Deep Discovery™ Inspector 6.7

AWS 配信ガイド

※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/dcx/s/solution/000207383?language=ja

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、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: APEM69876/231211_JP (2024/03)

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 Inspector 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 Inspector 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

第 1 章：AWS への導入について

対象読者 2

AWS アカウント 2

コストとライセンス 2

第 2 章：導入計画

導入の計画 4

アーキテクチャ 5

システム要件 5

導入オプション 7

留意点 9

準備する項目 10

第 3 章：導入

導入の概要 16

仮想アプライアンスの 起動 16

ネットワークインタフェースの 説明の設定 27

トラフィックミラーターゲットとしての 仮想アプライアンスの導入 29

NLB の背後への仮想アプライアンスの 導入 37

第 4 章：導入のテストとトラブルシューティング

チェック項目 52

導入のテスト 57

導入のトラブルシューティング 57

よくある質問 58
AWS に関連した Deep Discovery Inspector 仮想アプライアンスの変更点について教えてください。 59
Deep Discovery Inspector 仮想アプライアンスでは AWS EC2 自動スケーリングをサポートしていますか? 64
Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Amazon Machine Image (AMI) の作成をサポートしていますか? 64
Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Elastic Block Store (EBS) スナップショットの作成をサポートしていますか? 65
Deep Discovery Inspector では AWS Backup サービスはサポートされますか? 65
Deep Discovery Inspector の仮想アプライアンスを AWS に配置するために必要な IAM ポリシーについて教えてください。 66

索引

索引 69

はじめに

本書について

次の項目を参照してください。

- 2 ページの「ドキュメント」
- 3 ページの「対象読者」
- 3 ページの「ドキュメントの表記規則」

ドキュメント

Deep Discovery Inspector 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	管理者ガイドには、Deep Discovery Inspector を設定して管理する方法の詳細な手順、および Deep Discovery Inspector の概念や機能に関する説明が記載されています。
AWS 配信ガイド	AWS 配信ガイドには、Deep Discovery Inspector の AWS への導入の計画、実施、およびトラブルシューティングに関する要件および手順についての情報が含まれています。
インライン (LAN バイパス) ネットワークインタフェースカード インストールガイド	インライン (LAN バイパス) ネットワークインタフェースカードインストールガイドには、追加のバイパスネットワークインタフェースカードを、サポートされる Deep Discovery Inspector アプライアンスにインストール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。
インストールガイド	インストールガイドには、Deep Discovery Inspector 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	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 Inspector 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 Inspector 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 Inspector 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 Inspector のコンポーネントと機能、Deep Discovery Inspector 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/dcx/s/?language=ja

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

https://www.trendmicro.com/ja_jp/business/products/downloads.html?clk=left_nav&clkval=all_download&regs=jp

対象読者

この Deep Discovery Inspector 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

第 1 章

AWS への導入について

このマニュアルには、オンプレミスの Deep Discovery Inspector アプライアンスを AWS 上の Deep Discovery Inspector アプライアンスに展開するための追加情報が記載されています。Deep Discovery Inspector の機能の詳細については、https://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=5476&regs=jp&lang_loc=13 で「Deep Discovery Inspector 管理者ガイド」を参照してください。

対象読者

このガイドは、読者にネットワークの基礎知識があることを前提としています。また AWS に関するある程度の知識も必要です。AWS をはじめて使用する場合は、「ご利用開始のためのリソースセンター」(https://aws.amazon.com/getting-started/) および「トレーニングと認定」(https://aws.amazon.com/training/) を参照してください。これらのサイトでは、AWS 上でインフラストラクチャとアプリケーションを設計、導入、運用する方法を学ぶための資料が提供されています。

AWS アカウント

AWS アカウントをお持ちでない場合は、画面の指示に従って https://aws.amazon.com からアカウントを作成してください。サインアッププロセスでは、電話を受けたり、電話のテンキーを使用して PIN を入力したりする必要があります。

アカウントは AWS によってすべての AWS サービスに自動的にサインアップされますが、料金は使用するサービスについてのみ請求されます。

コストとライセンス

AMI バージョンの Deep Discovery Inspector 仮想アプライアンスにアクセスして使用するには、AWS Marketplace のアクティブな AWS アカウントを持ち、継続的に管理している必要があります。このような AWS アカウントを利用した購入、AWS アカウントの管理、および Deep Discovery Inspector 仮想アプライアンスの導入に必要な Amazon Web Service プラットフォーム/インフラストラクチャの使用は各ユーザの責任において行ってください。

Deep Discovery Inspector 仮想アプライアンスはプライベート AMI イメージで提供されます。プライベート AMI イメージを利用するには、詳しい手順についてトレンドマイクロ認定の販売代理店、アカウントマネージャ、またはエンジニアに問い合わせてください。

第 2 章

導入計画

導入の計画

次の手順は、AWS 環境への Deep Discovery Inspector 仮想アプライアンスの導入計画の概要を示しています。

手順

1. アーキテクチャを確認します。

   詳細については、5 ページの「アーキテクチャ」を参照してください。

2. システム要件を確認します。

   詳細については、5 ページの「システム要件」を参照してください。

3. Amazon VPC トラフィックミラーリングと統合するための導入オプションを選択します。

   詳細については、7 ページの「導入オプション」を参照してください。

4. Deep Discovery Inspector を導入する前に項目を準備します。

   詳細については、10 ページの「準備する項目」を参照してください。

5. Deep Discovery Inspector 仮想アプライアンスを導入します。

   詳細については、15 ページの「導入」を参照してください。

6. Deep Discovery Inspector 仮想アプライアンスの管理コンソールにアクセスします。

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

アーキテクチャ

Deep Discovery Inspector 仮想アプライアンスを AWS EC2 環境に導入することで、AWS VPC トラフィックミラーリングからミラーリングされたパケットを検索して分析できます。

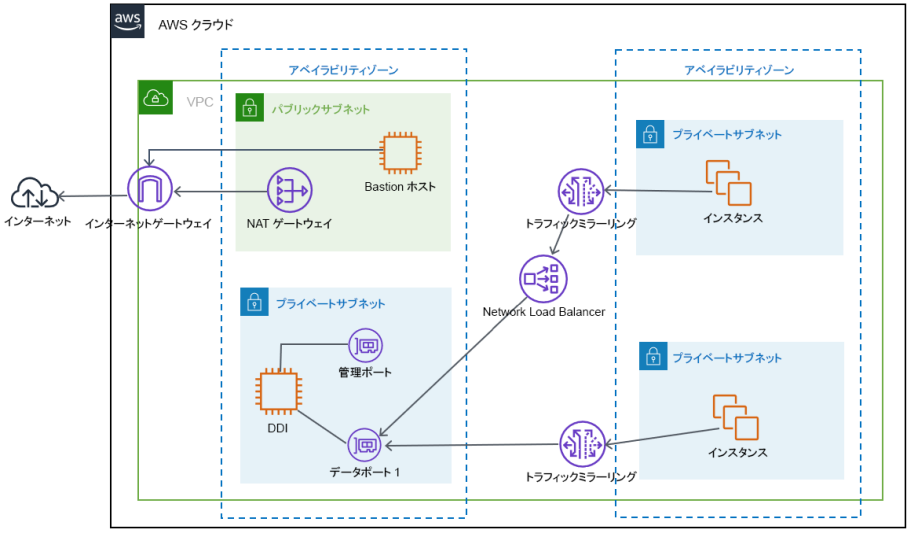


図 2-1. 導入のアーキテクチャ

システム要件

ライセンスモデルのスループットに 基づいて、次の最小限の仕様を満たすことをお勧めします。

注意

AWS 上の Deep Discovery Inspector 仮想アプライアンスで仮想アナライザを使用する場合は、外部仮想アナライザと Sandbox as a Service のみがサポートされます。

表 2-1. システム要件

スループット (Mbps)	AWS vCPU	AWS メモリ (GiB)	AWS ストレージ (GiB)	AWS ENI (Elastic Network Interface)	推奨される AWS EC2 インスタンスタイプ
250	8	32	500	2	• t3.2xlarge • t3a.2xlarge • m5.2xlarge • m5a.2xlarge
500 (日本語版では提供しておりません)	8	32	500	2	• t3.2xlarge • t3a.2xlarge • m5.2xlarge • m5a.2xlarge
1000	16	64	1000	2	• m5.4xlarge • m5a.4xlarge

注意

T3 インスタンスと T3a インスタンスは、初期設定で無制限モードで起動します。インスタンスタイプに対する無制限モードまたは標準モードの使用の詳細については、https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html を参照してください。

AWS EC2 インスタンスタイプの詳細については、https://aws.amazon.com/ec2/instance-types/を参照してください。

インスタンスタイプが最小限のシステム要件を満たしていれば、非推奨のインスタンスタイプを使用できます。

導入オプション

Amazon VPC トラフィックミラーリング機能と統合することで、Deep Discovery Inspector 仮想アプライアンスは次の 2 つの導入オプションによりネットワークセキュリティソリューションを 提供します。

- オプション 1: Deep Discovery Inspector 仮想アプライアンスをトラフィックミラーターゲットとして導入する

  ネットワークトラフィックは、ENI (Elastic Network Interface) ミラーソースから Deep Discovery Inspector 仮想アプライアンスのデータポートにミラーリングされます。このオプションは、次の図に示すようにトラフィックミラーフィルタの 設定に依存します。

  注意

  Deep Discovery Inspector 仮想アプライアンスが 複数のデータポートに接続されている場合、各データポートをトラフィックミラーターゲットとして設定できます。

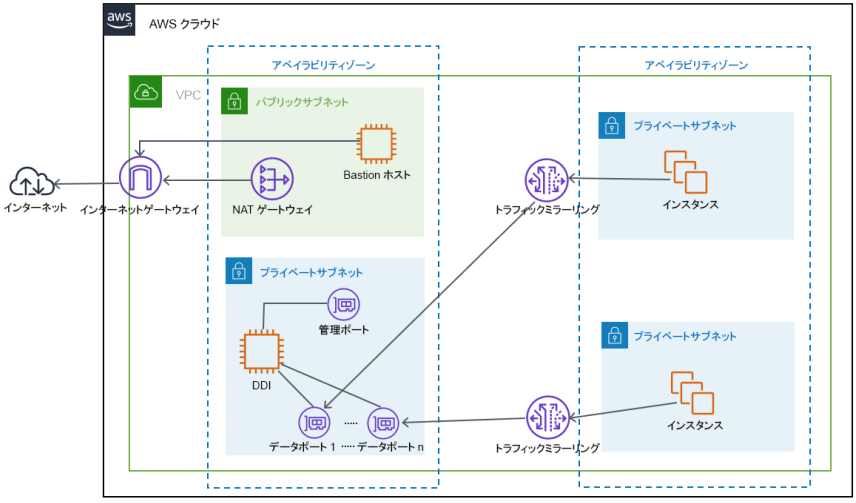


図 2-2. オプション 1: Deep Discovery Inspector 仮想アプライアンスをトラフィックミラーターゲットとして導入する

- オプション 2: Deep Discovery Inspector 仮想アプライアンスを NLB の背後に導入する

  ターゲットグループ内の Deep Discovery Inspector 仮想アプライアンスを NLB (Network Load Balancer) の背後に導入します。次の図に示すように、ネットワークトラフィックは NLB にミラーリングされ、NLB はターゲットグループに属する正常なインスタンスにトラフィックを転送します。

  注意

  NLB はミラーリングされたトラフィックを Deep Discovery Inspector 仮想アプライアンスのデータポート 1 にのみ転送します。

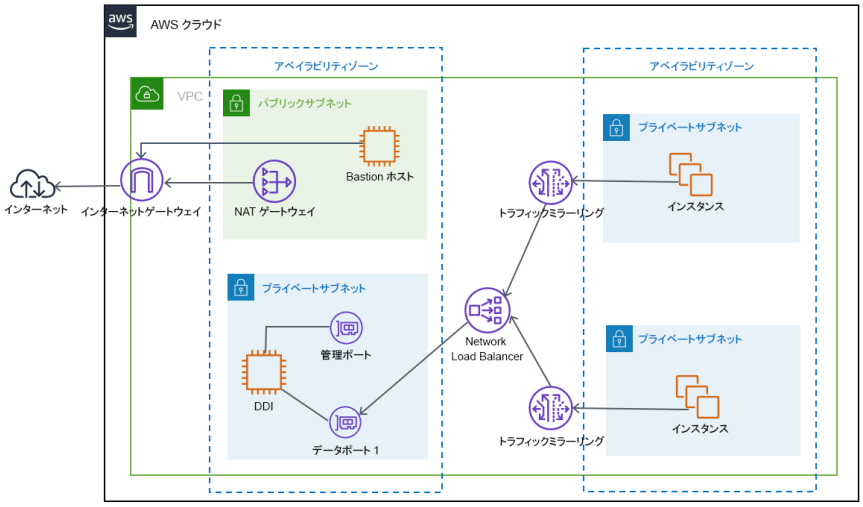


図 2-3. オプション 2: Deep Discovery Inspector 仮想アプライアンスを NLB の背後に導入する

留意点

AWS トラフィックミラーで適用される割り当て制限には、導入オプションに関する次の制限があります。

- ターゲットとしての非専有インスタンスタイプあたりのミラーソースの最大数: 10
- ターゲットとしての専有インスタンスタイプあたりのミラーソースの 最大数: 100

注意

制限事項の詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-considerations.html を参照してください。

導入は特定のオプションに限定されません。早期の検証のために Deep Discovery Inspector 仮想アプライアンスをトラフィックミラーターゲットとして導入し、その後、Deep Discovery Inspector 仮想アプライアンスの導入を NLB の背後に変更した場合、変更後の Deep Discovery Inspector 仮想アプラ

イアンスを再起動する必要はありません。高度な導入オプションでは、両方の導入オプションを VPC 環境に同時に組み込むことができます。

準備する項目

- Deep Discovery Inspector の AMI

  トレンドマイクロによって付与される、Deep Discovery Inspector 仮想アプライアンスのプライベート AMI

- Deep Discovery Inspector のアクティベーションコード

  Deep Discovery Inspector 仮想アプライアンスのアクティベーションコード

- AWS VPC とサブネット

  AWS のベストプラクティスに従ってパブリックとプライベートのサブネットで VPC を構成し、AWS 上で独自の仮想ネットワークを提供します。

  注意

  VPC とサブネットの作成方法の詳細については、https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html を参照してください。

  パブリックサブネット:

  - マネージド NAT ゲートウェイを配置して、プライベートサブネット内の Deep Discovery Inspector 仮想アプライアンスにアウトバウンドインターネットアクセスを 許可します。

    注意

    NAT ゲートウェイの作成方法の詳細については、https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html を参照してください。

  プライベートサブネット:

- Deep Discovery Inspector 仮想アプライアンスの管理ポートとデータポートは、VPC の同じサブネット内または異なるサブネット内に存在することができます。

- AWS VPC トラフィックミラーリング

  AWS VPC の機能であるトラフィックミラーリングを使用すると、Amazon EC2 インスタンスの Elastic Network Interface (ENI) からネットワークトラフィックをコピーできます。Deep Discovery Inspector のセキュリティアプライアンスと 監視アプライアンスは、個別のインスタンスとして配置することも、UDP リスナーとともに Network Load Balancer (NLB) の背後に一連のインスタンスとして配置することもできます。

  注意

  詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html を参照してください。

  - ネットワーク接続する 1 つ以上のインスタンス。このインスタンスはトラフィックミラーソースとして機能します。

    重要

    ミラーリングされるパケットのサイズには制限があり、8,947 バイトを超えるパケットは常に切り捨てられます。トラフィックミラーソースの MTU のサイズが 8,947 バイト以下に設定されていることを確認してください。トラフィックミラーソースとして 設定する AWS EC2 インスタンスの MTU を確認して設定するには、https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html#set_mtu および https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/network_mtu.html#set_mtu_windows を参照してください。

  - AWS Nitro System を備えたインスタンスのみがトラフィックミラーソースとして利用できます。詳細については、https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/を参照してください。

- (オプション) 次の項目が適切に設定された Network Load Balancer:
  - ターゲットグループ
- 次の項目が適切に設定されたトラフィックミラー:
  - トラフィックミラーフィルタ
  - トラフィックミラーターゲット
  - トラフィックミラーセッション

注意

トラフィックミラーターゲットとトラフィックミラーフィルタを 作成し、これらのリソースを使用してセッションを作成する方法の詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-getting-started.html を参照してください。

- AWS EC2 セキュリティグループ

インバウンド/アウトバウンドルール	タイプ	プロトコル	ポート	送信元	説明
インバウンド	HTTPS	TCP	443	インスタンスに到達可能な CIDR	Deep Discovery Inspector 仮想アプライアンスの管理コンソールへのアクセス用
インバウンド	SSH	TCP	22	インスタンスに到達可能な CIDR	Deep Discovery Inspector 仮想アプライアンスの事前設定コンソールへのアクセス用

インバウンド/アウトバウンドルール	タイプ	プロトコル	ポート	送信元	説明
インバウンド	カスタム UDP	UDP	4789	ミラーソースまたは NLB の CIDR	AWS のトラフィックミラーに必要な VXLAN トラフィック用
インバウンド	カスタム TCP	TCP	14789	NLB の CIDR	(オプション) Deep Discovery Inspector 仮想アプライアンスに実装された NLB のヘルスチェック応答用

注意

初期設定のセキュリティグループのアウトバウンドルールでは、すべてのトラフィックが許可されます。Deep Discovery Inspector 仮想アプライアンスは、初期設定のアウトバウンドルールで問題なく機能しますが、次の例外が適用されることがあります。

- 組織によっては、ポリシー上の理由で特定のプロトコルとポート番号がさらに必要になる場合があります。「Deep Discovery Inspector インストールガイド」の第 2 章「システムについて」を参照してください。
- 組織によっては、インフラストラクチャ上の理由でインターネットアクセスが許可されたドメインを持つアウトバウンドプロキシが必要になる場合があります。詳細なアドレスについては、https://docs.trendmicro.com/all/ent/ddi/v5.7/ja-jp/ddi_5.7_olh/access_trend_service.html を参照してください。

第 3 章

導入

導入の概要

ここでは、Deep Discovery Inspector 仮想アプライアンスと VPC トラフィックミラーリングを AWS 環境に導入するために必要な手順の概要を示します。

1. Deep Discovery Inspector 仮想アプライアンスを起動します。

   詳細については、16 ページの「仮想アプライアンスの起動」を参照してください。

2. (オプション) 仮想アプライアンスのネットワークインタフェースの 説明を設定します。

   詳細については、27 ページの「ネットワークインタフェースの 説明の設定」を参照してください。

3. 次のいずれかのオプションを選択して、AWS VPC トラフィックミラーリングを導入します。

   - トラフィックミラーターゲットとして仮想アプライアンスを導入する

     詳細については、29 ページの「トラフィックミラーターゲットとしての仮想アプライアンスの導入」を参照してください。

   - NLB の背後に仮想アプライアンスを導入する

     詳細については、37 ページの「NLB の背後への仮想アプライアンスの導入」を参照してください。

仮想アプライアンスの起動

手順

1. インスタンスを起動します。

   a. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。

   b. 画面上部のナビゲーションバーで、要件を満たすインスタンスのリージョンを選択します。

   c. Amazon EC2 コンソールのダッシュボードで、[インスタンスを起動] を選択します。

2. Deep Discovery Inspector の AMI を選択します。

   a. [Amazon マシンイメージ (AMI)] 画面の左側のペインで、[マイ AMI] > [所有権] > [共有ファイル] の順に選択します。

   b. 表示されるリストから [Trend Micro Deep Discovery Inspector <バージョン> JP] AMI を選択して、[選択] をクリックします。たとえば [Trend Micro Deep Discovery Inspector 5.7.xxxx JP] を選択します。

注意

何も表示されない場合、トレンドマイクロからユーザに権限が付与されていません。トレンドマイクロの販売代理店に問い合わせてください。

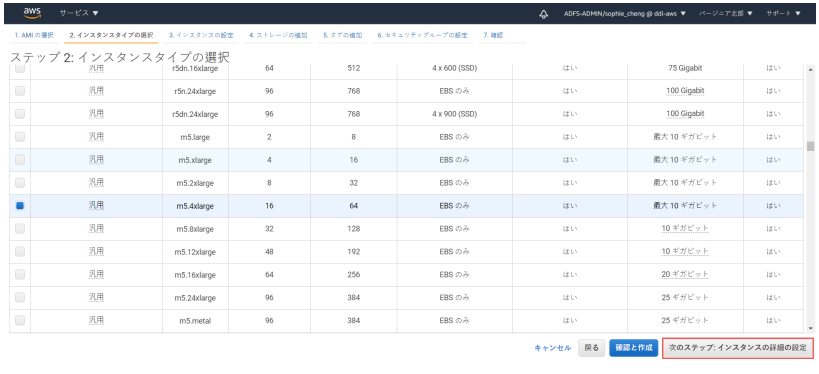
c. 検索結果が表示されたら、[Trend Micro Deep Discovery Inspector <バージョン>] の [選択] をクリックします。

3. インスタンスタイプを選択します。

a. [インスタンスタイプの選択] 画面で、ライセンスモデルのスループットに基づいて最小限の仕様を満たすインスタンスタイプを 選択します。

詳細については、5 ページの「システム要件」を参照してください。

b. [次のステップ: インスタンスの詳細の設定] を選択して、さらにインスタンスを設定します。



4. インスタンスの詳細を設定します。

a. [インスタンスの詳細の設定] 画面で、次の設定を変更します。

- ネットワーク: VPC を選択します。
- サブネット: インスタンスを起動するサブネットを選択します。データポートのサブネットに計画されているサブネットを選択します。
- 自動割り当てパブリック IP: [Disable] を選択します。トレンドマイクロでは、Deep Discovery Inspector 仮想アプライアンスを AWS NAT ゲートウェイの背後に配置することをお勧めします。

- Network interfaces: [デバイスの追加] を選択して、Deep Discovery Inspector 仮想アプライアンスのインスタンスのセカンダリネットワークインタフェースを 追加します。

重要

オンプレミスの Deep Discovery Inspector の管理ポートは、最初の NIC ポート (Deep Discovery Inspector の eth0) に固定されます。AWS 環境に適応するため、Deep Discovery Inspector 仮想アプライアンスでは、管理ポートのポートの割り当てがポート 1 (eth1) に、データポートのポートの割り当てがポート 0 (eth0) に変更されています。

- [デバイス] の [eth0]
  - サブネット: サブネットは前の手順で設定されています。
  - プライマリ IP: サブネットの範囲からプライベート IPv4 アドレスを入力するか、[自動的に割り当て] のままにして AWS がプライベート IPv4 アドレスを選択するようにします。

- [デバイス] の [eth1]
  - サブネット: 管理ポートのサブネットに計画されているサブネットを選択します。
  - プライマリ IP: サブネットの範囲からプライベート IPv4 アドレスを入力するか、[自動的に割り当て] のままにして AWS がプライベート IPv4 アドレスを選択するようにします。
  - IPv6 IP: (オプション) [IP の追加] をクリックしてサブネットの範囲から IPv6 アドレスを入力するか、[自動的に割り当て] のままにして AWS が IPv6 アドレスを選択するようにします。

b. [次のステップ: ストレージの追加] をクリックして、インスタンスのルートボリュームサイズを指定します。

5. ストレージを追加します。

a. [ストレージの追加] 画面で次の設定を行います。

- サイズ: ストレージサイズは、ライセンスモデルのスループットに基づいて最小限の仕様を満たす必要があります。

  詳細については、5 ページの「システム要件」を参照してください。

注意

ストレージサイズを拡大するには、[ボリュームタイプ]: [ルート] のストレージサイズを指定します。Deep Discovery Inspector 仮想アプライアンスは、[ボリュームタイプ] が [ルート] の場合のみストレージをパーティション化します。追加のストレージは使用されません。

- ボリュームタイプ: 初期設定値の [汎用 SSD (gp2)] を使用します。

b. [次のステップ: タグの追加] をクリックして、カスタムタグを追加します。

6. タグを追加します。

   a. [タグの追加] 画面で、キーと値の組み合わせを入力してタグを指定します。

      たとえば、[キー] に「`Name`」、[値] に「`vDDI-demo`」と入力します。

   b. [次のステップ: セキュリティグループの 設定] をクリックします。

7. セキュリティグループを設定します。

   a. [セキュリティグループの 設定] 画面で、セキュリティグループを 使用して Deep Discovery Inspector 仮想アプライアンスのインスタンスのファイアウォールルールを 定義します。

      - 既存のセキュリティグループを 使用するには、[既存のセキュリティグループを 選択] を選択して、目的のセキュリティグループを選択します。
      - 新しいセキュリティグループを 作成するには、[新しいセキュリティグループを 作成] を選択します。

   b. 選択したセキュリティグループに 次のルールが含まれていることを確認します。

      表 3-1. インバウンドルール

タイプ	プロトコル	ポート範囲	送信元	理由
SSH	TCP	22	インスタンスに到達可能な CIDR	Deep Discovery Inspector 仮想アプライアンスの事前設定コンソールへのアクセス用

タイプ	プロトコル	ポート範囲	送信元	理由
HTTPS	TCP	443	インスタンスに到達可能な CIDR	Deep Discovery Inspector 仮想アプライアンスの管理コンソールへのアクセス用
カスタム UDP	UDP	4789	ミラーソースまたは NLB の CIDR	AWS のトラフィックミラーに必要な VXLAN トラフィック用
カスタム TCP	TCP	14789	NLB の CIDR	Deep Discovery Inspector 仮想アプライアンスに実装された NLB のヘルスチェック応答用

注意

アウトバウンドルール: 初期設定のセキュリティグループのルールではすべてのトラフィックが許可されます。Deep Discovery Inspector 仮想アプライアンスは、初期設定のアウトバウンドルールで問題なく機能しますが、次の例外が発生することがあります。

- 組織によっては、ポリシー上の理由で特定のプロトコルとポート番号がさらに必要になる場合があります。「Deep Discovery Inspector インストールガイド」の第 2 章「システムについて」にある「アプライアンスで使用されるポート」を参照してください。
- 組織によっては、インフラストラクチャ上の理由でインターネットアクセスが許可されたドメインを持つアウトバウンドプロキシが必要になる場合があります。詳細なアドレスについては、https://docs.trendmicro.com/all/ent/ddi/v5.7/ja-jp/ddi_5.7_olh/access_trend_service.html を参照してください。

c. [確認と作成] をクリックします。

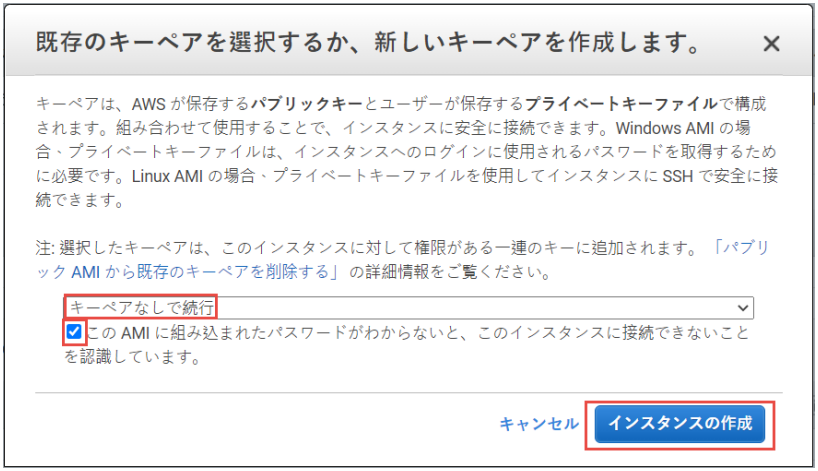
8. インスタンスの起動を確認し、キーのペアを選択します。

a. [インスタンスの起動を確認] 画面でインスタンスの詳細を確認し、[編集] リンクを使用して必要な変更を行います。

b. [起動] をクリックします。

c. [既存のキーペアを選択するか、新しいキーペアを作成します。] ダイアログボックスで、[キーペアなしで続行] を選択します。

d. インスタンスを起動するには、確認のチェックボックスをオンにして、[インスタンスの作成] をクリックします。



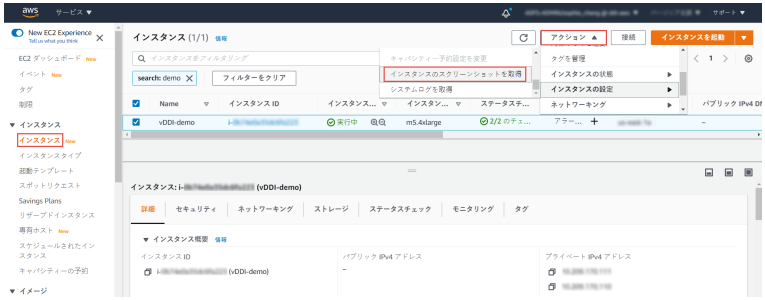
9. Deep Discovery Inspector 仮想アプライアンスの準備が完了するまで待ちます。

注意

Deep Discovery Inspector 仮想アプライアンスの準備には約 15 分かかります。

a. 次の手順に従って、Deep Discovery Inspector のインストール状況を確認します。

   1. 左側のナビゲーション画面で [インスタンス] をクリックします。
   2. Deep Discovery Inspector 仮想アプライアンスのインスタンスを選択します。
   3. [アクション] > [インスタンスの設定] > [インスタンスのスクリーンショットを取得] の順に選択します。



詳細については、https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html を参照してください。

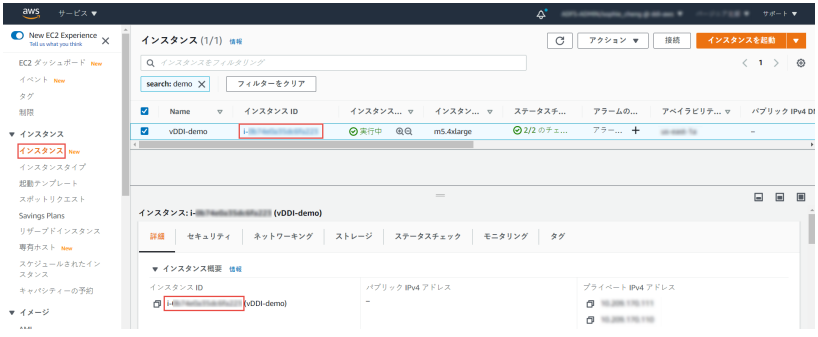
b. Deep Discovery Inspector 仮想アプライアンスの事前設定コンソールが表示されたら、Deep Discovery Inspector の準備は終了です。

ネットワークインタフェースの説明の設定

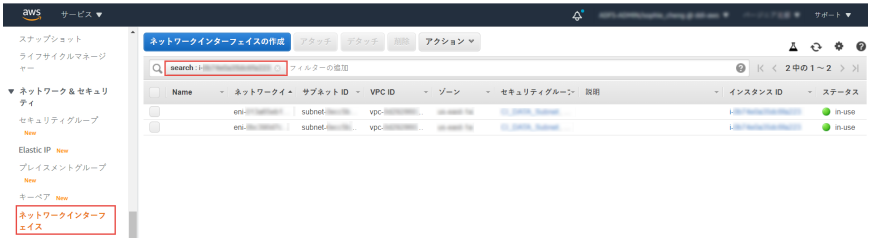
このタスクはオプションです。トレンドマイクロでは、インスタンスのネットワークインタフェースの 説明を設定することをお勧めします。多数の ENI で構成される長いリストから ENI を 1 つ選択する際、時間を節約して操作エラーを回避できます。

手順

1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
2. ナビゲーションペインで [インスタンス] を選択し、次の手順に従ってインスタンス ID をコピーします。
   a. 16 ページの「仮想アプライアンスの 起動」で作成した Deep Discovery Inspector 仮想アプライアンスを 検索します。
   b. [インスタンス ID] の値をコピーします。



3. ナビゲーションペインで [ネットワークインターフェイス] を選択し、インスタンス ID を検索することで Deep Discovery Inspector 仮想アプライアンスのネットワークインタフェースを 見つけます。



4. Deep Discovery Inspector 仮想アプライアンスのネットワークインタフェースを選択して、[アクション] > [説明の変更] の順に選択します。

5. [説明の変更] ダイアログボックスにネットワークインタフェースの 説明を入力し、[保存] を選択して、次の手順を実行します。

   a. eth0 の説明を「`Data port 1`」に設定します。

   b. eth1 の説明を「`Management port`」に設定します。

ヒント

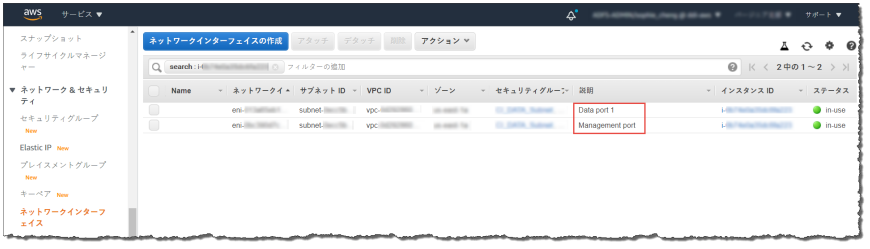
どのインタフェースが eth0 で、どのインタフェースが eth1 かを確認するには、次の手順を実行します。

a. インタフェースを選択します。

b. [アクション] > [IP アドレスの管理] の順にクリックします。

   ポートラベルが表示されます。

c. 元の画面に戻るには、[キャンセル] をクリックします。



トラフィックミラーターゲットとしての仮想アプライアンスの導入

手順

1. トラフィックミラーフィルタを 設定します。

   詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-filters.html を参照してください。

   a. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。

   b. [リージョン] セレクタで、VPC の作成時に使用した AWS のリージョンを選択します。

   c. ナビゲーションペインで、[トラフィックミラーリング] > [フィルターをミラーリングする] の順に選択します。

   d. [トラフィックミラーフィルタの 作成] を選択します。

   e. [名前タグ] に、トラフィックミラーフィルタの 名前を入力します。

      たとえば「`demo-traffic-mirror-filter`」と入力します。

   f. (オプション) [説明] に、トラフィックミラーフィルタの 説明を入力します。

      たとえば「`demo-traffic-mirror-filter`」と入力します。

   g. [amazon-dns] を選択します。

h. インバウンドルールを追加します。[インバウンドルール] > [追加] > [ルール] の順に選択し、トラフィックミラーソースのインバウンドトラフィックについて次の情報を指定します。

- 番号: ルールに割り当てる優先度を入力します。
- ルールアクション: パケットに対して実行するアクションを選択します。
- プロトコル: ルールに割り当てる L4 プロトコルを選択します。
- (オプション) 送信元ポート範囲: 送信元のポート範囲を入力します。
- (オプション) 送信先ポート範囲: 送信先のポート範囲を入力します。
- 送信元 CIDR ブロック: 送信元の CIDR ブロックを入力します。
- 送信先 CIDR ブロック: 送信先の CIDR ブロックを入力します。
- (オプション) 説明: ルールの説明を入力します。

値の例を次に示します。

- 番号: 初期設定の番号を使用します。
- ルールアクション: [accept] を選択します。
- プロトコル: [すべてのプロトコル] を選択します。
- 送信元 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 送信先 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 説明: 「`mirror all inbound traffic`」と入力します。

i. アウトバウンドルールを追加します。[アウトバウンドルール] > [追加] > [ルール] の順に選択し、トラフィックミラーソースのアウトバウンドトラフィックについて次の情報を指定します。

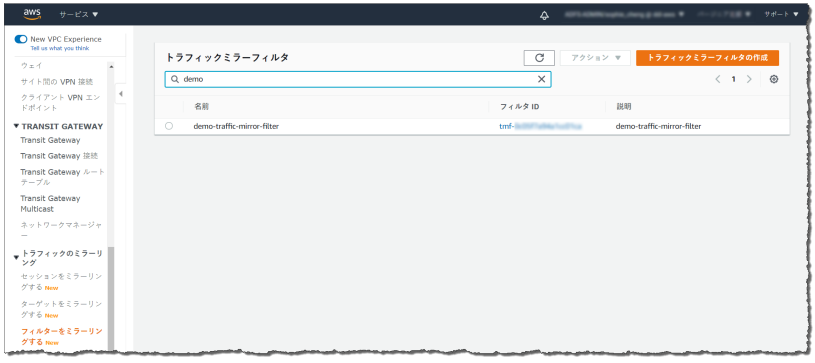
- 番号: ルールに割り当てる優先度を入力します。
- ルールアクション: パケットに対して実行するアクションを選択します。
- プロトコル: ルールに割り当てる L4 プロトコルを選択します。
- (オプション) 送信元ポート範囲: 送信元のポート範囲を入力します。
- (オプション) 送信先ポート範囲: 送信先のポート範囲を入力します。
- 送信元 CIDR ブロック: 送信元の CIDR ブロックを入力します。
- 送信先 CIDR ブロック: 送信先の CIDR ブロックを入力します。
- (オプション) 説明: ルールの説明を入力します。

値の例を次に示します。

- 番号: 初期設定の番号を使用します。
- ルールアクション: [accept] を選択します。
- プロトコル: [すべてのプロトコル] を選択します。
- 送信元 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 送信先 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 説明: 「`mirror all outbound traffic`」と入力します。

j. 追加するインバウンドルールおよびアウトバウンドルールごとに、前述の手順を繰り返します。

k. [作成] をクリックします。



2. トラフィックミラーターゲットを設定します。

   a. ナビゲーションペインで、[トラフィックのミラーリング] > [ターゲットをミラーリングする] の順に選択します。

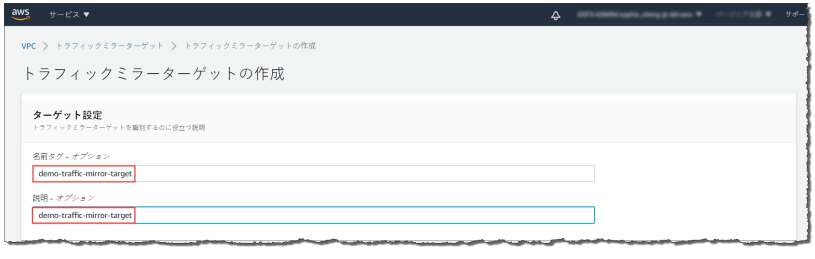
   b. [トラフィックミラーターゲットの作成] を選択します。

   c. [名前タグ] に、トラフィックミラーターゲットの名前を入力します。

      たとえば「`demo-traffic-mirror-target`」と入力します。

   d. (オプション) [説明] に、トラフィックミラーターゲットの説明を入力します。

      たとえば「`demo-traffic-mirror-target`」と入力します。



   e. [ターゲットタイプ] で、[ネットワークインターフェイス] を選択します。

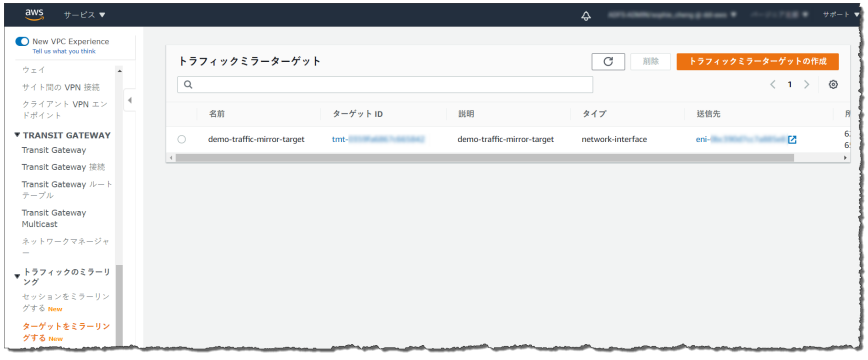
   f. [ターゲット] で、Deep Discovery Inspector 仮想アプライアンスの eth0 (サブネットに接続されているデータポート) をトラフィックミラーターゲットとして選択します。

注意

eth2 や eth3 など、Deep Discovery Inspector 仮想アプライアンスに接続されている任意のデータポートを選択できます。

Deep Discovery Inspector 仮想アプライアンスの管理ポートとして使用される eth1 ポートは選択しないでください。

g. [作成] をクリックします。



3. 前述の手順を繰り返して、AWS 環境内の Deep Discovery Inspector 仮想アプライアンスごとにトラフィックミラーターゲットを 作成します。

4. トラフィックミラーセッションを設定します。

   a. ナビゲーションペインで、[トラフィックのミラーリング] > [セッションをミラーリングする] の順に選択します。

   b. [トラフィックミラーセッションの作成] を選択します。

   c. [名前タグ] に、トラフィックミラーセッションの名前を入力します。

たとえば「demo-traffic-mirror-session」と入力します。

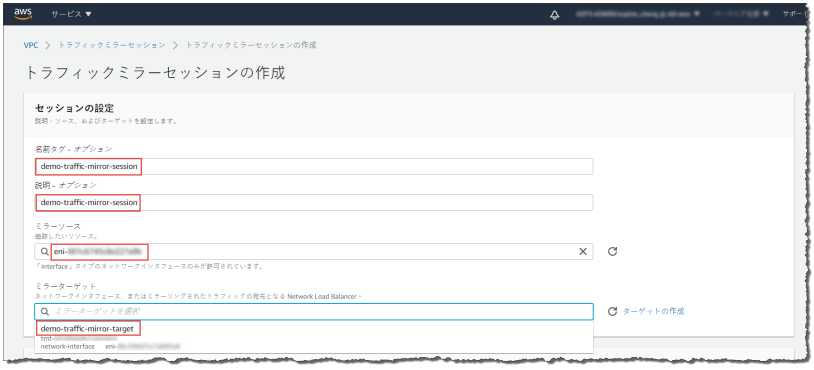
d. (オプション) [説明] に、トラフィックミラーセッションの説明を入力します。

たとえば「demo-traffic-mirror-session」と入力します。

e. [ミラーソース] で、監視するインスタンスのネットワークインタフェースを選択します。

f. [ミラーターゲット] で、トラフィックミラーターゲットを選択します。

たとえば [demo-traffic-mirror-target] を選択します。



g. [追加設定] で、次の手順を実行します。

- [セッション数] に、セッション番号「1」を入力します。

  セッション番号は、次の場合にトラフィックミラーセッションを評価する順序を決定します。

  - インタフェースが複数のセッションで使用されている場合
  - インタフェースが異なるトラフィックミラーターゲットとトラフィックミラーフィルタで 使用されている場合

  トラフィックは一度だけミラーリングされます。「1」は優先度が最も高いことを示します。有効な値は 1～32766 です。

- (オプション) [VNI] に、トラフィックミラーセッションに使用する VXLAN ID を入力します。

詳細については、https://tools.ietf.org/html/rfc7348 を参照してください。

値を指定しない場合、AWS では未使用の番号がランダムに割り当てられます。

- (オプション) [パケット長] に、ミラーリングする各パケット内のバイト数を入力します。

  パケット全体をミラーリングしない場合は、ミラーリングする各パケット内のバイト数を [パケット長] に設定します。たとえば、この値を 100 に設定すると、フィルタ条件を満たす VXLAN ヘッダの後の最初の 100 バイトがターゲットにコピーされます。

  パケット全体をミラーリングするには、このフィールドに値を入力しないでください。

- [フィルタ] で、ミラーリングするトラフィックを決定するトラフィックミラーフィルタを選択します。

  たとえば [demo-traffic-mirror-filter] を選択します。

- (オプション) [タグ] セクションで、タグを追加または削除します。

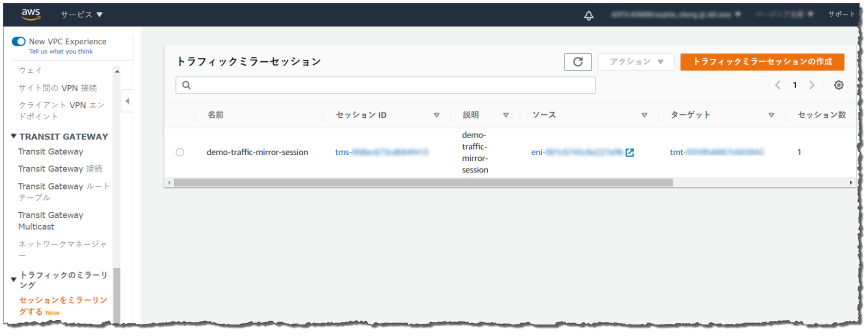
設定の例を次に示します。

- [セッション数] に、セッション番号「1」を入力します。
- [VNI] の値は空のままにします。AWS によってランダムな番号が割り当てられます。
- [パケット長] の値は空のままにします。AWS によってパケット全体がミラーリングされます。
- [フィルタ] で、[demo-traffic-mirror-filter] を選択します。

h. [作成] をクリックします。

注意

詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/working-with-traffic-mirroring.html で「*Working with Traffic Mirroring*」を参照してください。



5. 監視する送信元が複数ある場合、前述の手順を繰り返して、さらにトラフィックミラーセッションを作成します。

NLB の背後への仮想アプライアンスの導入

手順

1. ロードバランサーとリスナーを設定します。
   a. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
   b. ナビゲーションペインの [ロードバランシング] で、[ロードバランサー] を選択します。
   c. [ロードバランサーの作成] を選択します。
   d. [ネットワークロードバランサー] で、[作成] を選択します。
   e. [名前] に、ロードバランサーの名前を入力します。

      たとえば「`demo-nlb`」と入力します。
   f. [スキーム] で、[内部] を選択します。
   g. [リスナー] で、プロトコルを [UDP] に変更し、ミラーリングされたトラフィックを受信するポートに「`4789`」と入力します。
   h. [アベイラビリティゾーン] で、Deep Discovery Inspector 仮想アプライアンスのインスタンスに使用した VPC を選択し、データポート 1 (eth0 と呼ばれる) のサブネットを選択します。

注意

ロードバランサに対して複数の [アベイラビリティゾーン] を有効にする場合は、各ターゲットグループの 少なくとも 1 つのターゲットが各 [アベイラビリティゾーン] にあることを確認してください。そうでない場合、ロードバランサは Deep Discovery Inspector にトラフィックをルーティングしません。詳細については、https://docs.aws.amazon.com/elasticloadbalancing/latest/network/introduction.html#network-load-balancer-components を参照してください。

i. [IPv4 アドレス] で、[CIDR から割り当て済み] を選択して AWS がアドレスを割り当てるようにするか、[CIDR から IP を入力] を選択してアドレスを指定します。

j. [次の手順: セキュリティ設定の構成] をクリックします。

2. セキュリティ設定を行います。

   a. [セキュリティ設定の構成] 画面で変更する項目はありません。

   b. [次の手順: ルーティングの設定] をクリックします。

3. ターゲットグループを設定します。

   a. [ターゲットグループ] は、初期設定の [新しいターゲットグループ] のままにします。

   b. [名前] に、ターゲットグループの名前を入力します。

      たとえば「`demo-target-group`」と入力します。

   c. [ターゲットの種類] で、[インスタンス] を選択します。

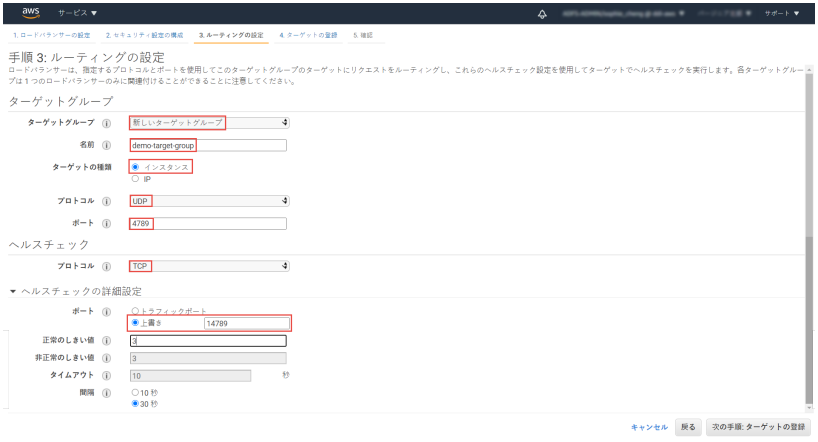
d. [プロトコル] で、[UDP] を選択します。

e. [ポート] に、「`4789`」と入力します。

f. [ヘルスチェック] の [プロトコル] で、[TCP] を選択します。

g. [ヘルスチェックの詳細設定] の [ポート] で、[上書き] を選択し、ポートに「`14789`」と入力します。

h. その他は初期設定のままにします。



i. [次の手順: ターゲットの登録] をクリックします。

4. ターゲットグループにターゲットを 登録します。

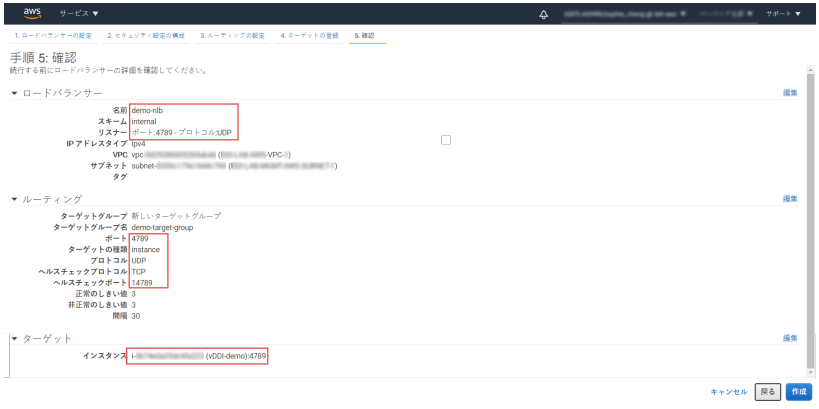
a. [インスタンス] で、Deep Discovery Inspector 仮想アプライアンスを選択します。

