動します。 スイッチ コマンド **reset x hdd:1** を使用します。`SV9-1> (enable)`**`reset 6 hdd:1`** `This command will reset module 6. Unsaved configuration on module 6 will be lost Do you want to continue (y/n) [n]? y Module 6 shut down in progress, please don't remove module until shutdown completed. !--- Output is suppressed.` または、起動デバイス変数が正しく設定されている限り、IDSM-2 で **reset** コマンドを使用できます。IDSM-2 の起動デバイス変数の設定を確認するには、スイッチ コマンド **show boot device x** を使用します。`SV9-1> (enable)`**`show boot device 6`** `Device BOOT variable = (null) (Default boot partition is hdd:1) Memory-test set to PARTIAL` IDSM-2 の起動デバイス変数を設定するには、スイッチ コンフィギュレーション コマンド **set boot device hdd:1 x** を使用します。`SV9-1> (enable)`**`set boot device hdd:1 6`** `Device BOOT variable = hdd:1 Memory-test set to PARTIAL Warning: Device list is not verified but still set in the boot string. SV9-1> (enable)` **`show boot device 6`** `Device BOOT variable = hdd:1 Memory-test set to PARTIAL` メンテナンス パーティション CLI から IDSM-2 をリセットするには、**reset** コマンドを使用します。`guest@idsm2-sv-rack.localdomain#`**`reset`** *`!--- Output is suppressed.`*
16. IDSM-2 がオンラインになることを確認します。 スイッチ コマンド **show module x** を使用します。IDSM-2 ソフトウェアのバージョンがアプリケーション パーティションのバージョンである (たとえば、*4.1(1)S47*) ことと状態が正常であることを確認します。`SV9-1> (enable)`**`show module 6`** `Mod Slot Ports Module-Type Model Sub Status --- ---- ----- --------- ---------- ---------- ---------- --- -------- 6 6 8 Intrusion Detection Syste WS-SVC-IDSM2 yes ok Mod Module-Name Serial-Num --- ---------- ---------- 6 SAD0645010J Mod MAC-Address(es) Hw Fw Sw --- ---------- ---------- 6 00-30-f2-71-e4-05 to 00-30-f2-71-e4-0c 0.102 7.2(1) 4.1(1)S47 Mod Sub-Type Sub-Model Sub-Serial Sub-Hw Sub-Sw --- ---------- ---------- ---------- ---------- 6 IDS 2 accelerator board WS-SVC-IDSUPG 0347FDB6B8 2.0`
17. アプリケーション パーティションに起動した IDSM-2 に接続します。 スイッチ コマンド **session x** を使用します。ユーザ名/パスワードとして、**cisco/cisco** を使用します。`SV9-1> (enable)`**`session 6`** `Trying IDS-6... Connected to IDS-6. Escape character is '^]'. login: cisco Password: You are required to change your password immediately (password aged) Changing password for cisco (current) UNIX password: New password: Retype new password: !-- Output is suppressed.`
18. **setup** コマンドを使用して IDSM-2 を設定します。`sensor#`**`setup`** `--- System Configuration Dialog --- At any point you may enter a question mark '?' for help. User ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'. Current Configuration: networkParams ipAddress 10.1.9.201 netmask 255.255.255.0 defaultGateway 10.1.9.1 hostname sensor telnetOption disabled accessList ipAddress 10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit exit service webServer general ports 443 exit exit Current time: Sat Sep 20 21:39:29 2003 Setup Configuration last modified: Sat Sep 20 21:36:30 2003 Continue with configuration dialog?[yes]: Enter host name[sensor]: idsm2-sv-rack Enter IP address[10.1.9.201]: 10.66.79.210 Enter netmask[255.255.255.0]: 255.255.255.224 Enter default gateway[10.1.9.1]: 10.66.79.193 Enter telnet-server status[disabled]: Enter web-server port[443]: Modify current access list?[no]: Modify system clock settings?[no]: The following configuration was entered. networkParams ipAddress 10.66.79.210 netmask`

```
255.255.255.224 defaultGateway 10.66.79.193 hostname idsm2-sv-rack accessList ipAddress
10.0.0.0 netmask 255.0.0.0 exit timeParams summerTimeParams active-selection none exit
exit service webServer general ports 443 exit exit [0] Go to the command prompt without
saving this config. [1] Return back to the setup without saving this config. [2] Save this
configuration and exit setup. Enter your selection[2]: Configuration Saved. sensor#
```

関連情報

- Cisco IDS Unix Director
- Catalyst 6500 シリーズ Intrusion Detection System (IDSM-1) サービス モジュール
- Catalyst 6500 シリーズ Intrusion Detection System (IDSM-2) サービス モジュール
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems