Deep Discovery™ Analyzer 7.1

インストールガイド

※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://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、およびスマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、およびウイルスバスター チェック！は、トレンドマイクロ株式会社の登録商標です。

P/N: APEM79310_210806_JP_R1 (2021/12)

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法令等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。

Deep Discovery Analyzer 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。

https://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。Deep Discovery Analyzer 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 (Global Privacy Notice) 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

本書について

第 1 章：はじめに

第 2 章：Deep Discovery Analyzer の配置の準備

第 3 章：アプライアンスのインストール

第 4 章：事前設定コンソールの使用

第 5 章：Deep Discovery Analyzer のアップグレード

第 6 章：テクニカルサポート

付録 A：付録

索引

はじめに

本書について

Deep Discovery Analyzer インストールガイドへようこそ。このガイドには、Deep Discovery Analyzer を配置、インストール、およびアップグレードするための要件と手順に関する情報が記載されています。

ドキュメント

Deep Discovery Analyzer のドキュメントには次のものがあります。

表 1. 製品ドキュメント

ドキュメント	説明
管理者ガイド	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 管理者ガイドには、Deep Discovery Analyzer を設定して管理する方法の詳細な手順、および Deep Discovery Analyzer の概念や機能に関する説明が記載されています。
インストールガイド	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 インストールガイドには、Deep Discovery Analyzer の導入計画とインストールの要件および手順、さらに事前設定コンソールを使用して初期設定とシステムタスクを実行する方法についての情報が含まれています。
Syslog コンテンツマッピングガイド	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 Syslog コンテンツマッピングガイドには、ログの管理基準や、Deep Discovery Analyzer の Syslog イベントを実装するための構文に関する情報が記載されています。
クイックスタートガイド	クイックスタートガイドには、Deep Discovery Analyzer をネットワークに接続して初期設定を実行するための手順がわかりやすく説明されています。
Readme	Readme には、オンラインヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれています。新機能、既知の問題、および製品リリースの履歴に関する情報を確認できます。
オンラインヘルプ	Deep Discovery Analyzer 管理コンソールからアクセスできる Web ベースのドキュメントです。 オンラインヘルプには、Deep Discovery Analyzer のコンポーネントと機能、Deep Discovery Analyzer を設定するために必要な手順が説明されています。

ドキュメント	説明
サポートポータル	サポートポータルは、問題の解決およびトラブルシューティングの情報を参照できるオンラインデータベースです。製品の既知の問題に関する最新の情報を得ることができます。サポートポータルにアクセスするには、以下の Web サイトをご覧ください。 https://success.trendmicro.com/jp/technical-support

対象読者

この Deep Discovery Analyzer のドキュメントは、IT 管理者とセキュリティアナリストを対象としています。ここでは次のトピックを含め、読者にネットワークと情報セキュリティに関する十分な知識があることを前提としています。

- ネットワークトポロジ
- データベース管理
- ウイルス対策とコンテンツのセキュリティ保護

ただし、サンドボックス環境や脅威イベントの相関分析については、読者がその知識を持っていないものとして説明します。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
注意	設定上の注意

表記規則	説明
 ヒント	推奨事項
 重要	必要な設定や初期設定、および製品の制限事項に関する情報
 警告!	重要な操作と設定オプション

用語

用語	説明
アップデートサーバ	パターンファイルなどの製品コンポーネントのアップデートを提供します。コンポーネントのアップデートを定期的にリリースします。
アクティブなプライマリアプライアンス	すべての管理タスクを実行するクラスタ化されたアプライアンスです。すべての設定を保持し、パフォーマンス向上のためにセカンダリアプライアンスに送信を割り当てます。
管理者	Deep Discovery Analyzer の管理担当者です。
クラスタリング	複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。
カスタムポート	サンドボックス分析専用の隔離されたネットワークに Deep Discovery Analyzer を接続するハードウェアポートです。
ダッシュボード	ウィジェットが表示される UI 画面です。

用語	説明
高可用性クラスタ	高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。
負荷分散クラスタ	負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。
管理コンソール	製品を管理するための Web ベースのユーザインタフェース。
管理ポート	管理ネットワークに接続するハードウェアポート。
パッシブなプライマリアプライアンス	アクティブなプライマリアプライアンスでエラーが発生し回復できない状態になるまでスタンバイしているクラスタ化されたアプライアンスです。高可用性を提供します。
役割ベースの管理	管理者がユーザアカウントを設定して管理コンソールへのアクセスを制御する方法を効率化します。
サンドボックスイメージ	設定とインストールが不要の、すぐに使用できるソフトウェアパッケージ (OS とアプリケーションのセット) です。仮想アナライザは OVA (Open Virtual Appliance) 形式のイメージファイルのみをサポートします。
サンドボックスインスタンス	サンドボックスイメージに基づく単一の仮想マシン。
セカンダリアプライアンス	パフォーマンスの向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理するクラスタ化されたアプライアンスです。

用語	説明
スタンドアロンアプライアンス	どのクラスタにも属さないアプライアンスです。クラスタ化されたアプライアンスは、アプライアンスをクラスタからデタッチすることでスタンドアロンアプライアンスに戻すことができます。
Threat Connect	環境内で検出された不審オブジェクトとトレンドマイクロ Smart Protection Network の脅威データを関連付けます。生成されるインテリジェンスレポートを使用すれば、潜在的な脅威について調べ、攻撃プロファイルに適した対応ができます。
仮想アナライザ	サンプルの管理および分析に使用する、隔離された仮想環境。仮想アナライザではサンプルの動作や特徴を監視して、そのサンプルにリスクレベルを割り当てます。
ウィジェット	目的の選択したデータセットを表示するためのカスタマイズ可能な画面です。
YARA	YARA ルールは、環境に固有の標的型攻撃およびセキュリティ脅威を特定するためのカスタマイズ可能な不正プログラム検出パターンです。

トレンドマイクロについて

トレンドマイクロは、サイバーセキュリティにおける世界的企業として、安全にデジタル情報をやり取りできる環境の実現に向けて継続的に取り組んでいます。個人消費者、企業、および政府機関向けの革新的ソリューションである XGen セキュリティ戦略を巧みに利用することで、つながるセキュリティをデータセンター、クラウドワークロード、ネットワーク、およびエンドポイントにもたらします。

Amazon Web Services、Microsoft、および VMware などの主要な環境に合わせて最適化された階層化ソリューションにより、組織は、今日の脅威から重要な情報を自動的に保護することができます。トレンドマイクロの提供する Connected Threat Defense によって、脅威インテリジェンスのシームレスな共有が可能になるとともに、一元化された可視性と調査の提供によって、組織の柔軟性が最大限に高まります。

トレンドマイクロのお客さまには、自動車、銀行、医療、電気通信、および石油といった産業にわたる、Fortune Global 500 企業の上位 10 社のうち 9 社が含まれています。

世界 50 か国の 6,500 人を超える従業員と、最先端のグローバルな脅威調査および脅威インテリジェンスによって、トレンドマイクロは「つながる世界」のセキュリティを確保できるようお客さまを支援します。詳細については、次のサイトを参照してください。https://www.trendmicro.com

第 1 章

はじめに

この章では、Deep Discovery Analyzer 7.1 およびこのリリースの新機能について説明します。

Deep Discovery Analyzer について

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。Deep Discovery Analyzer 内に作成可能なカスタムサンドボックス環境は、対象となるデスクトップソフトウェア設定と正確に一致するため、検出の精度が向上し、誤検出が減少します。

また Deep Discovery Analyzer には、任意のサードパーティ製品との統合を可能にする Web サービス API や、脅威を調査するための手動送信機能も用意されています。

新機能

表 1-1. Deep Discovery Analyzer 7.1 の新機能

機能/強化点	詳細
Trend Micro Vision One の統合	Service Gateway を介した Trend Micro Vision One との統合により、ハイブリッド環境における共同でのセキュリティ分析が可能になります。
メールでの送信	メールでの送信機能により、許可された送信者ドメインおよび SMTP サーバからのメールメッセージを受信して分析できるようになります。
仮想アナライザの機能強化	内部仮想アナライザが強化され、次の機能が追加されます。 • Windows 10 October 2020 Update イメージのサポート • SHA-256 オブジェクトの除外の種類 • 分析レポートの TLSH 情報

機能/強化点	詳細
監査ログの機能強化	ユーザが次のことを実行すると監査ログが生成されます。 • 調査パッケージまたは分析レポートの表示またはダウンロード • 送信のエントリの削除
システムログの機能強化	ICAP 事前検索のログを Syslog サーバに送信するオプションが提供されます。
運用レポートの機能強化	運用レポートが強化され、ICAP 事前検索のログが含まれるようになります。
インタフェース管理の機能強化	インタフェース管理の機能が強化され、トラブルシューティングを容易にするため、インタフェースの MAC アドレスが含まれるようになります。

サンプルの送信のフィルタと削除	[送信] 画面に次のものが含まれます。
	• 選択したサンプルと関連する分析データを削除するオプション ([完了] タブと [失敗] タブ)
	• 次の詳細検索フィルタ ([完了] タブ):
	  • MITRE ATT&CK™ Tactics
	  • MITRE ATT&CK™ Techniques
	  • 著しい特性

SNMP クエリの機能強化	SNMP クエリの機能が強化され、リアルタイムのアプリケーションイベントまたは指定した時間範囲内のイベントが含まれるようになります。
YARA ルールの機能強化	YARA ルールの機能が強化され、4.1.0 の公式な仕様がサポートされるようになります。
Deep Discovery Analyzer 6.9 および 7.0 からのインラインでの移行	ハードウェアモデルが 1100 および 1200 の場合、Deep Discovery Analyzer 6.9 または 7.0 の設定を 7.1 に自動的に移行できます。

機能と利点

Deep Discovery Analyzer には次の機能があります。

一元化されたサービスとしてのサンドボックスの有効化

メール、ネットワーク、エンドポイント、およびその他のサンプルソースの遅延のない処理を可能するスケーラブルなソリューションにより、最適なパフォーマンスを実現します。

カスタムサンドボックス

ご使用の環境について攻撃者が想定するデスクトップソフトウェア設定に合わせた環境でサンドボックスシミュレーションと分析を行い、誤検出の可能性を低減しながら最適な検出を実現します。

幅広いファイル分析範囲

複数の検出エンジンとサンドボックスを使用して、Windows 実行可能ファイル、Microsoft Office や PDF のドキュメント、Web コンテンツ、および圧縮ファイルなど広範囲にわたるファイルタイプを検査します。

YARA ルール

Deep Discovery Analyzer では YARA ルールを使用して不正プログラムを特定します。YARA ルールは、環境に固有の標的型攻撃およびセキュリティ脅威を特定するためのカスタマイズ可能な不正プログラム検出パターンです。

ドキュメントのセキュリティホール悪用の検出

専用の検出機能とサンドボックスを使用して、通常一般的な Office 文書や他のファイル形式で配信される不正プログラムやセキュリティホール悪用を検出します。

自動 URL 分析

統合製品により自動的に送信された URL のページ検索とサンドボックス分析を実行します。

詳細レポート

一元化されたダッシュボードやレポートを介して、サンプルの活動や C&C 通信の詳細など、詳しい分析結果を得られます。

アラート通知

アラート通知は、Deep Discovery Analyzer の状態をただちに知らせる機能です。

クラスタ化配置

複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。

トレンドマイクロ製品との統合

トレンドマイクロ製品との統合があらかじめサポートされており、Deep Discovery Analyzer のサンドボックス機能をトレンドマイクロのメールセキュリティ製品や Web セキュリティ製品でも使用できます。

