



Citrix ADC 12.1

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントのコンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使いの Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負わないものとします。

Contents

Citrix ADC の製品概要	3
Citrix ADC アプライアンスはネットワークのどこに適合しますか?	6
Citrix ADC アプライアンスとクライアント/サーバーとの通信方法	8
Citrix ADC 製品ラインの概要	15
ハードウェアをインストールします	17
Citrix ADC アプライアンスにアクセスする	18
ADC の初回構成	22
Citrix ADC の導入を保護する	22
高可用性の構成	23
RPC ノードのパスワードを変更	27
FIPS アプライアンスの初回構成	28
一般的なネットワークトポロジ	32
システム管理設定	36
システム設定	37
パケット転送モード	38
ネットワークインターフェイス	44
クロック同期	45
DNS の構成	46
SNMP 構成	48
構成を確認する	52
Citrix ADC アプライアンスでトラフィックを負荷分散する	55
負荷分散	57
パーシステンス設定	60

負荷分散設定を保護する機能の構成	66
一般的な負荷分散シナリオ	69
圧縮による負荷分散トラフィックの速度向上	72
SSL による負荷分散トラフィックのセキュリティ保護	78
一目でわかる機能	96
アプリケーションスイッチングとトラフィック管理機能	96
アプリケーションの速度向上機能	101
アプリケーションセキュリティとファイアウォール機能	101
アプリケーションの可視性機能	104

Citrix ADC の製品概要

April 21, 2022

このトピックでは、Citrix ADC アプライアンスの基本的な機能と構成の詳細について説明します。ネットワーク機器を設置および構成するシステムおよびネットワーク管理者は、この内容を参照してください。

Citrix ADC について

Citrix ADC アプライアンスは、アプリケーション固有のトラフィックを分析し、Web アプリケーションのレイヤー 4～レイヤー 7 (L4～L7) ネットワークトラフィックを、インテリジェントに分散、最適化、および保護するアプリケーションスイッチです。たとえば、Citrix ADC アプライアンスは、長時間持続する TCP 接続の代わりに、個別の HTTP 要求に基づいて負荷分散を行います。負荷分散機能は、サーバーの障害を遅らせ、クライアントとの切断を少なくします。ADC の機能は大まかに次のように分類されます：

1. データの切り替え
2. ファイアウォールのセキュリティ
3. 最適化
4. ポリシーインフラストラクチャ
5. パケットフロー
6. システムの制限

データの切り替え

アプリケーションサーバーの前に Citrix ADC を導入すれば、クライアント要求を送信する方法によって、トラフィックの最適な分散を実現できます。管理者は、HTTP または TCP 要求の本文に含まれる情報と、URL、アプリケーションデータタイプ、または Cookie などの L4～L7 ヘッダー情報に基づいて、アプリケーショントラフィックをセグメント化できます。多数の負荷分散アルゴリズムと広範なサーバーヘルスチェックによって、クライアント要求が適切なサーバーに確実に送信されるので、アプリケーションの可用性が向上します。

ファイアウォールのセキュリティ

Citrix ADC のセキュリティおよび保護機能は、アプリケーションレイヤー攻撃から Web アプリケーションを保護します。ADC アプライアンスでは適正なクライアント要求を許可して、不正な要求をブロックできます。サービス拒否 (Denial Of Service: DoS) 攻撃に対する防御機能を組み込んでおり、サーバーに大きな負担をかけるアプリケーショントラフィックの適正なサージから保護する機能をサポートしています。組み込まれたファイアウォールは、バッファオーバーフローの悪用、SQL インジェクション、クロスサイトスクリプト攻撃など、アプリケーション層の攻撃から Web アプリケーションを保護します。また、ファイアウォールは、企業の機密情報と重要な顧客データを保護する、個人情報盗難保護機能を備えています。

最適化

最適化は、SSL (Secure Sockets Layer) 処理、データ圧縮、クライアントキープアライブ、TCP バッファリング、サーバーからの静的および動的コンテンツのキャッシュなど、リソースを消費する処理をオフロードします。これにより、サーバーファーム内のサーバーのパフォーマンスが向上し、アプリケーションの処理速度が上昇します。ADC アプライアンスは、複数の透過的な TCP 最適化をサポートして、長い待ち時間と混雑したネットワークリンクによって発生する問題を緩和し、クライアントまたはサーバーの設定変更を行わずにアプリケーションのデリバリーを高速化します。

ポリシーインフラストラクチャ

「ポリシー」は、Citrix ADC のトラフィックフィルタリングと管理の詳細を定義し、「式」と「アクション」の 2 つの部分で構成されます。式は、ポリシーと一致する要求の種類を定義します。アクションは、要求が式と一致した場合に、ADC アプライアンスが実行する処理を示します。たとえば、式で特定の URL パターンをセキュリティ攻撃と一致させ、接続をドロップまたはリセットするよう設定します。各ポリシーには優先度があり、優先度によってポリシーを評価する順序が決定されます。

ADC アプライアンスがトラフィックを受信した場合、該当するポリシーの一覧によってトラフィックの処理方法が決定されます。一覧の各ポリシーには 1 つまたは複数の式が含まれており、それらが一緒になって、ポリシーと一致するために接続が満たす必要のある条件を定義します。

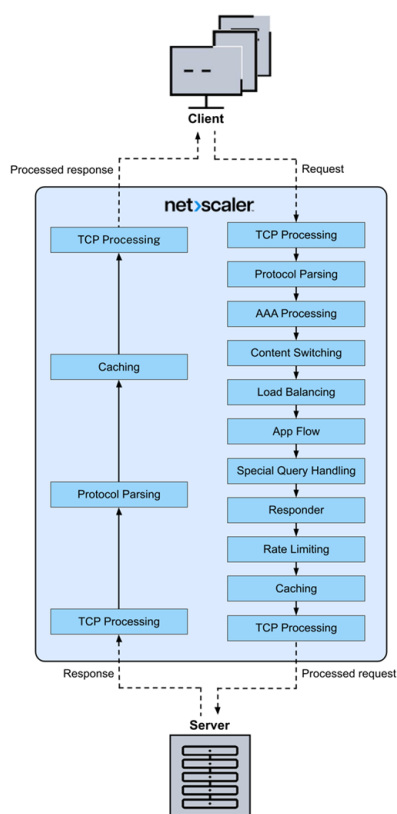
書き換えポリシーを除くすべてのポリシータイプで、ADC アプライアンスは要求と一致する最初のポリシーのみを実行します。書き換えポリシーの場合、ADC アプライアンスは順にポリシーを評価し、関連するアクションを順に実行します。必要な結果を得るには、ポリシーの優先度が重要です。

パケットフロー

要件に応じて、複数の機能を構成することを選択できます。たとえば、圧縮と SSL オフロードの両方を構成できます。この場合、発信パケットは圧縮されてから暗号化されて、クライアントに送信されます。

次の図は、Citrix ADC アプライアンスの DataStream パケットフローを示しています。DataStream は、MySQL と MS SQL のデータベースでサポートされています。

次の図は、Citrix ADC アプライアンスの DataStream パケットフローを示しています。DataStream は、MySQL と MS SQL のデータベースでサポートされています。DataStream 機能に関する情報については、「DataStream」を参照してください



注: コンテンツスイッチ仮想サーバーのトラフィックの場合、アプライアンスは次の順序でポリシーを評価します:

1. グローバルオーバーライドにバインドされる。
2. 負荷分散仮想サーバーにバインドされる。
3. コンテンツスイッチ仮想サーバーにバインドされる。
4. グローバルデフォルトにバインドされる。

このように、ポリシー規則が true で、gotopriorityexpression が END の場合、それ以上のポリシー評価を停止します。

コンテンツスイッチでは、負荷分散仮想サーバーが選択されていないか、コンテンツスイッチ仮想サーバーにバインドされていない場合、コンテンツスイッチ仮想サーバーにのみバインドされているレスポンスポリシーを評価します。

システムの制限

Citrix ADC ソフトウェア 9.2 以降をインストールする場合、Citrix ADC の各機能にはシステム制限があります。詳しくは、Citrix の記事 [CTX118716](#) を参照してください。

Citrix ADC アプライアンスはネットワークのどこに適合しますか？

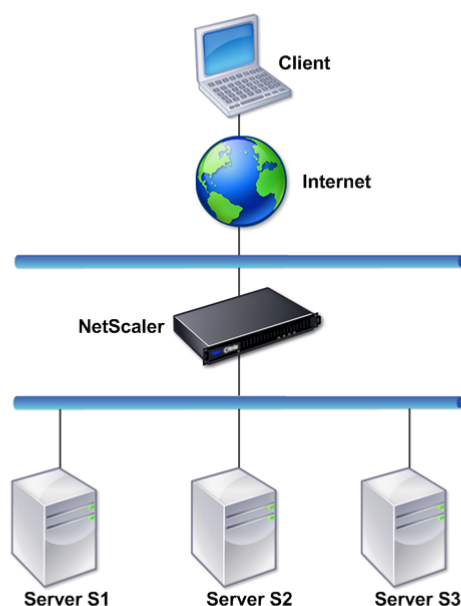
April 25, 2022

NetScaler アプライアンスはクライアントとサーバーの間に設置され、クライアント要求とサーバー応答は Citrix ADC アプライアンスを経由します。一般的な設置では、アプライアンス上で構成された仮想サーバーによって接続ポイントが提供され、クライアントはこれを使用してアプライアンスの背後にあるアプリケーションにアクセスします。この場合、アプライアンスは仮想サーバーに関連付けられたパブリック IP アドレスを所有し、実際のサーバーはプライベートネットワーク内で分離されています。また、アプライアンスを L2 ブリッジや L3 ルーターとして透過モードで動作させたり、これらのモードとそのほかのモードの特徴を組み合わせたりできます。

物理的な展開モード

クライアントとサーバーの間に論理的に設置される Citrix ADC アプライアンスは、インラインまたはワンアームのいずれかの物理モードで展開できます。インラインモードでは、複数のネットワークインターフェイスが異なる Ethernet セグメントに接続され、アプライアンスはクライアントとサーバーの間に配置されます。アプライアンスは、各クライアントネットワークに対する個別のネットワークインターフェイスと、各サーバーネットワークに対する個別のネットワークインターフェイスを持ちます。この構成では、アプライアンスとサーバーを異なるサブネット上に配置できます。アプライアンスの L4~L7 機能を透過的に利用して、サーバーをパブリックネットワーク内に配置し、クライアントがアプライアンスを介してサーバーに直接アクセスするよう構成できます。通常は、実際のサーバーを抽象化した仮想サーバー（後述）を構成します。次の図は、一般的なインライン展開の例を示しています。

図 1: インライン展開



ワンアームモードでは、アプライアンスの 1 つのネットワークインターフェイスのみが、Ethernet セグメントに接続されます。この場合のアプライアンスは、ネットワークのクライアント側とサーバー側を分離せずに、構成済みの仮想サーバーを介してアプリケーションへのアクセスを提供します。一部の環境では、ワンアームモードを使用すると、Citrix ADC の設定に必要なネットワーク変更を簡略化することができます。

インライン（ツーアーム）およびワンアーム展開の例については、「[一般的なネットワークトポロジを理解する](#)」を参照してください。

L2 デバイスとしての Citrix ADC

L2 デバイスとして機能する Citrix ADC アプライアンスは、L2 モードで動作すると言われています。L2 モードでは、以下のすべての条件が満たされている場合に、ADC アプライアンスがネットワークインターフェイス間でパケットを転送します。

- パケットの宛先が、別のデバイスの MAC（Media Access Control: メディアアクセスコントロール）アドレスである。
- 宛先 MAC アドレスが別のネットワークインターフェイス上にある。
- ネットワークインターフェイスが、同じ VLAN（Virtual LAN: 仮想 LAN）のメンバーである。

デフォルトでは、すべてのネットワークインターフェイスが定義済み VLAN（VLAN 1）のメンバーになります。ARP（Address Resolution Protocol: アドレス解決プロトコル）要求および応答は、同じ VLAN のメンバーであるすべてのネットワークインターフェイスに転送されます。ブリッジループを避けるため、別の L2 デバイスが Citrix ADC アプライアンスと並行して動作している場合、L2 モードを無効にする必要があります。

L2 と L3 モードがどのように相互作用するかについて詳しくは、「[パケット転送モード](#)」を参照してください。

L2 モードの構成については、「[パケット転送モード](#)」の「レイヤー 2 モードの有効化と無効化」を参照してください。

パケット転送デバイスとしての Citrix ADC

Citrix ADC アプライアンスは、パケット転送デバイスとして機能できます。この動作モードは L3 モードと呼ばれます。L3 モードを有効にすると、アプライアンスに属してない IP アドレス宛のすべてのユニキャストパケットがその宛先に転送されます。アプライアンスは、VLAN 間でパケットをルーティングすることもできます。

通常、L2 と L3 のどちらの動作モードでも、以下に含まれるパケットはアプライアンスによりドロップされます。

- マルチキャストフレーム
- アプライアンスの MAC アドレス（非 IP かつ非 ARP）宛の不明なプロトコルフレーム
- スパニングツリープロトコル（BridgeBPDU がオンになっていない場合）

L2 と L3 モードがどのように相互作用するかについて詳しくは、「[パケット転送モード](#)」を参照してください。

L3 モードの構成については、「[パケット転送モード](#)」を参照してください。

Citrix ADC アプライアンスとクライアント/サーバーとの通信方法

April 21, 2022

Citrix ADC アプライアンスは通常、サーバーファームの前に展開され、クライアント側で構成を変更しなくても、クライアントとサーバーの透過的な TCP プロキシとして機能します。この基本的な動作モードは「Request Switching 技術」と呼ばれ、Citrix ADC 機能の中核を成しています。Request Switching により、アプライアンスは TCP 接続を多重化してオフロードし、固定接続を維持し、要求（アプリケーションレイヤー）レベルでトラフィックを管理することができます。これらの機能が実現されるのは、アプライアンスが HTTP 要求をその TCP 接続から分離できるからです。

構成によっては、アプライアンスが要求をサーバーに転送する前に、トラフィックを処理する場合があります。たとえば、クライアントがサーバー上の安全なアプリケーションにアクセスしようとする場合に、アプライアンスは必要な SSL 処理を実行してから、トラフィックをサーバーに送信することがあります。

サーバーリソースへの効率的で安全なアクセスを実現するため、アプライアンスは、Citrix ADC 所有 IP アドレスと呼ばれる IP アドレスのセットを使用します。ネットワークトラフィックを管理するには、Citrix ADC 所有 IP アドレスを、構成の構築ブロックになる仮想エンティティに割り当てます。たとえば、負荷分散を構成するには、仮想サーバーを作成し、クライアント要求を受信してサービスに配布します。これらのサービスは、サーバー上のアプリケーションとして振る舞うエンティティです。

Citrix ADC 所有 IP アドレスについて

Citrix ADC アプライアンスでは、プロキシとして機能するためにさまざまな IP アドレス（「Citrix ADC 所有 IP アドレス」）が使用されます。主な Citrix ADC 所有 IP アドレスは、次のとおりです。

- Citrix ADC IP（NSIP）アドレス

NSIP アドレスは、アプライアンス自体に対する管理アクセスや一般的なシステムアクセス、および高可用性構成のアプライアンス間の通信用の IP アドレスです。

- 仮想サーバー IP（VIP）アドレス

VIP アドレスは仮想サーバーに関連付けられた IP アドレスです。クライアントが接続するパブリック IP アドレスです。広範なトラフィックを管理するアプライアンスでは、多くの VIP が構成されます。

- サブネット IP（SNIP）アドレス

SNIP アドレスは、接続の管理とサーバーの監視で使用します。各サブネットに複数の SNIP アドレスを指定できます。SNIP アドレスは VLAN にバインドできます。

- IP セット

IP セットは、アプライアンス上で SNIP として構成される IP アドレスのセットです。IP セットには、そのセットに含まれる IP アドレスの用途を識別するためのわかりやすい名前を付けます。

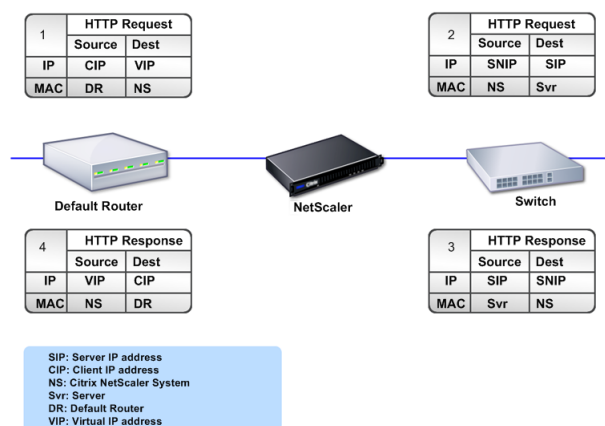
- ネットプロファイル

ネットプロファイル（ネットワークプロファイル）には、1 つの IP アドレスまたは IP セットが含まれます。ネットプロファイルは負荷分散またはコンテンツスイッチ仮想サーバー、サービス、サービスグループ、またはモニターにバインドされます。アプライアンスが物理サーバーまたはピアと通信するときは、このプロファイルでソース IP アドレスとして指定されているアドレスが使用されます。

トラフィックフローの管理方法

Citrix ADC アプライアンスは TCP プロキシとして機能するので、IP アドレスを変換してから、パケットをサーバーに送信します。仮想サーバーを構成した場合、クライアントはサーバーに直接接続する代わりに Citrix ADC 上の VIP に接続します。仮想サーバーの設定に基づく判断として、アプライアンスは適切なサーバーを選択し、クライアントの要求をそのサーバーに送信します。デフォルトでは、次の図に示すように、アプライアンスは SNIP アドレスを使用して、サーバーとの接続を確立します。

図 1: 仮想サーバーベースの接続



仮想サーバーがない場合、アプライアンスは受信した要求をサーバーへ透過的に転送します。この動作は、透過モードと呼ばれます。透過モードで動作している場合、アプライアンスは、着信したクライアント要求のソース IP アドレスを SNIP アドレスに変換しますが、宛先 IP アドレスは変更しません。このモードが動作するには、L2 または L3 モードが適切に構成されている必要があります。

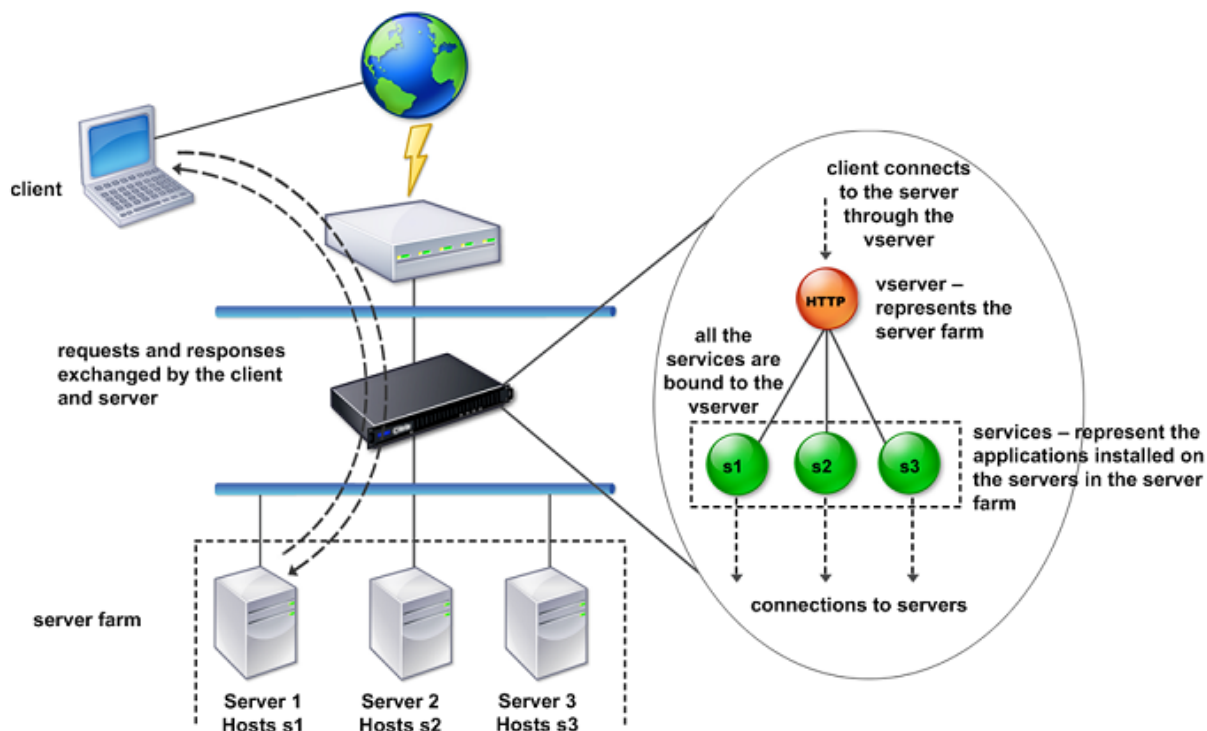
サーバーが実際のクライアント IP アドレスを必要とする場合には、アプライアンスを構成して、クライアント IP アドレスを追加フィールドとして挿入して HTTP ヘッダーを変更するか、またはサーバーとの接続に SNIP ではなくクライアント IP アドレスを使用することができます。

トラフィック管理構築ブロック

通常、Citrix ADC アプライアンスの構成は、トラフィック管理用の構築ブロックとして動作する一連の仮想エンティティで構築されます。この構築ブロックの手法により、トラフィックフローを分離できます。仮想エンティティは抽象型であり、通常、トラフィックを処理するための IP アドレス、ポート、およびプロトコルハンドラーを表しています。クライアントは、これらの仮想エンティティを介して、アプリケーションとリソースにアクセスします。最もよく使用されるエンティティは、「仮想サーバー」と「サービス」です。仮想サーバーはサーバーファームまたはリモートネットワーク内のサーバーグループとして振る舞い、サービスは各サーバー上の個々のアプリケーションとして機能します。

ほとんどの機能とトラフィックの設定値は、仮想エンティティを介して有効化されます。たとえば、特定の仮想サーバー経由でサーバーファームに接続するクライアントへのすべてのサーバー応答が、アプライアンスにより圧縮されるように構成できます。特定の環境に合わせてアプライアンスを構成するには、適切な機能を確認して仮想エンティティの正しい組み合わせを選択し、それらの機能を提供する必要があります。ほとんどの機能は、相互にバインドされた仮想エンティティをカスケードすることで提供されます。この場合の仮想エンティティは、提供されるアプリケーションの最終的な構造に組み込まれるブロックのようなものです。仮想エンティティを追加、削除、変更、バインド、有効化、および無効化して、機能を構成できます。次の図は、ここで説明されている概念を示しています。