たとえば [demo-ddi] を選択します。

b. インスタンスのリスナーポートを初期設定のままにして、[登録済みに追加] を選択します。

c. [次の手順: 確認] をクリックします。

[確認] 画面が表示されます。



5. ロードバランサーを作成します。

a. [確認] 画面で、[作成] をクリックします。

b. ロードバランサーが作成されたら、[閉じる] をクリックします。

c. ナビゲーションペインの [ロードバランシング] で、[ターゲットグループ] を選択します。

d. 新しく作成したターゲットグループを選択します。

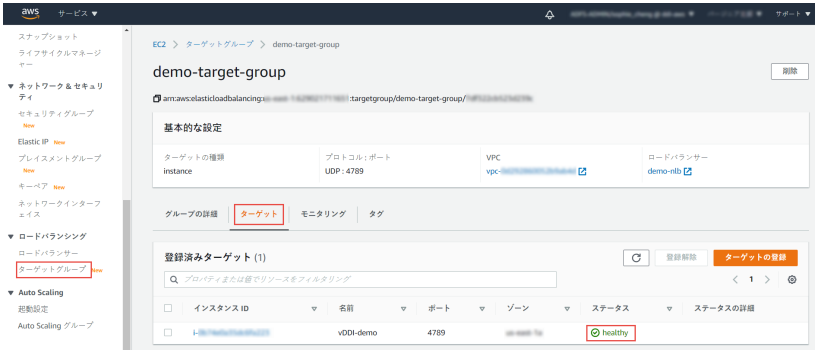
たとえば [demo-target-group] を選択します。

e. [ターゲット] を選択して、インスタンスの準備ができたことを確認します。

注意

インスタンスのステータスが [initial] である場合、インスタンスが登録プロセス中であるか、[healthy] と見なされる最小回数のヘルスチェックに成功していない可能性があります。1 つ以上のインスタンスのステータスが [healthy] になれば、ロードバランサーをテストできます。

NLB の作成後に Deep Discovery Inspector 仮想アプライアンスが起動される場合は、[ターゲットの登録] を使用して、NLB のターゲットグループに Deep Discovery Inspector 仮想アプライアンスを追加します。詳細については、https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-register-targets.html を参照してください。



6. トラフィックミラーフィルタを 設定します。

詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-filters.html を参照してください。

a. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。

b. [リージョン] セレクタで、VPC の作成時に使用した AWS のリージョンを選択します。

c. ナビゲーションペインで、[トラフィックのミラーリング] > [フィルターをミラーリングする] の順に選択します。

d. [トラフィックミラーフィルタの 作成] を選択します。

e. [名前タグ] に、トラフィックミラーフィルタの 名前を入力します。

たとえば「`demo-traffic-mirror-filter`」と入力します。

f. (オプション) [説明] に、トラフィックミラーフィルタの 説明を入力します。

たとえば「`demo-traffic-mirror-filter`」と入力します。

g. (オプション) [ネットワークサービス] で [amazon-dns] を選択します。

h. インバウンドルールを追加します。[インバウンドルール] > [追加] > [ルール] の順に選択し、トラフィックミラーソースのインバウンドトラフィックについて次の情報を指定します。

- 番号: ルールに割り当てる優先度を入力します。
- ルールアクション: パケットに対して実行するアクションを選択します。
- プロトコル: ルールに割り当てる L4 プロトコルを選択します。
- (オプション) 送信元ポート範囲: 送信元のポート範囲を入力します。

- (オプション) 送信先ポート範囲: 送信先のポート範囲を入力します。
- 送信元 CIDR ブロック: 送信元の CIDR ブロックを入力します。
- 送信先 CIDR ブロック: 送信先の CIDR ブロックを入力します。
- (オプション) 説明: ルールの説明を入力します。

値の例を次に示します。

- 番号: 初期設定の番号を使用します。
- ルールアクション: [accept] を選択します。
- プロトコル: [すべてのプロトコル] を選択します。
- 送信元 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 送信先 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 説明: 「`mirror all inbound traffic`」と入力します。

i. アウトバウンドルールを追加します。[アウトバウンドルール] > [追加] > [ルール] の順に選択し、トラフィックミラーソースのアウトバウンドトラフィックについて次の情報を指定します。

- 番号: ルールに割り当てる優先度を入力します。
- ルールアクション: パケットに対して実行するアクションを選択します。
- プロトコル: ルールに割り当てる L4 プロトコルを選択します。
- (オプション) 送信元ポート範囲: 送信元のポート範囲を入力します。
- (オプション) 送信先ポート範囲: 送信先のポート範囲を入力します。

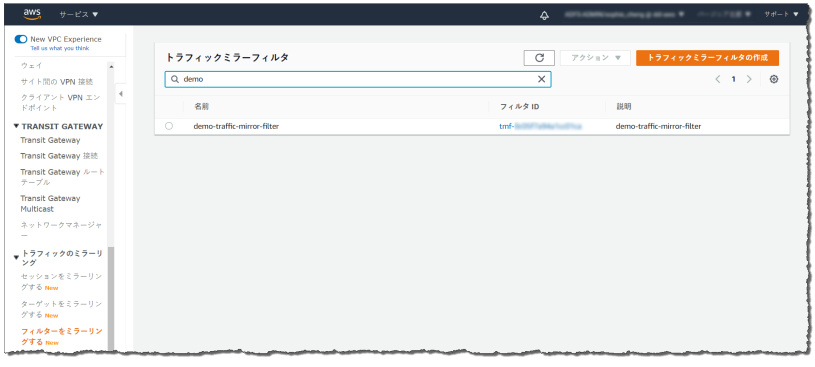
- 送信元 CIDR ブロック: 送信元の CIDR ブロックを入力します。
- 送信先 CIDR ブロック: 送信先の CIDR ブロックを入力します。
- (オプション) 説明: ルールの説明を入力します。

値の例を次に示します。

- 番号: 初期設定の番号を使用します。
- ルールアクション: [accept] を選択します。
- プロトコル: [すべてのプロトコル] を選択します。
- 送信元 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 送信先 CIDR ブロック: 「`0.0.0.0/0`」と入力します。
- 説明: 「`mirror all outbound traffic`」と入力します。

j. 追加するインバウンドルールおよびアウトバウンドルールごとに、前述の手順を繰り返します。

k. [作成] をクリックします。



7. トラフィックミラーターゲットを設定します。

   a. https://console.aws.amazon.com/vpc/で Amazon VPC コンソールを開きます。

   b. [リージョン] セレクタで、VPC の作成時に使用した AWS のリージョンを選択します。

   c. ナビゲーションペインで、[トラフィックのミラーリング] > [トラフィックミラーターゲット] の順に選択します。

   d. [トラフィックミラーターゲットの作成] を選択します。

   e. [名前タグ] に、トラフィックミラーターゲットの名前を入力します。

      たとえば「`demo-traffic-mirror-target`」と入力します。

   f. (オプション) [説明] に、トラフィックミラーターゲットの説明を入力します。

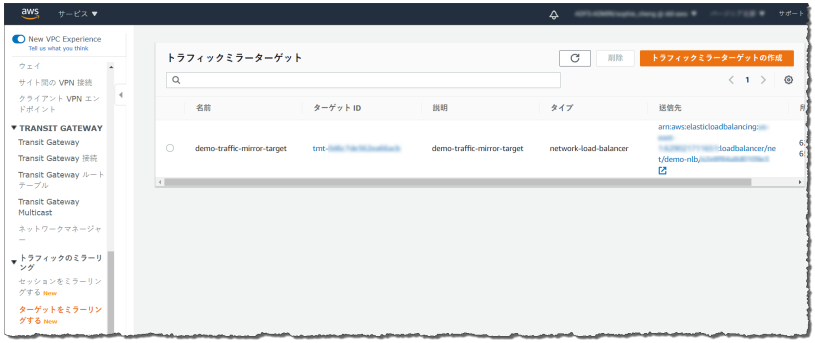
      たとえば「`demo-traffic-mirror-target`」と入力します。

   g. [ターゲットタイプ] で、[Network Load Balancer] を選択します。

   h. [ターゲット] で、トラフィックミラーターゲットとして Network Load Balancer を選択します。

      たとえば [demo-nlb] を選択します。

i. [作成] をクリックします。



8. トラフィックミラーセッションを設定します。

   a. ナビゲーションペインで、[トラフィックのミラーリング] > [セッションをミラーリングする] の順に選択します。

   b. [トラフィックミラーセッションの作成] を選択します。

   c. [名前タグ] に、トラフィックミラーセッションの名前を入力します。

      たとえば「`demo-traffic-mirror-session`」と入力します。

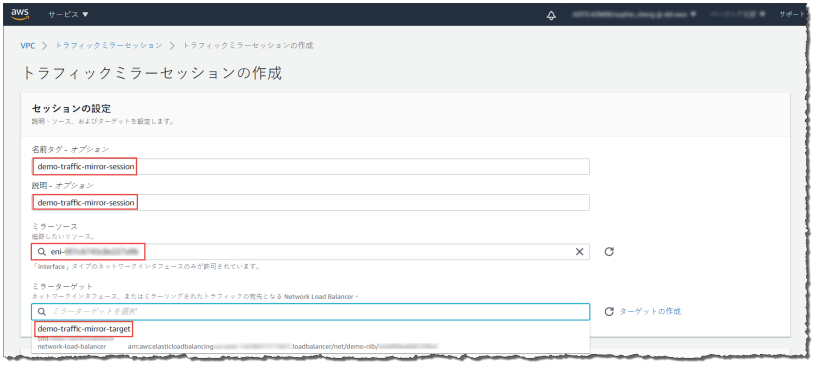
   d. (オプション) [説明] に、トラフィックミラーセッションの説明を入力します。

      たとえば「`demo-traffic-mirror-session`」と入力します。

   e. [ミラーソース] で、監視するインスタンスのネットワークインタフェースを選択します。

   f. [ミラーターゲット] で、トラフィックミラーターゲットを選択します。

たとえば [demo-traffic-mirror-target] を選択します。



g. [追加設定] で、次の手順を実行します。

- [セッション数] に、セッション番号「1」を入力します。

  セッション番号は、次の場合にトラフィックミラーセッションを評価する順序を決定します。

  - インタフェースが複数のセッションで使用されている場合
  - インタフェースが異なるトラフィックミラーターゲットとトラフィックミラーフィルタで 使用されている場合