サンプルの送信

Deep Discovery Analyzer では、次のいずれかの方法でサンプルを送信できます。

- 統合セキュリティ製品の Web サービス API

- 管理コンソールでの手動操作
- 許可された送信者ドメインおよび SMTP サーバからのメール

Connected Threat Defense

仮想アナライザによって生成された、不審オブジェクトや IOC (Indicators of Compromise) 検出情報を、他のトレンドマイクロのソリューションやサードパーティのセキュリティ製品と自動的に共有、脅威への迅速な対応を実現します。

ICAP の統合

Deep Discovery Analyzer では、ICAP (Internet Content Adaptation Protocol) クライアントとの統合がサポートされます。統合後は、Deep Discovery Analyzer で次の機能を実行できるようになります。

- ICAP クライアントから送信されたサンプルを ICAP サーバとして分析する
- 指定したネットワーク動作 (URL アクセス/ファイルのアップロード/ファイルのダウンロード) がブロックされた場合に、ユーザ設定ページをエンドユーザに表示する
- ICAP クライアントリストを設定することで、サンプルを送信できる ICAP クライアントを制御する
- 選択した MIME コンテントタイプに基づいてファイルの検索をバイパスする
- 実際のファイルタイプに基づいてファイルの検索をバイパスする
- RESPMOD モードでの URL 検索をバイパスする
- さまざまな検索モジュールを使用してサンプルを検索する
- 仮想アナライザが処理できるファイルタイプに基づいてサンプル送信をフィルタする

第 2 章

Deep Discovery Analyzer の配置の準備

この章では、Deep Discovery Analyzer を配置し、ネットワークに接続するために準備する必要のある項目について説明します。

Deep Discovery Analyzer がすでにネットワークに配置されており、それに Patch または HotFix を適用する場合は、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

配置の概要

製品仕様

標準の Deep Discovery Analyzer アプライアンスの仕様は次のとおりです。

使用しているアプライアンスがこれらのハードウェア仕様を満たしていない場合は、トレンドマイクロにお問い合わせください。

製品仕様 – 1100 アプライアンス

機能	仕様
ラックサイズ	2U 19 インチ規格ラック
可用性	RAID1
ストレージ容量	4 TB の空き容量 注意 Deep Discovery Analyzer のハードドライブではホットスワップがサポートされています。
ネットワーク接続	• 管理ポート: 1 x 1Gb/100/10Base copper • カスタムポート: 3 x 1Gb/100/10Base copper
寸法 (幅 x 奥行 x 高さ)	48.2 cm (18.98 インチ) x 75.58cm (29.75 インチ) x 8.73cm (3.44 インチ)
最大重量	31.5 kg (69.45 lb)
動作時の室温 電源	10～35 °C (相対湿度 10～80%) 750W、120～240VAC 50/60Hz

製品仕様 – 1200 アプライアンス

機能	仕様
ラックサイズ	2U 19 インチ規格ラック
可用性	RAID1
ストレージ容量	4 TB の空き容量 注意 Deep Discovery Analyzer のハードドライブではホットスワップがサポートされています。
ネットワーク接続	• 管理ポート: 1 x 1Gb/100/10Base copper • カスタムポート: 3 x 1Gb/100/10Base copper
寸法 (幅 x 奥行 x 高さ)	48.2 cm (18.98 インチ) x 75.13cm (29.58 インチ) x 8.68 cm (3.42 インチ)
最大重量	28.6 kg (63.05 lb)
動作時の室温 電源	10～35 °C (相対湿度 10～80%) 750W、120～240VAC 50/60Hz

配置の注意事項

Deep Discovery Analyzer アプライアンスはスタンドアロンアプライアンスとして配置および設定できます。スタンドアロンアプライアンスは他の Deep Discovery Analyzer アプライアンスの支援を受けることなく、すべての送信されたオブジェクトを処理します。エラーが発生して回復できない場合、検索および分析サービスを継続して提供することはできません。

複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。

ご使用環境の要件と使用可能な Deep Discovery Analyzer アプライアンスの数に応じて、次のクラスタ設定を使用できます。

表 2-1. クラスタ設定

クラスタ設定	説明
高可用性クラスタ	高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。 詳細については、28 ページの「高可用性クラスタ」を参照してください。
負荷分散クラスタ	負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。 詳細については、30 ページの「負荷分散クラスタ」を参照してください。
負荷分散機能を備えた高可用性クラスタ	負荷分散機能を備えた高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスとして役割を引き継ぎます。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。 詳細については、31 ページの「負荷分散機能を備えた高可用性クラスタ」を参照してください。

高可用性クラスタ

高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新

しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。

アプライアンスでエラーが発生して回復できない場合にも Deep Discovery Analyzer の機能を引き続き使えるようにするには、このクラスタ設定を使用してください。

次の図は、高可用性クラスタ設定に配置された 2 つの Deep Discovery Analyzer アプライアンスと、統合製品が Deep Discovery Analyzer と通信する方法を示しています。

注意

- 高可用性クラスタに配置する前に、Deep Discovery Analyzer アプライアンスのファームウェアを最新バージョンにアップデートすることをお勧めします。
- アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスは eth3 を使用して接続する必要があります。
- カテゴリ 6 以上の Ethernet ケーブルを使用して、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンス (必ず eth3 を使用) を直接接続することをお勧めします。
- 潜在的な障害点の発生を最小限に抑えるため、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスは直接接続することをお勧めします。
- 異なるデータセンター内に配置されているなど、アクティブなプライマリアプライアンスがパッシブなプライマリアプライアンスに直接接続されていない場合は、次の要件を満たす必要があります。
  - アプライアンスが Deep Discovery Analyzer 1100 または 1200 である
  - アプライアンス間の接続が次の条件を満たしている
    - ネットワークの遅延が 15 ミリ秒未満
    - パケット損失率が 0.000001%未満
    - ネットワーク帯域幅が 240Mbps より大きい

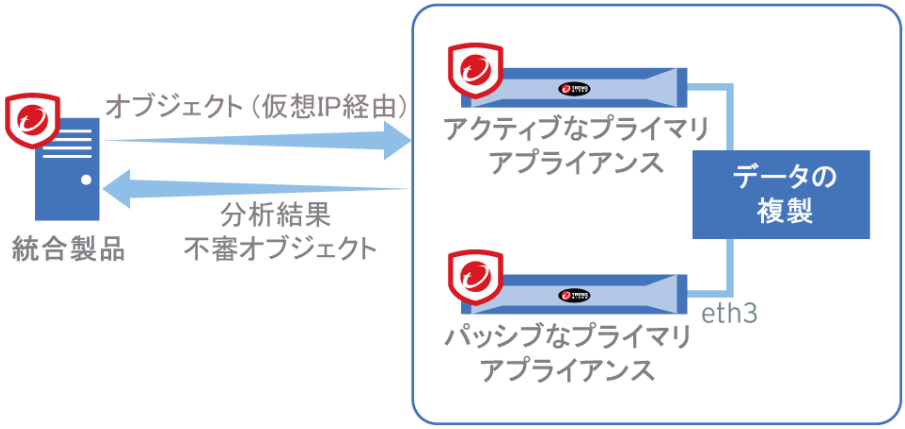

図 2-1. 高可用性クラスタ

負荷分散クラスタ

負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。

オブジェクト処理のパフォーマンスを向上させる必要がある場合は、このクラスタ設定を使用してください。

次の図は、負荷分散クラスタ設定に配置された Deep Discovery Analyzer アプライアンスと、統合製品が Deep Discovery Analyzer と通信する方法を示しています。

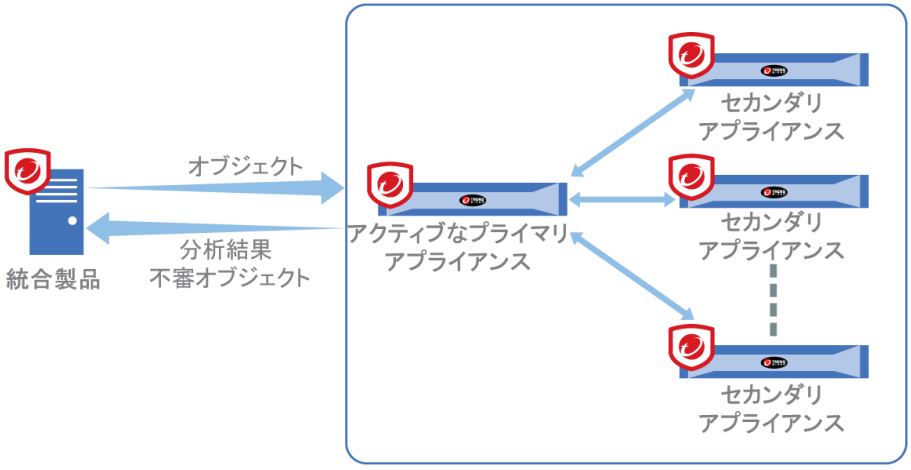

図 2-2. 負荷分散クラスタ

負荷分散機能を備えた高可用性クラスタ

負荷分散機能を備えた高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスとして役割を引き継ぎます。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。

高可用性クラスタリングと負荷分散クラスタリングの利点を組み合わせたい場合は、このクラスタ設定を使用してください。

次の図は、高可用性クラスタ設定に配置された Deep Discovery Analyzer アプライアンスと、統合製品が Deep Discovery Analyzer と通信する方法を示しています。

注意

- 高可用性クラスタに配置する前に、Deep Discovery Analyzer アプライアンスのファームウェアを最新バージョンにアップデートすることをお勧めします。
- アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスは eth3 を使用して接続する必要があります。
- カテゴリ 6 以上の Ethernet ケーブルを使用して、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンス (必ず eth3 を使用) を直接接続することをお勧めします。
- 潜在的な障害点の発生を最小限に抑えるため、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスは直接接続することをお勧めします。
- 異なるデータセンター内に配置されているなど、アクティブなプライマリアプライアンスがパッシブなプライマリアプライアンスに直接接続されていない場合は、次の要件を満たす必要があります。
  - アプライアンスが Deep Discovery Analyzer 1100 または 1200 である
  - アプライアンス間の接続が次の条件を満たしている
    - ネットワークの遅延が 15 ミリ秒未満
    - パケット損失率が 0.000001%未満
    - ネットワーク帯域幅が 240Mbps より大きい

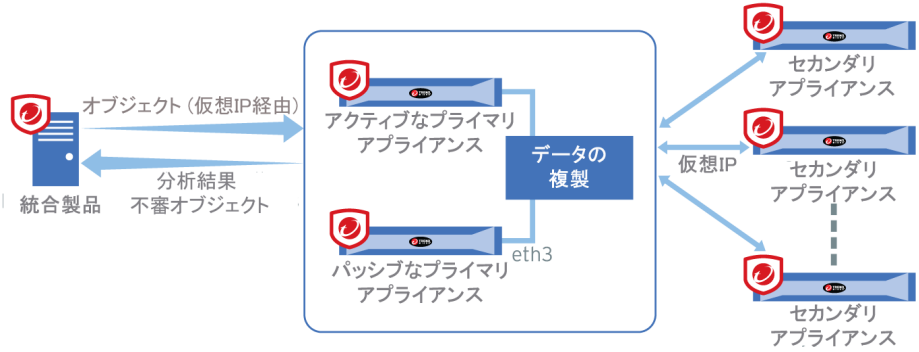

図 2-3. 負荷分散機能を備えた高可用性クラスタ

推奨ネットワーク環境

Deep Discovery Analyzer では、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可能性があります。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機能があり、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。

