TREND MICRO

InterScan Messaging Security Virtual Appliance™ 9.1 Patch 3

高可用性ガイド

Messaging Security

※注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
  https://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

P/N: MSEM98517/181030_JP (2019/03)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の条例において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

InterScan Messaging Security Virtual Appliance により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

http://www.go-tm.jp/data-collection-disclosure

重要： データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。InterScan Messaging Security Virtual Appliance における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシーに従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

IMSVA 高可用性ガイド 5
背景情報 5
IMSVA の配置 5
上位/下位に配置されるコンポーネント 6
高可用性機能のサポート 7
高可用性の目標 7
配置図 (高可用性非対応) 8
配置図 (高可用性対応) 10
高可用性に関する考慮事項 11
オプションの操作 14
ハードディスクを下位デバイスに追加する 14
下位デバイスを新しい上位デバイスに接続する 18
DDA エージェントを再起動する 27
MCP エージェントを再起動する 27
FAQ 27
上位デバイスで障害が発生した際、下位デバイスで実行中のサービスはどうなりますか? 28

IMSVA 高可用性ガイド

高可用性は多くの企業運営における最優先事項です。今日の競争社会では、小規模な専門的ビジネスからグローバル企業まで、より多くの企業が顧客、パートナー、および端末にサービスを休みなく提供することを求められています。ビジネスを動かすためにサーバベースシステムへの依存が強まり、サーバサービスを絶え間なく実行する必要があります。企業データベースやメールなどのミッションクリティカルなアプリケーションは、多くの場合、高可用性に対応して設計されたシステムおよびネットワーク構造に常駐させる必要があります。企業は、信頼できる継続的なサービスを提供できるように、高可用性を考慮してシステムを計画および設定する必要があります。

本書では、8.5 Service Pack 1 以降のバージョンで提供されている InterScan Messaging Security Virtual Appliance (以下、IMSVA) の高可用性サポートについて説明します。

内容は次のとおりです。

- 5 ページの「背景情報」
- 7 ページの「高可用性機能のサポート」
- 14 ページの「オプションの操作」
- 27 ページの「FAQ」

背景情報

ここでは、IMSVA および IMSVA コンポーネントの上位/下位配置について説明します。

IMSVA の配置

IMSVA は地理的に分散した企業環境に配置できます。このような環境を上位/下位配置といいます。

上位/下位配置は、上位デバイスがセントラルコントローラおよびデータリポジトリの役割を担うことを前提としています。IMSVA の配置では、ポリシーデータを含むすべての設定情報は、上位デバイスがホストするデータベース

に保存されます。すべての下位デバイスは、システムおよびポリシーの設定について上位デバイスと直接的または間接的に通信します。

パフォーマンス上の理由から、上位デバイスは通常メールメッセージを処理しませんが、設定可能なセントラルコントローラとして動作します。受信したメールメッセージは下位デバイスが処理します。

上位/下位配置で使用できる上位デバイスは 1 つのみです。結果として、配置全体で上位デバイスの可用性が非常に重要になります。ただし、上位デバイスが停止したからといって、配置全体の機能が必ずしも停止するわけではありません。

上位/下位に配置されるコンポーネント

次のコンポーネントは上位デバイスに配置されます。

- IMSVA 管理データベース。次のデータを保存します。
  - ポリシー
  - システム設定
  - ログ (システムイベントログとメッセージ追跡ログを含む)
  - 隔離されたメールメッセージのインデックス
  - レポート統計
  - IP プロファイラ統計
- DNS サーバ

  BIND で実装され、IP プロファイラ機能の DNS サービスを提供します。
- LDAP キャッシュ

  OpenLDAP で実装され、複数の LDAP サーバ情報を統合して提供します。このキャッシュのデータはポリシーの適用に使用できます。

注意

LDAP キャッシュは、複数の自社運用 LDAP サーバが選択されると有効になります。

次のコンポーネントは下位デバイスに配置されます。

- ポリシーサーバ
- IP プロファイラ

注意

下位デバイスを LDAP サーバに接続する場合は、1 つ以上の LDAP サーバが接続されていることを確認してください。自社運用 LDAP サーバが 1 つのみ接続されている場合、下位デバイスはその LDAP サーバにクエリを実行します。複数の自社運用 LDAP サーバが接続されている場合、下位デバイスはローカル LDAP キャッシュにクエリを実行します。