図 2: トラフィック管理構築ブロックのしくみ

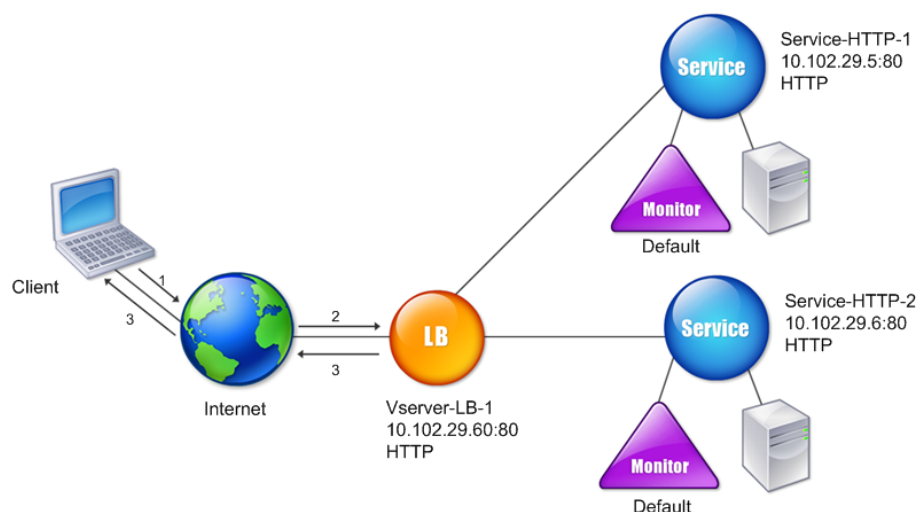


シンプルな負荷分散構成

次の図の例では、Citrix ADC アプライアンスがロードバランサーとして機能するように構成されています。この構成では、負荷分散に固有の仮想エンティティを構成し、それらを特定の順序でバインドする必要があります。ロードバランサーとして機能する場合、アプライアンスはクライアント要求を複数のサーバー間に分散して、リソース使用率を最適化します。

一般的な負荷分散構成の基本的な構築ブロックは、サービスと負荷分散仮想サーバーです。サービスはサーバー上のアプリケーションとして振る舞い、仮想サーバーはクライアントが接続する単一の IP アドレスを提供してサーバーを抽象化します。クライアント要求がサーバーに送信されるようにするため、各サービスを仮想サーバーにバインドする必要があります。つまり、各サーバーに対してサービスを作成し、サービスを仮想サーバーにバインドする必要があります。クライアントは VIP アドレスを使用して Citrix ADC アプライアンスに接続します。アプライアンスは VIP アドレスにクライアント要求を受信すると、負荷分散アルゴリズムによって決定されたサーバーに要求を送信します。負荷分散機能は、モニターと呼ばれる仮想エンティティを使用して、特定の構成済みサービス（サーバーおよびアプリケーション）が要求を受信できるかどうかを追跡します。

図 3: 負荷分散仮想サーバー、サービス、およびモニター



負荷分散アルゴリズムを構成するほか、負荷分散構成の動作やパフォーマンスに関する複数のパラメーターを構成できます。たとえば、送信元の IP アドレスに基づいてパーシステンスが維持されるように仮想サーバーを構成できます。この場合、特定の IP アドレスからのすべての要求が同じサーバーに送信されます。

仮想サーバーについて

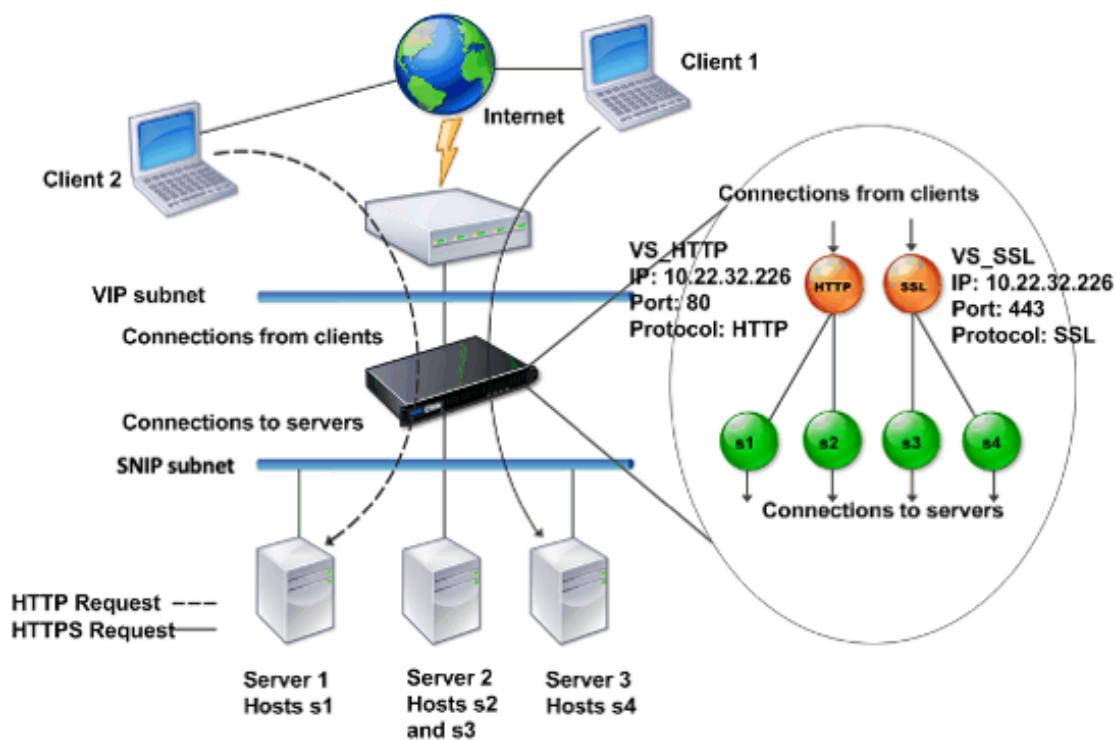
仮想サーバーは名前付きの Citrix ADC エンティティであり、外部クライアントはそのサーバー上でホストされたアプリケーションにアクセスします。仮想サーバーは英数字名、仮想 IP (VIP) アドレス、ポート、およびプロトコルによって表されます。仮想サーバーの名前はローカル上でのみ意味を持ち、仮想サーバーを識別しやすくするために指定されます。クライアントがサーバー上のアプリケーションにアクセスを試みる場合、クライアントは物理サーバーの IP アドレスではなく、VIP に要求を送信します。アプライアンスが VIP アドレスで要求を受信すると、仮想サーバーでの接続を終了して、クライアントに代わってサーバーとの独自の接続を使用します。仮想サーバーのポートおよびプロトコル設定値によって、その仮想サーバーが振る舞うアプリケーションが決定されます。たとえば、Web サーバーは、ポートとプロトコルがそれぞれ 80 と HTTP に設定された仮想サーバーとサービスによって構成されます。複数の仮想サーバーで同じ VIP アドレスを使用して、異なるプロトコルとポートを使用することもできます。

仮想サーバーは、さまざまな機能の配信ポイントとして動作します。圧縮、キャッシュ、SSL オフロードなどのほとんどの機能は、通常、仮想サーバーで有効になっています。アプライアンスは VIP アドレスで要求を受信すると、要求を受信したポートとそのプロトコルによって、適切な仮想サーバーを選択します。次にアプライアンスは、仮想サ

サーバーに構成されている機能に従って要求を処理します。

ほとんどの場合、仮想サーバーはサービスと協調して動作します。複数のサービスを 1 つの仮想サーバーにバインドすることができます。これらのサービスは、サーバーファーム内の物理サーバーで動作するアプリケーションとして振る舞います。アプライアンスは、VIP アドレスで受信した要求を処理した後、仮想サーバーで設定された負荷分散アルゴリズムの決定に従って、要求をサーバーに転送します。次の図は、これらの概念を示しています。

図 4: 単一の VIP アドレスを持つ複数の仮想サーバー



上の図は、VIP アドレスが同じでポートとプロトコルが異なる、2 つの仮想サーバーで構成された環境を示しています。これらの各仮想サーバーには、2 つのサービスがバインドされています。サービス s1 と s2 は VS_HTTP にバインドされており、サーバー 1 とサーバー 2 の HTTP アプリケーションとして動作しています。サービス s3 と s4 は VS_SSL にバインドされており、サーバー 2 とサーバー 3 の SSL アプリケーションとして動作しています（サーバー 2 は、HTTP アプリケーションと SSL アプリケーションの両方を提供します）。アプライアンスが VIP アドレスで HTTP 要求を受信すると、VS_HTTP の設定値により指定されたとして要求を処理し、サーバー 1 またはサーバー 2 に要求を送信します。同様に、アプライアンスが VIP アドレスで HTTPS 要求を受信すると、VS_SSL の設定値により指定されたとして要求を処理し、サーバー 2 またはサーバー 3 に要求を送信します。

仮想サーバーの IP アドレス、ポート番号、またはプロトコルに特定の値を指定せずに、ワイルドカード文字を使用して指定することもできます。このような仮想サーバーは、ワイルドカード仮想サーバーと呼ばれます。たとえば、特定の VIP の代わりにワイルドカード文字を使用し、特定のポート番号で仮想サーバーを構成した場合、アプライアンスは、そのプロトコルおよびポート宛のすべてのトラフィックをインターセプトして処理します。特定の VIP およびポート番号の代わりにワイルドカード文字を使用して仮想サーバーを構成した場合は、そのプロトコルのすべてのト

ラフィックをインターセプトして処理します。

仮想サーバーは、以下のカテゴリに分類できます。

- 負荷分散仮想サーバー

要求を受信して、適切なサーバーにリダイレクトします。適切なサーバーの選択は、ユーザーが設定したさまざまな負荷分散方式に基づいて行われます。

- キャッシュリダイレクト仮想サーバー

動的コンテンツに対するクライアント要求を配信元のサーバーにリダイレクトし、静的コンテンツに対するクライアント要求をキャッシュサーバーにリダイレクトします。キャッシュリダイレクト仮想サーバーは、通常、負荷分散仮想サーバーと一緒に動作します。

- コンテンツスイッチ仮想サーバー

クライアントが要求したコンテンツに基づいて、トラフィックをサーバーに送信します。たとえば、画像に対するすべてのクライアント要求を、画像のみを処理するサーバーに送信するコンテンツスイッチ仮想サーバーを作成できます。コンテンツスイッチ仮想サーバーは、通常、負荷分散仮想サーバーと一緒に動作します。

- VPN (Virtual Private Network: 仮想プライベートネットワーク) 仮想サーバー

トンネリングされたトラフィックを復号化して、イントラネットアプリケーションに送信します。

- SSL 仮想サーバー

SSL トラフィックを受信して復号化し、適切なサーバーにリダイレクトします。適切なサーバーの選択は、負荷分散仮想サーバーの選択と類似しています。

サービスについて

サービスは、サーバー上のアプリケーションとして機能します。通常、サービスは仮想サーバーと組み合わされていますが、仮想サーバーがなくてもアプリケーション固有のトラフィックを管理できます。たとえば、Citrix ADC アプライアンスで Web サーバーアプリケーションとして振る舞う HTTP サービスを作成できます。この Web サーバーでホストされた Web サイトへのアクセスをクライアントが試みると、アプライアンスが HTTP 要求をインターセプトして Web サーバーとの透過的な接続を作成します。

サービス専用モードでは、アプライアンスがプロキシとして機能します。NetScaler はクライアント接続を終了し、SNIP アドレスを使用してサーバーとの接続を確立し、着信したクライアント要求のソース IP アドレスを SNIP アドレスに変換します。クライアントは要求をサーバーの IP アドレスに直接送信しますが、サーバーは要求が SNIP アドレスから送られてきたものと見なします。アプライアンスは IP アドレス、ポート番号、およびシーケンス番号を変換します。

サービスは、機能を適用するポイントでもあります。SSL Acceleration の例を考えてみましょう。この機能を使用するには、SSL サービスを作成して、そのサービスに SSL 証明書をバインドする必要があります。アプライアンスは HTTPS 要求を受信すると、トラフィックを復号化し、クリアテキストとしてサーバーに送信します。サービス専用モードでは、限られたわずかな機能しか設定できません。

サービスは「モニター」と呼ばれるエンティティを使用して、アプリケーションのヘルスを追跡します。すべてのサービスには、サービスタイプに基づく「デフォルトモニター」がバインドされています。モニターで設定された値に従って、アプライアンスは定期的にアプリケーションにプローブを送信し、アプリケーションの状態を判定します。プローブが失敗した場合、アプライアンスはサービスがダウンしたものとマークします。このような場合、アプライアンスは、適切なエラーメッセージでクライアント要求に応答するか、設定された負荷分散ポリシーに従って要求を転送します。

Citrix ADC 製品ラインの概要

January 10, 2023

Citrix ADC の製品ラインは、アプリケーションレベルのセキュリティ、最適化、およびトラフィック管理を単一の統合アプライアンス上に集約して、インターネットおよびプライベートネットワーク経由のアプリケーション配信を最適化します。ユーザーはサーバールームに Citrix ADC アプライアンスを設置し、Citrix ADC アプライアンスを介してすべての接続を管理対象サーバーにルーティングします。次に、有効化された Citrix ADC 機能と設定されたポリシーが、着信および発信トラフィックに適用されます。

Citrix ADC アプライアンスは、既存の負荷分散装置、サーバー、キャッシュ、およびファイアウォールを補完する目的で、ネットワークに統合できます。クライアント側またはサーバー側にソフトウェアを追加する必要はなく、Citrix ADC の Web ベースの GUI および CLI 構成ユーティリティを使用して設定することができます。

このセクションでは、以下のトピックについて説明します：

- Citrix ADC ハードウェアプラットフォーム
- Citrix ADC エディション
- Citrix ADC ハードウェアでサポートされるリリース
- サポートされているブラウザー

Citrix ADC ハードウェアプラットフォーム

Citrix ADC ハードウェアは、さまざまなハードウェア仕様を持つさまざまなプラットフォームで利用できます。

[Citrix ADC MPX ハードウェアプラットフォーム](#)

[Citrix ADC SDX ハードウェアプラットフォーム](#)

Citrix ADC エディション

Citrix ADC オペレーティングシステムには、次の 3 つのエディションがあります。

- Standard

- 詳細設定
- Premium

Standard エディションと Advanced エディションでは、使用できる機能が制限されています。すべてのエディションで機能のライセンスが必要です。

Citrix ADC ソフトウェアエディションの詳細については、[Citrix ADC Editions データシート](#)を参照してください。

ライセンスを取得してインストールする方法については、「[ライセンス](#)」を参照してください。

Citrix ADC ハードウェアでサポートされているリリース

すべての Citrix ADC ハードウェアプラットフォームおよびこれらのプラットフォームでサポートされているソフトウェアリリースについては、次の互換性マトリックス表を参照してください。

[Citrix ADC MPX ハードウェア-ソフトウェア互換性マトリックス](#)

[Citrix ADC SDX ハードウェア-ソフトウェア互換性マトリックス](#)

サポートされているブラウザ

Citrix ADC GUI にアクセスするには、ワークステーションにサポートされている Web ブラウザーが必要です。

次の表に、NetScaler GUI バージョン 12.0、12.1、および 13.0 と互換性のあるブラウザを示します。

オペレーティングシステム	Web ブラウザー	バージョン
Windows 7 以降	Internet Explorer	11、Edge、それ以降
Windows 7 以降	Mozilla Firefox	45 以降
Windows 7 以降	Chrome	60 以降
MAC	Mozilla Firefox	45 以降
MAC	Safari	10.1.1 以降

Citrix ADC 11.1 と互換性のあるブラウザのバージョンは次のとおりです。

オペレーティングシステム	Web ブラウザー	バージョン
Windows 7 以降	Internet Explorer	8、9、10、11、Edge
Windows 7 以降	Mozilla Firefox	45 以降
Windows 7 以降	Chrome	60 以降

オペレーティングシステム	Web ブラウザー	バージョン
MAC	Mozilla Firefox	45 以降
MAC	Safari	10.1.1 以降

ハードウェアをインストールします

January 10, 2023

Citrix ADC アプライアンスをインストールする前に、インストール前のチェックリストを確認してください。

SDX アプライアンスを使用するには、表に記載されているリソースに記載されている手順に従って、以下のタスクを完了する必要があります。指定された順序でタスクを完了します。

タスク

説明

1. 安全、注意、警告、およびその他の情報を読む

製品を設置する前に、知っておく必要のある注意と危険に関する情報をお読みください。

2. インストールの準備

新しいアプライアンスを設置する前に、アプライアンスを開梱し、すべての部品が納品されたことを確認し、サイトとラックを準備し、基本的な電気安全上の注意事項に従ってください。

3. ハードウェアをインストールします

アプライアンスをラックマウントし、トランシーバー（使用可能な場合）を取り付け、アプライアンスをネットワークと電源に接続します。

4. アプライアンスを構成します。

GUI またはシリアルコンソールを使用して、Citrix ADC アプライアンスの初期設定を構成します。

これらのタスクを完了するには、次のドキュメントに記載されている手順に従ってください。

- [Citrix ADC MPX ハードウェアのドキュメント](#)
- [Citrix ADC SDX ハードウェアのドキュメント](#)

Citrix ADC アプライアンスにアクセスする

April 15, 2024

Citrix ADC アプライアンスには、コマンドラインインターフェイス（CLI）と GUI の両方があります。GUI には、アプライアンスを構成するための構成ユーティリティと、ダッシュボードと呼ばれる統計ユーティリティがあります。初回のアクセス用に、すべてのアプライアンスには出荷時にデフォルトの Citrix ADC IP アドレス（NSIP）192.168.100.1 とデフォルトのサブネットマスク 255.255.0.0 が割り当てられています。初回構成時に、新しい NSIP アドレスとそのサブネットマスクを割り当てることができます。

複数の Citrix ADC 装置の展開時に IP アドレスの競合が発生した場合は、以下の点について確認してください：

- ネットワーク上の別のデバイスに既に割り当てられている IP アドレスを、NSIP として選択していないかどうか。
- 複数の Citrix ADC アプライアンスに同じ NSIP を割り当てていないかどうか。
- NSIP は、すべての物理ポートでアクセス可能です。Citrix ADC のポートはホストポートであり、スイッチポートではありません。

次の表は、使用可能なアクセス方法の一覧です。

アクセス方法	ポート	デフォルト IP アドレス（必要/不要）
CLI	Console	×
CLI と GUI	イーサネット	○

コマンドラインインターフェイス

CLI には、ワークステーションをコンソールポートに接続してローカルでアクセスすることも、同じネットワーク上の任意のワークステーションから SSH（Secure Shell）を介して接続してリモートアクセスすることもできます。

コンソールポートを使用したコマンドラインインターフェイスへのログオン

アプライアンスには、ワークステーションに接続するためのコンソールポートがあります。アプライアンスにログオンするには、シリアルクロスオーバーケーブルと、端末エミュレーションプログラムを備えたワークステーションが必要です。

コンソールポートを使用して CLI にログオンするには、次の手順を実行します：

1. コンソールポートをワークステーションのシリアルポートに接続します。詳しくは、「[コンソールケーブルの接続](#)」を参照してください。

2. ワークステーションで、ハイパーターミナルまたはその他のターミナルエミュレーションプログラムを起動します。ログオンプロンプトが表示されない場合は、Enter キーを 1 回または数回押すことが必要な場合があります。
3. [User name] に **nsroot** を入力します。Password に **nsroot** を入力し、パスワードが機能しない場合はアプライアンスのシリアル番号を入力します。シリアル番号のバーコードは、アプライアンスの背面にあります。

SSH を使用したコマンドラインインターフェイスへのログオン

SSH プロトコルを使用すると、同じネットワーク上の任意のワークステーションからアプライアンスにリモートアクセスできます。SSH Version 1 (SSH1) または SSH Version 2 (SSH2) を使用できます。

動作している SSH クライアントがない場合は、以下の SSH クライアントプログラムをダウンロードしてインストールできます。

- PuTTY

複数のプラットフォームでサポートされている、オープンソースソフトウェアです。次のサイトから入手できます。

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

- Vandyke Software SecureCRT

Windows プラットフォームでサポートされている、市販のソフトウェアです。次のサイトから入手できます。

<http://www.vandyke.com/products/securecrt/>

これらのプログラムは Citrix ADC チームによってテストされ、Citrix ADC アプライアンスと正常に動作することが確認されています。そのほかのプログラムも正常に動作する可能性がありますが、テストは実施されていません。

SSH クライアントが正しくインストールされていることを確認するには、対象のクライアントを使用して、SSH 接続を受け付ける、ネットワーク上の任意のデバイスに接続します。

SSH クライアントを使用して Citrix ADC アプライアンスにログオンするには、次の手順を実行します：

1. ワークステーションで、SSH クライアントを起動します。
2. 初期構成には、デフォルトの IP アドレス (NSIP) である 192.168.100.1 を使用します。その後のアクセスでは、初回構成時に割り当てる NSIP を使用します。プロトコルとして SSH1 または SSH2 のいずれかを選択します。
3. [User name] に **nsroot** を入力します。Password に **nsroot** を入力し、パスワードが機能しない場合はアプライアンスのシリアル番号を入力します。シリアル番号のバーコードは、アプライアンスの背面にあります。たとえば、以下のようなものです。

```
1 login as: nsroot
2
3
```

```
4 Using keyboard-interactive authentication.
5
6
7 Password:
8
9
10 Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9
11
12
13
14
15
16 Done
17
18
19 >
20
21 <!--NeedCopy-->
```

Citrix ADC GUI

重要:

Citrix ADC GUI への HTTPS アクセスには、証明書とキーのペアが必要です。ADC では、証明書とキーのペアは内部サービスに自動的にバインドされます。デフォルトのキーサイズは、MPX または SDX アプライアンスで 1024 バイト、VPX インスタンスで 512 バイトです。ただし、最新の Web ブラウザーの多くは 1024 バイト未満のキーを受け入れません。このため、VPX 構成ユーティリティへの HTTPS アクセスがブロックされてしまいます。

また、ライセンスがない状態で MPX アプライアンスを起動して、その後でライセンスを追加してからアプライアンスを再起動すると、証明書のバインドが失われることがあります。