ネットワーク設定

ポートは、次の画像に示すようにアプライアンスの背面にあります。

ネットワークインタフェースポートには次のものがあります。

- 管理ポート (初期設定は 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 (管理ポートとして、または高可用性用に使用されていないポート): サンドボックス分析用に予約されているカスタムネットワークにアプライアンスを接続します。

注意

- インタフェース (初期設定は eth0) または NIC チーミングポートを管理ポートとして設定できます。
- 高可用性を使用する場合、eth3 は、2 つの同一のアプライアンスを直接接続するために使用します。サンドボックス分析には使用できません。
- 2 つの Deep Discovery Analyzer アプライアンスは必ず eth3 で接続されている必要があります。高可用性を使用しない場合は、eth1、eth2、および eth3 のいずれかがサンドボックス分析に使用できます。

Deep Discovery Analyzer には、管理ネットワークで使用可能な静的 IP アドレスが 1 つ必要です。

サンプル分析時に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、仮想アナライザに IP アドレスをさらに 1 つ割り当てることをお勧めします。[サンドボックス管理] > [ネットワーク接続] 画面で静的アドレスを指定できます。詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

配信の要件

要件	詳細
Deep Discovery Analyzer	トレンドマイクロから入手
Deep Discovery Analyzer インストール DVD	トレンドマイクロから入手
アクティベーションコード	トレンドマイクロから入手
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
イーサネットケーブル	• ケーブルの 1 本は、アプライアンスの管理ポートと管理ネットワークを接続します。 • ケーブルの 1 本は、カスタムポートとサンドボックス分析専用の隔離ネットワークを接続します。 • 高可用性を使用する場合、ケーブルの 1 本は、同一のアプライアンスの eth3 間を接続します。
IP アドレス	• 管理ネットワークの静的 IP アドレス 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 IP 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

要件	詳細
ソフトウェア	次のいずれかのブラウザ: • Microsoft Internet Explorer 11 • Microsoft Edge • Google Chrome • Mozilla Firefox
サードパーティソフトウェアのライセンス	サンドボックスイメージにインストールされているすべてのサードパーティソフトウェアのライセンス
製品統合の前提条件	別の製品と統合する場合、すべての統合要件を満たしていることを確認してください。 • 一部の統合製品では、Deep Discovery Analyzer と正しく統合するために追加の設定 (例: ホスト名、IP アドレス、SSL ポート) が必要です。詳細については、製品ドキュメントを参照してください。 • 一部の統合製品では、Deep Discovery Analyzer により提供される API キーが必要です。統合製品に登録した後、Deep Discovery Analyzer の API キーを変更した場合は、Deep Discovery Analyzer を統合製品から削除して再度追加します。 • ICAP (Internet Content Adaptation Protocol) クライアントは RFC 3507 に準拠している必要があります。

ログオンアカウント情報

コンソール	目的	初期設定のアカウント情報	実際の情報
事前設定コンソール	初期設定のタスクを実行します。51 ページの「事前設定コンソールでネットワークアドレスを設定する」を参照してください。	• Deep Discovery Analyzer ログイン (設定不可): `admin` • パスワード: `Admin1234!`	パスワード:

コンソール	目的	初期設定のアカウント情報	実際の情報
管理コンソール	• 製品の設定 • レポートの表示およびダウンロード	• ユーザ名 (設定不可): `admin` • パスワード: `Admin1234!`	パスワード:
		その他のユーザアカウント (管理コンソールの [管理] > [アカウント/連絡先] > [アカウント] で設定)	ユーザアカウント 1: ユーザ名: パスワード:
			ユーザアカウント 2: ユーザ名: パスワード:

アプライアンスで使用されるポート

次の表は、Deep Discovery Analyzer で使用されるポートとその目的を示しています。

表 2-2. Deep Discovery Analyzer で使用されるポート

ポート	プロトコル	機能	目的
21	TCP	アウトバウンド	Deep Discovery Analyzer では、このポートを使用してバックアップデータを FTP サーバに送信します。
22	TCP	インバウンドおよびアウトバウンド	次のことを実行します。 • コンピュータを使用して SSH 経由で事前設定コンソールにアクセスします。 • バックアップデータを SFTP サーバに送信します。

ポート	プロトコル	機能	目的
			• デバッグログを SFTP サーバに送信します。
53	TCP/UDP	アウトバウンド	このポートは DNS による名前解決用に使用されます。
67	UDP	アウトバウンド	IP アドレスが動的に割り当てられている場合、DHCP サーバに要求を送信します。
68	UDP	インバウンド	DHCP サーバから応答を受信します。
80	TCP	インバウンド (初期設定では無効)	このポートは初期設定で無効になっています。Deep Discovery Analyzer では、仮想アナライザイメージアップロードツールでこのポートを使用します。
123	UDP	インバウンドおよびアウトバウンド	NTP サーバに接続して時間を同期します。
137	UDP	アウトバウンド	NetBIOS を使用して IP アドレスをホスト名に解決します。
161	UDP	インバウンド	Deep Discovery Analyzer のこのポートは SNMP マネージャからの要求を待機するために使用されます。
162	UDP	アウトバウンド	Deep Discovery Analyzer では、このポートを使用して SNMP マネージャへ SNMP トラップメッセージを送信します。
443	TCP	インバウンド	次のことを実行します。 • コンピュータを使用して HTTPS 経由で管理コンソールにアクセスします。 • クラスタ環境内の他の Deep Discovery Analyzer アプライアンスと通信します。 • Trend Micro Apex Central と通信します。

ポート	プロトコル	機能	目的
			• Manual Submission Tool を使用してコンピュータからファイルを受信します。 • 統合製品からサンプルを受信します。 • Deep Discovery Analyzer の Web サービスプロトコルを介して統合製品に不審オブジェクトのリストと分析情報を送信します。
		アウトバウンド	次のことを実行します。 • トレンドマイクロ Threat Connect に接続します。 • Web レピュテーションサービスに接続してブロックの理由をクエリします。 • macOS に関連したサンプルを分析するために Sandbox as a Service に接続します。 • 機械学習型検索エンジンに接続します。 • アップデートサーバに接続してコンポーネントをアップデートします。 • CSSS (Certified Safe Software Service) を使用してファイルの安全性を確認します。 • オンプレミスバージョンの Deep Discovery Director と通信します。 • サポート契約ポータルで Deep Discovery Analyzer の製品ライセンスを確認します。 • Trend Micro Smart Protection Network を使用して Web レピュテーションサービスに対してクエリを実行します。 • ファイルサンプルの分析時にコミュニティファイルレピュテーションサービ

ポート	プロトコル	機能	目的
			スに接続してファイル出現率を調べます。 • コミュニティドメイン/IP レピュテーションサービスに接続します。 • 動的な URL 検索に接続します。 • Vision One との統合のために Service Gateway と通信します。
ユーザ指定		インバウンド	次のことを実行します。 • ICAP プロトコルを使用して ICAP クライアントからサンプルを受信します。 • メールメッセージを介してサンプルを受信します。 • ユーザが VNC クライアントを使用して仮想アナライザインスタンスに接続することを可能にします。
		アウトバウンド	次のことを実行します。 • Syslog サーバにログを送信します。 • プロキシサーバに接続します。 • Smart Protection Server に接続します。 • Microsoft Active Directory サーバに接続します。 • SMTP にて通知と予約レポートを送信します。

第 3 章

アプライアンスのインストール

この章では、Deep Discovery Analyzer のインストールタスクについて説明します。

Deep Discovery Analyzer は新規アプライアンスにすでにインストールされています。ファームウェアを再インストールまたはアップグレードする必要がある場合のみ、タスクを実行してください。

インストールタスク

手順

1. アプライアンスでインストール準備を行います。詳細については、42 ページの「ハードウェアを設定する」を参照してください。
2. Deep Discovery Analyzer をインストールします。詳細については、44 ページの「Deep Discovery Analyzer をインストールする」を参照してください。
3. 事前設定コンソールでアプライアンスの IP アドレスを設定します。詳細については、51 ページの「事前設定コンソールでネットワークアドレスを設定する」を参照してください。

ハードウェアを設定する

手順

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、換気と冷却が適切に行われるよう前後左右に少なくとも 2 インチ (約 5cm) の隙間を空けてください。

2. アプライアンスを電源につなぎます。

   Deep Discovery Analyzer には、750W のホットプラグ対応電源ユニットが 2 つ搭載されています。1 台は主電源、もう 1 台はバックアップとして動作します。対応する AC 電源スロットは、次の画像に示すようにアプライアンスの背面にあります。

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。

   - 管理ポート: アプライアンスを管理ネットワークに接続するハードウェアポートです。

     注意

     初期設定の管理ポートは eth0 です。カスタムポート上に管理ポートを設定することもできます。

     詳細については、54 ページの「管理ポートを設定する」を参照してください。

   - カスタムポート: サンドボックス分析専用の隔離されたネットワークにアプライアンスを接続するハードウェアポートです。

     注意

     カスタムポートは eth1、eth2、または eth3 のいずれか 1 ポートのみ利用可能です。

     高可用性を使用する場合、eth3 は、2 つの同一のアプライアンスを直接接続するために使用します。サンドボックス分析には使用できません。

     2 つの Deep Discovery Analyzer アプライアンスは必ず eth3 で接続されている必要があります。高可用性を使用しない場合は、eth1、eth2、および eth3 のいずれかがサンドボックス分析に使用できます。

6. (オプション) ファイバネットワークインタフェースカード (NIC) を、空いているフルハイト、フルレングスの拡張スロットに取り付け、ファイバネットワークケーブルを接続します。

注意

- Deep Discovery Analyzer アプライアンスではホットスワップはサポートされていません。NIC を取り付ける前に、アプライアンスの電源を切ってください。

  Deep Discovery Analyzer には最大 2 つの NIC を追加で取り付けられます。

- Deep Discovery Analyzer では最大 4 つのネットワークポートが追加でサポートされます。

- NIC をアプライアンスのスロット番号の順番に従って取り付けます。取り付けた NIC を別の NIC と入れ替えることはできません。

  たとえば、NIC1 がスロット 1 に、また NIC2 がスロット 2 に挿入されている場合、NIC1 をスロット 2 に入れ替え、NIC2 をスロット 1 に入れ替えることはできません。ただし、NIC1 をスロット 2 に入れ替え、NIC2 をスロット 3 に入れ替えることはできます。

7. アプライアンスの電源を入れます。

注意

電源ボタンは、アプライアンスのフロントパネルのベゼルの裏側にあります。

Deep Discovery Analyzer をインストールする

手順

1. アプライアンスの電源を入れます。

注意

電源ボタンは、アプライアンスのフロントパネルのベゼルの裏側にあります。

POST (power-on self-test) 画面が表示されます。

2. Deep Discovery Analyzer のインストールパッケージ DVD を挿入します。
3. アプライアンスを再起動します。

   POST 画面が表示されます。
4. [Deep Discovery Analyzer Appliance Installation] 画面が表示されます。
5. [1. Install Appliance] を選択し、<Enter> キーを押します。

   - シリアルポート経由で Deep Discovery Analyzer をインストールしている場合は、[2. Install Appliance via Serial Port] を選択し、<Enter> キーを押します。

   [使用許諾契約] が表示されます。
6. 同意できる場合は、[同意する] をクリックします。

   ディスクの選択画面が表示されます。
7. Deep Discovery Analyzer ソフトウェアをインストールするディスクを選択します。
8. [続行] をクリックします。

   プログラムにより、ハードウェアの最小要件に適合するかどうかが確認され、[ハードウェアプロファイル] 画面が表示されます。
9. [続行] をクリックします。

   警告!