高可用性機能のサポート

ここでは、高可用性を有効にする前と後の IMSVA の配置図を示し、配置に関する考慮事項について説明します。

高可用性は、IMSVA 8.5 Service Pack 1 以降でサポートされます。下位デバイスが上位デバイスのデータベースへの接続に失敗すると自動的に有効になります。

高可用性の目標

上位デバイスの機能が停止したときにも上位/下位の配置での高可用性を保証するため、次の目標を達成する必要があります。リストは上から重要度の高い順に並べています。

1. 下位デバイスが影響を受けずにメールメッセージを正常に処理できること。
2. 下位デバイスが再起動されても継続してメールメッセージを処理できること。
3. 下位デバイスからシステム設定を継続して使用できること。

既存の IMSVA の配置での高可用性を実現するために設定を変更する必要はありません。上位デバイスがオフラインになると、次のようになります。

- 下位デバイスは影響を受けずにメールメッセージの処理を続行します。
- 下位デバイスを自由に再起動できます。
- ポリシー適用の LDAP クエリが影響を受けることはありません。
- 設定が影響を受けることはありません。
- 上位デバイスの回復後、MTA イベント、メッセージ追跡イベント、ポリシーイベントなどのログアクセスが失われることはありません。

注意

ログサイズや機能停止時間の長さによっては、遅延したログの上位デバイスへのアップロードに数時間から数日かかる場合があります。

配置図 (高可用性非対応)

次の図は、高可用性に対応する前の、上位/下位の形態で配置されている IMSVA 内の元のコンポーネントと接続を示しています。

注意

高可用性は、IMSVA 8.5 Service Pack 1 以降でサポートされます。

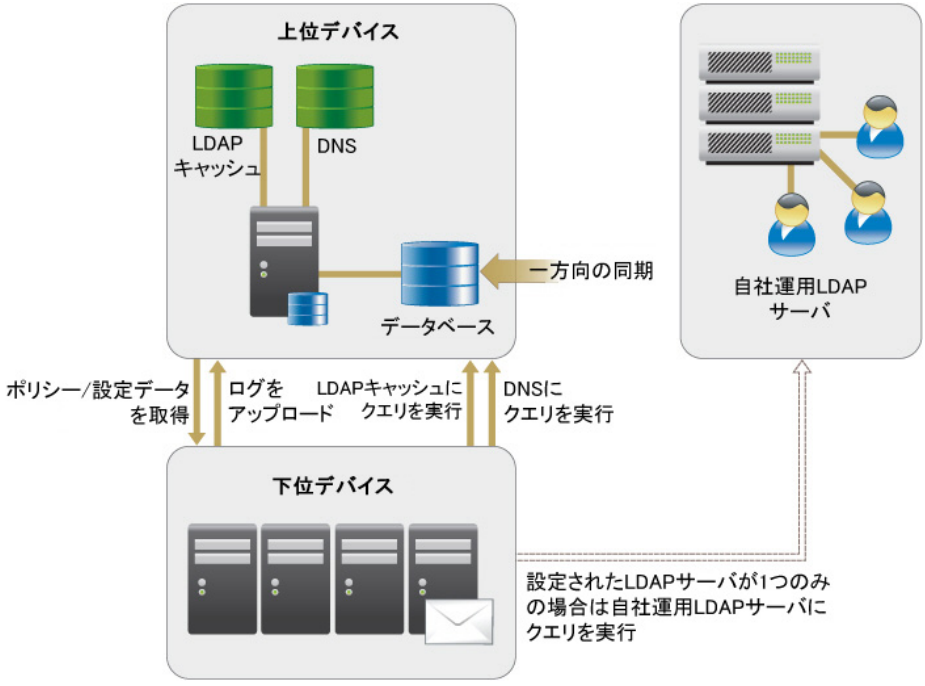


図 1. 元のコンポーネントと接続

配置図 (高可用性対応)