GUI への HTTPS アクセスのために、Citrix ADC に少なくとも 1024 バイトの証明書とキーのペアをインストールすることをお勧めします。また、ADC を起動する前に適切なライセンスをインストールしてください。

GUI には、構成ユーティリティと「ダッシュボード」と呼ばれる統計ユーティリティが含まれています。アプライアンスのイーサネットポートに接続されたワークステーションを介して、これらのツールにアクセスします。

GUI を実行するワークステーションのシステム要件は、次のとおりです。

- Windows ベースのワークステーションの場合は、Pentium 166 MHz 以上のプロセッサが必要です。
- Linux ベースのワークステーションの場合は、Linux カーネル v2.2.12 以降と [glibc](#) バージョン 2.12-11 以降を実行する、Pentium プラットフォームが必要です。32MB 以上の RAM が必要であり、48MB 以上を推奨します。ワークステーションは、ディスプレイをローカルホストに設定し、16 ビットカラーモードで KDE および KWM のウィンドウマネージャーをサポートする必要があります。
- Solaris ベースのワークステーションの場合は、Solaris 2.6、Solaris 7、または Solaris 8 を実行する Sun が必要です。

構成ユーティリティとダッシュボードにアクセスするには、サポートされている Web ブラウザーがワークステーションにインストールされている必要があります。

次のブラウザーがサポートされています。

オペレーティングシステム:

Windows 7

ブラウザー: Internet Explorer (バージョン 9、10、11)、Mozilla Firefox (バージョン 3.6.25 以降)、Google Chrome (最新)。

オペレーティングシステム:

Windows 64 ビット

ブラウザー: Internet Explorer (バージョン 8、9、10、11)、Google Chrome (最新バージョン)

オペレーティングシステム:

MAC

ブラウザー: Mozilla Firefox (バージョン 3.6.25 以降)、Safari (バージョン 5.1.3 以降)、Google Chrome (最新バージョン)

Citrix ADC GUI を使用

構成ユーティリティにログオンしたら、状況依存ヘルプが付属するグラフィックインターフェイスを介して、アプライアンスを構成できます。

GUI にログオンするには、次の手順を実行します:

1. Web ブラウザーを開いて、Citrix ADC IP (NSIP) を HTTP アドレスとして入力します。初回構成がまだ完了していない場合は、デフォルトの NSIP (<http://192.168.100.1>) を入力します。[Citrix Logon] ページが開きます。

注: 2 台の Citrix ADC アプライアンスが高可用性ペアとしてセットアップされている場合は、GUI にアクセスするときにセカンダリ Citrix ADC アプライアンスの IP アドレスを入力しないでください。このような方法でアクセスすると、GUI を使用してセカンダリアプライアンスを構成しても、その変更内容がプライマリ Citrix ADC アプライアンスに適用されません。

2. [User Name] ボックスに「**nsroot**」と入力します。
3. [Password] ボックスに、初回構成時に **nsroot** アカウントに割り当てた管理パスワードを入力し、[Login] をクリックします。パスワードが機能しない場合はアプライアンスのシリアル番号を入力します。シリアル番号のバーコードは、アプライアンスの背面にあります。

オンラインヘルプにアクセスするには、右上隅の [Help] メニューの [Help] を選択します。

統計ユーティリティの使用

ダッシュボード（統計ユーティリティ）は、Citrix ADC アプライアンスのパフォーマンスを監視できる図と表を表示する、ブラウザーベースのアプリケーションです。

ダッシュボードにログオンするには、次の手順を実行します：

1. Web ブラウザーを開いて、NSIP を HTTP アドレスとして入力します。[Citrix Logon] ページが開きます。
2. [User Name] ボックスに「**nsroot**」と入力します。
3. [Password] ボックスに、初回構成時に**nsroot**アカウントに割り当てた管理パスワードを入力します。パスワードが機能しない場合はアプライアンスのシリアル番号を入力します。シリアル番号のバーコードは、アプライアンスの背面にあります。

ADC の初回構成

January 10, 2023

Citrix ADC MPX アプライアンスの初期構成については、「[Citrix MPX アプライアンスの初期構成](#)」を参照してください。

Citrix ADC MPX アプライアンスの初期構成については、「[Citrix MPX アプライアンスの初期構成](#)」を参照してください。

NITRO API

NITRO API を使用して Citrix ADC アプライアンスを構成できます。NITRO では、Representational State Transfer (REST) インターフェイスを介して機能が提供されます。そのため、NITRO アプリケーションはあらゆるプログラミング言語で開発することができます。さらに、Java、.NET、または Python で開発する必要があるアプリケーションの場合、NITRO API は、個別のソフトウェア開発キット (SDK) としてパッケージ化された関連ライブラリを介して提供されます。詳しくは、「[NITRO API](#)」を参照してください。

Citrix ADC の導入を保護する

February 15, 2024

Citrix ADC アプライアンスの展開ライフサイクルを通じてセキュリティを維持するために、次のセキュリティの側面を考慮することをお勧めします。

- 物理的セキュリティ

- アプライアンスのセキュリティ
- Network Security
- 管理と管理

展開が異なれば、セキュリティに関する考慮事項も異なる場合があります。Citrix ADC の安全な導入ガイドラインは、特定のセキュリティ要件に基づいて適切な安全な導入を決定するのに役立つ一般的なセキュリティガイダンスを提供します。

Citrix ADC アプライアンスを安全に展開するためのガイドラインの詳細については、「[Citrix ADC の安全な導入ガイドライン](#)」を参照してください。

高可用性の構成

April 21, 2022

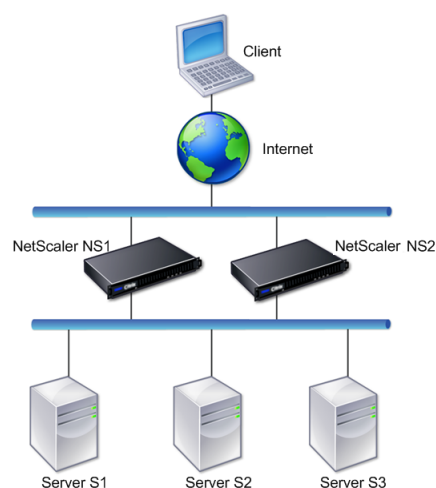
2 台の Citrix ADC アプライアンスを高可用性構成で展開できます。この構成では、1 台の装置がアクティブに接続を受け付けてサーバーを管理し、2 台目の装置は 1 台目の装置を監視します。高可用性構成では、アクティブに接続を受け付けてサーバーを管理する Citrix ADC はプライマリ装置と呼ばれ、もう 1 台はセカンダリ装置と呼ばれます。プライマリ装置が故障した場合は、セカンダリ装置がプライマリになって、アクティブに接続の受け付けを開始します。

高可用性ペアの各 Citrix ADC アプライアンスは、「ハートビートメッセージ」または「ヘルスチェック」と呼ばれる定期的なメッセージを送信してもう一方の装置を監視し、ピアノードのヘルスまたは状態を判定します。プライマリ装置のヘルスチェックが失敗した場合、セカンダリ装置は指定された時間、接続を再試行します。高可用性について詳しくは、「[高可用性](#)」を参照してください。指定された時間内に再試行が成功しない場合、セカンダリ装置は「フェールオーバー」と呼ばれるプロセスによって、プライマリ装置の役割を引き継ぎます。次の図は、2 つの高可用性構成を示しています。1 つはワンアームモード構成で、もう 1 つはツアームモード構成です。

図 1: ワンアームモードでの高可用性



図 2: ツーアームモードでの高可用性



ワンアーム構成では、NS1 と NS2 の両方、およびサーバー S1、S2、S3 がスイッチに接続されています。

ツワーアーム構成では、NS1 と NS2 の両方が 2 つのスイッチに接続されています。サーバー S1、S2、S3 は、2 番目のスイッチに接続されています。クライアントとサーバーの間のトラフィックは、NS1 または NS2 のいずれかを経由します。

高可用性環境をセットアップするには、1 台の ADC アプライアンスをプライマリとして、もう 1 台のアプライアンスをセカンダリとして設定します。各 ADC アプライアンスで次のタスクを実行します。

- ノードを追加します。
- 未使用のインターフェイスの高可用性モニターを無効にします。

ノードを追加

ノードは、ピア Citrix ADC アプライアンスの論理表現です。ID と NSIP でピア装置を識別します。アプライアンスはこれらのパラメーターを使用して、ピアと通信してその状態を追跡します。ノードを追加すると、プライマリ装置とセカンダリ装置は、非同期的にハートビートメッセージを交換します。ノード ID は 64 以下の整数です。

CLI 経由

コマンドラインインターフェイスを使用してノードを追加するには、次の手順に従います。

コマンドプロンプトで次のコマンドを入力し、ノードを追加して構成を確認します。

- add HA node <id> <IP アドレス>
- show HA node <id>

例

```
1  add HA node 0 10.102.29.170
2  Done
3  > show HA node 0
4  1)      Node ID:      0
5          IP:    10.102.29.200 (NS200)
6          Node State: UP
7          Master State: Primary
8          SSL Card Status: UP
9          Hello Interval: 200 msec
10         Dead Interval: 3 sec
11         Node in this Master State for: 1:0:41:50 (days:hrs:min:
           sec)
12  <!--NeedCopy-->
```

GUI 経由

GUI を使用してノードを追加するには、次の手順に従います。

1. **[System] > [High Availability]** に移動します。
2. **[Nodes]** タブで **[Add]** をクリックします。
3. **[Create HA Node]** ページの **[Remote Node IP Address]** テキストボックスに、リモートノードの NSIP アドレス（たとえば、10.102.29.170）を入力します。
4. **[Configure remote system to participate in High Availability setup]** チェックボックスがオンになっていることを確認します。**[Remote System Login Credentials]** の下のボックスに、リモートノードのログイン情報を入力します。
5. **[Turn off HA monitor on interfaces/channels that are down]** チェックボックスをオンにして、ダウンしているインターフェイスでの HA モニターを無効にします。

追加したノードが **[Nodes]** タブの一覧に表示されていることを確認します。

未使用のインターフェイスの高可用性モニターを無効にします

高可用性モニターは、インターフェイスを監視する仮想エンティティです。接続されていない、またはトラフィックに使用されていないインターフェイスのモニターを、無効にする必要があります。ステータスが DOWN になっているインターフェイスでモニターが有効になっている場合、ノードの状態は NOT UP になります。高可用性構成では、プライマリノードが NOT UP 状態になると、高可用性フェールオーバーが行われる可能性があります。以下のような場合、インターフェイスには DOWN のマークが付けられます。

- インターフェイスが接続されていない。
- インターフェイスが正常に動作していない。
- インターフェイスを接続するケーブルが正常に機能していない。

CLI 経由

コマンドラインインターフェイスを使用して未使用のインターフェイスの高可用性モニターを無効化するには、次の手順を実行します

コマンドプロンプトで次のコマンドを入力し、未使用のインターフェイスの高可用性モニターを無効にして構成を確認します。

- `set interface <id> -haMonitor OFF`
- `show interface <id>`

例

```
1 > set interface 1/8 -haMonitor OFF
2 Done
3 > show interface 1/8
4 Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
5 flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
6 MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
7 238h55m44s
8 Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
9 throughput 0
10 RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
11 TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
12 NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
13 Muted(0)
14 Bandwidth thresholds are not set.
15 <!--NeedCopy-->
```

未使用のインターフェイスで高可用性モニターが無効になっている場合、そのインターフェイスの `showinterface` コマンドの出力には「HAMON」が含まれません。

GUI 経由

GUI を使用して未使用のインターフェイスの高可用性モニターを無効にするには、次の手順に従います。

1. [System] > [Network] > [Interfaces] に移動します。
2. モニターを無効にする必要があるインターフェイスを選択します。
3. [開く] をクリックします。[Modify Interface] ダイアログボックスが開きます。
4. [HA Monitoring] で [OFF] をクリックします。
5. [OK] をクリックします。
6. インターフェイスを選択すると、ページ下部の詳細に「HA Monitoring: OFF」が表示されることを確認してください。

RPC ノードのパスワードを変更

April 21, 2022

各アプライアンスがほかの Citrix ADC アプライアンスと通信するには、それらのアプライアンスについての知識 (Citrix ADC アプライアンスでの認証方法など) が必要です。RPC ノードは、構成およびセッション情報のシステム間通信に使用される内部システムエンティティです。1 つの RPC ノードが各 Citrix ADC アプライアンスに存在し、他の Citrix ADC アプライアンスの IP アドレスや認証に使用されるパスワードなどの情報を格納します。他の Citrix ADC アプライアンスに接続する Citrix ADC アプライアンスは、RPC ノード内のパスワードをチェックします。

GUI を使用して **RPC** ノードのパスワードを変更するには

1. [System] > [Network] > [RPC] の順に選択します。
2. **RPC** ペインで、ノードを選択して [Edit] をクリックします。
3. [Configure RPC Node] に、新しいパスワードを入力します。
4. [Source IP Address] に、ピアシステムノードとの通信に使用する既存のノードの IP アドレスを入力します。

← Configure RPC Node

Node IP Address
10.102.126.35

Password ①

Confirm Password

☐ Reset Password

Source IP Address* ①

☒ Secure

☐ Validate Server Certificate

OK Close

5. **[Secure]** を選択し、**[OK]** をクリックします。

注

[Secure] オプションを有効にすると、アプライアンスはそのノードから他の RPC ノードに送信されるすべての RPC 通信を暗号化して、RPC 通信を保護します。

CLI を使用して **RPC** ノードのパスワードを変更するには

コマンドラインで、次のコマンドを入力します：

```
1 set ns rpcNode <IPAddress> {
2   -password }
3   [-secure ( YES | NO )]
4 show ns rpcNode
5 <!--NeedCopy-->
```

例：

```
1 > set ns rpcNode 192.0.2.4 -password mypassword -secure YES
2   Done
3 > show rpcNode
4   .
5   .
6   .
7   IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
8       SrcIP:   *           Secure:  ON
9   Done
10 >
11
12 <!--NeedCopy-->
```

FIPS アプライアンスの初回構成

April 25, 2022

メモ

- FIPS FAQ は次の場所にあります： [FIPS FAQ](#)。
- VPX FIPS 構成については次を参照してください： [Citrix ADC VPX FIPS 認定アプライアンス](#)。

構成ユーティリティへの HTTPS アクセスおよびセキュアリモートプロシージャコールには、証明書とキーのペアが必要です。RPC ノードは、構成およびセッション情報のシステム間通信に使用される内部システムエンティティです。アプライアンスごとに 1 つの RPC ノードが存在します。このノードに格納されるパスワードは、接続するアプライアンスによって提供されるパスワードと比較して調べられます。各アプライアンスがほかの Citrix ADC アプラ

アイアンスと通信するには、それらのアプライアンスについての知識（他のアプライアンスでの認証方法など）が必要です。RPC ノードはこの情報を保持しており、それにはほかの Citrix ADC アプライアンスの IP アドレスや、認証に使用されるパスワードなどが含まれます。

Citrix ADC MPX アプライアンス仮想アプライアンスでは、証明書とキーのペアは内部サービスに自動的にバインドされます。FIPS アプライアンスでは、FIPS カードのハードウェアセキュリティモジュール（HSM）に証明書とキーのペアをインポートする必要があります。そのためには、FIPS カードを構成し、証明書とキーのペアを作成して、それを内部サービスにバインドする必要があります。

CLI を使用してセキュアな HTTPS の構成

CLI を使用してセキュアな HTTPS を構成するには、次の手順を実行します

1. アプライアンスの FIPS カードでハードウェアセキュリティモジュール（HSM）を初期化します。HSM の初期化について詳しくは、「[HSM の構成](#)」を参照してください。
2. アプライアンスが高可用性セットアップの一部である場合は、SIM を有効にします。プライマリアプライアンスおよびセカンダリアプライアンス上での SIM の有効化について詳しくは、「[高可用性セットアップでの FIPS アプライアンスの構成](#)」を参照してください。
3. FIPS キーをアプライアンスの FIPS カードの HSM にインポートします。コマンドプロンプトで入力します。

```
import ssl fipskey serverkey -key ns-server.key -inform PEM
```

4. 証明書とキーのペアを追加します。コマンドプロンプトで入力します。

```
add certkey server -cert ns-server.cert -fipskey serverkey
```

5. 前の手順で作成した証明書キーを次の内部サービスにバインドします。コマンドプロンプトで入力します。

```
bind ssl service nshttps-127.0.0.1-443 -certkeyname server
```

```
bind ssl service nshttps-::11-443 -certkeyname server
```

GUI を使用して安全な HTTPS を構成する

GUI を使用して安全な HTTPS を構成するには、次の手順に従います。

1. アプライアンスの FIPS カードでハードウェアセキュリティモジュール（HSM）を初期化します。HSM の初期化について詳しくは、「[HSM の構成](#)」を参照してください。
2. アプライアンスが高可用性セットアップの一部である場合は、セキュア情報システム（SIM）を有効にします。プライマリアプライアンスおよびセカンダリアプライアンス上での SIM の有効化について詳しくは、「[高可用性セットアップでの FIPS アプライアンスの構成](#)」を参照してください。
3. FIPS キーをアプライアンスの FIPS カードの HSM にインポートします。FIPS キーのインポートについて詳しくは、「[既存の FIPS キーのインポート](#)」を参照してください。

4. **[Traffic Management]** > **[SSL]** > **[Certificates]** に移動します。
5. 詳細ペインで、**[Install]** をクリックします。
6. **[Install Certificate]** ダイアログボックスで、証明書の詳細を入力します。
7. **[Create]** をクリックしてから、**[Close]** をクリックします。
8. **[Traffic Management]** > **[Load Balancing]** > **[Services]** の順に移動します。
9. 詳細ペインの **[Action]** タブで、**[Internal Services]** をクリックします。
10. 一覧から `nshttps-127.0.0.1-443` を選択し、**[Open]** をクリックします。
11. **[Available]** ペインの **[SSL Settings]** タブで、手順 7 で作成した証明書を選択して **[Add]** をクリックし、**[OK]** をクリックします。
12. 一覧から `nshttps-::11-443` を選択し、**[Open]** をクリックします。
13. **[Available]** ペインの **[SSL Settings]** タブで、手順 7 で作成した証明書を選択して **[Add]** をクリックし、**[OK]** をクリックします。
14. **[OK]** をクリックします。

CLI を使用してセキュア RPC を構成する

CLI を使用してセキュア RPC を設定するには、次の手順に従います。

1. アプライアンスの FIPS カードでハードウェアセキュリティモジュール (HSM) を初期化します。HSM の初期化について詳しくは、「[HSM の構成](#)」を参照してください。
2. 安全な情報システム (SIM) を有効にします。プライマリアプライアンスおよびセカンダリアプライアンス上での SIM の有効化について詳しくは、「[高可用性セットアップでの FIPS アプライアンスの構成](#)」を参照してください。
3. FIPS キーをアプライアンスの FIPS カードの HSM にインポートします。コマンドプロンプトで入力します。

```
import ssl fipskey serverkey -key ns-server.key -inform PEM
```

4. 証明書とキーのペアを追加します。コマンドプロンプトで入力します。

```
add certkey server -cert ns-server.cert -fipskey serverkey
```

5. 証明書とキーのペアを次の内部サービスにバインドします。コマンドプロンプトで入力します。

```
bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server
```

```
bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server
```

```
bind ssl service nsrpcs-::11-3008 -certkeyname server
```

6. セキュア RPC モードを有効にします。コマンドプロンプトで入力します。

```
set ns rpcnode <IP address> -secure YES
```

RPC ノードのパスワードの変更の詳細については、「[RPC ノードのパスワードを変更](#)」を参照してください。

GUI を使用してセキュア RPC を構成する

GUI を使用してセキュア RPC を設定するには、次の手順に従います。

1. アプライアンスの FIPS カードでハードウェアセキュリティモジュール (HSM) を初期化します。HSM の初期化について詳しくは、「[HSM の構成](#)」を参照してください。
2. 安全な情報システム (SIM) を有効にします。プライマリアプライアンスおよびセカンダリアプライアンス上での SIM の有効化について詳しくは、「[高可用性セットアップでの FIPS アプライアンスの構成](#)」を参照してください。
3. FIPS キーをアプライアンスの FIPS カードの HSM にインポートします。FIPS キーのインポートについて詳しくは、「[既存の FIPS キーのインポート](#)」を参照してください。
4. **[Traffic Management]** > **[SSL]** > **[Certificates]** に移動します。
5. 詳細ペインで、**[Install]** をクリックします。
6. **[Install Certificate]** ダイアログボックスで、証明書の詳細を入力します。
7. **[Create]** をクリックしてから、**[Close]** をクリックします。
8. **[Traffic Management]** > **[Load Balancing]** > **[Services]** の順に移動します。
9. 詳細ペインの **[Action]** タブで、**[Internal Services]** をクリックします。
10. 一覧から **nsrpcs-127.0.0.1-3008** を選択し、**[Open]** をクリックします。
11. **[Available]** ペインの **[SSL Settings]** タブで、手順 7 で作成した証明書を選択して **[Add]** をクリックし、**[OK]** をクリックします。
12. 一覧から **nskrpcs-127.0.0.1-3009** を選択し、**[Open]** をクリックします。
13. **[Available]** ペインの **[SSL Settings]** タブで、手順 7 で作成した証明書を選択して **[Add]** をクリックし、**[OK]** をクリックします。
14. 一覧から **nsrpcs-:::11-3008** を選択し、**[Open]** をクリックします。
15. **[Available]** ペインの **[SSL Settings]** タブで、手順 7 で作成した証明書を選択して **[Add]** をクリックし、**[OK]** をクリックします。
16. **[OK]** をクリックします。
17. **[System]** > **[Network]** > **[RPC]** の順に選択します。
18. 詳細ペインで IP アドレスを選択して、**[Open]** をクリックします。
19. **[Configure RPC Node]** ダイアログボックスで、**[Secure]** を選択します。
20. **[OK]** をクリックします。

一般的なネットワークトポロジ

April 25, 2022

「[Citrix ADC アプライアンスはネットワークのどこに適合しますか?](#)」の「物理的な導入モード」の説明に従って、クライアントとサーバー間のインラインまたはワンアームのいずれかのモードで Citrix ADC アプライアンスを導入できます。インラインモードでは、一般的な導入タイプであるツーアームトポロジを使用します。