   インストールにはディスクの再パーティション設定が含まれます。ディスク上のすべてのデータが失われます。

   確認メッセージが表示されます。
10. [続行] をクリックします。

    インストールプログラムによりディスクが再パーティションされ、インストール用に環境が準備されます。完了後、アプライアンスが再起動され、Deep Discovery Analyzer ソフトウェアがインストールされます。

事前設定コンソールでアプライアンスの IP アドレスを設定して、配置プロセスを完了します。詳細については、51 ページの「事前設定コンソールでネットワークアドレスを設定する」を参照してください。

注意

リモートによるシステム管理とトラブルシューティングを可能にするため、アプライアンスで iDRAC (Integrated Dell Remote Access Controller) を設定することをお勧めします。

第 4 章

事前設定コンソールの使用

この章では、Deep Discovery Analyzer の事前設定コンソールの使用方法について説明します。

事前設定コンソール

事前設定コンソールは、次の操作を実行できる Bash ベースの (UNIX シェル) インタフェースです。

- ネットワーク設定
- 高可用性の詳細の表示
- Ping を使用したリモートホストへの接続テスト
- デバッグログの収集とアップロード
- admin アカウントのリセットおよび事前設定コンソールのパスワードの変更
- 管理ポートの設定
- アプライアンスの再起動またはシャットダウン

次の表では、事前設定コンソールで実行できるタスクについて説明します。

タスク	手順
ログオン	有効なログオンアカウント情報を入力します。初期設定のアカウント情報は次のとおりです。 • ユーザ名: `admin` • パスワード: `Admin1234!`
アプライアンスのネットワークアドレスの設定 [Configuring appliance IP address]	アプライアンスの IP アドレス、サブネットマスク、ゲートウェイ、および DNS を指定します。詳細については、51 ページの「事前設定コンソールでネットワークアドレスを設定する」を参照してください。

タスク	手順
高可用性の詳細の表示 [View high availability details]	アクティブおよびパッシブなアプライアンスのホスト名、IP アドレス、および同期ステータスを表示します。 **注意** 高可用性は事前設定コンソールでは設定できません。高可用性を設定するには管理コンソールを使用します。詳細については、「Deep Discovery Analyzer 管理者ガイド」の [高可用性] タブと [クラスタ] タブに関するトピックを参照してください。
リモートホストへの Ping [Ping remote host]	有効な IP アドレスまたは FQDN を入力して、[Ping] をクリックします。
事前設定コンソールのパスワードの変更および admin アカウントのリセット	パスワードを変更して admin アカウントを (ロック解除の状態および管理者の役割に) リセットするには、現在のパスワードを入力し、新しいパスワードを 2 回入力してから、[Save] を選択します。
SSH 接続の有効化と無効化	SSH 接続を有効または無効にします。
デバッグログの収集とアップロード	デバッグログを Deep Discovery Analyzer から収集し、SFTP サーバにアップロードします。
管理ポートの設定	管理ポートとして使用するインタフェースを選択します。 詳細については、54 ページの「管理ポートを設定する」を参照してください。
再起動	[Main Menu] で [Restart] を選択し、<Enter> キーを押します。 次の画面で [OK] を選択し、<Enter> キーを押します。
電源オフ	[Main Menu] で [Power off] を選択し、<Enter> キーを押します。 次の画面で [OK] を選択し、<Enter> キーを押します。

タスク	手順
ログオフ	[Main Menu] で [Log off] を選択し、<Enter> キーを押します。 次の画面で [OK] を選択し、<Enter> キーを押します。

事前設定コンソールの基本操作

事前設定コンソールの基本操作を実行するには、次に示すキーボードのキーを使用します。

重要

スクロールロックを無効にして (キーボードの <Scr Lk> キーを使用)、次の操作を実行します。

キーボードのキー	操作
上矢印と下矢印 	フィールド間を移動します。
	番号付きリスト内の項目間を移動します。 **注意** 項目番号を入力して、特定の項目に移動することもできます。
	テキストボックス間を移動します。
左矢印と右矢印 	ボタン間を移動します。ボタンは山カッコ <> で囲まれています。
	テキストボックス内の文字間を移動します。
<Enter> キー 	選択された項目またはボタンをクリックします。

キーボードのキー	操作
<Tab> キー  	画面のセクション間を移動します。1 つのセクションでは、矢印キー (上、下、左、および右キー) を組み合わせて使用する必要があります。

事前設定コンソールでネットワークアドレスを設定する

手順

1. 有効なログオンアカウント情報を入力します。初期設定のアカウント情報は次のとおりです。

   - ユーザ名: `admin`
   - パスワード: `Admin1234!`

   > **注意**
   >
   > 入力した文字は画面に表示されません。
   >
   > このパスワードは、Web ベースの管理コンソールへのログオンに使用されるパスワードと同じです。詳細については、35 ページの「ログオンアカウント情報」を参照してください。

   [Main Menu] 画面が表示されます。

2. [Configure appliance IP address] を選択し、<Enter> キーを押します。

   [Appliance IP Settings] 画面が表示されます。

3. 次の必要な設定を指定します。

項目	ガイドライン
IPv4 アドレス [IPv4 address]	• 仮想 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。 • 次のアドレスと競合しないように設定します。

項目	ガイドライン
	• サンドボックスネットワーク: [仮想アナライザ] > [サンドボックス管理] > [ネットワーク接続] で設定したアドレス • 仮想 IP アドレス: [管理] > [システム設定] > [高可用性] で設定 • 仮想アナライザ: `1.1.0.0/27`、`1.1.2.0/24`、`192.0.2.0/24`、`198.18.0.0/15`、`198.51.100.0/24`、および `203.0.113.0/24` • ブロードキャスト: `255.255.255.255` • マルチキャスト: `224.0.0.0 - 239.255.255.255` • リンクローカル: `169.254.1.0 - 169.254.254.255` • クラス E: `240.0.0.0 - 255.255.255.255` • ローカルホスト: `127.0.0.1/8` **注意** IP アドレスを変更すると管理コンソール URL も変わります。
サブネットマスク [Subnet mask]	サブネットマスクの一般的な形式を使用する必要があります。
IPv4 ゲートウェイ [IPv4 gateway]	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 [IPv4 DNS server 1]	DNS サーバの IP を指定します。
IPv4 DNS サーバ 2 (オプション) [IPv4 DNS server 2]	DNS サーバの IP を指定します。

4. (オプション) IPv6 の設定を行います。
5. <Save> をクリックします。

   設定が正常に保存されると、[Main Menu] 画面が表示されます。

事前設定コンソールで高可用性の詳細を表示する

始める前に

ログオンするアプライアンスに応じて [High Availability] 画面の表示は異なります。

[High Availability] 画面を使用して、高可用性の設定の詳細を表示できます。

注意

パッシブなプライマリアプライアンスでは、この画面を使用してクラスタからアプライアンスをデタッチできます。

手順

1. 有効なログオンアカウント情報を入力します。初期設定のアカウント情報は次のとおりです。

   - ユーザ名: `admin`
   - パスワード: `Admin1234!`

   

   注意

   入力した文字は画面に表示されません。

   このパスワードは、Web ベースの管理コンソールへのログオンに使用されるパスワードと同じです。詳細については、35 ページの「ログオンアカウント情報」を参照してください。

   [Main Menu] 画面が表示されます。

2. [View high availability details] を選択して <Enter> キーを押します。

   [High Availability] 画面が表示されます。

   次の表に、画面上のラベルと高可用性の設定の詳細を示します。

表 4-1. [High Availability] 画面

ラベル	詳細
モード [Mode]	アプライアンスのクラスタモード
ステータス [Status]	パッシブなプライマリアプライアンスの同期ステータス
ホスト名 [Host name]	アプライアンスのホスト名
管理 IP アドレス [Management IP address]	アプライアンスの管理 IP アドレス
IPv4 仮想アドレス [IPv4 virtual address]	アクティブなプライマリアプライアンスの IPv4 仮想アドレス
IPv6 仮想アドレス [IPv6 virtual address]	アクティブなプライマリアプライアンスの IPv6 仮想アドレス

3. (オプション) パッシブなプライマリアプライアンスでは、<Tab> キーで [Detach] に移動して <Enter> キーを押すと、パッシブなプライマリアプライアンスがデタッチされます。

   注意

   パッシブなプライマリアプライアンスをデタッチすると、高可用性が無効になります。

4. <Tab> キーを押して [Back] に移動し、<Enter> キーを押します。

   [Main Menu] 画面が表示されます。

管理ポートを設定する

事前設定コンソールを使用して、選択したインタフェースで管理ポートを設定できます。

手順

1. 有効なログオンアカウント情報を入力します。初期設定のアカウント情報は次のとおりです。

   - ユーザ名: `admin`
   - パスワード: `Admin1234!`

   注意

   入力した文字は画面に表示されません。

   このパスワードは、Web ベースの管理コンソールへのログオンに使用されるパスワードと同じです。詳細については、35 ページの「ログオンアカウント情報」を参照してください。

   [Main Menu] 画面が表示されます。

2. [Configure management port] を選択し、<Enter> キーを押します。

   [Configure Management Port] 画面が表示されます。

3. <Tab> キーを押して、管理ポートとして使用するインタフェースに移動し、<Enter> キーを押します。

   注意

   - ポートリストには初期設定の管理ポート eth0 が含まれます。
   - eth0 が NIC チームのメンバーである場合に、eth0 を管理ポートとして選択すると、その NIC チームは自動的に無効になります。

4. <Tab> キーを押して <Save> に移動し、<Enter> キーを押します。

   設定が正常に保存されると、[Main Menu] 画面が表示されます。

第 5 章

Deep Discovery Analyzer のアップグレード

この章では、旧バージョンの Deep Discovery Analyzer からファームウェアをアップグレードする方法について説明します。

アプライアンスのファームウェアをアップグレードする

トレンドマイクロでは、報告された既知の問題に対する新しいファームウェアバージョン、または製品に適用するアップグレードを不定期にリリースしています。使用可能なファームウェアバージョンについては、https://appweb.trendmicro.com/ecs/Default.aspx を参照してください。

Deep Discovery Analyzer 7.1 では、次のバージョンからデータと設定を直接移行できます。

- Deep Discovery Analyzer 7.0
- Deep Discovery Analyzer 6.9

注意

ハードウェアモデル 1100 および 1200 にファームウェアのアップデートを適用すると、Deep Discovery Analyzer によって、Deep Discovery Analyzer 6.9 または 7.0 の設定が自動的に 7.1 に移行されます。

Deep Discovery Analyzer でファームウェアをアップグレードするには、次のいずれかの方法を使用します。

- Deep Discovery Analyzer 管理コンソール
- Deep Discovery Director からの計画配信。詳細については、Deep Discovery Director のドキュメントを参照してください。