次の図は、高可用性モードの IMSVA 内の現在のコンポーネントと接続を示しています。

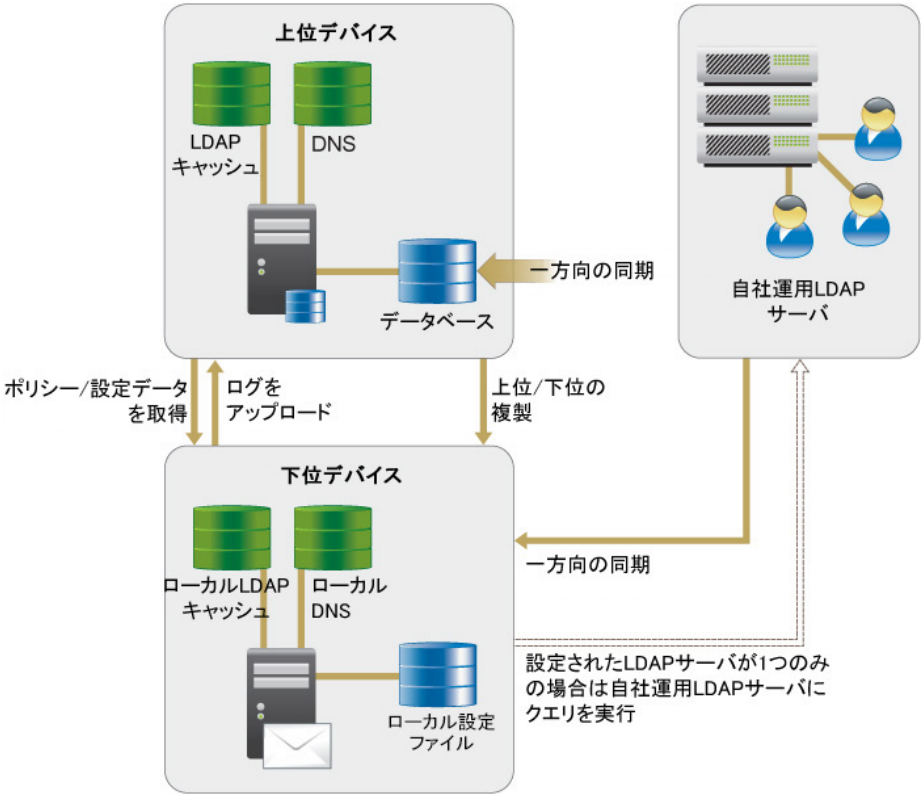


図 2. 現在のコンポーネントと接続

7 ページの「高可用性の目標」で定義された目的を達成するため、下位デバイスは次のように機能強化されています。

- ローカルポリシーサーバに保存されたポリシーやその他の設定の紛失を防止します。

- IP プロファイラ用に、ローカル DNS サーバを提供します。
- LDAP 関連機能用に、ローカル LDAP サーバを提供します。
- IP プロファイラから DNS クエリを要求された場合、ローカル DNS サーバにクエリを実行します。

注意

DNS クエリには、下位デバイスのローカル DNS サーバと、上位デバイスでホストされる DNS サーバとの同期が必要です。

- LDAP クエリを要求された場合、ローカル LDAP サーバ (または、設定される LDAP サーバが 1 つのみの場合は自社運用 LDAP サーバ) にクエリを実行します。

高可用性に関する考慮事項

- 上位デバイスの最長機能停止時間の見積もり。

  メールメッセージはネットワークを絶え間なく流れていますが、機能停止中は一時的に、管理コンソールへのアクセスおよびメールルーティングの追跡ができなくなります。さらに、機能停止中に生成されたログは下位デバイスに保存され、上位デバイスが回復するまでアップロードされません。高可用性を保証するには、上位デバイスの最長機能停止時間の計算が必要です。

注意

受信メールメッセージの件数を基に最長機能停止時間を計算する方法の詳細は、12 ページの「上位デバイスのダウンタイムを計算する」を参照してください。

- ローカルディスクへの頻繁な設定のバックアップ。

  頻繁にバックアップすることにより、上位デバイスの回復にかかる時間を短縮できます。エクスポート処理を自動化する手順の詳細については、25 ページの「自動エクスポートおよびインポート機能を有効にする」を参照してください。