  トラフィックは一度だけミラーリングされます。「1」は優先度が最も高いことを示します。有効な値は 1〜32766 です。

- (オプション) [VNI] に、トラフィックミラーセッションに使用する VXLAN ID を入力します。

  詳細については、https://tools.ietf.org/html/rfc7348 を参照してください。

  値を指定しない場合、AWS では未使用の番号がランダムに割り当てられます。

- (オプション) [パケット長] に、ミラーリングする各パケット内のバイト数を入力します。

  パケット全体をミラーリングしない場合は、ミラーリングする各パケット内のバイト数を [パケット長] に設定します。たとえ

ば、この値を 100 に設定すると、フィルタ条件を満たす VXLAN ヘッダの後の最初の 100 バイトがターゲットにコピーされます。

パケット全体をミラーリングするには、このフィールドに値を入力しないでください。

- [フィルタ] で、ミラーリングするトラフィックを決定するトラフィックミラーフィルタを 選択します。

  たとえば [demo-traffic-mirror-filter] を選択します。

- (オプション) [タグ] セクションで、タグを追加または削除します。

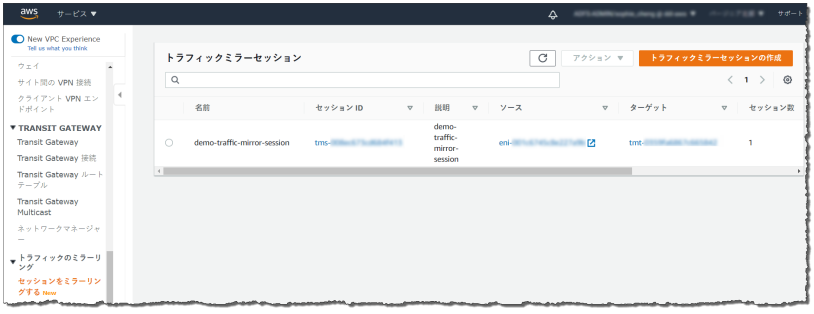
設定の例を次に示します。

- [セッション数] に、セッション番号「1」を入力します。
- [VNI] の値は空のままにします。AWS によってランダムな番号が割り当てられます。
- [パケット長] の値は空のままにします。AWS によってパケット全体がミラーリングされます。
- [フィルタ] で、[demo-traffic-mirror-filter] を選択します。

h. [作成] をクリックします。

注意

詳細については、https://docs.aws.amazon.com/vpc/latest/mirroring/working-with-traffic-mirroring.html を参照してください。



9. 監視する送信元が複数ある場合、前述の手順を繰り返して、さらにトラフィックミラーセッションを作成します。

第 4 章

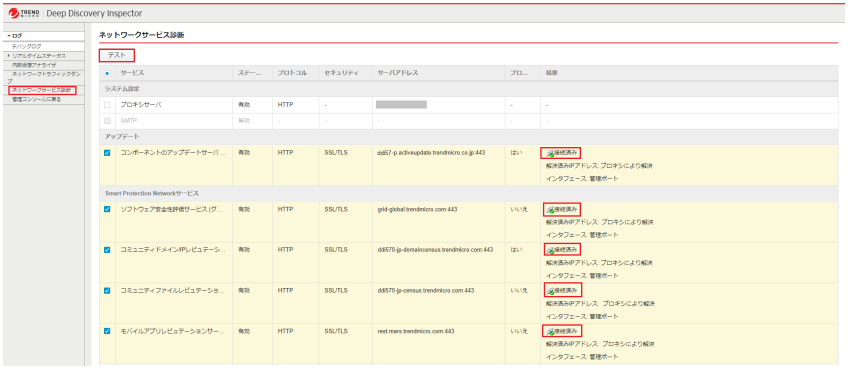
導入のテストとトラブルシューティング

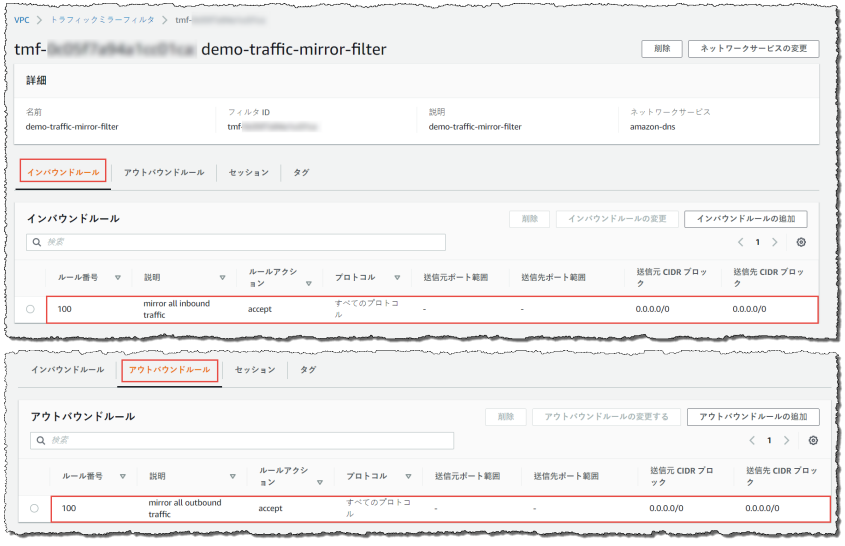
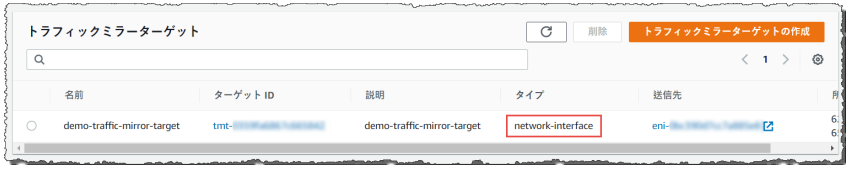
チェック項目

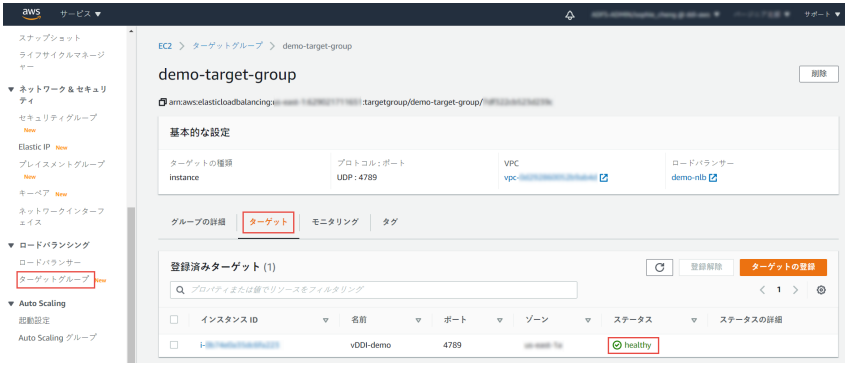
導入が成功していることを次のチェック項目で確認します。

表 4-1. チェック項目

番号	説明
1	IPv4 アドレスを使用して、Deep Discovery Inspector 仮想アプライアンスの管理コンソールにログインします。 管理 IP アドレスは、次の手順により Amazon EC2 コンソールで確認できます。 1. https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。 2. ナビゲーションペインで [インスタンス] を選択します。 3. Deep Discovery Inspector 仮想アプライアンスを選択します。 4. [アクション] > [ネットワーキング] > [IP アドレスの管理] の順に選択します。 5. [eth1] を展開します。[プライベート IP アドレス] に、Deep Discovery Inspector 仮想アプライアンスの管理コンソールの IP アドレスが表示されています。 

番号	説明
2	アクティベーションコードを使用して、Deep Discovery Inspector アプライアンスをアクティブにします。
3	Deep Discovery Inspector アプライアンスのコンポーネントをアップデートします。
4	次の手順に従って Deep Discovery Inspector アプライアンスにネットワークサービス診断テストを実行し、すべてのテストが成功することを確認します。 1. `https://<仮想アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動して、[ネットワークサービス診断] をクリックします。 2. 有効なサービスを 1 つ以上選択して、[テスト] をクリックします。 3. 接続に問題がなければ、テストしたすべてのサービスの結果は [接続] になります。 

番号	説明
5	トラフィックミラーフィルタに、インバウンドトラフィックとアウトバウンドトラフィックの両方で HTTP プロトコルを許可するルールが含まれていることを確認します。 
6	Deep Discovery Inspector をトラフィックミラーターゲットとして導入する場合は、[demo-traffic-mirror-target] などのミラーターゲットが、Deep Discovery Inspector 仮想アプライアンスを送信先として設定されていることを確認します。 

番号	説明
7	Deep Discovery Inspector を NLB の背後に導入する場合は、[demo-traffic-mirror-target] などのミラーターゲットが、NLB を送信先として設定されていることを確認してください。 
8	[demo-traffic-mirror-session] などのミラーセッションについて、次のフィールドが適切に設定されていることを確認します。 • ソース • ターゲット • セッション番号 • フィルタ
9	Deep Discovery Inspector を NLB の背後に導入する場合は、[demo-target-group] などのターゲットグループ内の登録済みインスタンスのステータスが [healthy] であることを確認します。 

導入のテスト

次の手順を実行して、Deep Discovery Inspector 仮想アプライアンスの導入を検証できます。

手順

1. テスト用 EC2 インスタンスのテスト用 Web サイトにアクセスします。

   Linux インスタンスの例を次に示します。

   Deep Discovery Inspector をトラフィックミラーターゲットとして導入している場合や、Deep Discovery Inspector を NLB の背後に導入している場合は、テスト用 EC2 インスタンスをトラフィックミラーソースとして設定する必要があります。

   次の例では「`hxxp`」を「`http`」に置き換えてください。

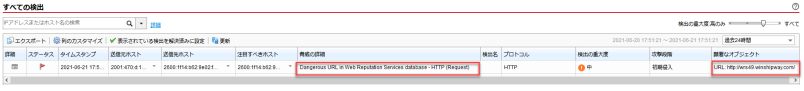
   ```
   ~$ curl hxxp://wrs49.winshipway.com/
   ```

2. Deep Discovery Inspector 仮想アプライアンスで検出を確認します。

   a. Deep Discovery Inspector 仮想アプライアンスの管理コンソールにログインします。

   b. [検出] > [すべての検出] の順に選択します。

   c. Web サイトが検出されていることを確認します。



導入のトラブルシューティング

Amazon EC2 でのパケット受信の問題をトラブルシューティングするためのヒントを次に示します。

- Deep Discovery Inspector 仮想アプライアンスのネットワークトラフィックダンプを使用する

Deep Discovery Inspector 仮想アプライアンスで、[トラブルシューティング] > [ネットワークトラフィックダンプ] の順に選択し、パケットをキャプチャしてデータポートの受信を確認します。

- ネットワーク ACL 設定を検証する

  詳細については、https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html を参照してください。