重要

複数の Deep Discovery Analyzer アプライアンスを配置および設定してクラスタを形成している場合は、移行タスクについて 60 ページの「クラスタ内のアプライアンスのファームウェアをアップグレードする」を参照してください。

注意

続行する前に、すべての管理コンソールタスクを完了していることを確認してください。アップグレードプロセスには時間がかかることがあります。

手順

1. ファームウェアイメージを入手します。
2. 管理コンソールのログオンページで [セッションタイムアウトの延長を有効にする] を選択し、有効なユーザ名とパスワードを使用してログオンします。
3. 設定をバックアップします。次の操作を実行します。
   a. [管理] > [システムメンテナンス] の順に選択し、[バックアップ] タブをクリックします。
   b. [エクスポート] をクリックします。
4. [管理] > [アップデート] に移動して、[ファームウェア] タブをクリックします。
5. [アップデートファイル] 横のボックスまたは [参照] をクリックして、ファームウェアのアップグレードファイルを選択します。
6. [インストール] をクリックします。

   画面にファームウェアのアップグレードステータスが表示されます。

   重要

   アップグレードが完了するまで、ブラウザを閉じたり、表示を更新したり、別のページに移動したり、管理コンソールでタスクを実行したり、アプライアンスの電源をオフにしたりしないでください。

   ファームウェアのアップグレードが完了すると、Deep Discovery Analyzer が自動的に再起動します。
7. ブラウザのキャッシュをクリアしてから、管理コンソールにアクセスします。

クラスタ内のアプライアンスのファームウェアをアップグレードする

複数の Deep Discovery Analyzer アプライアンスを配置および設定してクラスタを形成している場合は、クラスタの設定手順に従って Deep Discovery Analyzer アプライアンスをアップグレードします。

表 5-1. クラスタ内のアプライアンスのファームウェアのアップグレード手順

クラスタ設定	タスク
高可用性クラスタ	1. パッシブなプライマリアプライアンスをデタッチします。 2. アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスの両方を個々にアップグレードします。 詳細については、58 ページの「アプライアンスのファームウェアをアップグレードする」を参照してください。 3. パッシブなプライマリアプライアンスをクラスタに再度追加します。
負荷分散クラスタ	すべての Deep Discovery Analyzer アプライアンスを個々にアップグレードします。
負荷分散機能を備えた高可用性クラスタ	1. パッシブなプライマリアプライアンスをデタッチします。 2. アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスの両方を個々にアップグレードします。 詳細については、58 ページの「アプライアンスのファームウェアをアップグレードする」を参照してください。 3. パッシブなプライマリアプライアンスをクラスタに再度追加します。 4. すべてのセカンダリアプライアンスを個々にアップグレードします。 詳細については、58 ページの「アプライアンスのファームウェアをアップグレードする」を参照してください。

第 6 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/ 駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 A

付録

ここで説明する内容には、次の項目が含まれます。

管理コンソール

Deep Discovery Analyzer には管理コンソールが組み込まれており、これを使用して製品を設定し、管理できます。

次のいずれかの Web ブラウザを使用して、管理ネットワーク上の任意のコンピュータから管理コンソールを開きます。

- Microsoft Internet Explorer 11
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

注意

Web ブラウザの JavaScript が有効になっていることを確認してください。

ログオンするには、ブラウザ画面を開き、次の URL を入力します。

`https://<アプライアンスの IP アドレス>/pages/login.php`

Deep Discovery Analyzer の管理コンソールには、次のいずれかの方法でログオンできます。

- 68 ページの「ローカルアカウントを使用したログオン」
- 74 ページの「シングルサインオンによるログオン」

ローカルアカウントを使用したログオン

手順

1. [ログオン] 画面で、管理コンソールのログオンアカウント情報 (ユーザ名とパスワード) を入力します。

   初めてログオンする場合は、次の初期設定の管理者ログオンアカウント情報を使用します。

- ユーザ名: `admin`
- パスワード: `Admin1234!`

注意

お使いのアカウントに応じて、[ユーザ名] フィールドに次のいずれかの情報を入力します。

- ユーザ名
- ユーザプリンシパル名 (UPN)
- メールアドレス

2. (オプション) [セッションタイムアウトの延長を有効にする] を選択し、ログオンセッションのセッションタイムアウトを延長します。初期設定のセッションタイムアウトは 10 分です。

   セッションタイムアウトの設定を変更するには、[管理] > [システム設定] の順に選択し、[セッションタイムアウト] タブをクリックします。

3. [ログオン] をクリックします。
4. 初めてログオンする場合は、アカウントのパスワードを変更した後、管理コンソールにアクセスできるようになります。

[アカウント] タブ

[アカウント] タブは、ユーザアカウントの作成および管理に使用します。

注意

- クラスタ環境では、セカンダリ Deep Discovery Analyzer アプライアンスは、初期設定の管理者アカウント (admin) を除くすべてのローカルユーザアカウントをアクティブなプライマリアプライアンスから同期します。
- 同期したアカウントでセカンダリアプライアンスの管理コンソールにログインすると、アカウントのパスワードを変更するように求められます。

手順

1. [管理] > [アカウント/連絡先] の順に選択します。
2. [アカウント] タブをクリックします。
3. 次のオプションを使用してユーザアカウントを管理します。
   - 新しいユーザアカウントを追加するには、[追加] をクリックします。

     [アカウントの追加] 画面が開きます。詳細については、71 ページの「ユーザアカウントを設定する」を参照してください。
   - アカウントを削除するには、1 つ以上のユーザアカウントを選択して [削除] をクリックします。

     重要
     - Deep Discovery Analyzer の初期設定の管理者アカウントは削除できません。
     - ログオンしているアカウントは削除できません。
   - アカウントを手動でロック解除するには、アカウントを選択して [ロック解除] をクリックします。

     Deep Discovery Analyzer には、ユーザが 5 回連続して誤ったパスワードを入力した場合にアカウントをロックするセキュリティ機能があります。この機能は無効にできません。ロックされたアカウントは 10 分後に自動的にロック解除されます。管理者はロックされたアカウントを手動でロック解除できます。

     一度にロック解除できるユーザアカウントは 1 つのみです。
4. 既存のアカウントを変更するには、アカウントのユーザ名をクリックします。

   [アカウントの編集] 画面が開きます。詳細については、71 ページの「ユーザアカウントを設定する」を参照してください。
5. 表内のエントリが多い場合は、次のオプションを使用してユーザアカウントリストを管理します。

- 特定の種類のアカウントのみを表示するには、[種類] ドロップダウンからアカウントの種類を選択します。
- 名前をアルファベット順に並べ替えるには、[名前] 列をクリックします。
- エントリを絞り込むには、[検索] テキストボックスにいくつかの文字を入力します。入力すると、入力した文字に一致するエントリが表示されます。Deep Discovery Analyzer は、現在のページのすべてのセルを対象に一致を検索します。
- 画面の最下部にあるパネルには、ユーザアカウントの合計数が表示されます。すべてのユーザアカウントを同時に表示できない場合は、ページ区切りコントロールを使用して、ビューに表示されていないアカウントを表示します。

ユーザアカウントを設定する

手順

1. [管理] > [アカウント/連絡先] の順に選択して、[アカウント] タブに移動します。
2. 次のいずれかを実行します。
   - [追加] をクリックして、新しいユーザアカウントを作成します。
   - 既存のユーザアカウント名をクリックして、その設定を変更します。
3. ローカルアカウントを追加するには、アカウントの [種類] に [ローカルユーザ] を選択し、次の情報を入力します。
   - 名前:アカウント所有者の名前。
   - ユーザ名:最大 40 文字まで入力できます。

   注意

   新規アカウントの作成と管理コンソールのログオンプロセスでは、ユーザ名の大文字と小文字は区別されません。

- パスワード:パスワードは 8 文字以上で、アルファベットの大文字と小文字、数字、および特殊文字を組み合わせて入力してください。

  注意

  - より複雑なパスワード要件を設定するには、[管理] > [システム設定] > [パスワードポリシー] タブでグローバルパスワードポリシーを設定します。パスワードポリシーが画面に表示され、ユーザアカウントを追加するにはこのポリシーの条件を満たす必要があります。
  - ユーザのパスワード入力時に入力の誤りが許容される再試行数を超えた場合、Deep Discovery Analyzer はそのユーザアカウントを無効に設定します (ロック)。このようなアカウントは [アカウント] 画面でロック解除できます。

- パスワードの確認入力:パスワードを再度入力します。
- (オプション) 説明:最大 40 文字まで入力できます。

注意

新しいローカルユーザアカウントで管理コンソールに初めてログインすると、アカウントのパスワードを変更するように求められます。

4. Active Directory ユーザを追加するには、アカウントの [種類] に [Active Directory ユーザ] を選択し、次の情報を入力します。
   - ユーザの名前またはグループ:ユーザプリンシパル名 (UPN) またはユーザグループ名を指定します。

     注意

     特定のユーザ名またはグループを簡単に見つけるには、テキストボックスにいくつかの文字を入力し、[検索] をクリックします。

   - (オプション) 説明:最大 40 文字まで入力できます。
5. ローカルアカウントのパスワードを変更するには、[パスワードの変更] を選択し、必要なフィールドを設定します。

注意

- 管理者としてログインしている場合は、新しいパスワードを 2 回入力することでローカルユーザアカウントのパスワードを変更できます。ローカルユーザアカウントの元のパスワードを入力する必要はありません。
- ローカルユーザアカウントのパスワードが管理者により変更された場合、ユーザはログイン時に再度アカウントのパスワードを変更するように求められます。

6. このユーザアカウントの役割と関連付けられた権限を選択します。
   - 管理者: 送信されたオブジェクト、分析結果、および製品設定にフルアクセスできます。
   - 調査者: 送信されたオブジェクトの再分析、オブジェクトの送信、および調査パッケージ (送信されたオブジェクトを含む) のダウンロードを実行でき、分析結果と製品設定に読み取り専用でアクセスできます。
   - オペレータ: 送信されたオブジェクト、分析結果、および製品設定に読み取り専用でアクセスできます。
7. (オプション) [連絡先に追加] を選択してユーザアカウントを [連絡先] リストに追加し、次の情報を入力します。

注意

連絡先は初期設定でメールアラート通知を受信します。

   - メールアドレス
   - (オプション) 電話番号
8. [保存] をクリックします。

シングルサインオンによるログオン

Deep Discovery Analyzer で SAML 統合に必要な設定を行うことで、既存の ID プロバイダの認証情報を使用して Deep Discovery Analyzer の管理コンソールにアクセスできます。

詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

手順

1. [ログオン] 画面で、ドロップダウンリストからサービス名を選択します。
2. [シングルサインオン (SSO)] をクリックします。

   組織のログオンページが自動的に表示されます。
3. 画面の指示に従ってアカウントの認証情報を入力し、Deep Discovery Analyzer の管理コンソールにアクセスします。

導入タスク

手順

1. 有効なアクティベーションコードを使用して、製品ライセンスをアクティベートします。詳細については、75 ページの「ライセンス」を参照してください。
2. Deep Discovery Analyzer のホスト名と IP アドレスを指定します。詳細については、77 ページの「[ネットワーク] タブ」を参照してください。
3. Deep Discovery Analyzer がプロキシサーバ経由で管理ネットワークに接続する場合は、プロキシ設定を行います。詳細については、79 ページの「[プロキシ] タブ」を参照してください。
4. 日付と時刻を設定して、Deep Discovery Analyzer の機能が予定どおりに動作するようにします。詳細については、80 ページの「[時間] タブ」を参照してください。