一般的なツーアームトポロジを設定します

ツーアームトポロジでは、1つのネットワークインターフェイスはクライアントネットワークに接続され、もう1つのネットワークインターフェイスはサーバーネットワークに接続されます。これにより、すべてのトラフィックが仮想アプライアンスを通過するようになります。このトポロジでは、ハードウェアの再接続が必要になり、一時的にダウン時間が発生する場合があります。ツーアームトポロジの基本的なバリエーションは複数サブネットと透過モードです。複数サブネットでは、通常、仮想アプライアンスがパブリックサブネット上に、サーバーがプライベートサブネット上に配置されます。透過モードでは、仮想アプライアンスとサーバーの両方がパブリックネットワーク上に配置されます。

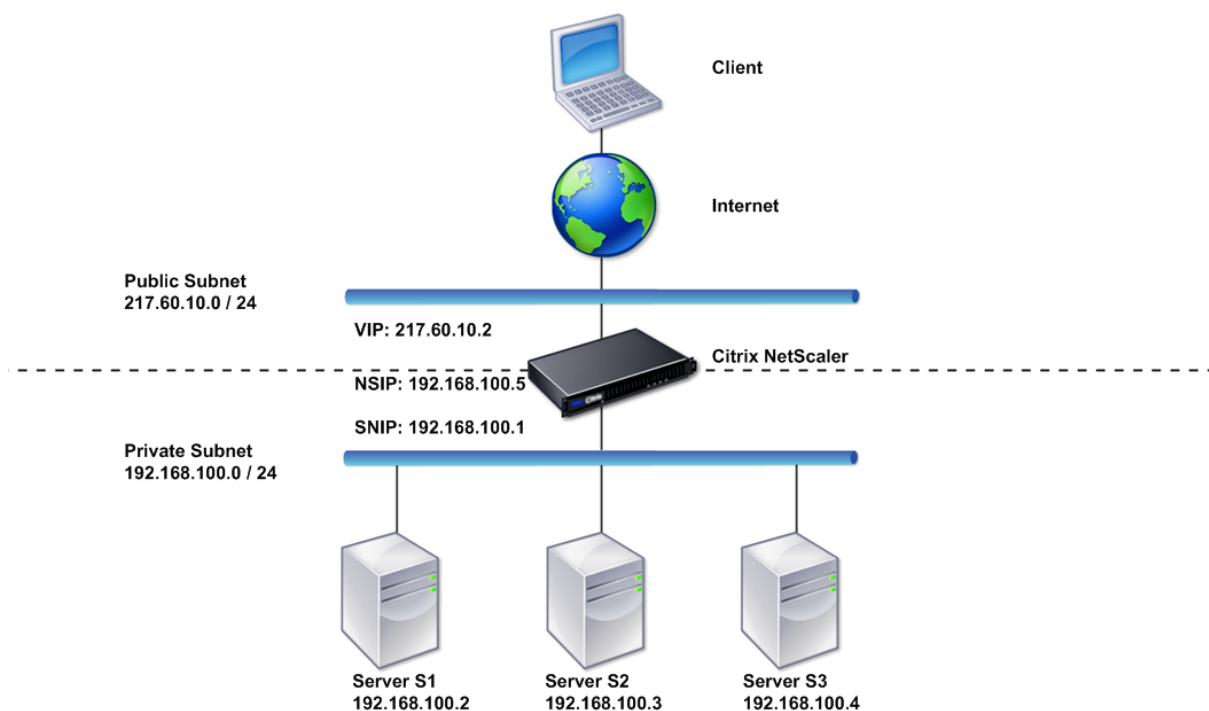
シンプルなツーアーム複数サブネットトポロジのセットアップ

最もよく使用されるトポロジの1つで、Citrix ADC アプライアンスはクライアントのサーバーの間にインラインに配置され、仮想サーバーはクライアント要求を処理するように設定されます。この構成は、クライアントとサーバーが異なるサブネット上にある場合に使用されます。たいいていの場合、クライアントとサーバーは、それぞれパブリックサブネット上とプライベートサブネット上にあります。

たとえば、サーバー S1、S2、および S3 を管理するためにツーアームモードで展開されたアプライアンスについて考えてみましょう。アプライアンス上で HTTP の仮想サーバーが構成されており、各サーバー上で HTTP サービスが実行されています。これらのサーバーはプライベートサブネット上にあり、アプライアンスでこれらのサーバーと通信するための SNIP が構成されています。MIP の代わりに SNIP を使用するため、アプライアンスで USNIP (Use SNIP) オプションを有効にする必要があります。

次の図に示すように、VIP はパブリックサブネット 217.60.10.0 上にあり、NSIP、サーバー、および SNIP はプライベートサブネット 192.168.100.0/24 上にあります。

図 1: ツーアームモード、複数のサブネットのトポロジ図



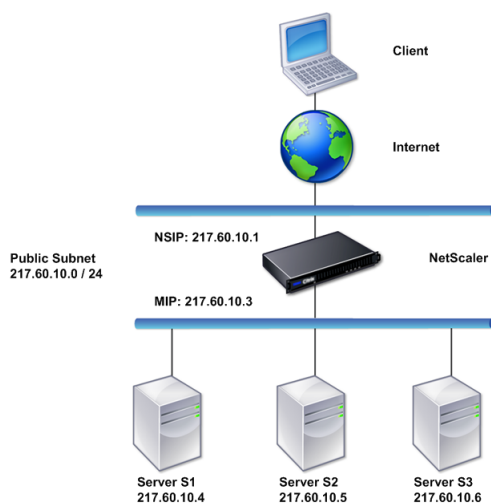
複数のサブネットを持つツーアームモードで Citrix ADC アプライアンスを展開するには、次の手順に従います。

1. 「[NetScaler IP アドレス \(NSIP\) の構成](#)」の説明に従って、NSIP とデフォルトゲートウェイを構成します。
2. 「[サブネット IP アドレスの構成](#)」の説明に従って、SNIP を構成します。
3. 「[USNIP モードを有効または無効にするには](#)」の説明に従って、USNIP オプションを有効にします。
4. 「[仮想サーバーの作成](#)」および「[サービスの構成](#)」の説明に従って、仮想サーバーとサービスを構成します。
5. 一方のネットワークインターフェイスをプライベートサブネットに、もう一方のインターフェイスをパブリックサブネットに接続します。

シンプルなツーアーム透過トポロジのセットアップ

クライアントが仮想サーバーの仲介なしでサーバーに直接アクセスする必要がある場合は、透過モードを使用します。クライアントはサーバーにアクセスできる必要があるため、サーバー IP アドレスはパブリックにする必要があります。次の図に示す例では、Citrix ADC アプライアンスがクライアントとサーバーの間に配置されています。そのため、トラフィックはアプライアンスを経由する必要があります。パケットをブリッジするため、L2 モードを有効にする必要があります。NSIP と MIP は、同じパブリックサブネット上 (217.60.10.0/24) にあります。

図 2: ツーアーム、透過モードのトポロジ図



Citrix ADC アプライアンスをツーアームの透過モードで展開するには、次の手順に従います。

1. 「[NetScaler IP アドレス \(NSIP\) の構成](#)」の説明に従って、NSIP とデフォルトゲートウェイを構成します。
2. 「[レイヤー 2 モードの有効化と無効化](#)」の説明に従って、L2 モードを有効にします。
3. 管理対象サーバーのデフォルトゲートウェイを、MIP として構成します。
4. ネットワークインターフェイスを、スイッチの適切なポートに接続します。

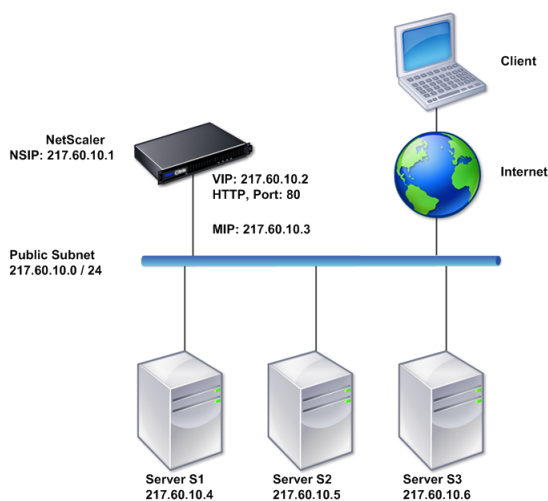
一般的なワンアームトポロジのセットアップ

ワンアームトポロジの 2 つの基本的なバリエーションは、1 つのサブネットを持つトポロジと複数のサブネットを持つトポロジです。

シンプルなワンアームシングルサブネットトポロジのセットアップ

クライアントとサーバーが同じサブネット上にある場合は、単一のサブネットでワンアームトポロジを使用できます。たとえば、サーバー S1、S2、および S3 を管理するためにワンアームモードで展開された Citrix ADC アプライアンスについて考えてみます。ADC アプライアンスで HTTP の仮想サーバーが構成されており、そのサーバー上で HTTP サービスが実行されています。次の図に示すように、Citrix ADC IP アドレス (NSIP)、マップされた IP アドレス (MIP)、およびサーバーの IP アドレスは同じパブリックサブネット上 (217.60.10.0/24) にあります。

図 3: ワンアームモード、シングルサブネットのトポロジ図



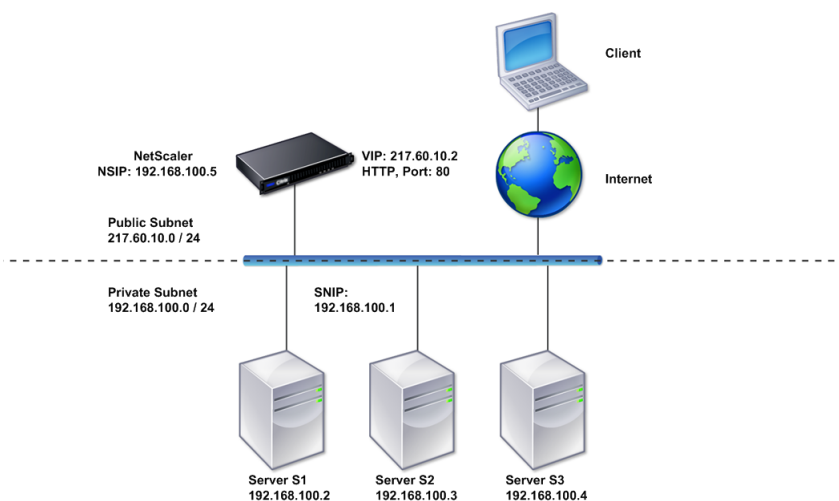
Citrix ADC アプライアンスを単一サブネットのワンアームモードで展開するには、次の手順に従います。

1. 「[Citrix ADC IP アドレス \(NSIP\) の構成](#)」の説明に従って、NSIP とデフォルトゲートウェイを構成します。
2. 「[仮想サーバーの作成](#)」および「[サービスの構成](#)」の説明に従って、仮想サーバーとサービスを構成します。
3. 一方のネットワークインターフェイスをスイッチに接続します。

シンプルなワンアーム複数サブネットトポロジのセットアップ

クライアントとサーバーが異なるサブネット上にある場合は、複数のサブネットを持つワンアームトポロジを使用できます。たとえば、サーバー S1、S2、および S3 を管理するためにワンアームモードで導入された Citrix ADC アプライアンスについて考えてみましょう。これらのサーバーはネットワーク上のスイッチ SW1 に接続されています。アプライアンスで HTTP の仮想サーバーが構成されており、そのサーバー上で HTTP サービスが実行されています。これら 3 つのサーバーはプライベートサブネット上にあるので、SNIP (Subnet IP: サブネット IP) アドレスはこれらのサーバーと通信するように設定されています。アプライアンスが MIP の代わりに SNIP を使用するよう、[Use Subnet IP address (USNIP)] を有効にする必要があります。次の図に示すように、仮想 IP アドレス (VIP) はパブリックサブネット上 (217.60.10.0/24) にあります。NSIP、SNIP、およびサーバーの IP アドレスはプライベートサブネット上 (192.168.100.0/24) にあります。

図 4: ワンアームモード、複数のサブネットのトポロジ図



複数のサブネットを持つワンアームモードで Citrix ADC アプライアンスを展開するには、次の手順に従います。

1. 「[NetScaler IP アドレス \(NSIP\) の構成](#)」の説明に従って、NSIP とデフォルトゲートウェイを構成します。
2. 「[サブネット IP アドレスの構成](#)」の説明に従って、SNIP を構成し、USNIP オプションを有効にします。
3. 「[仮想サーバーの作成](#)」および「[サービスの構成](#)」の説明に従って、仮想サーバーとサービスを構成します。
4. 一方のネットワークインターフェイスをスイッチに接続します。

システム管理設定

April 21, 2022

初期構成が整ったら、Citrix ADC アプライアンスの動作を定義し、接続管理を容易にする設定を構成できます。HTTP 要求と応答を処理するためのいくつかのオプションがあります。ルーティング、ブリッジング、および MAC ベースの転送モードは、Citrix ADC アプライアンスにアドレス指定されていないパケットを処理するために使用できます。ネットワークインターフェイスの特性を定義し、インターフェイスを集約できます。タイミングの問題を防ぐために、Citrix クロックをネットワークタイムプロトコル (NTP) サーバーと同期させることができます。Citrix ADC アプライアンスは、権限のあるドメインネームサーバー (ADNS) としてなど、さまざまな DNS モードで動作できます。システム管理用に SNMP を設定し、システムイベントの syslog ロギングをカスタマイズできます。展開する前に、構成が完全で正しいことを確認してください。

システム設定

April 21, 2022

システム設定の構成には、接続のキープアライブとサーバーオフロードを有効にするための HTTP ポートの設定、各サーバーの最大接続数の設定、接続あたりの最大要求件数の設定などの基本的なタスクが含まれます。プロキシ IP アドレスが適さない環境では、クライアント IP アドレス挿入を有効にして、HTTP Cookie バージョンを変更できます。

データ接続用のエフェメラルポートの代わりに、特定のポート範囲で FTP 接続が開かれるように Citrix ADC アプライアンスを構成することもできます。ファイアウォールですべてのポートを開くのは危険なので、この方法によってセキュリティが向上します。1,024~64,000 までの任意の範囲を設定できます。

展開前に、確認チェックリストを使用して構成内容を確認します。HTTP パラメーターと FTP ポート範囲を構成するには、Citrix ADC GUI を使用します。

次の表に記載された HTTP パラメーターの種類を変更できます。

パラメータータイプ: HTTP ポート情報

指定: 管理対象サーバーが使用する Web サーバーの HTTP ポート。ポートを指定すると、アプライアンスは、指定されたポートと一致する宛先ポートを持つクライアント要求に対して要求のスイッチ操作を実行します。

注:

着信したクライアント要求が、アプライアンスで指定されたサービスまたは仮想サーバー宛でない場合、要求の宛先ポートは、グローバルに構成されたいずれかの HTTP ポートと一致する必要があります。これにより、アプライアンスは接続のキープアライブとサーバーオフロードを実行できます。

パラメータータイプ: 制限

指定: 各管理対象サーバーへの最大接続数、および、各接続を介して送信される要求の最大件数。たとえば、[Max Connections] が「500」に設定され、アプライアンスが 3 台のサーバーを管理している場合、3 台のサーバーそれぞれに対し、最大 500 個の接続を開くことができます。デフォルトでは、アプライアンスは管理する任意のサーバーに対して任意の数の接続を作成できます。接続あたりの要求数を無制限に指定するには、[Max Requests] を「0」に設定します。

注:

Apache HTTP サーバーを使用している場合は、[Max Connections] を、Apache httpd.conf ファイルの MaxClients パラメーターと同じ値に設定する必要があります。その他の Web サーバーの場合、このパラメーターの設定はオプションとなります。

パラメータータイプ: クライアント IP の挿入

指定: HTTP 要求ヘッダーへのクライアント IP アドレスの挿入を有効または無効にします。隣接するテキストボックスで、ヘッダーフィールドの名前を指定できます。アプライアンスが管理する Web サーバーが SNIP アドレスを

受信すると、サーバーはそのアドレスをクライアント IP アドレスとして識別します。一部のアプリケーションでは、ログを記録するため、または Web サーバーが提供するコンテンツを動的に決定するために、クライアント IP アドレスが必要です。

クライアントから、アプライアンスが管理している 1 台、数台、またはすべてのサーバーに送信された HTTP ヘッダー要求に、実際のクライアント IP アドレスを挿入する機能を有効にできます。これによって、(Apache モジュール、ISAPI インターフェイス、または NSAPI インターフェイスを使用して) サーバーを少し変更するだけで、挿入されたアドレスにアクセスできるようになります。

パラメータータイプ: クッキーバージョン

指定: COOKIEINSERT パースシステムが仮想サーバーに設定されている場合に使用される HTTP Cookie バージョン。デフォルトでは、インターネットで最も一般的な種類であるバージョン 0 を使用します。代わりにバージョン 1 を指定することも可能です。

パラメータータイプ: 要求/応答

指定: 特定の種類の要求を処理し、HTTP エラー応答のログを有効または無効にするオプション。

パラメータータイプ: サーバーヘッダーの挿入

指定: Citrix ADC で生成された HTTP 応答にサーバーヘッダーを挿入します。

GUI を使用して HTTP パラメーターを設定するには、次の手順に従います。

1. ナビゲーションペインで、**[System]** を展開し、**[Settings]** をクリックします。
2. 詳細ペインで、**[Change HTTP Parameters]** をクリックします。
3. **[Configure HTTP parameters]** ダイアログボックスで、上記の表に一覧表示された見出しの下に表示されている一部またはすべてのパラメーターの値を指定します。
4. **[OK]** をクリックします。

GUI を使用して FTP ポート範囲を設定するには、次の手順に従います。

1. ナビゲーションペインで、**[System]** を展開し、**[Settings]** をクリックします
2. 詳細ペインの **[Settings]** で、**[Change global system settings]** をクリックします。
3. **[FTP Port Range]** の **[Start Port]** および **[End Port]** ボックスに、指定する範囲の最小ポート番号と最大ポート番号（たとえば、「5000」と「6000」）をそれぞれ入力します。
4. **[OK]** をクリックします。

パケット転送モード

April 21, 2022

Citrix ADC アプライアンスは、アプライアンスが所有する IP アドレス宛ではないパケット（つまり NSIP、MIP、SNIP、構成済みサービス、または構成済み仮想サーバーの IP アドレス宛でないパケット）をルーティングまたはブ

リッジできます。デフォルトでは、L3 モード（ルーティング）が有効になり、L2 モード（ブリッジ）が無効になりますが、この構成は変更できます。アプライアンスがパケットを評価し、パケットの処理、ルーティング、ブリッジ、廃棄のいずれかを行う方法を次のフローチャートに示します。

図 1: レイヤー 2 モードとレイヤー 3 モード間の相互作用

アプライアンスは次のモードを使用して、受信したパケットを転送できます。

- レイヤー 2 (L2) モード
- レイヤー 3 (L3) モード
- MAC ベース転送モード

レイヤー 2 モードの有効化と無効化

レイヤー 2 モードは、レイヤー 2 フォワード（ブリッジ）機能を制御します。このモードを使用して、Citrix ADC アプライアンスをレイヤー 2 デバイスとして動作させ、自分宛ではないパケットをブリッジするように設定することができます。このモードを有効にした場合、パケットはどの MAC アドレスにも転送されません。これは、パケットがアプライアンスの任意のインターフェイスに着信することができ、各インターフェイスが独自の MAC アドレスを持っているからです。

レイヤー 2 モードを無効にした場合（デフォルト）、アプライアンスは、自分の MAC アドレス宛ではないパケットをドロップします。別のレイヤー 2 デバイスがアプライアンスと並列に設置されている場合は、レイヤー 2 モードを無効にしてブリッジ（レイヤー 2）ループを防ぐ必要があります。構成ユーティリティまたはコマンドラインを使用して、レイヤー 2 モードを有効にできます。

注：アプライアンスはスパニングツリープロトコルをサポートしていません。L2 モードが有効な場合に、ループを避けるために、アプライアンス上の 2 つのインターフェイスを同じブロードキャストドメインに接続しないでください。

CLI を使用してレイヤー 2 モードを有効または無効にするには

コマンドプロンプトで次のコマンドを入力し、レイヤー 2 モードを有効または無効にして、有効または無効になっていることを確認します。

- `enable ns mode \<モード\>`
- `disable ns mode \<モード\>`
- `show ns mode`

例

```
enable ns mode l2
```



```

Done
show ns mode

Mode Acronym Status
-----
1) Fast Ramp FR ON
2) Layer 2 mode L2 ON
.
.
.
Done
disable ns mode l2
Done
show ns mode

Mode Acronym Status
-----
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
Done

```

GUI を使用してレイヤー 2 モードを有効または無効にするには

1. ナビゲーションペインで、**[System]** を展開し、**[Settings]** をクリックします。
2. 詳細ペインの **[Modes and Features]** で **[Configure modes]** をクリックします。
3. **[Configure Modes]** ダイアログボックスで、** [Layer 2 Mode] ** チェックボックスをオンにしてレイヤー 2 モードを有効にします。レイヤー 2 モードを無効にするには、チェックボックスをオフにします。
4. **[OK]** をクリックします。詳細ペインに「Enable/Disable Mode(s)?」メッセージが表示されます。
5. **[Yes]** をクリックします。

レイヤー 3 モードの有効化と無効化

レイヤー 3 モードは、レイヤー 3 フォワード機能を制御します。このモードを使用して、Citrix ADC アプライアンスがルーティングテーブルを参照して自分宛ではないパケットを転送するように設定できます。レイヤー 3 モードを有効にした場合（デフォルト）、アプライアンスはルートテーブルのルックアップを実行して、アプライアンス所有の IP アドレス宛ではないすべてのパケットを転送します。レイヤー 3 モードを無効にした場合、アプライアンスはこれらのパケットをドロップします。

CLI を使用してレイヤ **3** モードを有効または無効にするには

コマンドプロンプトで次のコマンドを入力し、レイヤー 3 モードを有効または無効にして、有効または無効になっていることを確認します。

- enable ns mode \<モード\>
- disable ns mode \<モード\>
- show ns mode

例

```
enable ns mode l3
Done
show ns mode
```

Mode Acronym Status

```
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
.
```

Done

```
disable ns mode l3
Done
show ns mode
```

Mode Acronym Status

```
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 OFF
.
.
```