- 以前に上位デバイスに割り当てられていたものと同じ IP アドレスを使用します。

  障害が発生した上位デバイスを回復できない場合は、代わりにそのデバイスのホットスタンバイを使用します。元の上位デバイスと同じ IP アドレスを使用して、IMSVA のコンポーネント間で通信の問題が発生する可能性を回避します。

  新しい上位デバイスへの接続方法の詳細については、18 ページの「下位デバイスを新しい上位デバイスに接続する」を参照してください。

上位デバイスのダウンタイムを計算する

上位デバイスで障害が発生すると、MTA や検索サービスで生成されたさまざまなログがローカルハードディスクに一時的に保存されます。これらのログは統合されて内部キャッシュに保存されます。上位デバイスが回復するとログは中央データベースにアップロードされますが、ログファイルのサイズ制限によっては、これらのログが削除される前に上位デバイスを回復させる必要があります。ログを下位デバイスに保持できる最長期間は、次の要素に応じて異なります。

- ログの保持期間

  ログの保持期間を設定するには、管理コンソールを開いて [ログ] > [設定] の順に選択し、[ログファイルを保存する日数] に値を入力します。

- ディスクの空き容量

  ローカルハードディスクにはメールメッセージも保存されます。使用可能なディスク領域が指定したしきい値 (初期設定で 10,240MB) を下回ると、IMSVA によって通知メッセージが送信されます。しきい値を設定するには、[管理] > [通知] の順に選択し、[イベント] タブをクリックして、[いずれかのホストでデータパーティションの空き容量が次の値を下回った場合] に値を入力します。

- 内部ログキャッシュサイズ

  初期設定の内部ログキャッシュサイズは 2GB です。この値を設定するには、[ログ] > [設定] の順に選択して、[サービス別ログファイルの最大サイズ] に値を入力します。

1 通のメッセージに関するログの保存には、平均 200 バイトのディスク容量を必要とします。メッセージトラフィックの平均サイズに基づいて、上位デバイスのダウンタイムの間にログを保存しておく期間を予測できます。

たとえば、A 社は 1 つの IMSVA サーバにつき、1 日平均 55,000 通のメールメッセージを処理しています。計算すると、ログサイズの合計は 1 日につき 11MB です。A 社のメールメッセージのピーク時の件数は、IMSVA サーバ 1 つにつき 2,760 通です。ピーク値を基にすると、メールメッセージの最大数は、IMSVA サーバ 1 つにつき 1 日 66,240 通です。計算すると、これらのメールメッセージから毎日 13MB のログが生成されます。IMSVA サーバの内部ログキャッシュでは、これらのログを約 150 日間保存できます。ただし、IMSVA は 90 日を超えたログを自動的に削除します。結果として、保持期間は 90 日間となります。

B 社の平均メッセージトラフィックは A 社の 2 倍で、ピーク時のメールメッセージの件数はさらに高くなっています。平均メッセージトラフィックは 1 日につきメールメッセージ 110,000 件で、メールメッセージのピーク件数は 1 時間あたり 9,000 件です。ピーク値を基にすると、メールメッセージの最大数は、IMSVA サーバ 1 つにつき 1 日 220,000 通です。計算すると、これらのメールメッセージから毎日 44MB のログが生成されます。IMSVA では、これらのログを内部ログキャッシュに約 45 日間保存できます。

注意

IP プロファイラのデータは、上位デバイスのダウンタイム中にはアップデートできません。

ダウンタイム中は仮想アナライザエージェントが一時停止します。上位デバイスが回復したら、仮想アナライザエージェントを手動で再起動します。詳細については、27 ページの「DDA エージェントを再起動する」を参照してください。

ダウンタイム中は Trend Micro Management Communication Protocol (MCP) エージェントが一時停止します。上位デバイスが回復したら、MCP エージェントを手動で再起動します。詳細については、27 ページの「MCP エージェントを再起動する」を参照してください。

ダウンタイム中はメールメッセージが暗号化されません。暗号化ポリシーに一致する送信メールメッセージは除外対象と見なされ、初期設定の検索処理は「[隔離および通知]」 となります。