5. SMTP を設定して、メールで通知を送信できるようにします。詳細については、81 ページの「[SMTP] タブ」を参照してください。

6. サンドボックスインスタンスを仮想アナライザにインポートします。詳細については、83 ページの「[イメージ] タブ」を参照してください。

7. 仮想アナライザのネットワーク設定を実行して、サンドボックスインスタンスが外部接続先に接続できるようにします。詳細については、86 ページの「外部接続を有効にする」を参照してください。

8. (オプション) 高可用性または負荷分散クラスタで使用する追加の Deep Discovery Analyzer アプライアンスを配置および設定します。詳細については、88 ページの「[クラスタ] タブ」を参照してください。

9. Deep Discovery Analyzer と統合するために、サポートされているトレンドマイクロ製品を設定します。

   詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

10. オブジェクトを送信するすべての送信元に重みとタイムアウト値を設定する事で、送信元間で使用する仮想アナライザのリソースの割り当てを調整します。

    詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

ライセンス

[管理] > [ライセンス] 画面にて、Deep Discovery Analyzer のサポート契約情報の表示、アクティベート、およびサポート契約の更新を行います。

Deep Discovery Analyzer のサポート契約では、購入日から 1 年間、製品アップデート (トレンドマイクロのアップデートを含む) および基本的なテクニカルサポートを受けることができます。このライセンスによって分析のための脅威サンプルのアップロード、および仮想アナライザからの Trend Micro Threat Connect へのアクセスも実行できます。さらに、分析のために、トレンドマイクロのクラウドサンドボックスにサンプルを送信することもできます。

最初の 1 年が終了すると、サポート契約は年ベースで更新する必要があり、その際はトレンドマイクロの最新の料金が適用されます。

サポート契約は、お客さまの組織とトレンドマイクロの間の契約です。この契約では、適用される料金の支払いと引き換えにお客さまがテクニカルサポートおよび製品のアップデートを受ける権利が規定されます。トレンドマイクロ製品の購入時に、製品とともにお客さまに渡される使用許諾契約にその製品のサポート契約の条件が記載されています。

サポート契約には有効期限があります。ソフトウェアの使用権にはありません。サポート契約の有効期限が満了すると、トレンドマイクロからテクニカルサポートを受ける権利、および Trend Micro Threat Connect にアクセスする権利が無効になります。

通常、サポート契約の有効期限の 90 日前に、お客さまに契約の中止が保留中であることを警告するメール通知の送信が開始されます。サポート契約は、販売店、トレンドマイクロの営業担当、または次のトレンドマイクロのサポート契約ポータルからメンテナンスの更新料をお支払いいただくことでアップデートできます。

https://olr.trendmicro.com/registration/jp/ja/login.aspx

[ライセンス] 画面には、次の情報およびオプションが含まれます。

表 A-1. 製品詳細

フィールド	詳細
製品名	製品の名前が表示されます。
ファームウェアのバージョン	製品の完全なビルド番号が表示されます。
使用許諾契約	[トレンドマイクロ使用許諾契約] へのリンクが表示されます。リンクをクリックすると、使用許諾契約を表示または印刷できます。

表 A-2. ライセンスの詳細

フィールド	詳細
アクティベーションコード	ここにアクティベーションコードが表示されます。サポート契約の有効期限が満了した場合は、トレンドマイクロから新しいアクティベーションコードを入手してください。サポート契約を更新するには、[新しいアクティベーションコード] をクリックして、新しいアクティベーションコードを入力します。 [ライセンス] 画面が再表示され、サポート契約の有効期限までの残余日数が表示されます。
ステータス	[アクティベート済み]、[アクティベーション未完了]、[猶予期間]、[有効期限切れ]、または [体験版の有効期限終了] のいずれかが表示されます。 トレンドマイクロの Web サイトでライセンス情報の詳細を表示するには、[詳細情報をオンラインで確認] をクリックします。たとえばサポート契約の更新後など、ステータスの変更後に正しいステータスが画面に表示されない場合は、[更新] をクリックしてください。
種類	• 製品版: すべての製品機能へのアクセスを提供します • 体験版: すべての製品機能へのアクセスを提供します
有効期限	サポート契約の有効期限が表示されます。サポートサービスの継続をご希望される場合は、有効期限の満了前にサポート契約を更新してください。

[ネットワーク] タブ

この画面を使用して、Deep Discovery Analyzer アプライアンスのホスト名、IPv4 アドレス、および IPv6 アドレスと、TLS 1.2 の適用を含めたその他のネットワーク設定を行います。

IPv4 アドレスは必須で、初期設定は `192.168.252.2` です。IPv4 アドレスは、すべての配置タスクを完了した後すぐに変更してください。

Deep Discovery Analyzer は、Trend Micro Smart Protection Network、アップデートサーバ、Threat Connect などのトレンドマイクロがホストするサービスにアクセスするときには、指定された IP アドレスを使用してインターネッ

トに接続します。IP アドレスによって、管理コンソールにアクセスするための URL も決まります。

[常に TLS 1.2 を使用する] を選択すると、Deep Discovery Analyzer での受信および送信接続のデータセキュリティを強化できます。

注意

Payment Card Industry Data Security Standard (PCI-DSS) v3.2 に準拠するには、アプライアンスはすべての受信および送信接続に TLS 1.2 のみを使用する必要があります。

統合製品およびサービスが TLS 1.2 をサポートする最新バージョンを使用していることを確認してください。詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

次の製品/サービスが TLS 1.2 を使用するように設定されていることを確認します。

- [管理] > [アップデート] > [コンポーネントのアップデート設定] のアップデートサーバは、HTTPS を使用する必要があります。
- [管理] > [統合製品/サービス] > [ICAP] の ICAP 設定は、SSL 経由の ICAP を使用する必要があります。
- [管理] > [統合製品/サービス] > [Syslog] の Syslog サーバは、SSL を使用する必要があります。

  [管理] > [統合製品/サービス] > [メールでの送信] のメールでの送信設定は、SSL/TLS または STARTTLS を使用する必要があります。
- [管理] > [システム設定] > [SMTP] の SMTP サーバは、SSL/TLS または STARTTLS を使用する必要があります。

次の表は、設定の制限を示しています。

表 A-3. 設定の制限

フィールド	制限事項
ホスト名	高可用性を使用している場合は変更できません。

フィールド	制限事項
IPv4 アドレス	• IPv4 仮想アドレスとは異なる必要があります。 • IPv4 仮想アドレスと同じネットワークセグメント内に存在している必要があります。
IPv6 アドレス	• IPv6 仮想アドレスとは異なる必要があります。 • IPv6 仮想アドレスと同じネットワークセグメント内に存在している必要があります。 • IPv6 仮想アドレスが設定されている場合は削除できません。 • 高可用性を使用している場合は追加または削除できません。

[プロキシ] タブ

Deep Discovery Analyzer がプロキシサーバ経由でインターネットまたは管理ネットワークに接続する場合は、プロキシ設定を行います。

次の設定を行います。

表 A-4. [プロキシ] タブのタスク

タスク	手順
HTTP プロキシサーバを使用する	プロキシ設定を有効化するにはこのオプションを選択します。
サーバ名または IP アドレス	プロキシサーバのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。 管理コンソールでは、ホスト名にダブルバイトでエンコードされた文字は使用できません。ホスト名にこのような文字が含まれる場合は、代わりに IP アドレスを入力してください。
ポート番号	Deep Discovery Analyzer がプロキシサーバの接続に使用するポート番号を入力します。

タスク	手順
プロキシサーバへの接続に認証を使用	プロキシサーバの接続に認証が必要な場合は、このオプションを選択します。Deep Discovery Analyzer では次の認証方法がサポートされます。 • 認証なし • 基本認証 • ダイジェスト認証 • NTLMv1 認証
ユーザ名	認証に使用するユーザ名を入力します。 **注意** このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。
パスワード	認証に使用するパスワードを入力します。 **注意** このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。

[時間] タブ

インストール後すぐに日付と時間を設定します。

手順

1. [管理] > [システム設定] の順に選択し、[時間] タブをクリックします。

   [時間] 画面が表示されます。

2. [日時の設定] をクリックします。

   設定パネルが表示されます。

3. 次の方式のいずれかを選択して、適切な設定を行います。

- [NTP サーバに接続] を選択し、NTP サーバのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。
- [手動で設定] を選択し、時間を設定します。

4. [保存] をクリックします。
5. [タイムゾーンの設定] をクリックします。

   設定パネルが表示されます。
6. 適切なタイムゾーンを選択します。

   注意

   適用可能な場合は、夏時間 (DST) が使用されます。
7. [保存] をクリックします。
8. [形式の設定] をクリックします。

   設定パネルが表示されます。
9. 希望の日時の形式を選択します。
10. [保存] をクリックします。

[SMTP] タブ

Deep Discovery Analyzer では、メールで通知を送信するときに SMTP 設定を使用します。

手順

1. [管理] > [システム設定] の順に選択し、[SMTP] タブをクリックします。
2. 次の情報を指定します。

表 A-5. [SMTP] タブのタスク

フィールド	手順
サーバアドレス	SMTP サーバのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。 管理コンソールでは、ホスト名にダブルバイトでエンコードされた文字は使用できません。ホスト名にこのような文字が含まれる場合は、代わりに IP アドレスを入力してください。
ポート番号	SMTP サーバで使用するポート番号を入力します。
接続のセキュリティ	接続に使用するセキュリティの種類を指定します。 指定できる値は「なし」、「STARTTLS」、または「SSL/TLS」です。
送信者のメールアドレス	送信者のメールアドレスを入力します。
SMTP サーバの接続に認証を使用	サーバで認証が必要な場合は、[SMTP サーバの接続に認証を使用] を選択してユーザ名とパスワードを指定します。 警告! SMTP サーバ上の有効なユーザ名とパスワードを指定してください。ユーザ名とパスワードが正しくない場合、一部の SMTP サーバにおいて、Deep Discovery Analyzer サーバからの通信が拒否されることがあります。

3. (オプション) 外部 SMTP サーバへの接続をテストするには、次の手順を実行します。

   a. [接続テスト] をクリックします。

   b. 受信者のメールアドレスを入力します。

   c. [OK] をクリックします。

注意

Deep Discovery Analyzer から受信者にテストメールメッセージは送信されません。

4. [保存] をクリックします。

[イメージ] タブ

初期設定では、仮想アナライザにイメージは含まれていません。サンプルを分析するには、少なくとも 1 つのイメージを OVA (Open Virtual Appliance) 形式で準備してアップロードする必要があります。

既存の VirtualBox または VMware イメージを使用するか、VirtualBox を使用して新しいイメージを作成できます。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」 (https://appweb.trendmicro.com/ecs/default.aspx) の第 2 章と第 3 章を参照してください。

アップロードする前に、Virtual Analyzer Image Preparation Tool を使用してイメージを検証および設定します。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」の第 4 章を参照してください。

最大 3 つのイメージをインポートできます。ご使用の製品のハードウェア仕様に応じて、イメージごとに配信可能なインスタンス数が決まります。

[イメージ] 画面では次の情報を確認できます。

- イメージに設定されたインスタンス数
- 使用中のインスタンス数

次の表は、[イメージ] 画面で実行できるタスクを示しています。

タスク	説明
イメージのインポート	[インポート] をクリックして、新しい仮想アナライザイメージをアップロードします。 詳細については、84 ページの「イメージをインポートする」を参照してください。
イメージのエクスポート	イメージを選択して、[エクスポート] をクリックします。