Done

GUI を使用してレイヤー 3 モードを有効または無効にするには

1. ナビゲーションペインで、[System] を展開し、[Settings] をクリックします。
2. 詳細ペインの [Modes and Features] で [Configure modes] をクリックします。
3. [Configure Modes] ダイアログボックスで、[Layer 3 Mode (IP Forwarding)] チェックボックスをオンにしてレイヤー 3 モードを有効にします。To disable Layer 3 mode, clear the check box.
4. [OK] をクリックします。詳細ペインに「Enable/Disable Mode(s)?」メッセージが表示されます。
5. [Yes] をクリックします。

MAC ベースの転送モードを有効または無効にします

Citrix ADC アプライアンスがソースの MAC アドレスを記憶しているので、MAC ベース転送を使用して、パケットの転送時にトラフィックをより効率的に処理し、複数のルートや ARP ルックアップを防ぐことができます。複数のルックアップを防ぐため、アプライアンスは、ARP ルックアップを実行するすべての接続のソース MAC アドレスをキャッシュして、データを同じ MAC アドレスに返します。

MAC ベース転送は、VPN デバイスを使用している場合に便利です。これは、アプライアンスによって、特定の VPN を経由するすべてのトラフィックが同じ VPN デバイスを通過するようになるからです。

次の図は、MAC ベース転送のプロセスを示しています。

図 2: MAC ベースの転送プロセス

MAC ベース転送を有効にした場合、アプライアンスは次の MAC アドレスをキャッシュします。

- 受信接続のソース（ルーター、ファイアウォール、VPN デバイスなどの通信デバイス）
- 要求に応答するサーバー

サーバーがアプライアンスを介して応答する場合、アプライアンスは、応答パケットの宛先 MAC アドレスをキャッシュしたアドレスに設定し、トラフィックが対称的に流れるようにして、応答をクライアントに転送します。このプロセスでは、ルートテーブルのルックアップ機能と ARP ルックアップ機能が回避されます。ただし、アプライアンスが接続を開始した場合は、ルックアップ機能でルートと ARP テーブルが使用されます。MAC ベース転送を有効にするには、構成ユーティリティを使用するか、またはコマンドラインを使用します。

一部の展開環境では、着信および発信パスが、異なるルーターを経由する必要があります。このような状況では、MAC ベース転送がトポロジデザインに違反します。着信および発信パスが異なるルーターを経由する必要のあるグローバルサーバー負荷分散（Global Server Load Balancing: GSLB）サイトの場合は、MAC ベース転送を無効にし、アプライアンスのデフォルトルーターを発信ルーターとして使用する必要があります。

MAC ベース転送を無効にして、レイヤー 2 またはレイヤー 3 接続を有効にした場合、ルートテーブルは、発信接続と着信接続に別のルーターを指定できます。MAC ベース転送を無効にするには、構成ユーティリティを使用するか、またはコマンドラインを使用します。

CLI を使用して **MAC** ベースの転送を有効または無効にするには

コマンドプロンプトで次のコマンドを入力し、MAC ベース転送を有効または無効にして、有効または無効になっていることを確認します。

- enable ns mode \<モード\>
- disable ns mode \<モード\>
- show ns mode

例

““ pre codeblock

```
enable ns mode mbf
Done
show ns mode
```

1	Mode	Acronym	Status	1) Fast
2	-----	-----	-----	2) Layer 2
	Ramp	FR	ON	6)
	mode	L2	OFF	.
	MAC-based forwarding	MBF	ON	.
	Done >			.

```
disable ns mode mbf
Done
show ns mode
```

1	Mode	Acronym	Status	1) Fast
2	-----	-----	-----	2) Layer 2
	Ramp	FR	ON	6)
	mode	L2	OFF	.
	MAC-based forwarding	MBF	OFF	.
	Done >			.

GUI を使用して MAC ベースの転送を有効または無効にするには

1. ナビゲーションペインで、[System] を展開し、[Settings] をクリックします。
2. 詳細ペインの [Modes and Features] グループで [Configure modes] をクリックします。
3. ** [Configure Modes] ** ダイアログボックスで MAC ベース転送モードを有効にするには、** [MAC Based Forwarding] ** チェックボックスをオンにします。MAC ベース転送を無効にするには、このチェックボックスをオフにします。

4. **[OK]** をクリックします。詳細ペインに「Enable/Disable Mode(s)?」メッセージが表示されます。
5. **[Yes]** をクリックします。

ネットワークインターフェイス

April 21, 2022

Citrix ADC インターフェイスにはスロット/ポート表示に番号が付けられています。個々のインターフェイスの特性を変更することに加えて、特定のホストグループだけにトラフィックが許可されるように VLAN を構成できます。リンクを高速チャネルに集約することもできます。

仮想 LAN

Citrix ADC アプライアンスは、(レイヤー 2) ポートと IEEE802.1Q タグ付き仮想 LAN (VLAN) をサポートします。VLAN 構成は、トラフィックを特定のワークステーショングループだけに制限しなければならない場合に便利です。IEEE 802.1q タグ付け機能を使用して複数の VLAN に属するように、ネットワークインターフェイスを構成できます。

構成した VLAN は、IP サブネットにバインドできます。これにより、(サブネット上のホストのデフォルトルーターとして構成されている場合) ADC アプライアンスは、これらの VLAN 間で IP 転送を実行します。

Citrix ADC アプライアンスは、次のタイプの VLAN をサポートします。

- デフォルト VLAN

デフォルトでは、Citrix ADC アプライアンスのネットワークインターフェイスは、タグなしのネットワークインターフェイスとして、単一のポートベース VLAN に含まれています。このデフォルト VLAN は、VID が 1 であり、永続的に存在します。デフォルト VLAN を削除したり、その VID を変更したりすることはできません。

- ポートベース VLAN

排他的なレイヤー 2 ブロードキャストドメインを共有するネットワークインターフェイスのセットは、ポートベース VLAN のメンバーシップを定義します。複数のポートベース VLAN を構成できます。インターフェイスをタグなしメンバーとして新しい VLAN に追加すると、デフォルト VLAN から自動的に削除されます。

- タグ付き VLAN

ネットワークインターフェイスは、VLAN のタグ付きまたはタグなしメンバーになることができます。各ネットワークインターフェイスは、唯一の VLAN (ネイティブ VLAN) のタグなしメンバーです。タグなしネットワークインターフェイスは、タグなしフレームとしてネイティブ VLAN のフレームを転送します。タグ付きネットワークインターフェイスは、複数の VLAN の一部になることができます。タグ付きを設定する場合は、リンクの両端で VLAN 設定が一致していることを確認してください。構成ユーティリティを使用し、VLAN のタグ付きメンバーとしてポートをバインドできる、タグ付き VLAN (nsvlan) を定義できます。この VLAN を

構成するには ADC アプライアンスを再起動する必要があるため、ネットワークの初回構成中に実行する必要があります。

リンクアグリゲートチャンネル

リンクアグリゲーションは、複数ポートからの着信データを、1つの高速リンクに結合します。リンクアグリゲートチャンネルを構成すると、Citrix ADC アプライアンスとほかの接続デバイス間の通信チャンネルの容量と可用性が増加します。アグリゲートされたリンクは「チャンネル」とも呼ばれます。

ネットワークインターフェイスをチャンネルにバインドした場合、チャンネルのパラメーターは、ネットワークインターフェイスのパラメーターよりも優先されます。ネットワークインターフェイスは、1つのチャンネルにのみバインドできます。ネットワークインターフェイスをリンクアグリゲートチャンネルにバインドすると、VLAN 構成が変更されます。つまり、ネットワークインターフェイスをチャンネルにバインドすると、ネットワークインターフェイスは以前属していた VLAN から削除され、デフォルト VLAN に追加されます。ただし、チャンネルを元の VLAN や新しい VLAN にバインドすることができます。たとえば、ネットワークインターフェイス 1/2 と 1/3 を、ID が 2 の VLAN にバインドしていて、それらをリンクアグリゲートチャンネル LA/1 にバインドした場合、ネットワークインターフェイスはデフォルト VLAN に移動されますが、VLAN 2 にバインドすることができます。

注：また、リンクアグリゲーション制御プロトコル（Link Aggregation Control Protocol: LACP）を使用して、リンクアグリゲーションを構成することもできます。詳しくは、「[Link Aggregation Control Protocol を使用したリンクアグリゲーションの構成](#)」を参照してください。

クロック同期

April 21, 2022

Citrix ADC アプライアンスを設定して、ローカルの時刻を、NTP（Network Time Protocol: ネットワークタイムプロトコル）サーバーの時刻と同期することができます。これにより、NetScaler のクロックの設定は、ネットワーク上のほかのサーバーと同じ日付と時刻になります。NTP は、UDP（User Datagram Protocol: ユーザーデータグラムプロトコル）ポート 123 を、トランスポートレイヤーとして使用します。NTP 構成ファイルで NTP サーバーを追加し、アプライアンスがこれらのサーバーから定期的に更新を受け取るようにする必要があります。

ローカルの NTP サーバーがない場合は、公式 NTP サイト（<http://www.ntp.org>）で、パブリックなオープンアクセス NTP サーバーの一覧を検索できます。

アプライアンスでクロック同期を構成するには、次の手順に従います：

1. コマンドラインにログオンし、shell コマンドを入力します。
2. シェルプロンプトで、ntp.conf ファイルを/etc ディレクトリから/nsconfig ディレクトリにコピーします。ファイルが/nsconfig ディレクトリに既に存在する場合は、ntp.conf ファイルから次のエントリが削除されていることを確認します。

```
1 restrict localhost
2
3 restrict 127.0.0.2
```

これらのエントリは、デバイスをタイムサーバーとして実行する場合のみ必要となります。ただし、この機能は Citrix ADC アプライアンスではサポートされていません。

3. /nsconfig/ntp.conf を編集して、ファイルのサーバーと制限エントリの下に、必要な NTP サーバーの IP アドレスを入力します。
4. /nsconfig ディレクトリに rc.netscaler という名前のファイルがない場合は作成します。
5. /nsconfig/rc.netscaler を編集して、/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log & というエントリを追加します。

このエントリは、ntpd サービスを開始し、ntp.conf ファイルをチェックして、メッセージを /var/log ディレクトリ。

注: Citrix ADC アプライアンスとタイムサーバーの時間差が 1000 秒を超える場合、ntpd サービスは ADC ログへのメッセージで終了します。これを避けるには、強制的に時刻を同期する -g オプションを使用して ntpd を開始する必要があります。/nsconfig/rc.netscaler に次のエントリを追加します。

```
1 /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
```

時間差が大きく、強制的に時刻を同期したくない場合は、日付を手動で設定してから ntpd を再び開始できます。アプライアンスとタイムサーバー間の時間差は、シェルで次のコマンドを実行することによって確認できます。

```
1 ntpdate -q <IP address or domain name of the NTP server>
2 <!--NeedCopy-->
```

6. アプライアンスを再起動して、クロック同期を有効にします。

注: アプライアンスを再起動する前に時刻同期を開始したい場合は、手順 5 で rc.netscaler ファイルに追加した次のコマンドをシェルプロンプトで入力します。

```
1 /usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ ntpd.log &
2 <!--NeedCopy-->
```

DNS の構成

April 21, 2022

ADNS (Authoritative Domain Name Server)、DNS プロキシサーバー、エンドリゾルバー、またはフォワーダーとして機能するように、Citrix ADC アプライアンスを構成できます。SRV レコード、AAAA レコード、A レコー

ド、MX レコード、NS レコード、CNAME レコード、PTR レコード、SOA レコードなど、DNS リソースレコードを追加できます。また、アプライアンスは外部 DNS サーバーの負荷を分散できます。

アプライアンスをフォワーダーとして構成する方法が一般的です。この構成では、外部ネームサーバーを追加する必要があります。外部ネームサーバーを追加したら、構成が正しいことを確認する必要があります。

外部ネームサーバーを追加、削除、有効化、および無効化することができます。IP アドレスを指定してネームサーバーを作成するか、既存の仮想サーバーをネームサーバーとして設定できます。

ネームサーバーを追加する場合は、IP アドレスまたは VIP (Virtual IP: 仮想 IP) アドレスを指定できます。IP アドレスを使用する場合、アプライアンスはラウンドロビン方式で、構成したネームサーバーに要求を負荷分散します。VIP を使用する場合、任意の負荷分散方式を指定できます。

CLI を使用してネームサーバーを追加します

コマンドプロンプトで次のコマンドを入力し、ネームサーバーを追加して構成を確認します。

- add dns nameServer <IP>
- show dns nameServer <IP>

例

“ pre codeblock

```
add dns nameServer 10.102.29.10
Done
show dns nameServer 10.102.29.10
1) 10.102.29.10 - State: DOWN
Done
“
```

GUI を使用してネームサーバーを追加する

1. **[Traffic Management]** > **[DNS]** > **[Name Servers]** の順に選択します。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Create Name Server]** ダイアログボックスで、**[IP Address]** を選択します。
4. **[IP Address]** ボックスにネームサーバーの IP アドレス（たとえば、「10.102.29.10」）を入力します。外部ネームサーバーを追加する場合は、**[Local]** チェックボックスをオフにします。
5. **[Create]** をクリックしてから、**[Close]** をクリックします。
6. 追加したネームサーバーが **[Name Servers]** ペインに表示されることを確認します。

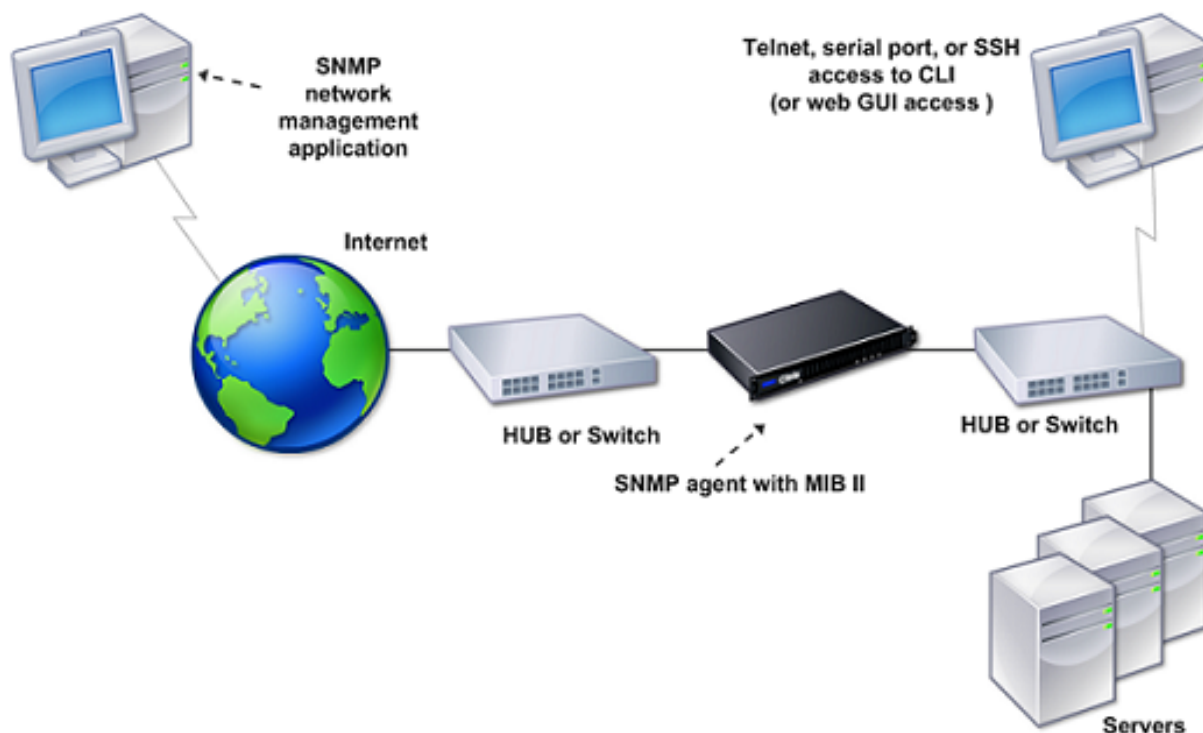
SNMP 構成

April 21, 2022

外部のコンピューターで実行されている SNMP (Simple Network Management Protocol: 簡易ネットワーク管理プロトコル) ネットワーク管理アプリケーションは、Citrix ADC アプライアンスの SNMP エージェントにクエリを発行します。エージェントは、ネットワーク管理アプリケーションで要求されたデータを MIB (Management Information Base: 管理情報ベース) で検索して、データをアプリケーションに送信します。

SNMP の監視では、トラップメッセージとアラームを使用します。SNMP トラップメッセージは、異常な状態を通知するためにエージェントが生成する非同期イベントです。このメッセージは、アラームによって通知されます。たとえば、CPU 使用率が 90% を超えたときに通知する場合は、その条件に対するアラームをセットアップできます。次の図は、SNMP が有効化および構成されている Citrix ADC アプライアンスを備えたネットワークを示しています。

図 1: Citrix ADC アプライアンスの SNMP



Citrix ADC の SNMP エージェントは、SNMP version 1 (SNMPv1)、SNMP version 2 (SNMPv2)、および SNMP version 3 (SNMPv3) をサポートしています。エージェントはバイリンガルモードで動作しているので、SNMPv2 クエリ (Get-Bulk など) と SNMPv1 クエリを処理できます。また、SNMP エージェントは SNMPv2 に準拠したトラップを送信し、counter64 などの SNMPv2 データタイプをサポートしています。SNMPv1 マネージャー (ADC アプライアンスからの SNMP 情報を要求する、他のサーバー上のプログラム) は、SNMP クエリを処理するときに NS-MIB-smiv1.mib ファイルを使用します。SNMPv2 マネージャーは、NS-MIB-smiv2.mib ファイルを使用します。

Citrix ADC アプライアンスは、次のエンタープライズ固有の MIB をサポートします。

- 標準 MIB-2 グループのサブセット。MIB-2 グループの SYSTEM、IF、ICMP、UDP、および SNMP を提供します。
- システムエンタープライズ MIB。システム固有の設定と統計情報を提供します。

SNMP の設定には、SNMP エージェントにクエリを発行できるマネージャーを指定し、SNMP トラップメッセージを受信する SNMP トラップリスナーを追加し、SNMP アラームを設定する作業が含まれます。

SNMP マネージャーを追加する

SNMP Version 1、2、または 3 に準拠する管理アプリケーションを実行するワークステーションを構成して、アプライアンスにアクセスできます。このようなワークステーションは、「SNMP マネージャー」と呼ばれます。アプライアンスに SNMP マネージャーを指定しない場合、アプライアンスは、ネットワーク上のすべての IP アドレスから SNMP クエリを受け付けて応答します。1 つまたは複数の SNMP マネージャーを設定する場合、アプライアンスは、それらの特定の IP アドレスからのみ SNMP クエリを受け付けて応答します。SNMP マネージャーの IP アドレスを指定する場合は、ネットマスクパラメーターを使用して、サブネット全体からのアクセス権を付与できます。最大 100 個の SNMP マネージャーまたはネットワークを追加できます。CLI を使用して SNMP マネージャーを追加するには

コマンドプロンプトで次のコマンドを入力し、SNMP マネージャーを追加して構成を確認します。

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
```

```
show snmp manager <IPAddress>
```

例:

```
add snmp manager 10.102.29.5 -netmask 255.255.255.255
```

```
show snmp manager 10.102.29.5
```

```
10.102.29.5 255.255.255.255
```

GUI を使用して **SNMP** マネージャーを追加するには:

1. ナビゲーションペインで **[System]**、**[SNMP]** の順に展開して、**[Managers]** をクリックします。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Add SNMP Manager]** ダイアログボックスの **[IP Address]** ボックスに、管理アプリケーションを実行しているワークステーションの IP アドレス（たとえば、「10.102.29.5」）を入力します。
4. **[Create]** をクリックしてから、**[Close]** をクリックします。
5. 追加した SNMP トラップが、ペインの下部にある **[Details]** セクションに表示されていることを確認します。

SNMP トラップリスナーの追加

アラームを構成したら、アプライアンスによるトラップメッセージの送信先となるトラップリスナーを指定します。トラップリスナーの IP アドレスや宛先ポートなどのパラメーターを指定する以外に、トラップの種類（汎用または専用）と SNMP のバージョンを指定できます。

汎用または専用のトラップを受信するために、最大 20 のトラップリスナーを構成できます。

CLI を使用して SNMP トラップリスナーを追加するには

コマンドプロンプトで次のコマンドを入力し、SNMP トラップを追加して構成を確認します。

- `add snmp trap specific <IP>`
- `show snmp trap`

例：

```
1 Trap type: SPECIFIC
2 Destination IP: 10.102.29.3
3 TD: 0
4 Destination Port: 162
5 Source IP: NetScaler IP
6 Version: V2
7 Min-Severity: -
8 AllPartition: DISABLED
9 Community: public
10 <!--NeedCopy-->
```

GUI を使用して SNMP トラップリスナーを追加するには

1. ナビゲーションペインで [System]、[SNMP] の順に展開して、[Traps] をクリックします。
2. 詳細ペインで、[Add] をクリックします。
3. [Create SNMP Trap Destination] ダイアログボックスの [Destination IP Address] ボックスに、IP アドレス（たとえば、「10.102.29.3」）を入力します。
4. [Create] をクリックしてから、[Close] をクリックします。
5. 追加した SNMP トラップが、ペインの下部にある [Details] セクションに表示されていることを確認します。

SNMP アラームを構成する

いずれかのアラームに該当するイベントが発生した場合にアプライアンスがトラップメッセージを生成するように構成できます。アラームを構成するには、アラームを有効にして、トラップを生成する重要度レベルを設定します。Critical、Major、Minor、Warning、および Informational という、5 つの重要度レベルがあります。アラームの重要度が、トラップに指定した重要度と一致する場合のみ、トラップが送信されます。

一部のアラームは、デフォルトで有効になっています。SNMP アラームを無効にすると、該当するイベントが発生してもアプライアンスはトラップメッセージを生成しません。たとえば、Login-Failure SNMP アラームを無効にすると、ログインが失敗してもアプライアンスはトラップメッセージを生成しません。

CLI を使用してアラームを有効または無効にするには

コマンドプロンプトで次のコマンドを入力し、アラームを有効または無効にして、有効または無効になっていることを確認します。

- `set snmp alarm \< トラップ名 \> \[-state ENABLED \| DISABLED \|]`
- `show snmp alarm \< トラップ名 \>`

例