- セキュリティグループ設定を検証する

  詳細については、https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html を参照してください。トラフィックミラーターゲットの場合、トラフィックミラーターゲットに関連付けられているセキュリティグループ内のトラフィックミラーソースからの [VXLAN トラフィック (UDP port 4789)] を許可する必要があります。

注意

NLB の背後に Deep Discovery Inspector を導入する場合、Deep Discovery Inspector 仮想アプライアンスに関連付けられているセキュリティグループで Deep Discovery Inspector 仮想アプライアンスに対しての [カスタムトラフィック (TCP port 14789)] を許可する必要がある場合があります。

よくある質問

- 59 ページの「AWS に関連した Deep Discovery Inspector 仮想アプライアンスの変更点について教えてください。」
- 64 ページの「Deep Discovery Inspector 仮想アプライアンスでは AWS EC2 自動スケーリングをサポートしていますか?」

- 64 ページの「Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Amazon Machine Image (AMI) の作成をサポートしていますか?」
- 65 ページの「Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Elastic Block Store (EBS) スナップショットの作成をサポートしていますか?」
- 65 ページの「Deep Discovery Inspector では AWS Backup サービスはサポートされますか?」
- 66 ページの「Deep Discovery Inspector の仮想アプライアンスを AWS に配置するために必要な IAM ポリシーについて教えてください。」

AWS に関連した Deep Discovery Inspector 仮想アプライアンスの変更点について教えてください。

AWS 環境に適応するため、Deep Discovery Inspector 仮想アプライアンスにいくつかの軽微な変更が加えられています。これらの変更は主要機能には影響しません。変更内容について次に示します。

- 管理ポートのポートの割り当ての変更

  オンプレミスの Deep Discovery Inspector の管理ポートは、最初の NIC ポート (eth0 と呼ばれる) に固定されます。この変更により、Amazon EC2 コンソールに一貫した情報が提供されます。

  Deep Discovery Inspector 仮想アプライアンスでは、管理ポートのポートの割り当てがポート 1 (eth1 と呼ばれる) に、データポートのポートの割り当てがポート 0 (eth0 と呼ばれる) に変更されています。

- 管理ポートの IPv4 アドレスでの DHCP のみのサポート

IPv4 として設定されている管理ポートでは、DHCP のみがサポートされます。割り当てられている IPv4 アドレスを変更するには、Amazon EC2 コンソールを使用します。

割り当てられている IPv4 アドレスを変更するには、Amazon EC2 コンソールで次の手順を実行します。

1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
2. ナビゲーションペインで [インスタンス] を選択し、Deep Discovery Inspector 仮想アプライアンスを選択します。
3. [アクション] > [ネットワーキング] > [ネットワークインターフェイスのデタッチ] の順に選択します。
4. ドロップダウンリストから [eth1] を選択し、[デタッチ] をクリックします。
5. ナビゲーションペインで [ネットワークインターフェイス] を選択します。

   ネットワークインタフェースを 作成するか (詳細については、https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#create_eni を参照してください)、Deep Discovery Inspector 仮想アプライアンスの 管理ポートに接続する IPv4 アドレスを探します。

6. 前の手順で作成または探したネットワークインタフェースを 選択して、[アタッチ] をクリックします。
7. Deep Discovery Inspector 仮想アプライアンスのインスタンス ID を選択して、[アタッチ] をクリックします。

8. Deep Discovery Inspector 仮想アプライアンスを 再起動します。
9. Deep Discovery Inspector 仮想アプライアンスの 管理ポート (eth1) に新しい IPv4 アドレスが割り当てられていることを確認します。

- 管理ポートの IPv6 アドレスでの DHCP のみのサポート

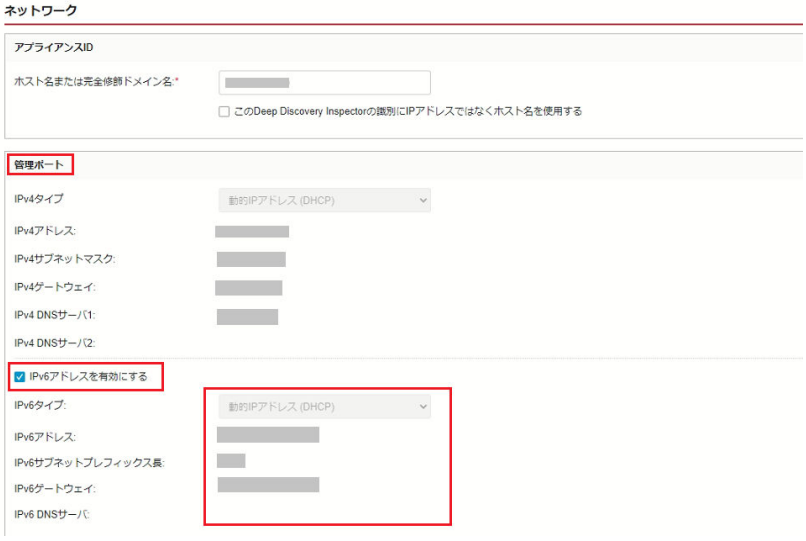
  AWS では、IPv6 アドレスは Amazon EC2 コンソールで管理されます。Amazon EC2 コンソールでネットワークインタフェースに IPv6 が割り当てられている場合、AWS 上の Deep Discovery Inspector 仮想アプライアンスは IPv6 アドレスを自動的に取得します。

  IPv6 アドレスを割り当てるには、次の手順を実行します。

  1. https://console.aws.amazon.com/ec2/で Amazon EC2 コンソールを開きます。
  2. ナビゲーションペインで [インスタンス] を選択します。

3. Deep Discovery Inspector 仮想アプライアンスを選択して、[アクション] > [ネットワーキング] > [IP アドレスの管理] の順に選択します。
4. [eth1] の [IPv6 アドレス] で [新しい IP アドレスの割り当て] を選択します。サブネット範囲内の IPv6 アドレスを指定するか、[自動割り当て] のままにして Amazon が IPv6 アドレスを選択できるようにします。

5. [はい、更新します] をクリックします。
6. Deep Discovery Inspector 仮想アプライアンスの管理コンソールにログインします。
7. [管理] > [システム設定] > [ネットワーク] の順に選択します。
8. [管理ポート] で [Ipv6 アドレスを有効にする] を選択します。
9. [保存] をクリックします。
10. Deep Discovery Inspector 仮想アプライアンスを再起動します。
11. [管理] > [システム設定] > [ネットワーク] の順に選択して、Deep Discovery Inspector 仮想アプライアンスに IPv6 アドレスが割り当てられていることを確認します。



- 内部仮想アナライザの非サポート

  AWS で Deep Discovery Inspector 仮想アプライアンスを起動する場合は、外部仮想アナライザと Sandbox as a Service のみがサポートされます。

Deep Discovery Inspector 仮想アプライアンスでは AWS EC2 自動スケーリングをサポートしていますか?

いいえ。Deep Discovery Inspector 仮想アプライアンスでは AWS EC2 自動スケーリングをサポートしていません。

Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Amazon Machine Image (AMI) の作成をサポートしていますか?

いいえ。Deep Discovery Inspector では、Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの AMI の作成をサポートしていません。

インストール後、Deep Discovery Inspector 仮想アプライアンスは UUID を自動的に作成し、この UUID をトレンドマイクロのグローバルサービスと通信するあらゆる場所で使用します。VM クローンを作成すると、制限付きサービスの状態ステータスに異常が生じます。

Deep Discovery Inspector 仮想アプライアンスがインスタンス ID の変更を検出した場合、Deep Discovery Inspector 仮想アプライアンスの管理コンソールに警告メッセージが表示されます。

Deep Discovery Inspector では Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの Elastic Block Store (EBS) スナップショットの作成をサポートしていますか?

いいえ。Deep Discovery Inspector では、Deep Discovery Inspector 仮想アプライアンスの EC2 インスタンスからの EBS スナップショットの作成をサポートしていません。

インストール後、Deep Discovery Inspector 仮想アプライアンスは UUID を自動的に作成し、この UUID をトレンドマイクロのグローバルサービスと通信するあらゆる場所で使用します。VM クローンを作成すると、制限付きサービスの状態ステータスに異常が生じます。

Deep Discovery Inspector 仮想アプライアンスがインスタンス ID の変更を検出した場合、Deep Discovery Inspector 仮想アプライアンスの管理コンソールに警告メッセージが表示されます。

Deep Discovery Inspector では AWS Backup サービスはサポートされますか?

Deep Discovery Inspector では AWS Backup サービスはサポートされません。

インストール後、Deep Discovery Inspector 仮想アプライアンスは UUID を自動的に作成し、この UUID をトレンドマイクロのグローバルサービスと通信するあらゆる場所で使用します。VM クローンを作成すると、統合サービスの状態ステータスに異常が生じます。

Deep Discovery Inspector がインスタンス ID の変更を検出した場合、Deep Discovery Inspector 仮想アプライアンスの管理コンソールに警告メッセージが表示されます。

Deep Discovery Inspector の仮想アプライアンスを AWS に配置するために必要な IAM ポリシーについて教えてください。

IAM (Identity and Access Management) とは、AWS の機能で、誰にリソースの使用を認証および認可するかを制御するために使用できます。Deep Discovery Inspector を配置するには、IAM ユーザに次の権限があることを確認してください。

AWS サービス	ポリシー名
EC2 インスタンス	• AmazonEC2FullAccess • IAMReadOnlyAccess • AllowAssumeCIEC2Deployment • AmazonEC2SpotFleetTaggingRole
EC2 のネットワークとセキュリティ	• AmazonEC2FullAccess • IAMReadOnlyAccess • AllowAssumeCIEC2Deployment • AmazonEC2SpotFleetTaggingRole
EC2 の負荷分散	• AmazonEC2FullAccess • IAMReadOnlyAccess • AllowAssumeCIEC2Deployment • AmazonEC2SpotFleetTaggingRole

AWS サービス	ポリシー名
VPC トラフィックミラーリング	• AmazonEC2FullAccess • IAMReadOnlyAccess • AllowAssumeCIEC2Deployment • AmazonEC2SpotFleetTaggingRole
AWS Marketplace	AWSMarketplaceManageSubscriptions
AWS Compute Optimizer の調査結果	ComputeOptimizerReadOnlyAccess

索引