クライアントがメールメッセージの受信に POP3 を使用している場合は、クライアントの POP3 サーバを上位デバイスから下位デバイスに変更します。

オプションの操作

ここでは、上位デバイスがオフラインになった場合に実行可能な操作について説明します。

ハードディスクを下位デバイスに追加する

下位デバイス上のハードディスクの容量が不十分な場合は、次の手順を実行します。

手順

1. シェル画面を起動して、root ユーザとしてログオンします。
2. /dev 以下のディスクパーティションを確認します。

   ```
   ls /dev/sd*
   ```

   注意

   初期設定では、sda、sda1、sda2 のディスクパーティションがあります。

3. 新しいハードディスクをインストールします。
   a. IMSVA サーバのデバイスの電源をオフにします。
   b. ハードディスクを挿入します。
   c. サーバの電源をオンにします。
4. IMSVA の再起動後、シェル画面で/dev の下に新しいハードディスクがあることを確認します。

   ```
   ll /dev/sd*
   ```

   出力内容に「sdb」などの新しいディスクが表示されます。

   注意

   以降のコマンドでは、ディスク名に「sdb」を使用します (変更していない場合)。

5. 新しいハードディスクにプライマリパーティションを作成します。

   a. 次のように入力します。

      ```
      fdisk /dev/sdb
      ```

   b. 「m」と入力して <Enter> キーを押し、コマンドの主な機能のメニューを表示します。

      注意

      使用可能な処理については、17 ページの「コマンドの動作」を参照してください。

   c. 「n」と入力して新しいパーティションを追加し、<Enter> キーを押します。

      次の出力が表示されます。

      ```
      e extended

      p primary partition (1-4)
      ```

   d. 「p」と入力してプライマリパーティションを追加し、<Enter> キーを押します。

      次の出力が表示されます。

      ```
      Partition number (1-4):
      ```

   e. パーティション番号に「1」と入力して、<Enter> キーを押します。

      次の出力が表示されます。

      ```
      First cylinder (1-5221, default 1):

      Using default value 1

      Last cylinder or +size or +sizeM or +sizeK (1-5221,
      default 5221):

      Using default value 5221
      ```

   f. 「w」と入力してパーティションテーブルをアップデートし、<Enter> キーを押します。

次の出力が表示されます。

```
The partition table has been altered!

Calling ioctl() to re-read partition table.

Syncing disks.
```

g. 次のコマンドを使用して、新しいパーティション (sdb1) を確認します。

```
ll /dev/sd*
```

6. 新しいハードディスクを ext3 ファイルシステムでフォーマットします。

```
mkfs.ext3 /dev/sdb1
```

7. パーティションに物理ボリュームを作成します。

```
pvcreate /dev/sdb1
```

8. 新しい物理ボリュームをボリュームグループに追加します。

```
vgextend IMSVA /dev/sdb1
```

9. スプールまたは app_data に領域を割り当てます。

注意

app_data は、IMSVA でメール領域とキューを格納するディレクトリです。

a. 次のコマンドを実行して、サービスを停止します。

```
imssctl.sh stop

service crond stop
```

b. 次のコマンドを実行して、app_data をアンマウントします。

```
umount /var/app_data
```

c. 次のコマンドを実行して、app_data に領域を割り当てます。

```
lvextend -L +100G /dev/mapper/IMSVA-App_data

e2fsck -f /dev/mapper/IMSVA-App_data
```

```
resize2fs /dev/mapper/IMSVA-App_data
```

注意

前述のコマンドで、100G は 100GB を意味します。これは、app_data に割り当てる必要がある領域のサイズです。

d. 次のコマンドを実行して、app_data をマウントします。

```
mount -t ext3 /dev/mapper/IMSVA-App_data /var/app_data
```

10. IMSVA サーバを再起動します。

コマンドの動作

a 起動可能フラグの切り替え

b bsd ディスクラベルの編集

c dos 互換フラグの切り替え

d パーティションの削除

l 既知のパーティションタイプのリスト表示

m このメニューの表示

n 新規パーティションの追加

o 空の新規 DOS パーティションテーブルの作成

p パーティションテーブルの表示

q 変更を保存せずに終了

s 空の新規 Sun ディスクラベルの作成

t パーティションのシステム ID の変更

u 表示/エントリ単位の変更

v パーティションテーブルの確認

w テーブルをディスクに書き込んで終了

x **拡張機能 （エキスパートのみ）**

下位デバイスを新しい上位デバイスに接続する

古い上位デバイスが復元できない場合は、新しい上位デバイスをインストールします。次の手順を実行して、下位デバイスを新しい上位デバイスに接続してください。

次の手順を実行する前に、設定を元の上位デバイスから新しい上位デバイスにインポートしてください。設定の自動エクスポートおよびインポート方法の詳細については、25 ページの「自動エクスポートおよびインポート機能を有効にする」を参照してください。