```
set snmp alarm LOGIN-FAILURE -state ENABLED
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
-----
1) LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
Done
```

CLI を使用してアラームの重大度を設定するには

コマンドプロンプトで次のコマンドを入力し、アラームの重要度を設定して重要度が正しく設定されていることを確認します。

- `set snmp alarm \< トラップ名 \> \[-severity \< 重要度 \> \|]`
- `show snmp alarm \< トラップ名 \>`

例

```
set snmp alarm LOGIN-FAILURE -severity Major
Done
show snmp alarm LOGIN-FAILURE
Alarm Alarm Threshold Normal Threshold Time State Severity Logging
-----
1) LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
Done
```

GUI を使用してアラームを構成するには

1. ナビゲーションペインで [System]、[SNMP] の順に展開して、[Alarms] をクリックします。
2. 詳細ペインでアラーム（たとえば、[LOGIN-FAILURE]）を選択し、[Open] をクリックします。
3. [Configure SNMP Alarm] ダイアログボックスでアラームを有効にするには、[State] の一覧で [Enabled] を選択します。アラームを無効にするには、[Disabled] を選択します。
4. [Severity] ドロップダウンリストで、重要度のオプション（たとえば、[Major]）を選択します。
5. [OK] をクリックし、[Close] をクリックします。
6. ペインの下部にある [Details] セクションを表示し、SNMP アラームのパラメーターが正しく構成されていることを確認します。

構成を確認する

April 21, 2022

システムの設定が終了したら、次のチェックリストに記入して設定を確認します。

設定チェックリスト

- 実行中のビルド:
- 非互換性の問題はない（非互換性の問題は対象ビルドのリリースノートに記載されています）。
- ポート設定（速度、二重、フロー制御、監視）がスイッチのポートと同じである。
- ピーク時にすべてのサーバー側接続をサポートするように、SNIP アドレスが十分に設定されている。
 - 設定済みの SNIP IP アドレス数: ____
 - 予想される同時サーバー接続数:
[] 62,000 [] 124,000 [] Other_____

トポロジ設定チェックリスト

ルートを使用して、他のサブネット上のサーバーを解決した。

入力したルート

-
- Citrix ADC アプライアンスが官民トポロジにある場合、リバース NAT が構成されています。
 - ADC アプライアンスで設定されたフェールオーバー（高可用性）設定が、ワンアームまたはツーアーム構成で解決される。使用されないネットワークインターフェイスをすべて無効化:

-
- ADC アプライアンスが外部負荷分散装置の後ろに配置されている場合、外部負荷分散装置の負荷分散ポリシーが「least connection」ではない。

外部負荷分散装置に設定されている負荷分散ポリシー：

-
- ADC アプライアンスがファイアウォールの前に配置されている場合、ファイアウォールのセッションタイムアウトが 300 秒以上に設定されている。

注：Citrix ADC アプライアンスでの TCP アイドル接続のタイムアウトは 360 秒です。ファイアウォール上でも 300 秒以上のタイムアウトが設定されている場合、接続が先に閉じられないためにアプライアンスで TCP 接続の多重化が行われることがあります。

セッションタイムアウトに設定されている値： _____

サーバー設定チェックリスト

- 「キープアライブ」がすべてのサーバーで有効になっている。

キープアライブタイムアウトに設定されている値： _____

- デフォルトゲートウェイが正しい値に設定されている（デフォルトゲートウェイは、Citrix ADC アプライアンスまたはアップストリームルーターのいずれかである必要があります。）デフォルトゲートウェイは次のとおりです。

-
- サーバーのポート設定（速度、二重、フロー制御、監視）がスイッチのポート設定と同じである。

-
- Microsoft® Internet Information Server を使用している場合、バッファリングがサーバーで有効になっている。

- Apache Server を使用している場合、MaxConn（最大接続数）パラメーターがサーバーと Citrix ADC アプライアンスで設定されている。

設定されている MaxConn（最大接続数）の値：

-
- Netscape Enterprise Server を使用する場合、接続パラメーターあたりの最大リクエスト数は Citrix ADC アプライアンスで設定されます。設定されている接続ごとの最大要求数の値：

ソフトウェア機能の設定チェックリスト

- レイヤー 2 モード機能を無効にする必要があるかどうか（別のレイヤー 2 デバイスが Citrix ADC アプリアランスと並行して動作している場合は無効にします。）

有効または無効にする理由

- MAC ベース転送機能を無効にする必要があるかどうか（リターントラフィックが使用する MAC アドレスが異なる場合は、無効にする必要があります）。

有効または無効にする理由

- ホストベースの再使用を無効にする必要があるかどうか（サーバーに仮想ホストがあるかどうか）。

有効または無効にする理由

- サージ保護機能のデフォルト設定を変更する必要があるかどうか。

設定を変更または保持する理由

アクセスチェックリスト

- クライアント側ネットワークから、システム IP の ping を実行できる。
- サーバー側ネットワークから、システム IP の ping を実行できる。
- 管理対象サーバーは、Citrix ADC を介して ping を実行できます。
- 管理対象サーバーから、インターネットホストの ping を実行できる。
- ブラウザーを介して、管理対象サーバーにアクセスできる。
- ブラウザーを使用して、管理対象サーバーからインターネットにアクセスできる。
- SSH を使用してシステムにアクセスできる。
- すべての管理対象サーバーへの管理者アクセスが機能している。

注:

ping ユーティリティを使用している場合は、ping されるサーバーで ICMP ECHO を有効にしてください。そうしないと、ping が失敗します。

ファイアウォールチェックリスト

次のファイアウォール要件が満たされている。

- UDP 161 (SNMP)
- UDP 162 (SNMP トラップ)
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Citrix ADC アプライアンスでトラフィックを負荷分散する

April 21, 2022

負荷分散機能は、クライアント要求を複数のサーバーに分散して、リソース使用率を最適化します。限られた数のサーバーが多数のクライアントにサービスを提供する実際のシナリオでは、サーバーが過負荷になり、サーバーファームのパフォーマンスが低下する可能性があります。Citrix ADC アプライアンスは、負荷分散基準を使用して、各クライアント要求を、要求が到着したときに処理するのに最適なサーバーに転送することにより、ボトルネックを防ぎます。

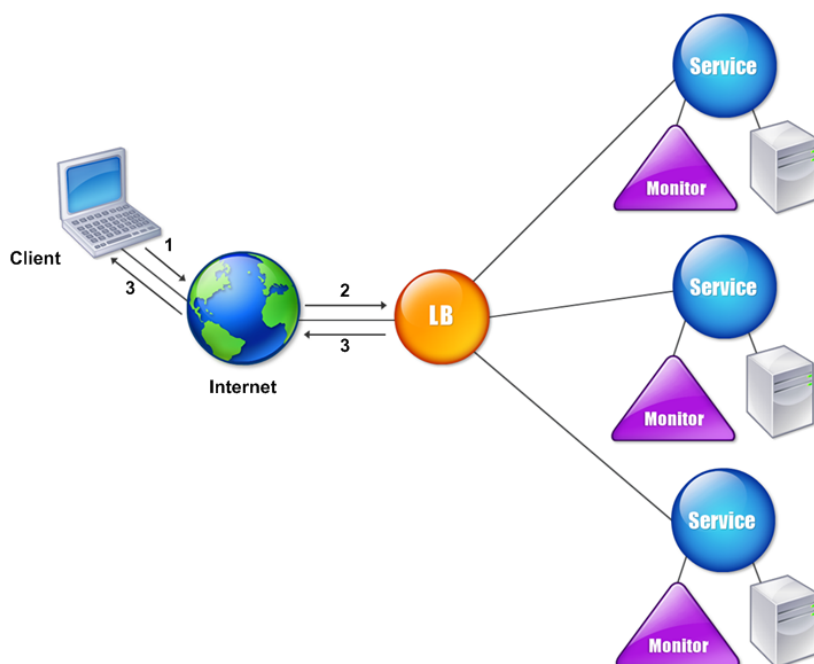
負荷分散を構成するには、サーバーファーム内の複数のサーバーをプロキシし、それらの間で負荷を分散する仮想サーバーを定義します。

クライアントがサーバーへの接続を開始すると、仮想サーバーはクライアント接続を終了し、選択したサーバーとの新しい接続を開始するか、サーバーとの既存の接続を再利用して負荷分散を実行します。負荷分散機能は、レイヤー 4 (TCP および UDP) からレイヤー 7 (FTP、HTTP、および HTTPS) までのトラフィック管理を提供します。

Citrix ADC アプライアンスは、負荷分散方法と呼ばれるいくつかのアルゴリズムを使用して、サーバー間で負荷を分散する方法を決定します。デフォルトの負荷分散方法は、最小接続方法です。

一般的な負荷分散の展開は、次の図で説明するエンティティで構成されます。

図 1: 負荷分散アーキテクチャ



エンティティは次のように機能します。

- 仮想サーバー。IP アドレス、ポート、およびプロトコルで表されるエンティティ。仮想サーバーの IP アドレス (VIP) は通常、パブリック IP アドレスです。クライアントはこの IP アドレスに接続要求を送信します。仮想サーバーは、サーバーのバンクを表します。
- **Service**。サーバーまたはサーバー上で実行されているアプリケーションの論理表現。サーバーの IP アドレス、ポート、およびプロトコルを識別します。サービスは仮想サーバーにバインドされています。
- サーバーオブジェクト。IP アドレスで表されるエンティティ。サーバーオブジェクトは、サービスを作成するときに作成されます。サービスの IP アドレスは、サーバーオブジェクトの名前として使用されます。サーバーオブジェクトを作成してから、サーバーオブジェクトを使用してサービスを作成することもできます。
- モニター。サービスの状態を追跡するエンティティ。アプライアンスは、各サービスにバインドされたモニターを使用してサーバーを定期的にプローブします。サーバーが指定された応答タイムアウト内に応答せず、指定された数のプローブが失敗した場合、サービスは DOWN とマークされます。次に、アプライアンスは残りのサービス間で負荷分散を実行します。

負荷分散

April 21, 2022

負荷分散を構成するには、まずサービスを作成する必要があります。次に、仮想サーバーを作成して、サービスをその仮想サーバーにバインドします。デフォルトでは、Citrix ADC アプライアンスはモニターを各サービスにバインドします。サービスをバインドしたら、すべての構成内容が正しいことを確認します。

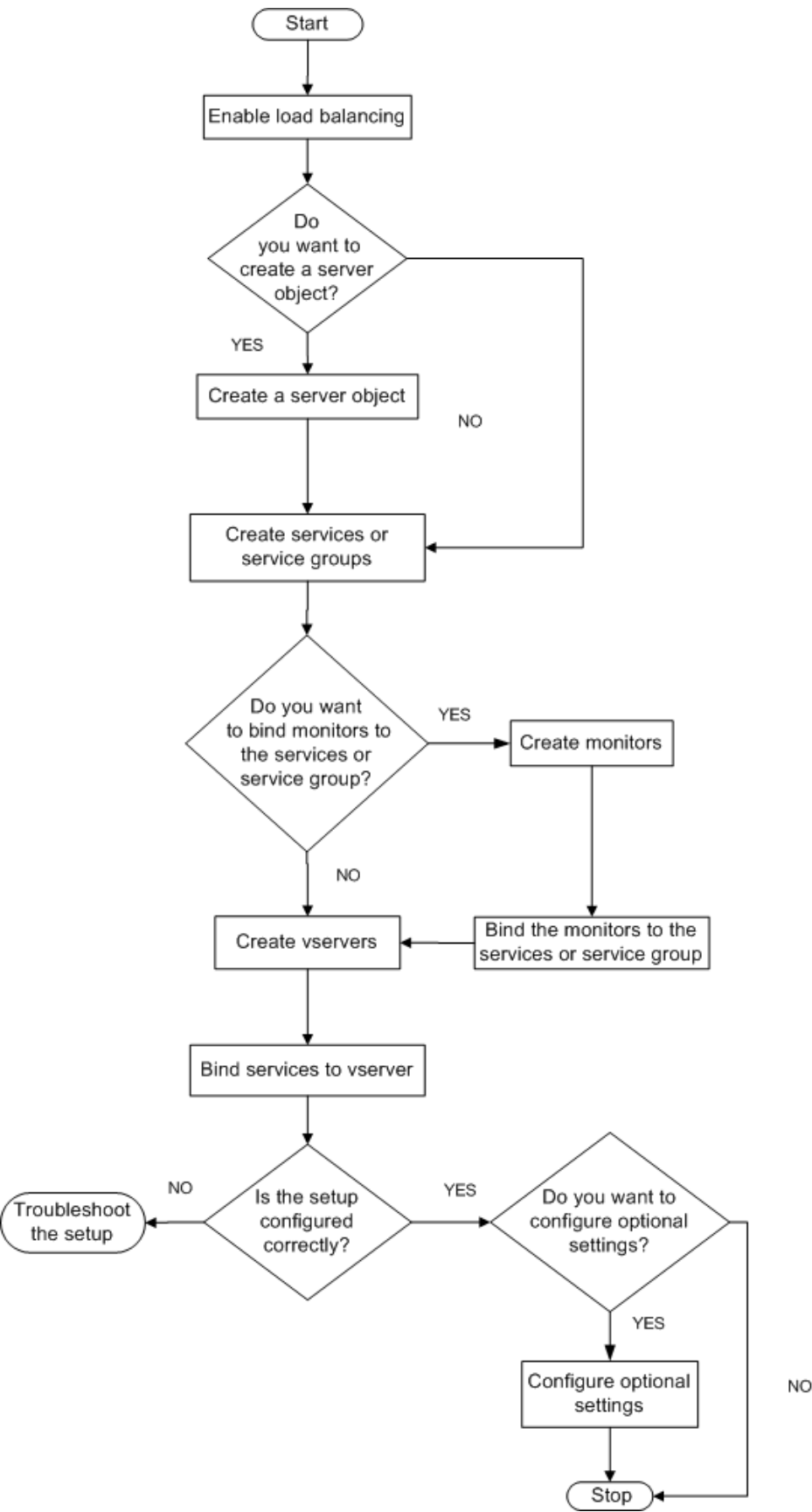
注:

構成を適用した後で、各エンティティがどのように実行されているかを示す統計情報を表示できます。統計ユーティリティ、または
`stat lb vserver <仮想サーバー名>` コマンドを使用します。仮想サーバー名 >

オプションで、サービスに重要度 (Weight) を割り当てることができます。割り当てられた重要度に基づいてサービスが負荷分散されます。ただし、負荷分散機能の導入時には詳細な重要度を構成せずに、基本的なパーシステンス設定 (特定サーバーへの接続の保持) と構成保護設定のみを行えます。

次のフローチャートは、一連の構成タスクを示しています。

図 1: 負荷分散を構成するための一連のタスク



負荷分散を有効にする

負荷分散を構成する前に、負荷分散機能が有効になっているか確認します。

CLI を使用して負荷分散を有効にするには

コマンドプロンプトで次のコマンドを入力し、負荷分散を有効にして構成を確認します。

- enable feature lb
- show feature

例

““ pre codeblock

```
enable feature lb
Done
show feature
```

1	Feature	Acronym	Status	
2	-----	-----	-----	1) Web
	Logging	WL	OFF	2) Surge
	Protection	SP	OFF	3) Load Balancing
	LB	ON	.	9) SSL
	Offloading	SSL	ON	. . . Done
	<!--NeedCopy-->	``		

GUI を使用して負荷分散を有効にするには

1. ナビゲーションペインで、[System] を展開し、[Settings] をクリックします。
2. 詳細ペインの [Modes and Features] で、[Change basic features] をクリックします。
3. [Configure Basic Features] ダイアログボックスで、[Load Balancing] チェックボックスをオンにして [OK] をクリックします。
4. 「Enable/Disable Feature(s)?」メッセージが表示されたら、[はい] をクリックします。

サービスと仮想サーバーの構成

負荷分散するサービスを特定したら、負荷分散の初回構成を実装できます。これを行うには、サービスオブジェクトと負荷分散仮想サーバーを作成して、それらをバインドします。

CLI を使用して初期負荷分散構成を実装するには

コマンドプロンプトで次のコマンドを入力し、初回構成を実装して確認します。

- `add service \<名前\> \<IP アドレス\> \<サービスタイプ\> \<ポート\>`
- `add lb vserver \<仮想サーバー名\> \<サービスタイプ\> \[\<IP アドレス\> \<ポート\> \]`
- `bind lb vserver \<名前\> \<サービス名\>`
- `show service bindings \<サービス名\>`

例

```

1 > add service service-HTTP-1 10.102.29.5 HTTP 80
2 Done
3 > add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
4 Done
5 > bind lb vserver vserver-LB-1 service-HTTP-1
6 Done
7 > show service bindings service-HTTP-1
8     service-HTTP-1 (10.102.29.5:80) - State : DOWN
9
10     1)          vserver-LB-1 (10.102.29.60:80) - State : DOWN
11 Done
12 <!--NeedCopy-->

```

GUI を使用して初期負荷分散構成を実装するには

1. [Traffic Management] [Load Balancing] の順に選択します。
2. 詳細ペインの [Getting Started] で、[Load Balancing wizard] をクリックし、ウィザードの説明に従って基本的な負荷分散セットアップを作成します。
3. ナビゲーションペインに戻り、[Load Balancing] を展開して、[Virtual Servers] をクリックします。
4. 構成した仮想サーバーを選択し、ページの下部に表示されるパラメーターが正しく構成されていることを確認します。
5. [開く] をクリックします。
6. [Services] タブの各サービスで [Active] チェックボックスがオンになっていることを確認し、各サービスが仮想サーバーにバインドされていることを確認します。

パーシステンス設定

April 21, 2022

仮想サーバーにより実行されるサービスへの接続を維持したい場合（電子商取引で使用される接続など）は、その仮想サーバーに対してパーシステンスを構成する必要があります。アプライアンスは、まず構成されている負荷分散方

式に基づいてサーバーを選択しますが、それ以降は同じクライアントからのすべての要求を同じサーバーに転送します。

パーシステンスを構成すると、サーバーの初回選択時以降の要求で、負荷分散方式が無視されます。構成したパーシステンスの適用先サービスがダウンしている場合は、負荷分散方式に基づいて新しいサービスが選択され、同じクライアントからのそれ以降の要求はそのサービスに永続的に割り当てられます。選択したサービスが Out Of Service 状態の場合、未処理の要求の処理は続行されますが、新しい要求や接続は受け付けられません。シャットダウン期間が経過すると、既存の接続が閉じます。次の表は、設定できるパーシステンスの種類を示しています。

永続性タイプ	固定接続数
Source IP、SSL Session ID、Rule、DESTIP、SRCIPDESTIP	250K
CookieInsert、URL passive、Custom Server ID	メモリの上限。CookieInsert の場合、タイムアウトが 0 でなければ、メモリの上限に達するまで任意の数の接続が許可されます。

表 1. 同時持続的接続の数の制限

アプライアンスのリソース不足により構成済みのパーシステンスが維持できない場合は、負荷分散方式に基づいてサーバーが選択されます。パーシステンスは、その種類で構成された時間だけ保持されます。一部のパーシステンスの種類は、特定の仮想サーバーに固有です。次の表は、それらの関係を示しています。

Persistence					
TypeHeader					
1	HTTP	HTTPS	TCP	UDP/IP	SSL_Bridge
接続元 IP	はい	はい	はい	はい	はい
CookieInsert	はい	はい	いいえ	いいえ	いいえ
SSL Session ID	いいえ	はい	いいえ	いいえ	はい
URL Passive	はい	はい	いいえ	いいえ	いいえ
Custom Server ID	はい	はい	いいえ	いいえ	いいえ
規則	はい	はい	いいえ	いいえ	いいえ
SRCIPDESTIP	-	-	はい	はい	-
DESTIP	-	-	はい	はい	-

表 2. 仮想サーバーのタイプごとに使用可能な永続性タイプ

仮想サーバーのグループに対して、パーシステンスを指定することもできます。グループに対してパーシステンスを有効にすると、クライアント要求を受信した仮想サーバーに関係なく、クライアント要求は同じサーバーに送信され

ます。パーシステンスの構成時間が経過すると、着信したクライアント要求に対して、グループの任意の仮想サーバーが選択されます。

一般的に使用される 2 つのパーシステンスの種類は、Cookie に基づくパーシステンスと URL のサーバー ID に基づくパーシステンスです。

Cookie に基づくパーシステンスの設定

Cookie に基づくパーシステンスを有効にすると、Citrix ADC アプライアンスは、HTTP 応答の Set-Cookie ヘッダーフィールドに、HTTP Cookie を追加します。Cookie には、HTTP 要求の送信先のサービスに関する情報が含まれています。クライアントは Cookie を保存して、それ以降のすべての要求に含めます。ADC は Cookie を使用して、これらの要求に対するサービスを選択します。HTTP または HTTPS タイプの仮想サーバーに対して、この種類のパーシステンスを使用できます。

Citrix ADC アプライアンスは、<NSC_XXXX>=<ServiceIP> <ServicePort> の Cookie を挿入します。

各項目の意味は次のとおりです：

- «NSC_XXXX» は、仮想サーバー名から導出される仮想サーバー ID です。
- «ServiceIP» は、サービスの IP アドレスの 16 進数値です。
- «ServicePort» は、サービスのポートの 16 進数値です。

ADC は、Cookie を挿入するときに ServiceIP と ServicePort を暗号化し、Cookie を受け取ったときにこれらを復号化します。

注：クライアントが HTTP Cookie を保存できない場合は、以降の要求に HTTP Cookie が含まれなくなり、パーシステンスは適用されません。

デフォルトでは、ADC アプライアンスは Netscape 仕様に準拠して、HTTP Cookie バージョン 0 を送信します。また、RFC 2109 に準拠して、バージョン 1 を送信することもできます。

HTTP Cookie に基づくパーシステンスに対して、タイムアウト値を設定できます。以下の点に注意してください：

- HTTP Cookie バージョン 0 が使用されている場合、Citrix ADC アプライアンスは、世界協定時刻 (GMT) とタイムアウト値の合計として計算される、Cookie の有効期限 (HTTP Cookie の expires 属性) の絶対 GMT を挿入します。
- HTTP Cookie バージョン 1 が使用されている場合、ADC アプライアンスは相対有効期限 (HTTP Cookie の Max-Age 属性) を挿入します。この場合、クライアントソフトウェアが実際の有効期限を計算します。

注：現在インストールされているほとんどのクライアントソフトウェア (Microsoft Internet Explorer と Netscape ブラウザー) は、HTTP Cookie バージョン 0 を理解しますが、一部の HTTP プロキシは HTTP Cookie バージョン 1 を理解します。

タイムアウト値を 0 に設定すると、使用されている HTTP Cookie バージョンに関係なく、ADC アプライアンスは有効期限を指定しなくなります。この場合、有効期限はクライアントソフトウェアに依存し、そのような Cookie は、

そのソフトウェアがシャットダウンすると、無効になります。この種類のパーシステンスはシステムリソースを消費しません。したがって、好きな数だけ永続的なクライアントを含めることができます。

管理者は HTTPCookie のバージョンを変更できます。

CLI を使用して **HTTPCookie** のバージョンを変更するには

コマンドプロンプトで次を入力します。