タスク	説明
サンドボックスのインスタンス数の変更	イメージを選択して、[変更] をクリックします。 詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

イメージをインポートする

最大 4 つのイメージをアップロードできます (1 つの Linux イメージと 3 つの Windows イメージ)。ご使用の製品のハードウェア仕様に応じて、アップロード可能なイメージ数、およびイメージごとに配信可能なインスタンス数が決まります。

仮想アナライザは最大 30GB の OVA ファイルをサポートします。

重要

イメージが追加または削除された場合、またはインスタンスが変更された場合、仮想アナライザは分析を停止して、すべてのサンプルをキューに保持します。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[イメージ] タブをクリックします。

   [イメージ] 画面が表示されます。

2. [インポート] をクリックします。

   [イメージのインポート] 画面が表示されます。

3. [プラットフォーム] オプションを選択します。

4. イメージソースを選択して、適切な設定を行います。

   a. 最大 50 文字でイメージ名を入力します。このイメージ名は後から変更できません。

   b. イメージに割り当てるインスタンス数を選択します。

c. OVA ファイルの URL またはネットワーク共有パスを入力します。

d. (オプション) [プロキシサーバを使用して接続する] を選択します。

e. (オプション) 認証が必要な場合は、ログオンアカウント情報を入力します。

5. [インポート] をクリックします。

インポート処理を開始する前に、仮想アナライザで OVA ファイルが検証されます。

注意

- [HTTP/HTTPS または FTP サーバ] を選択すると、Deep Discovery Analyzer でイメージがダウンロードされてから、仮想アナライザにインポートされます。この処理は、ダウンロードが完了する前のみキャンセルできます。
- Deep Discovery Analyzer では、インポート元として HTTP/1.0 以降に準拠した HTTP サーバへの接続がサポートされます。

トレンドマイクロ仮想アナライザイメージアップロードツールを使用してイメージをアップロードする

仮想アナライザは 1～30GB までの OVA ファイルをサポートします。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[イメージ] タブをクリックします。
2. [インポート] をクリックします。
3. [プラットフォーム] オプションを選択します。
4. [送信元] で [イメージアップロードツール] を選択します。
5. [ダウンロード] をクリックし、イメージアップロードツールをダウンロードします。

6. ファイル `VirtualAnalyzerImageImportTool.exe` を開きます。
7. Deep Discovery Analyzer の IP アドレスを入力します。

   イメージのアップロード後、Deep Discovery Analyzer がただちにインスタンスを配信します。インスタンスの配信が完了するまで待ちます。

イメージのアップロードプロセスは、次の理由によって、停止するか失敗と見なされることがあります。

- 接続が確立されていないか、製品がビジー状態の可能性がある。
- アプライアンスへの接続が中断された
- 接続がタイムアウトした
- メモリの割り当てが失敗した
- Windows のソケット初期化が失敗した
- イメージファイルが壊れている
- イメージのアップロードが完了しなかった
- イメージのアップロードがキャンセルされた

外部接続を有効にする

仮想アナライザが設定されると、サンプル分析が一時停止して設定が無効になります。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[ネットワーク接続] タブをクリックします。

   [ネットワーク接続] 画面が表示されます。
2. [外部接続の有効化] を選択します。

   設定パネルが表示されます。

3. サンドボックスインスタンスで使用する接続の種類を選択します。
   - カスタム: 任意のユーザ定義ネットワークです。

     重要
     管理ネットワークから隔離された環境を使用することをお勧めします。

   - 管理ネットワーク: 初期設定の社内イントラネットです。

     警告!
     管理ネットワークへの接続を有効にすると、ネットワーク内で不正プログラムの蔓延やその他の不正な活動を引き起こす可能性があります。

4. [カスタム] を選択した場合は、次を設定します。
   - ネットワークアダプタ: 接続された状態のアダプタを選択します。
   - IP アドレス: IPv4 のアドレスを入力します。
   - サブネットマスク
   - ゲートウェイ
   - DNS
5. サンドボックスでネットワーク接続にプロキシサーバが必要な場合は、[専用のプロキシサーバを使用する] を選択して次を指定します。
   - サーバアドレス
   - ポート番号
   - ユーザ名: このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。
   - パスワード: このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。
6. [保存] をクリックします。

[クラスタ] タブ

複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。

ご使用環境の要件と使用可能な Deep Discovery Analyzer アプライアンスの数に応じて、次のクラスタ設定を使用できます。

表 A-6. クラスタ設定

クラスタ設定	説明
高可用性クラスタ	高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。
負荷分散クラスタ	負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。
負荷分散機能を備えた高可用性クラスタ	負荷分散機能を備えた高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスとして役割を引き継ぎます。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。

次の表は、使用可能な設定モードと関連付けられたアプライアンスの動作を示しています。

表 A-7. クラスタ設定モード

設定モード	説明
プライマリ (アクティブ)	• 管理コンソールに完全にアクセスできます。 • すべての設定を保持します。
プライマリ (パッシブ)	• 管理コンソールにアクセスできません。 • アクティブなプライマリアプライアンスの設定に基づいて自動的に設定されます。 • スタンバイ状態 • アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、アクティブなプライマリアプライアンスとして役割を引き継ぎます。 • 送信を処理しません。

設定モード	説明

セカンダリ	• アクティブなプライマリアプライアンスの設定に基づいて自動的に設定されます。
	• IP アドレスまたは仮想 IP アドレスを使用してアクティブなプライマリアプライアンスを特定します。
	• パフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。
	• 管理コンソールには設定可能な設定を含む画面のみが表示されます。アクセス可能な画面は次のとおりです。
	  • [仮想アナライザ] > [サンドボックス管理] > [ネットワーク接続]
	  • [仮想アナライザ] > [サンドボックス管理] > [macOS 向けサンドボックス]
	  • [管理] > [アップデート] > [HotFix/Patch]
	  • [管理] > [アップデート] > [ファームウェア]
	  • [管理] > [統合製品/サービス] > [SAML 認証]
	  • [管理] > [システム設定] > [ネットワーク]
	  • [管理] > [システム設定] > [ネットワークインタフェース]
	  • [管理] > [システム設定] > [HTTPS 証明書]
	  • [管理] > [システム設定] > [クラスタ]
	  • [管理] > [アカウント/連絡先] > [アカウント]
	  • [管理] > [システムログ]
	  • [管理] > [システムメンテナンス] > [ネットワークサービス診断]
	  • [管理] > [システムメンテナンス] > [電源オフ/再起動]
	  • [管理] > [システムメンテナンス] > [デバッグ]
	  • [管理] > [ライセンス]

[ノード] リスト

[ノード] リストはアクティブなプライマリアプライアンスに表示されます。

[ノード] リストには、次の情報が含まれます。

表 A-8. [ノード] リストの列

列	説明
ステータス	アプライアンスの接続ステータス。ステータスアイコンの上にマウスを重ねると詳細が表示されます。
モード	アプライアンスのクラスタモード。
管理 IP アドレス	アプライアンスの管理 IP アドレス。
ホスト名	アプライアンスのホスト名。
前回の接続	アプライアンスがアクティブなプライマリアプライアンスに最後に接続した日時。 注意 アプライアンスがパッシブなプライマリアプライアンスである場合、データはありません (ダッシュで表示)。

詳細	アプライアンスの動作ステータスの詳細情報。
	• スタンドアロンアプライアンスの場合:
	  • スタンドアロンアプライアンス: アプライアンスはスタンドアロンアプライアンスです。
	• パッシブなプライマリアプライアンスの場合:
	  • 完全同期: パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスと完全に同期されています。
	  • n%同期しています: パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスから設定を同期しています。
	  • 同期エラー: パッシブなプライマリアプライアンスからアクティブなプライマリアプライアンスに接続できません。アプライアンスが eth3 を使用して直接接続されており、eth3 がサンドボックス分析に使用されていないことを確認してください。

列	説明

	ヒント
	このフィールドには、接続の遅延とスループットの情報も表示されます。
	• セカンダリアプライアンスの場合:
	  • 一致しないコンポーネントバージョン: アクティブなプライマリアプライアンスとセカンダリアプライアンスの 1 つ以上のコンポーネントのバージョンが異なります。すべてのアプライアンスで同じコンポーネントのバージョンを使用してください。
	  • 接続なし: アクティブなプライマリアプライアンスが、過去 10 秒間にセカンダリアプライアンスから接続ステータスに関する情報を受信しませんでした。セカンダリアプライアンスの電源がオンになっており、アクティブなプライマリアプライアンスにネットワーク経由で接続できることを確認してください。
	  • 無効な API キー: セカンダリアプライアンスが無効な API キーで設定されています。セカンダリアプライアンスの [アクティブなプライマリ API キー] を確認してください。
	  • 互換性がないソフトウェアバージョン: アクティブなプライマリアプライアンスとセカンダリアプライアンスのファームウェア、HotFix、および Patch のバージョンが異なります。すべてのアプライアンスで同じファームウェア、HotFix、および Patch のバージョンを使用してください。
	  • 予期しないエラー: 予期しないエラーが発生しました。問題が解決しない場合は、テクニカルサポートにお問い合わせください。

処理	アプライアンスモードとステータスに応じて実行可能な処理。 • アクティブなプライマリアプライアンスの場合: • スワップ: プライマリアプライアンスの役割をスワップします。現在のパッシブなプライマリアプライアンスをプライマリモード (アクティブ) に設定し、現在のアクティブなプライマリアプライアンスをプライマリモード (パッシブ) に設定します。パッシブなプライマリアプライアンスがアクティブなプライマリアプライアンスからすべての設定を同期したときに表示されます。詳細につ

列	説明

	いては、96 ページの「アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスをスワップする」を参照してください。
	• パッシブなプライマリアプライアンスの場合:
	  • デタッチ: パッシブなプライマリアプライアンスをデタッチします。高可用性が無効になり、パッシブなプライマリアプライアンスがスタンドアロンアプライアンスとして使用可能になります。パッシブなプライマリアプライアンスがアクティブなプライマリアプライアンスからすべての設定を同期したときに表示されます。詳細については、96 ページの「クラスタからパッシブなプライマリアプライアンスをデタッチする」を参照してください。
	  • 削除: アクセスできないパッシブなプライマリアプライアンスを削除します。高可用性を無効にします。アクティブなプライマリアプライアンスが eth3 経由でパッシブなプライマリアプライアンスに接続できない場合に表示されます。詳細については、97 ページの「クラスタからパッシブなプライマリアプライアンスを削除する」を参照してください。
	• セカンダリアプライアンスの場合:
	  • 削除: アクセスできないセカンダリアプライアンスを削除します。オブジェクトの処理能力に影響します。セカンダリアプライアンスは 10 秒ごとにアクティブなプライマリアプライアンスへの接続を試行します。アクティブなプライマリアプライアンスがセカンダリアプライアンスから 1 分間接続ステータスに関する情報を受信しない場合に表示されます。詳細については、100 ページの「クラスタからセカンダリアプライアンスを削除する」を参照してください。