注意

以降の手順では、新しい上位デバイスの IP アドレスを 10.204.168.98、下位デバイスの IP アドレスを 10.204.168.100 とします。

元の上位デバイスのすべてのログと隔離メッセージは、新しい上位デバイスの管理コンソールには表示できないことに注意してください。

手順

1. 元の上位デバイスとは異なる IP アドレスを使用して、新しい上位デバイスをインストールします。

   a. 新しい上位デバイスに、元の上位デバイスと同じビルドをインストールします。

      注意

      新しい上位デバイスが使用可能になる前に下位デバイスが接続して、下位デバイスのサービスが正常に動作しなくなることを防ぐために、新しい上位デバイスには別の IP アドレスを使用します。

   b. 元の設定を新しいサーバにインポートします。

2. すべての下位デバイスの IP アドレスを、新しい上位デバイスに追加します。

a. 上位デバイスの管理コンソールにログオンします。

b. [管理] > [IMSVA 設定] > [接続] の順に選択します。

初期設定で [コンポーネント] タブが表示されます。

c. [下位 IP アドレス] タブをクリックします。

d. [IP アドレスの追加] で、下位デバイスの IP アドレスを指定します。

e. [>>] をクリックします。

IP アドレスが IP アドレステーブルに表示されます。

f. [保存] をクリックします。

3. 下位デバイスの情報を取得します。

a. 次の図に示すように、`imss.ini` ファイルを開いて scanner_id を見つけます。

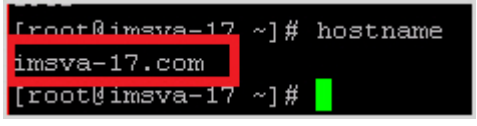
```
# vi /opt/trend/imss/config/imss.ini
```

注意

ここに示す図はすべて参考例です。

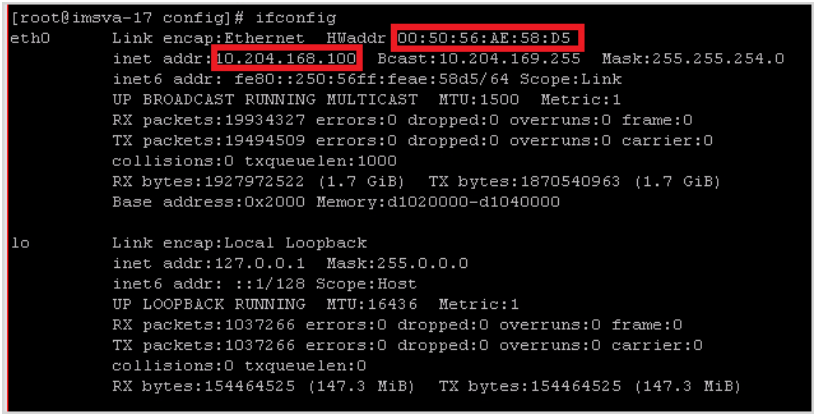
b. hostname を取得して、scanner_name として使用します。

```
# hostname
```



c. デバイスの IP アドレスと MAC アドレスを取得して、それぞれ ip_addr および mac_addr として使用します。

```
# ifconfig
```



d. アプリケーションのバージョンを取得して、app_ver として使用します。

```
#S99IMSS version
```

4. 新しい上位デバイスで tb_component_list データベーステーブルをアップデートします。

a. データベースにログオンします。

```
# /opt/trend/imss/PostgreSQL/bin/psql imss sa
```

b. データベーステーブルで設定を確認します。

```
# select * from tb_component_list;
```

注意

前述の図に示したコンポーネントとプロセスには、次のものが含まれます。

- daemon:検索デーモン
- policy:ポリシーサービス
- euq:エンドユーザメール隔離
- nrs:メールレピュテーションサービス
- ipprofiler:IP プロファイラ