```
1 set ns param [-cookieversion ( 0 | 1 )]  
2 <!--NeedCopy-->
```

例:

```
1 set ns param -cookieversion 1  
2 <!--NeedCopy-->
```

GUI を使用して **HTTPCookie** のバージョンを変更するには

1. [System] > [Settings] に移動します。
2. 詳細ペインで、[Change HTTP Parameters] をクリックします。
3. [Configure HTTP Parameters] ダイアログボックスの [Cookie] で、[Version 0] または [Version 1] を選択します。

注: パラメーターについて詳しくは、「Cookie に基づくパーシステンスの設定」を参照してください。

CLI を使用して **Cookie** に基づいて永続性を構成するには

コマンドプロンプトで次のコマンドを入力し、Cookie に基づくパーシステンスを構成して確認します。

```
1 set lb vserver <name> -persistenceType COOKIEINSERT  
2  
3 show lb vserver <name>  
4 <!--NeedCopy-->
```

例:

```
1 set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT  
2 Done  
3 show lb vserver vserver-LB-1  
4     vserver-LB-1 (10.102.29.60:80) - HTTP    Type: ADDRESS  
5     .  
6     .  
7     .  
8     Persistence: COOKIEINSERT (version 0)  
9     Persistence Timeout: 2 min
```



```
10      .
11      .
12      .
13      Done
14      <!--NeedCopy-->
```

GUI を使用して **Cookie** に基づいて永続性を構成するには

1. [Traffic Management] > [Load Balancing] > [Virtual Servers] の順に選択します。
2. 詳細ペインで、パーシステンスを設定する仮想サーバー（たとえば、vserver-LB-1）を選択し、[Open] をクリックします。
3. [Configure Virtual Server (Load Balancing)] ダイアログボックスの [Method and Persistence] タブにある [Persistence] リストで、[COOKIEINSERT] を選択します。
4. [Time-out (min)] テキストボックスに、タイムアウト値（たとえば、「2」）を入力します。
5. [OK] をクリックします。
6. パーシステンスを設定した仮想サーバーを選択して、ペインの下部にある [Details] セクションを表示し、仮想サーバーが正しく構成されていることを確認します。

URL のサーバー ID に基づくパーシステンスの構成

Citrix ADC アプライアンスは、URL のサーバー ID に基づいて永続性を維持できます。「URL パッシブパーシステンス」と呼ばれる方法では、ADC はサーバー応答からサーバー ID を抽出して、クライアント要求の URL クエリに埋め込みます。サーバー ID は、16 進数で表記された IP アドレスとポートです。ADC は、以降のクライアント要求からサーバー ID を抽出し、それを使用してサーバーを選択します。

URL パッシブパーシステンスでは、ペイロード式またはポリシーインフラストラクチャ式を設定し、クライアント要求に含まれるサーバー ID の場所を指定する必要があります。式について詳しくは、「[ポリシーの構成とリファレンス](#)」を参照してください。

注：サーバー ID をクライアント要求から抽出できない場合、サーバーの選択は負荷分散方式に基づいて行われます。

例：ペイロード式

式「URLQUERY contains sid=」では、クライアント要求の URL クエリから、「sid=」の後のサーバー ID が抽出されます。したがって、URL <http://www.citrix.com/index.asp?\\&sid;c0a864100050> のリクエストは、IP アドレス 10.102.29.10 とポート 80 のサーバーに送信されます。

タイムアウト値は、この種類のパーシステンスには影響しません。このパーシステンスは、サーバー ID がクライアント要求から抽出できる限り維持されます。この種類のパーシステンスはシステムリソースを消費しないため、保持されるクライアント数に制限はありません。

注:

パラメーターについて詳しくは、「[負荷分散](#)」を参照してください。

CLI を使用して **URL** のサーバー **ID** に基づいて永続性を構成するには

コマンドプロンプトで次のコマンドを入力し、URL のサーバー ID に基づくパーシステンスを構成して確認します。

```
1 set lb vserver <name> -persistenceType URLPASSIVE
2
3 <show lb vserver <name>
4 <!--NeedCopy-->
```

例:

```
1 set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
2 Done
3 show lb vserver vserver-LB-1
4     vserver-LB-1 (10.102.29.60:80) - HTTP    Type: ADDRESS
5     .
6     .
7     .
8     Persistence: URLPASSIVE
9     Persistence Timeout: 2 min
10    .
11    .
12    .
13 Done
14 <!--NeedCopy-->
```

GUI を使用して **URL** のサーバー **ID** に基づいて永続性を構成するには

1. [Traffic Management] > [Load Balancing] > [Virtual Servers] の順に選択します。
2. 詳細ペインで、パーシステンスを設定する仮想サーバー（たとえば、vserver-LB-1）を選択し、[Open] をクリックします。
3. [Configure Virtual Server (Load Balancing)] ダイアログボックスの [Method and Persistence] タブにある [Persistence] リストで、[URLPASSIVE] を選択します。
4. [Time-out (min)] テキストボックスに、タイムアウト値（たとえば、「2」）を入力します。
5. [Rule] ボックスに、有効な式を入力します。また、[Rule] ボックスの横にある [Configure] をクリックし、[Create Expression] ダイアログボックスを使用して式を作成します。
6. [OK] をクリックします。
7. パーシステンスを設定した仮想サーバーを選択して、ペインの下部にある [Details] セクションを表示し、仮想サーバーが正しく構成されていることを確認します。

負荷分散設定を保護する機能の構成

April 21, 2022

正しく動作していない仮想サーバーに関する通知を提供するように URL リダイレクトを構成できます。また、プライマリ仮想サーバーが使用できなくなった場合にその役割を引き継ぐバックアップ仮想サーバーを構成することもできます。

URL リダイレクトの構成

HTTP または HTTPS タイプの仮想サーバーがダウンしたり無効になったりしたときに、アプライアンスのステータスを通信するためのリダイレクト URL を構成できます。この URL は、ローカルリンクでもリモートリンクでも構いません。アプライアンスでは、HTTP 302 リダイレクトが使用されます。

リダイレクトは、絶対 URL でも相対 URL でも構いません。構成したリダイレクト URL に絶対 URL が含まれている場合、着信した HTTP 要求で指定された URL に関係なく、その絶対 URL にリダイレクトされます。構成したリダイレクト URL にドメイン名のみが含まれている場合（相対 URL）、そのドメインに着信 URL を追記した場所にリダイレクトされます。

注：負荷分散仮想サーバーで、バックアップ仮想サーバーとリダイレクト URL の両方を構成した場合、バックアップ仮想サーバーがリダイレクト URL よりも優先されます。この場合は、プライマリおよびバックアップ仮想サーバーの両方がダウンしているときに、リダイレクトが使用されます。

CLI を使用してクライアント要求を **URL** へリダイレクトするように仮想サーバーを構成するには

コマンドプロンプトで次のコマンドを入力し、クライアント要求が URL にリダイレクトされるように仮想サーバーを構成して確認します。

- `set lb vserver <名前> -redirectURL <URL>`
- `show lb vserver \<名前\>`

例

```
1 > set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.  
   com/mysite/maintenance  
2   Done  
3 > show lb vserver vserver-LB-1  
4   vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS  
5   State: DOWN  
6   Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)  
7   .  
8   .  
9   .  
10  Redirect URL: http://www.newdomain.com/mysite/maintenance
```

```
11      .
12      .
13      .
14      Done
15      >
16      <!--NeedCopy-->
```

GUI を使用してクライアント要求を **URL** へリダイレクトするように仮想サーバーを構成するには

1. [Traffic Management] > [Load Balancing] > [Virtual Servers] の順に選択します。
2. 詳細ペインで、URL リダイレクトを構成する仮想サーバー（たとえば、vserver-LB-1）を選択し、[Open] をクリックします。
3. [Configure Virtual Server (Load Balancing)] ダイアログボックスで、[Advanced] タブの [Redirect URL] テキストボックスに、URL（たとえば、「<http://www.newdomain.com/mysite/maintenance>」）を入力して [OK] をクリックします。
4. サーバーに設定したリダイレクト URL が、ペインの下部にある [Details] セクションに表示されていることを確認します。

バックアップ仮想サーバーの設定

プライマリ仮想サーバーがダウンしているか無効である場合、アプライアンスは接続またはクライアント要求をバックアップ仮想サーバーに送信し、クライアントトラフィックをバックアップ仮想サーバーからサービスに転送できます。アプライアンスは、サイトの停止またはメンテナンスに関する通知メッセージをクライアントに送信することもできます。バックアップ仮想サーバーはプロキシであり、クライアントに対して透過的です。

仮想サーバーを作成したり、既存の仮想サーバーのオプションパラメーターを変更したりする場合は、バックアップ仮想サーバーを構成できます。また、既存のバックアップ仮想サーバーに対してバックアップ仮想サーバーを構成し、カスケードされたバックアップ仮想サーバーを作成することもできます。バックアップ仮想サーバーをカスケードする最大の深さは、10 です。アプライアンスは、起動しているバックアップ仮想サーバーを検索し、その仮想サーバーにアクセスしてコンテンツを提供します。

プライマリおよびバックアップ仮想サーバーがダウンしたり、それらのサーバーの処理要求数がしきい値に達したりしたときに、プライマリで URL がリダイレクトされるように構成できます。

注：バックアップ仮想サーバーが存在しない場合は、リダイレクト URL を構成しないとエラーメッセージが表示されます。バックアップ仮想サーバーとリダイレクト URL の両方が構成されている場合は、バックアップ仮想サーバーが優先されます。

CLI を使用してバックアップ仮想サーバーを構成するには

コマンドプロンプトで次のコマンドを入力し、バックアップサーバーを構成して確認します。

- `set lb vserver \< 名前> \[-backupVserver \< 文字列\>\]`
- `show lb vserver \< 名前>`

例

“ pre codeblock

```
set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
Done
show lb vserver vserver-LB-1
vserver-LB-1 (10.102.29.60:80) - HTTP Type: ADDRESS
State: DOWN
Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
.
.
.
Backup: vserver-LB-2
.
.
.
Done
“
```

GUI を使用してバックアップ仮想サーバーをセットアップするには

1. [Traffic Management] > [Load Balancing] > [Virtual Servers] の順に選択します。
2. 詳細ペインで、バックアップ仮想サーバーを設定する仮想サーバー（たとえば、vserver-LB-1）を選択し、[Open] をクリックします。
3. [Configure Virtual Server (Load Balancing)] ダイアログボックスの [Advanced] タブにある [Backup Virtual Server] リストで、バックアップ仮想サーバー（たとえば、vserver-LB-2）を選択し、[OK] をクリックします。
4. 設定したバックアップ仮想サーバーが、ペインの下部にある [Details] セクションに表示されていることを確認します。

注：ダウンしたプライマリサーバーが復帰した場合でも、その仮想サーバーをプライマリとして明示的に再設定するまでバックアップ仮想サーバーがプライマリサーバーとして動作するようにするには、[Disable Primary When Down] チェックボックスをオンにします。

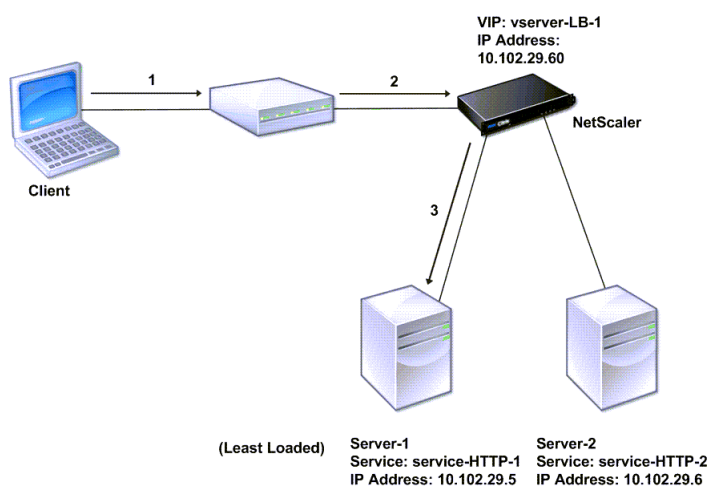
一般的な負荷分散シナリオ

April 25, 2022

負荷分散セットアップでは、Citrix ADC アプライアンスはクライアントとサーバーファームの間に論理的に配置され、サーバーへのトラフィックフローを管理します。

次の図は、基本的な負荷分散構成のトポロジを示しています。

図 1: 基本的な負荷分散トポロジ

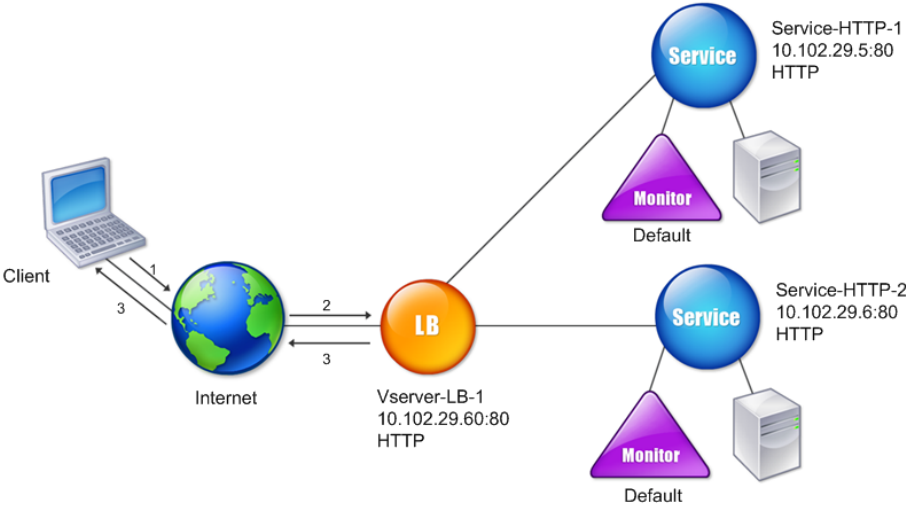


仮想サーバーは、クライアントからの要求に対してサービスを選択して割り当てます。サービス「service-HTTP-1」と「service-HTTP-2」が作成されて、「virtual server-LB-1」という仮想サーバーにバインドされている、前の図のシナリオについて考えてみましょう。virtual server-LB-1 は、クライアント要求を service-HTTP-1 または service-HTTP-2 に転送します。システムは Least Connections 負荷分散方式を使用して、各要求のサービスを選択します。次の表は、システムで設定する必要がある基本的なエンティティの名前と値を示しています。

表 1. LB 構成パラメーター値

次の図は、前の表で説明した負荷分散のサンプル値と、必須パラメーターを示しています。

図 2: 負荷分散エンティティモデル



次の表に、コマンドラインインターフェイスを使用してこの負荷分散セットアップを構成するためのコマンドを示します。

タスク	コマンド
負荷分散を有効にする	<code>enable feature lb</code>
「service-HTTP-1」というサービスを作成する	<code>add service service-HTTP-1 10.102.29.5 HTTP 80</code>
「service-HTTP-2」というサービスを作成する	<code>add service service-HTTP-2 10.102.29.6 HTTP 80</code>
「vserver-LB-1」という仮想サーバーを作成する	<code>add lb vserver vserver-LB-1 HTTP 10.102.29.60 80</code>
「service-HTTP-1」というサービスを「vserver-LB-1」という仮想サーバーにバインドする	<code>bind lb vserver vserver-LB-1 service-HTTP-1</code>
「service-HTTP-2」というサービスを「vserver-LB-1」という仮想サーバーにバインドする	<code>bind lb vserver vserver-LB-1 service-HTTP-2</code>

表 2. 初期構成タスク

初期構成タスクの詳細については、「[基本的な負荷分散のセットアップ](#)」を参照してください。

タスク	コマンド
「vserver-LB-1」という仮想サーバーのプロパティを表示する	<code>show lb vserver vserver-LB-1</code>
「vserver-LB-1」という仮想サーバーの統計情報を表示する	<code>stat lb vserver vserver-LB-1</code>
「service-HTTP-1」というサービスのプロパティを表示する	<code>show service service-HTTP-1</code>
「service-HTTP-1」というサービスの統計情報を表示する	<code>stat service service-HTTP-1</code>
「service-HTTP-1」というサービスのバインド情報を表示する	<code>show service bindings service-HTTP-1</code>

表 3. 検証タスク

タスク	コマンド
「vserver-LB-1」という仮想サーバーにパーシステンスを構成する	<code>set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2</code>
「vserver-LB-1」という仮想サーバーに COOKIEINSERT パーシステンスを構成する	<code>set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT</code>
「vserver-LB-1」という仮想サーバーに URLPassive パーシステンスを構成する	<code>set lb vserver vserver-LB-1 -persistenceType URLPASSIVE</code>
クライアント要求を「vserver-LB-1」という仮想サーバー上の URL へリダイレクトするように仮想サーバーを構成する	<code>set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance</code>
「vserver-LB-1」という仮想サーバーにバックアップ仮想サーバーを設定する	<code>set lb vserver vserver-LB-1 -backupVserver vserver-LB-2</code>

表 4. カスタマイズタスク

パーシステンスの構成について詳しくは、「[パーシステンス設定の選択と構成]」を参照してください。(</en-us/citrix-adc/12-1/getting-started-with-citrix-adc/load-balancing/configure-persistence-settings.html>) クライアント要求を URL にリダイレクトするための仮想サーバーの構成およびバックアップ仮想サーバーのセットアップについて詳しくは、「[負荷分散設定を保護する機能の構成](#)」を参照してください。

圧縮による負荷分散トラフィックの速度向上

April 21, 2022

圧縮は、帯域幅の使用を最適化する一般的な手段であり、ほとんどの Web ブラウザーで圧縮データがサポートされています。圧縮機能を有効にすると、Citrix ADC アプライアンスがクライアントからの要求をインターセプトして、そのクライアントが圧縮コンテンツに対応しているかどうかを判断します。また、アプライアンスがサーバーからの HTTP 応答を受信すると、そのコンテンツを調べて圧縮可能かどうかを決定します。コンテンツが圧縮可能な場合、アプライアンスはコンテンツを圧縮し、応答のヘッダーを変更して実行した圧縮の種類を示し、圧縮コンテンツをクライアントに転送します。

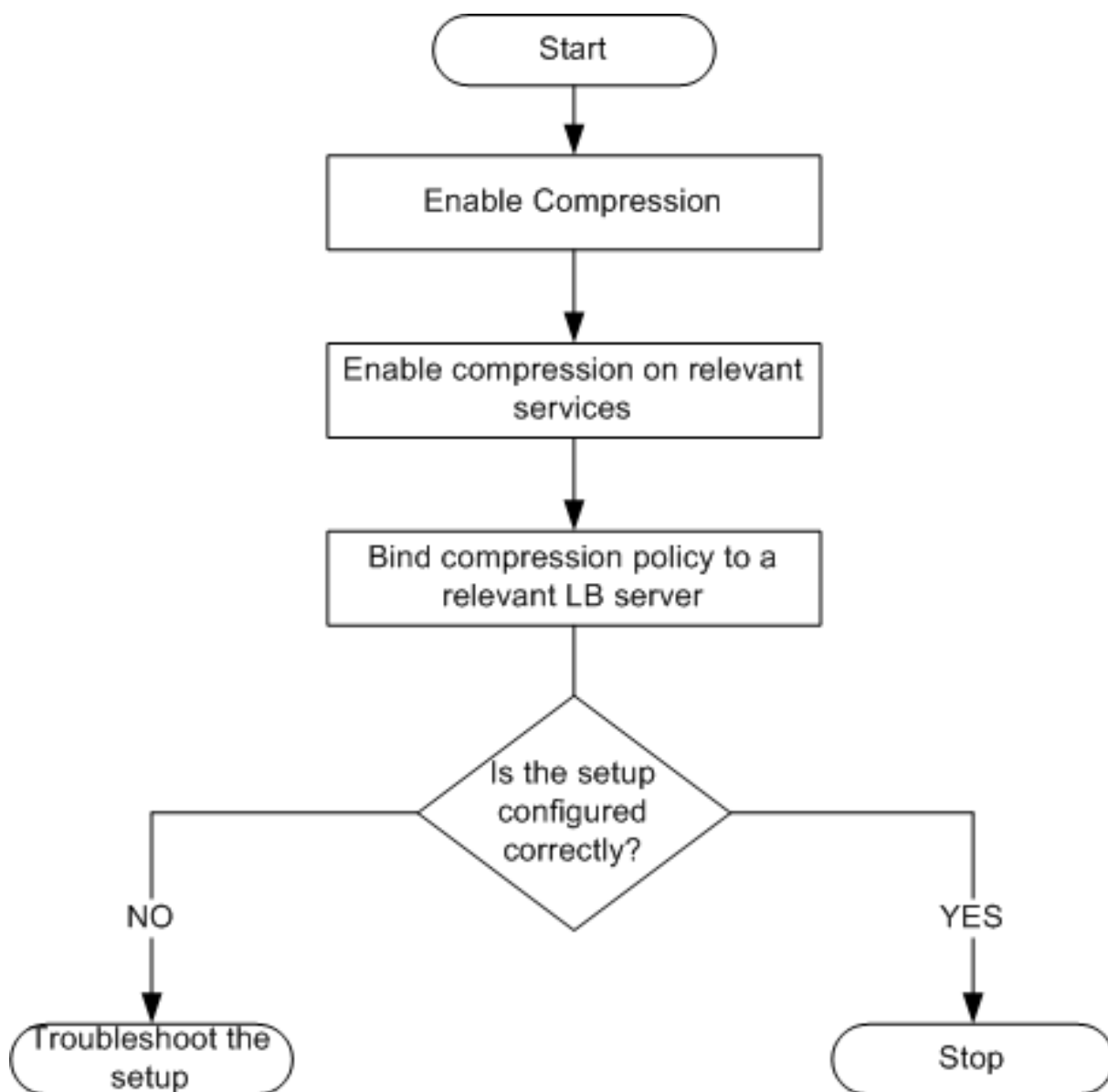
Citrix ADC 圧縮は、ポリシーベースの機能です。ポリシーは要求と応答をフィルタリングして圧縮される応答を特定し、各応答に適用する圧縮の種類を指定します。アプライアンスは、text/html、text/plain、text/xml、text/css、text/rtf、application/msword、application/vnd.ms-excel、application/vnd.ms-powerpoint などの一般的な MIME タイプを圧縮する複数の組み込みポリシーを提供します。また、カスタムポリシーを作成することもできます。アプライアンスは、application/octet-stream、binary、bytes などの圧縮済みの MIME タイプや、GIF、JPEG などの画像形式を圧縮しません。

圧縮を構成するには、グローバルな圧縮機能を有効にしてから、圧縮対象の応答を配信するサービスごとに圧縮を有効にする必要があります。負荷分散またはコンテンツスイッチ向けに仮想サーバーを構成済みの場合は、それらの仮想サーバーにポリシーをバインドする必要があります。それ以外の場合、アプライアンスを経由するすべてのトラフィックにポリシーが適用されます。

圧縮を構成するタスクの順序

次のフローチャートは、負荷分散セットアップで基本的な圧縮を構成するタスクの順序を示しています。

図 1: 圧縮を構成するためのタスクの順序



注：上図の手順では、負荷分散が構成済みであることが想定されています。

圧縮を有効化

デフォルトでは、圧縮が無効になっています。クライアントに送信される HTTP 応答の圧縮を許可するには、圧縮機能を有効にする必要があります。

CLI を使用して圧縮を有効にするには

コマンドプロンプトで次のコマンドを入力し、圧縮を有効化して構成を確認します。

- enable ns feature CMP

- show ns feature