[更新] をクリックして、[ノード] リスト内の情報を更新します。

クラスタにパッシブなプライマリアプライアンスを追加する

次の表は、パッシブなプライマリアプライアンスをクラスタに追加する前に、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスの両方が満たす必要のある要件を示しています。

表 A-9. 高可用性クラスタリングの要件

要件	説明
ハードウェアモデル	ハードウェアモデル (1100 または 1200) が同じである必要があります。
物理的な接続	eth3 を使用して相互に直接接続することをお勧めします。
ファームウェア、HotFix、および Patch のバージョン	同じである必要があります。
ホスト名	異なる必要があります。
IP アドレス	対称的である必要があります。 • アクティブなプライマリアプライアンスで IPv4 アドレスのみが設定されている場合、パッシブなプライマリアプライアンスで IPv4 アドレスと IPv6 アドレスの両方を設定することはできません。 • アクティブなプライマリアプライアンスで IPv4 アドレスと IPv6 アドレスが設定されている場合、パッシブなプライマリアプライアンスで IPv4 アドレスのみを設定することはできません。
ネットワークセグメント	同じネットワークセグメント内に存在している必要があります。
仮想 IP アドレス	アクティブなプライマリアプライアンスで設定されている必要があります。

高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。

注意

- ネットワークに Trend Micro Apex Central が設定されている場合は、プライマリアプライアンス (高可用性クラスタの場合、仮想 IP アドレス) を Apex Central に登録してください。
- 高可用性を使用する場合は、仮想 IP アドレスを使用して登録してください。

手順

1. 41 ページのアプライアンスのインストールの説明に従って、インストールと配置のタスクを実行します。
2. パッシブなプライマリアプライアンスを設定します。
   a. パッシブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [プライマリモード (パッシブ)] を選択します。
   c. [アクティブなプライマリ IP アドレス] にアクティブなプライマリアプライアンスの IPv4 アドレスまたは IPv6 アドレスを入力します。
   d. [接続テスト] をクリックします。
   e. [保存] をクリックします。

      アプライアンスのスタンバイ画面にリダイレクトされます。

- パッシブなプライマリアプライアンスで実行していたオブジェクトの処理は停止されます。
- パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスからすべての設定を同期します。同期が完了するまでの時間はアプライアンスモデルによって異なります。

重要

アプライアンスの同期中は次のタスクを実行できません。

- アクティブなプライマリアプライアンスとしての役割の引き継ぎ
- 別のモードへの切り替え

- パッシブなプライマリアプライアンスの管理コンソールにアクセスすることはできません。アプライアンスの管理と同期ステータスの監視は、アクティブなプライマリアプライアンスの管理コンソールから実行してください。

アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスをスワップする

プライマリアドレスをスワップすると、現在のパッシブなプライマリアプライアンスがプライマリモード (アクティブ) に設定され、現在のアクティブなプライマリアプライアンスがプライマリモード (パッシブ) に設定されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. [スワップ] をクリックして、プライマリアプライアンスをスワップします。

クラスタからパッシブなプライマリアプライアンスをデタッチする

パッシブなプライマリアプライアンスをデタッチすると、高可用性が無効になり、アプライアンスをスタンドアロンアプライアンスとして使用できるようになります。パッシブなプライマリアプライアンスがデタッチされると、ノードリストに表示されなくなります。

製品をアップデートまたはアップグレードするには、パッシブなプライマリアプライアンスをデタッチします。

重要

パッシブなプライマリアプライアンスをデタッチしても、アプライアンスの設定はリセットされません。スタンドアロンアプライアンスとして使用する場合は、アプライアンスを再インストールすることをお勧めします。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. [デタッチ] をクリックして、クラスタからパッシブなプライマリアプライアンスをデタッチします。

クラスタからパッシブなプライマリアプライアンスを削除する

切断されたまたは異常な状態のパッシブなプライマリアプライアンスをクラスタから削除すると、ノードリスト内の混乱が緩和されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. ノードリストのパッシブなプライマリアプライアンスの横に [削除] が表示されるまで待機します。
3. [削除] をクリックして、クラスタからパッシブなプライマリアプライアンスを削除します。

注意

パッシブなプライマリアプライアンスは、アクティブなプライマリアプライアンスに再接続されると自動的にクラスタに再結合されます。

クラスタにセカンダリアプライアンスを追加する

セカンダリアプライアンスのファームウェア、HotFix、および Patch のバージョンがアクティブなプライマリアプライアンスと同じであることを確認します。

アプライアンスのファームウェア、HotFix、および Patch のバージョンを表示するには、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

必要に応じてアプライアンスのファームウェア、HotFix、および Patch のバージョンをアップデートまたはアップグレードします。詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

注意

- ネットワークに Trend Micro Apex Central が設定されている場合は、プライマリアプライアンス (高可用性クラスタの場合、仮想 IP アドレス) を Apex Central に登録してください。
- 高可用性を使用する場合は、仮想 IP アドレスを使用して登録してください。

手順

1. 41 ページのアプライアンスのインストールの説明に従って、インストールと配置のタスクを実行します。
2. セカンダリアプライアンスを設定します。
   a. セカンダリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [セカンダリモード] を選択します。
   c. [アクティブなプライマリ IP アドレス] にアクティブなプライマリアプライアンスの IPv4 アドレスまたは IPv6 アドレスを入力します。

      注意

      高可用性を使用している場合は、IPv4 仮想アドレスまたは IPv6 仮想アドレスを入力してください。

d. [アクティブなプライマリ API キー] にアクティブなプライマリアプライアンスの API キーを入力します。

e. [接続テスト] をクリックします。

ヒント

セカンダリアプライアンスでは、アクティブなプライマリアプライアンスへの接続をいつでもテストできます。接続の問題について詳細情報を確認するには、[接続テスト] をクリックします。

f. [保存] をクリックします。

3. (オプション) セカンダリアプライアンスで追加の設定を実行します。

a. サンドボックスのネットワーク接続を設定します。

詳細については、86 ページの「外部接続を有効にする」を参照してください。

注意

アクティブなプライマリアプライアンスの外部ネットワーク接続設定を使用することをお勧めします。

b. [macOS 向けサンドボックス] を設定します。

詳細については、「Deep Discovery Analyzer 管理者ガイド」を参照してください。

c. アプライアンスのネットワークを設定します。

詳細については、77 ページの「[ネットワーク] タブ」を参照してください。

d. アカウントを追加します。

詳細については、69 ページの「[アカウント] タブ」を参照してください。

注意

セカンダリアプライアンスは、アクティブなプライマリアプライアンスのサンドボックス割り当ての割合に基づいてサンドボックスインスタンスを自動的に配信します。次の表は、設定の例を示しています。

表 A-10. 2 つのイメージを使用した設定例

アプライアンスの種類	DEEP DISCOVERY ANALYZER ハードウェアモデル	インスタンスの最大数 (合計)	WINDOWS 7 インスタンスの数	WINDOWS 8.1 インスタンスの数
プライマリアプライアンス	1200 または 1100	60	40	20
セカンダリアプライアンス	1200 または 1100	60	40	20

クラスタからセカンダリアプライアンスを削除する

クラスタから切断されたセカンダリアプライアンスを削除すると、アクティブなプライマリアプライアンスのノードリストやウィジェットの混雑が緩和されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. ノードリストのセカンダリアプライアンスの横に [削除] が表示されるまで待機します。

注意

セカンダリアプライアンスは 10 秒ごとにアクティブなプライマリアプライアンスへの接続を試行します。アクティブなプライマリアプライアンスが 1 分以内に接続ステータスに関するメッセージを受信しない場合、[ノード] リストのセカンダリアプライアンスの横に [削除] が表示されます。

セカンダリアプライアンスは、アクティブなプライマリアプライアンスに再接続されると自動的にクラスタに再結合されます。

3. [削除] をクリックして、クラスタからセカンダリアプライアンスを削除します。

   セカンダリアプライアンスがアクティブなプライマリアプライアンスのノードリストとウィジェットから削除されます。

アクティブなプライマリアプライアンスをセカンダリアプライアンスで置き換える

アクティブなプライマリアプライアンスが応答を停止しているか復元できず、さらにパッシブなプライマリアプライアンスも配置されていない場合は、同じクラスタ内のセカンダリアプライアンスで置き換えることができます。

ヒント

高可用性のため、パッシブなプライマリアプライアンスを配置することをお勧めします。詳細については、93 ページの「クラスタにパッシブなプライマリアプライアンスを追加する」を参照してください。

重要

応答を停止したときにアクティブなプライマリアプライアンスで分析されていた送信には結果は表示されません。

手順

1. アクティブなプライマリアプライアンスの電源をオフにします。
2. 同じクラスタからセカンダリアプライアンスを選択し、新しいアクティブなプライマリアプライアンスとして設定します。
   a. セカンダリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [プライマリモード (アクティブ)] を選択します。
   c. [保存] をクリックします。
3. 新しいアクティブなプライマリアプライアンスの IP アドレスを設定します。

詳細については、77 ページの「[ネットワーク] タブ」を参照してください。

注意

元のアクティブなプライマリアプライアンスと同じ IP アドレスを使用することをお勧めします。これにより、セカンダリアプライアンスと統合製品を再設定せずに接続できます。

4. 新しいアクティブなプライマリアプライアンス上で設定を確認します。

注意

設定がセカンダリアプライアンスに適用されるまで最大 1 日かかります。

初期設定の admin アカウントをリセットする

初期設定の admin アカウントのパスワードを忘れた場合は、Deep Discovery Analyzer アプライアンスのシリアル接続を介してアカウントをリセットできます。

次を準備します。

- シリアルポートがあり、端末エミュレーションプログラム (PuTTY など) がインストールされたコンピュータ
- シリアルケーブル

手順

1. Deep Discovery Analyzer アプライアンスの前面で情報タグを引き出し、サービスタグに記載されている英数字の最後の 5 文字を書き留めます。
2. Deep Discovery Analyzer アプライアンスの電源が入っていることを確認します。
3. コンピュータのシリアルポートを、Deep Discovery Analyzer アプライアンスの背面パネルのシリアルポートに接続します。

4. コンピュータで、シリアル接続用の通信ポート番号 (COM1 など) を確認します。
5. 端末エミュレーションプログラムを開き、次の接続設定を使用してシリアル通信セッションを開始します。

パラメータ	設定
接続の種類	シリアル
ポート	コンピュータの通信ポート番号 (COM1 など)
ボーレート	115200
データビット	8
ストップビット	1
パリティ	なし
フロー制御	XON/XOFF

端末画面がカーソルとともに表示されます。

6. <Enter> キーを押します。

ログオン画面が表示されます。

注意

事前設定コンソールの使用については、50 ページの「事前設定コンソールの基本操作」を参照してください。

7. すでに事前設定コンソールにログインしている場合は、[Log Off] を選択して <Enter> キーを押します。
8. 有効なログオンアカウント情報を入力します。初期設定のアカウント情報は次のとおりです。
   - ユーザ名: `admin`
   - パスワード: サービスタグに記載されている英数字の最後の 5 文字

[Reset Admin Account] 画面が表示されます。

9. 新しいパスワードを 2 回入力します。
10. [Save] を選択し、<Enter> キーを押します。
11. パスワードがリセットされたら、[OK] を選択して <Enter> キーを押し、ログオン画面に戻ります。

注意

システムでは admin アカウントに次の処理も実行されます。

- アカウントの役割を管理者にリセットする
- アカウントがロックされている場合はロック解除する

索引