1 はそのコンポーネントまたはプロセスが実行中でないこと、2 は実行中であることを示します。

c. tb_component_list テーブルをアップデートします。

```
Insert into tb_component_list
(scanner_id,scanner_name,ip_addr,daemon,policy,euq,nrs,
ipprofiler,os_ver,app_ver,mac_addr)
VALUES(2,'imsva-17.com','10.204.168.100',2,2,2,2,2,
'2.6.32','9.1.0.1592','00:50:56:98:62:C3');
```

注意

- 前述の下線の値を、19 ページの「3」番目の手順で取得した情報に置き換えます。
- 他の文字列値は、上位デバイスの値と必ず一致するようにします。

5. 新しい上位デバイスの tb_trusted_ip_list データベーステーブルをアップデートします。

a. データベースにログオンします。

```
# /opt/trend/imss/PostgreSQL/bin/psql imss sa
```

b. データベーステーブルで設定を確認します。

```
# select * from tb_trusted_ip_list;
```

```
imss=# select * from tb_trusted_ip_list;
    ip_addr     | scanner_id
----------------+------------
 10.204.168.98  |          1
 10.204.168.100 |         -1
(2 rows)
```

注意

scanner_id の値が 19 ページの「3」番目の手順で取得した値と異なる場合は、次の手順に進みます。値が一致する場合は、次の手順をスキップします。

c. tb_trusted_ip_list テーブルをアップデートします。

```
update tb_trusted_ip_list set scanner_id=2 where
ip_addr='10.204.168.100';
```

注意

scanner_id の値は、19 ページの「3」番目の手順で取得した値に置き換えます。

d. tb_scanner_id_seq テーブルをアップデートします。

```
select nextval('tb_scanner_id_seq') as nextid;
```

6. (オプション)以下を設定している場合は、新しい上位デバイスで手動で設定してください。

- Control Manager の設定
- 暗号化設定
- Deep Discovery Advisor の設定

注意

LDAP サーバを 2 つ設定している場合は、インポート中に一部の機能が無効になる場合があります。次のパスの機能を確認して、無効になっている場合は有効にします。

- [管理] > [接続] > [LDAP]
- [クラウドプレフィルタ] > [ポリシーリスト] > [ポリシー] > [条件] > [有効な受信者] > [定期メンテナンス]
- [管理] > [SMTP ルーティング] > [メッセージルール] > [リレー管理] > [不明な受信者を拒否する]

7. 現在の新しい上位デバイスの IP アドレスを、元の上位デバイスの IP アドレスに置き換えます。
   a. [管理] > [IMSVA 設定] > [設定ウィザード] の順に選択します。
   b. [次へ] をクリックします。

      [ローカルシステム設定] 画面が表示されます。
   c. 上位デバイスの IP アドレスを変更します。
8. 上位デバイスおよび下位デバイスの両方で次のコマンドを使用して、すべてのサービスを再起動します。

   ```
   # imssctl.sh restart
   ```
9. [システムステータス] 画面で、サービスが「開始」状態になっていることを確認します。

注意

エンドユーザメール隔離 (EUQ) サービスが有効な場合は、23 ページの「10」番目の手順から24 ページの「13」番目の手順に進んでください。それ以外の場合は、これらの手順をスキップします。

10. 下位デバイスの EUQ データベースをアタッチします。
    a. 上位デバイスの管理コンソールにログオンします。
    b. [管理] > [IMSVA 設定] > [接続] の順に選択します。

c. [データベース] タブをクリックします。

d. [EUQ データベース] で [アタッチ] をクリックします。

[EUQ データベースのアタッチ] 画面が表示されます。

e. 19 ページの「3」番目の手順で取得したサーバ IP アドレスを使用して、必要に応じて他の情報を指定します。

f. [OK] をクリックします。

11. 上位デバイスの管理コンソールでエンドユーザメール隔離を設定します。

a. 管理コンソールにログオンします。

b. [管理] > [エンドユーザメール隔離] の順に選択します。

[エンドユーザメール隔離管理] タブが表示されます。

c. [エンドユーザメール隔離を有効にする] チェックボックスをオフにして、[保存] をクリックします。

d. [エンドユーザメール隔離を有効にする] チェックボックスをオンにして、[保存] をクリックします。

12. [システムステータス] に移動して、エンドユーザメール隔離サービスが起動したことを確認します。

13. [管理] > [エンドユーザメール隔離] の順に選択します。[すべて (承認済み送信者リストとスパムメール情報) を再配布] をクリックして、[再配布] をクリックします。

