TREND MICRO™

Deep Discovery™ Analyzer 1200 クイックスタートガイド

Deep Discovery Analyzerは、トレンドマイクロやサードパーティのセキュリティ製品において標的型攻撃に対する保護を強化する、カスタムサンドボックスによるサンプル分析サーバです。トレンドマイクロのメールセキュリティ製品やWebセキュリティ製品と統合することができ、他のDeep Discovery製品のサンドボックス分析を補完および一元管理するためにも使用できます。

1 箱を開いて内容物を確認する

Deep Discovery Analyzerの箱に、以下のアイテムが含まれていることを確認します。

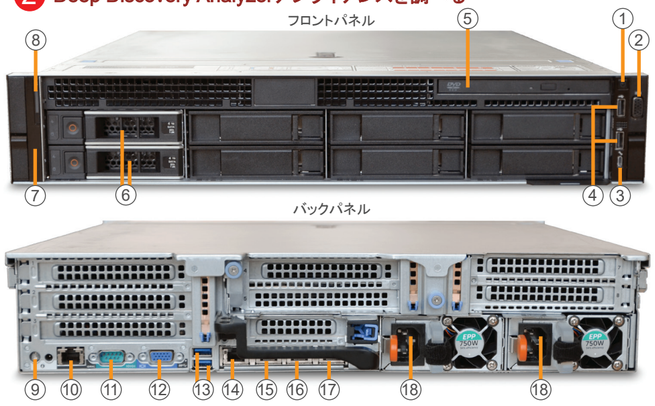
ラックレール

ドキュメントとDVD

Deep Discovery Analyzerアプライアンス

電源コード

2 Deep Discovery Analyzerアプライアンスを調べる



(1) 電源インジケータ/ボタン
(2) 前面ビデオコネクタ
(3) iDRACダイレクトポート
(4) USB 2.0コネクタ
(5) 光学ドライブ
(6) ハードドライブ
(7) システム状態とシステムIDインジケータ
(8) ステータスLEDインジケータ
(9) システムIDボタン
(10) iDRACポート
(11) シリアルコネクタ
(12) 背面ビデオコネクタ
(13) USB 3.0コネクタ
(14) 管理ポートeth0*
(15) カスタムポートeth1**
(16) カスタムポートeth2**
(17) カスタムポートeth3**,***
(18) 電源コネクタ

* 管理ポートeth0: 管理ネットワークにアプライアンスを接続します。
** カスタムポートeth1、eth2、eth3: サンドボックス分析専用の隔離ネットワークにアプライアンスを接続します。
*** カスタムポートeth3: 高可用性を使用する場合、アプライアンスを同一アプライアンスのeth3に接続します。サンドボックス分析に使用できるのは、eth1とeth2のみです。

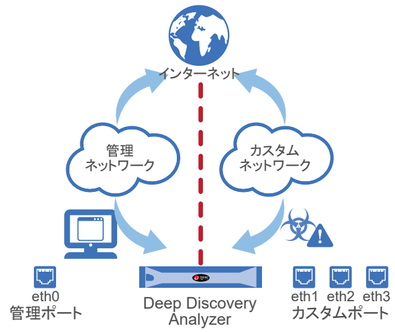
3 推奨ネットワーク環境

Deep Discovery Analyzerは管理ネットワークに接続する必要があります。管理ネットワークは通常、組織のイントラネットです。配置した後、管理者は管理ネットワーク上の任意のコンピュータから設定作業を実行できます。

サンプル分析にはカスタムネットワークを使用することをお勧めします。カスタムネットワークは独自のネットワーク設定でインターネットに接続されている必要があります。

Deep Discovery Analyzerにはカスタムネットワークにプロキシを設定するオプションがあり、プロキシ認証もサポートされます。

カスタムネットワーク内の不正なサンプルが管理ネットワーク内のホストに影響を及ぼさないよう、ネットワークは互いに独立している必要があります。



4 配置チェックリスト

要件	詳細
アクティベーションコード	トレンドマイクロから取得します
モニタとVGAケーブル	アプライアンスのVGAポートに接続します
USBキーボード	アプライアンスのUSBポートに接続します
USBマウス	アプライアンスのUSBポートに接続します
Ethernetケーブル	• アプライアンスの管理ポートを管理ネットワークに接続するケーブルを1本 • カスタムポートをサンドボックス分析専用の隔離ネットワークに接続するケーブルを1本 • 高可用性を使用する場合、ケーブルの1本は、同一のDeep Discovery Analyzerアプライアンス上のeth3間を接続します。
インターネット接続が有効なコンピュータ	次のソフトウェアがインストールされているコンピュータ • Microsoft Internet Explorer 10または11、Microsoft Edge、Mozilla Firefox、あるいはGoogle Chrome
IPアドレス	• 管理ネットワーク内の静的IPv4アドレスを1つ • サンドボックスインスタンスでインターネット接続が必要な場合は、仮想アナライザ用のIPv4アドレスをもう1つ • 高可用性を使用する場合は仮想IPアドレスをもう1つ

5 ハードウェアを設定する

1. 標準的な19インチ4本柱のラック、または頑丈な机などの安定した場所にアプライアンスを設置します。

注意: アプライアンスを設置する際は、適切な通気と冷却を確保するために周囲に5cm以上の空間を設けてください。

2. アプライアンスを電源に接続します。
3. モニタをアプライアンス背面のVGAポートに接続します。
4. キーボードとマウスをアプライアンス背面のUSBポートに接続します。
5. Ethernetケーブルを管理ポートとカスタムポートに接続します。
6. アプライアンスの電源を入れます。

6 初期設定を実行する

1. 事前設定コンソールのログオン画面で、次の初期設定のログオンアカウント情報を入力します。
   - ユーザ名: admin
   - パスワード: Admin1234!

注意: 入力したパスワードの文字は画面に表示されません。

2. [Configure device IP address] を選択し、<Enter> キーを押します。
3. 次のネットワークアドレスを指定します。
   - IPv4アドレス: 仮想アナライザのアドレスやカスタムネットワークアドレスと競合しないようにする必要があります。
   - サブネットマスク
   - IPv4ゲートウェイ: IPアドレスと同じサブネット内に存在している必要があります。
   - IPv4 DNSサーバ1
4. <Tab> キーを押して [Save] に移動し、<Enter> キーを押します。

追加の設定手順については、管理者ガイドの導入に関する章を参照してください。

7 管理コンソールにアクセスする

1. サポートされているWebブラウザを使用して、次のWebサイトの管理コンソールを開きます。
   https://< Deep Discovery Analyzer IP Address>/pages/login.php

   注意:
   - インターネットセキュリティレベルを [中] に設定し、ActiveXのバイナリおよびスクリプトの動作を有効にします。
   - 初期設定で指定したIPアドレスを使用します。
2. ログオン画面で、次の初期設定のアカウント情報を入力します。
   - ユーザ名: admin
   - パスワード: Admin1234!
3. [ログオン] をクリックします。
4. 初期設定のパスワードを変更します。

8 連絡先情報

- Webサイト: http://www.trendmicro.com/
- 電話: 03-5334-3601 (営業代表)
- 住所: 〒151-0053 東京都渋谷区代々木 2-1-1 新宿マインズタワー

アイテムコード: ADAXZA-AQ0106