自動エクスポートおよびインポート機能を有効にする

IMSVA には、設定の自動エクスポートおよびインポート機能があります。自動エクスポートは毎日午前 4 時に実行され、自動インポートは毎日午前 4 時 30 分に実行されます。

手順

1. 新しい上位デバイスをインストールします。
2. 元の上位デバイスと新しい上位デバイスで、自動エクスポートおよびインポート機能を有効にします。
   - 元の上位デバイスで、次の操作を実行します。
     a. 次のコマンドを使用して、`imss.ini` スクリプトファイルを開きます。

        # vi /opt/trend/imss/config/imss.ini

     b. ファイルに次の情報を追加します。

```
[AutoImportExport]
AutoImpExpEnable=on
AutoImpExpDirection=export
AutoImpExpFTPServer=192.168.0.1
AutoImpExpFTPPort=21
AutoImptExpFTPDir=/home/export
AutoImptExpFTPUser=test
AutoImpExpFTPPwd=test
```

> **注意**
> 前述の下線のキー値は一例です。実際の設定に置き換えてください。これらのキーの詳細については、26 ページの「キーと設定」を参照してください。

   - 新しい上位デバイスで、次の操作を実行します。
     a. 次のコマンドを使用して、`imss.ini` スクリプトファイルを開きます。

        # vi /opt/trend/imss/config/imss.ini

b. ファイルに次の情報を追加します。

```
[AutoImportExport]
AutoImpExpEnable=on
AutoImpExpDirection=import
AutoImpExpFTPServer=192.168.0.1
AutoImpExpFTPPort=21
AutoImptExpFTPDir=/home/export
AutoImptExpFTPUser=test
AutoImpExpFTPPwd=test
```

注意

前述の下線のキー値は一例です。実際の設定に置き換えてください。これらのキーの詳細については、26 ページの「キーと設定」を参照してください。

FTP サーバに複数の IP アドレスがある場合、インポート機能は使用できません。

キーと設定

表 1. 自動インポートおよびエクスポート機能のキー

キー名	使用可能な値	初期設定値	説明
AutoImpExpEnable	on/off	off	on:この機能を有効にする off:この機能を無効にする
AutoImpExpDirection	export/import	export	export:IMSVA からデータを自動的にエクスポートする import:IMSVA にデータを自動的にインポートする
AutoImpExpFTPServer	ホスト名/IP	空白	FTP サーバのホスト名または IP アドレス
AutoImpExpFTPPort	ポート番号	空白	FTP サーバのポート番号

キー名	使用可能な値	初期設定値	説明
AutoImptExpFTPDir	ディレクトリ	空白	エクスポートしたデータを保存する FTP サーバのディレクトリ
AutoImptExpFTPUser	ユーザ名	空白	FTP サーバへのログオンに使用するユーザ名
AutoImpExpFTPPwd	パスワード	空白	FTP サーバへのログオンに使用するパスワード

DDA エージェントを再起動する

手順

1. IMSVA 下位デバイスにログオンします。
2. 次のコマンドを実行します。

```
# S99DTASAGENT restart
```

MCP エージェントを再起動する

手順

1. IMSVA 下位デバイスにログオンします。
2. 次のコマンドを実行します。

```
# S99CMAGENT restart
```

FAQ

この項では、よくある質問 (FAQ) に対する回答を提供します。

上位デバイスで障害が発生した際、下位デバイスで実行中のサービスはどうなりますか?

下位デバイスで実行中のサービスは自動的に再起動され、切断された上位デバイスとの TCP 接続を閉じます。サービスの再起動の順序は非同期です。上位デバイスが回復すると、これらのサービスはもう一度非同期的に再起動され、再接続します。