```
1      > enable ns feature CMP
2
3
4
5
6      Done
7
8
9      > show ns feature
10
11
12
13
14
15          Feature                      Acronym      Status
16
17          -----
18
19
20      1)      Web Logging                WL           ON
21
22
23      2)      Surge Protection            SP           OFF
24
25
26
27      .
28
29
30      7) Compression Control CMP ON
31
32
33      8)      Priority Queuing            PQ           OFF
34
35
36      .
37
38
39      Done
40      <!--NeedCopy-->
```

GUI を使用して圧縮を有効にするには

1. ナビゲーションペインで、[System] を展開し、[Settings] をクリックします。
2. 詳細ペインの [Modes and Features] で、[Change basic features] をクリックします。
3. [Configure Basic Features] ダイアログボックスで、[Compression] チェックボックスをオンにしてから [OK] をクリックします。
4. [Enable/Disable Feature(s)?] ダイアログボックスで、[Yes] をクリックします。

データを圧縮するサービスの設定

グローバルな圧縮設定を有効にしたら、圧縮対象のファイルを配信するサービスごとに圧縮を有効にする必要があります。

CLI を使用して特定のサービスの圧縮を有効にするには

コマンドプロンプトで次のコマンドを入力し、特定のサービスの圧縮を有効化して構成を確認します。

- `set service \<名前> -CMP YES`
- `show service \<名前>`

```
1 > show service SVC_HTTP1
2
3
4 SVC_HTTP1 (10.102.29.18:80) - HTTP
5
6
7 State: UP
8
9
10 Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)
11
12
13 Time since last state change: 0 days, 03:03:37.200
14
15
16 Server Name: 10.102.29.18
17
18
19 Server ID : 0    Monitor Threshold : 0
20
21
22 Max Conn: 0      Max Req: 0      Max Bandwidth: 0 kbits
23
24
25 Use Source IP: NO
26
27
28 Client Keepalive(CKA): NO
29
30
31 Access Down Service: NO
32
33
34 TCP Buffering(TCPB): NO
35
36
37 HTTP Compression(CMP): YES
38
```

```
39
40 Idle timeout: Client: 180 sec   Server: 360 sec
41
42
43 Client IP: DISABLED
44
45
46 Cacheable: NO
47
48
49 SC: OFF
50
51
52 SP: OFF
53
54
55 Down state flush: ENABLED
56
57
58
59
60
61 1)      Monitor Name: tcp-default
62
63
64 State: DOWN      Weight: 1
65
66
67 Probes: 1095      Failed [Total: 1095 Current: 1095]
68
69
70 Last response: Failure - TCP syn sent, reset received.
71
72
73 Response Time: N/A
74
75
76 Done
77 <!--NeedCopy-->
```

GUI を使用して特定のサービスの圧縮を有効にするには

1. [Traffic Management] > [Load Balancing] > [Services] の順に移動します。
2. 詳細ペインで圧縮を設定するサービス（たとえば、[service-HTTP-1]）を選択し、[Open] をクリックします。
3. [Advanced] タブの [Settings] で、[Compression] チェックボックスをオンにして [OK] をクリックします。
4. サービスが選択されている場合はペインの下部にある **[Details]** に [HTTP Compression(CMP): ON] が表示されていることを確認します。

仮想サーバーへの圧縮ポリシーのバインド

仮想サーバーに圧縮ポリシーをバインドすると、ポリシーは、その仮想サーバーに関連付けられたサービスによってのみ評価されます。仮想サーバーへの圧縮ポリシーのバインドは、[Configure Virtual Server (Load Balancing)] ダイアログボックスまたは [Compression Policy Manager] ダイアログボックスを使用して行います。このトピックには、[Configure Virtual Server (Load Balancing)] ダイアログボックスを使用して、圧縮ポリシーを負荷分散仮想サーバーにバインドする手順が含まれています。[Compression Policy Manager] ダイアログボックスを使用して負荷分散仮想サーバーに圧縮ポリシーをバインドする方法については、「[ポリシーマネージャーによるポリシーの構成およびバインド](#)」を参照してください。

コマンドラインを使用して仮想サーバーへの圧縮ポリシーをバインドまたはバインド解除するには

コマンドプロンプトで次のコマンドを入力し、負荷分散仮想サーバーへの圧縮ポリシーをバインドまたはバインド解除して構成を確認します。

- (bind|unbind) lb vserver \<名前> -policyName \<文字列>
- show lb vserver \<名前>

例:

```
1      bind lb vserver lbvip -policyName ns_cmp_msapp
2      Done
3      > show lb vserver lbvip
4      lbvip (8.7.6.6:80) - HTTP Type: ADDRESS
5      State: UP
6      Last state change was at Thu May 28 05:37:21 2009 (+685 ms)
7      Time since last state change: 19 days, 04:26:50.470
8      Effective State: UP
9      Client Idle Timeout: 180 sec
10     Down state flush: ENABLED
11     Disable Primary Vserver On Down : DISABLED
12     Port Rewrite : DISABLED
13     No. of Bound Services : 1 (Total) 1 (Active)
14     Configured Method: LEASTCONNECTION
15     Current Method: Round Robin, Reason: Bound service's state changed to
16     UP
17     Mode: IP
18     Persistence: NONE
19     Vserver IP and Port insertion: OFF
20     Push: DISABLED Push VServer:
21     Push Multi Clients: NO
22     Push Label Rule:
23     Bound Service Groups:
24     1) Group Name: Service-Group-1
25
26     1) Service-Group-1 (10.102.29.252: 80) - HTTP State: UP Weight: 1
27
```

```
28 1) Policy : ns_cmp_msapp Priority:0
29 Done
30 <!--NeedCopy-->
```

GUI を使用して負荷分散仮想サーバーへの圧縮ポリシーをバインドまたはバインド解除するには

1. [Traffic Management] > [Load Balancing] > [Virtual Servers] の順に選択します。
2. 詳細ペインで、圧縮ポリシーのバインドまたはバインド解除を行う仮想サーバー（たとえば、[Vserver-LB-1]）を選択し、[Open] をクリックします。
3. [Configure Virtual Server (Load Balancing)] ダイアログボックスで、[Policies] タブの [Compression] をクリックします。
4. 次のいずれかを行います：
 - 圧縮ポリシーをバインドする場合は、[Insert Policy] をクリックしてから仮想サーバーにバインドするポリシーを選択します。
 - 圧縮ポリシーをバインド解除する場合は、仮想サーバーからバインド解除するポリシーの名前を選択し、[Unbind Policy] をクリックします。
5. [OK] をクリックします。

SSL による負荷分散トラフィックのセキュリティ保護

April 21, 2022

Citrix ADC SSL オフロード機能は、SSL トランザクションを行う Web サイトのパフォーマンスを、透過的に向上させます。SSL オフロードでは、CPU 負荷の高い SSL 暗号化および復号化タスクをローカル Web サーバーからアプライアンスにオフロードすることにより、SSL データの処理によるサーバーパフォーマンスの低下を引き起こすことなく、Web アプリケーションを安全に配信できます。SSL トラフィックを復号化すると、あらゆる標準サービスで処理できるようになります。SSL プロトコルは、さまざまな種類の HTTP および TCP データとシームレスに機能して、このようなデータを使用するトランザクションに、セキュリティ保護されたチャネルを提供します。

SSL を設定するには、まず SSL を有効にする必要があります。次に、アプライアンスで HTTP または TCP サービスおよび SSL 仮想サーバーを構成し、そのサービスを仮想サーバーにバインドします。証明書とキーのペアを追加して SSL 仮想サーバーにバインドする必要もあります。Outlook Web Access サーバーを使用する場合は、SSL サポートを有効にするアクションとそのアクションに適用するポリシーを作成する必要があります。SSL 仮想サーバーは、暗号化された着信トラフィックをインターセプトして、ネゴシエートしたアルゴリズムを使用してそのトラフィックを復号化します。復号化されたデータは、アプライアンス上のほかのエンティティに転送され、適切に処理されます。

SSL オフロードの詳細については、「[SSL オフロードおよび SSL アクセラレーション](#)」を参照してください。

SSL を設定するタスクの順序

SSL を設定するには、まず SSL を有効にする必要があります。次に、Citrix ADC アプライアンスで SSL 仮想サーバーと HTTP または TCP サービスを作成する必要があります。最後に、有効な SSL 証明書と設定済みのサービスを、SSL 仮想サーバーにバインドする必要があります。

SSL 仮想サーバーは、暗号化された着信トラフィックを傍受して、ネゴシエートしたアルゴリズムを使用してそのトラフィックを解読します。復号化されたデータは、Citrix ADC アプライアンス上のほかのエンティティに転送され、適切に処理されます。

次のフローチャートには、基本的な SSL オフロードセットアップを設定するタスクの順序が示されています。

図 1: SSL オフロードを構成するための一連のタスク



SSL オフロードを有効にする

SSL オフロードを設定する前に、SSL 機能を有効にする必要があります。SSL 機能を有効にしなくてもアプライアンス上で SSL ベースのエンティティを設定できますが、それらのエンティティは SSL を有効にするまで動作しません。

CLI を使用して **SSL** を有効にする

コマンドプロンプトで次のコマンドを入力し、SSL オフロードを有効にして構成を確認します。

- enable ns feature SSL
- show ns feature

```
1 > enable ns feature ssl
2
3
4
5
6 Done
7
8
9 > show ns feature
10
11
12 Feature Acronym Status
13
14 -----
15
16
17
18 1) Web Logging WL ON
19
20
21 2) SurgeProtection SP OFF
22
23
24 3) Load Balancing LB ON . . .
25
26
27 9) SSL Offloading SSL ON
28
29
30 10) Global Server Load Balancing GSLB ON . .
31
32
33 Done >
34 <!--NeedCopy-->
```

GUI を使用して SSL を有効にする

1. ナビゲーションペインで、**[System]** を展開し、**[Settings]** をクリックします。
2. 詳細ペインの **[Modes and Features]** で、**[Change basic features]** をクリックします。
3. **[SSL Offloading]** チェックボックスをオンにして、**[OK]** をクリックします。
4. **[Enable/Disable Feature(s)?]** ダイアログボックスで、**[Yes]** をクリックします。

HTTP サービスを作成する

アプライアンス上の各サービスは、サーバー上の個々のアプリケーションとして機能します。構成したサービスは、アプライアンスがネットワーク上のサーバーにアクセスしてその状態を監視できるようになるまで無効状態になります。このトピックでは、HTTP サービスを作成する手順について説明します。

注: TCP トラフィックの場合は、このトピックと以降のトピックと同じ手順を使用しますが、HTTP サービスの代わりに TCP サービスを作成します。

CLI を使用して HTTP サービスを追加します

コマンドプロンプトで次のコマンドを入力し、HTTP サービスを追加して構成を確認します。

```
1 - add service <name> (<IP> | <serverName>) <serviceType> <port>
2 - show service <name>
3 <!--NeedCopy-->
```

例:

```
1 > add service SVC_HTTP1 10.102.29.18 HTTP 80
2
3
4 Done
5
6
7 > show service SVC_HTTP1
8
9
10 SVC_HTTP1 (10.102.29.18:80) - HTTP
11
12
13 State: UP
14
15
16 Last state change was at Wed Jul 15 06:13:05 2009
17
18
19 Time since last state change: 0 days, 00:00:15.350
20
21
```

```
22      Server Name: 10.102.29.18
23
24
25      Server ID : 0    Monitor Threshold : 0
26
27
28      Max Conn: 0      Max Req: 0      Max Bandwidth: 0 kbits
29
30
31      Use Source IP: NO
32
33
34      Client Keepalive(CKA): NO
35
36
37      Access Down Service: NO
38
39
40      TCP Buffering(TCPB): NO
41
42
43      HTTP Compression(CMP): YES
44
45
46      Idle timeout: Client: 180 sec    Server: 360 sec
47
48
49      Client IP: DISABLED
50
51
52      Cacheable: NO
53
54
55      SC: OFF
56
57
58      SP: OFF
59
60
61      Down state flush: ENABLED
62
63
64
65
66
67 1)      Monitor Name: tcp-default
68
69
70          State: UP      Weight: 1
71
72
73          Probes: 4      Failed [Total: 0 Current: 0]
74
```

```

75
76             Last response: Success - TCP syn+ack received.
77
78
79             Response Time: N/A
80
81
82     Done
83
84
85
86 <!--NeedCopy-->

```

GUI を使用して HTTP サービスを追加します

次の手順を実行します：

1. **[Traffic Management] > [SSL Offload] > [Servers]** の順に選択します。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Create Service]** ダイアログボックスの **[Service Name]**、**[Server]**、および **[Port]** ボックスに、それぞれサービスの名前、IP アドレス、およびポート（たとえば、「SVC_HTTP1」、「10.102.29.18」、「80」）を入力します。
4. **[Protocol]** ボックスの一覧で、サービスの種類（ここでは **[HTTP]**）を選択します。
5. **[Create]** をクリックしてから、**[Close]** をクリックします。構成した HTTP サービスが、**[Services]** ページに表示されます。
6. 作成したサービスを選択して、ペインの下部にある **[Details]** セクションを表示し、パラメーターが正しく構成されていることを確認します。

SSL ベースの仮想サーバーを追加する

基本的な SSL オフロードセットアップでは、SSL 仮想サーバーは暗号化されたトラフィックをインターセプトおよび復号化して、仮想サーバーにバインドされているサービスにクリアテキストメッセージを送信します。CPU 負荷の高い SSL 処理をアプライアンス側にオフロードすると、バックエンドサーバーでより多くの要求を処理できるようになります。

CLI を使用して SSL ベースの仮想サーバーを追加します

コマンドプロンプトで次のコマンドを入力し、SSL ベースの仮想サーバーを追加して構成を確認します。

```

1 - add lb vserver <name> <serviceType> [<IPAddress> <port>]
2 - show lb vserver <name>
3 <!--NeedCopy-->

```

注意: 安全に接続するには、SSL ベースの仮想サーバーを有効にする前に、有効な SSL 証明書を SSL ベースの仮想サーバーにバインドする必要があります。

例:

```
1 > add lb vserver vserver-SSL-1 SSL 10.102.29.50 443
2
3
4
5
6 Done
7
8
9 > show lb vserver vserver-SSL-1
10
11
12 vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS
13
14
15 State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
    06:33:08 2009 (+176 ms)
16
17
18 Time since last state change: 0 days, 00:03:44.120
19
20
21 Effective State: DOWN Client Idle Timeout: 180 sec
22
23
24 Down state flush: ENABLED
25
26
27 Disable Primary Vserver On Down : DISABLED
28
29
30 No. of Bound Services : 0 (Total) 0 (Active)
31
32
33 Configured Method: LEASTCONNECTION Mode: IP
34
35
36 Persistence: NONE
37
38
39 Vserver IP and Port insertion: OFF
40
41
42 Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
    Done
43 <!--NeedCopy-->
```

GUI を使用して SSL ベースの仮想サーバーを追加します

次の手順を実行します：

1. **[Traffic Management] > [SSL Offload] > [Virtual Servers]** の順に選択します。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Create Virtual Server (SSL Offload)]** ダイアログボックスの **[Name]**、**[IP Address]**、および **[Port]** ボックスに、それぞれ仮想サーバーの名前、IP アドレス、およびポート（たとえば、「Vserver-SSL-1」、「10.102.29.50」、「443」）を入力します。
4. **[Protocol]** ボックスの一覧で、仮想サーバーの種類（たとえば、[SSL]）を選択します。
5. **[Create]** をクリックしてから、**[Close]** をクリックします。
6. 作成した仮想サーバーを選択して、ペインの下部にある **[Details]** セクションを表示し、パラメーターが正しく構成されていることを確認します。証明書とキーのペアとサービスが仮想サーバーにバインドされていないため、仮想サーバーは **DOWN** としてマークされます。

注意：安全に接続するには、SSL ベースの仮想サーバーを有効にする前に、有効な SSL 証明書を SSL ベースの仮想サーバーにバインドする必要があります。

サービスの SSL 仮想サーバーへのバインド

SSL 仮想サーバーが復号化した受信データは、その仮想サーバーにバインドされたサービスに転送されます。

アプライアンスとサーバーの間のデータ転送は、暗号化したりクリアテキストで送信したりできます。アプライアンスとサーバーの間のデータ転送を暗号化する場合、トランザクション全体がエンドツーエンドで保護されることになります。エンドツーエンドのセキュリティのためのシステム構成について詳しくは、「[SSL オフロードおよびアクセラレーション](#)」を参照してください。

CLI を使用してサービスを仮想サーバーにバインドします

コマンドプロンプトで次のコマンドを入力し、サービスを SSL 仮想サーバーにバインドして構成を確認します。

```
1 - bind lb vserver <name> <serviceName>
2 - show lb vserver <name>
3 <!--NeedCopy-->
```

例：

```
1 > bind lb vserver vserver-SSL-1 SVC_HTTP1
2
3
4
5
6 Done
7
8
```

```
9 > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) - SSL
    Type:
10
11
12 ADDRESS State: DOWN[Certkey not bound]
13
14
15 Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)
16
17
18 Time since last state change: 0 days, 00:31:53.70
19
20
21 Effective State: DOWN Client Idle
22
23
24 Timeout: 180 sec
25
26
27 Down state flush: ENABLED Disable Primary Vserver On Down :
28
29
30 DISABLED No. of Bound Services : 1 (Total) 0 (Active)
31
32
33 Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
    IP and
34
35
36 Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
    NO Push Label Rule:
37
38
39
40
41
42 1) SVC_HTTP1 (10.102.29.18: 80) - HTTP
43
44
45 State: DOWN Weight: 1
46
47
48 Done
49 <!--NeedCopy-->
```

GUI を使用してサービスを仮想サーバーにバインドする

1. **[Traffic Management]** > **[SSL Offload]** > **[Virtual Servers]** の順に選択します。
2. 詳細ペインで仮想サーバーを選択して、**[Open]** をクリックします。
3. **[Services]** タブの **[Active]** 列で、選択した仮想サーバーにバインドするサービスの横にあるチェックボッ

クスをオンにします。

4. **[OK]** をクリックします。
5. ペインの下部にある **[Details]** セクションの **[Number of Bound Services]** カウンターが、仮想サーバーにバインドしたサービスの数だけ増加することを確認します。

証明書とキーのペアの追加

SSL 証明書は、SSL キー交換および暗号化/復号化プロセスに含まれるエレメントです。証明書は、SSL サーバーのアイデンティティを確立するために SSL ハンドシェイク中に使用されます。Citrix ADC アプライアンスに含まれている、有効な既存の SSL 証明書を使用するか、独自の SSL 証明書を作成できます。アプライアンスは、最大 4096 ビットの RSA/DSA 証明書をサポートします。

注：

信頼される証明機関から発行された有効な SSL 証明書を使用することをお勧めします。無効な証明書や自分で作成した証明書は、一部の SSL クライアントと互換性がありません。

SSL 処理に使用する前に、証明書を対応するキーとペアにする必要があります。次に、証明書とキーのペアを仮想サーバーにバインドすると、SSL 処理に使用できるようになります。

CLI を使用して証明書キーペアを追加します

コマンドプロンプトで次のコマンドを入力し、証明書とキーのペアを作成して構成を確認します。

```
1 - add ssl certKey <certkeyName> -cert <string> [-key <string>]
2 - show sslcertkey <name>
3 <!--NeedCopy-->
```

例：

```
1 > add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
2 Done
3
4
5 > show sslcertkey CertKey-SSL-1
6
7
8 Name: CertKey-SSL-1 Status: Valid,
9
10 Days to expiration:4811 Version: 3
11
12
13 Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
14 C=US,ST=California,L=San
15
16
```

```
17      Jose,O=Citrix ANG,OU=NS Internal,CN=default
18
19
20      Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
      21:26:47 2022 GMT
21
22
23      Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
      CN=default Public Key
24
25
26      Algorithm: rsaEncryption Public Key
27
28
29      size: 1024
30
31
32      Done
33      <!--NeedCopy-->
```

GUI を使用して証明書キーペアを追加します

次の手順を実行します：

1. **[Traffic Management]** > **[SSL]** > **[Certificates]** に移動します。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Install Certificate]** ダイアログボックスの **[Certificate-Key Pair Name]** ボックスに、追加する証明書とキーのペアの名前（たとえば、「Certkey-SSL-1」）を入力します。
4. **[Details]** の **[Certificate File Name]** で、**[Browse (Appliance)]** をクリックして証明書を検索します。証明書とキーはともに、アプライアンスの `/nsconfig/ssl/` ディレクトリに保存されます。ローカルシステムにある証明書を使用するには、**[Local]** を選択します。
5. 使用する証明書を選択して、**[Select]** をクリックします。
6. **[Private Key File Name]** で、**[Browse (Appliance)]** をクリックして秘密キーファイルを検索します。ローカルシステムにある秘密キーを使用するには、**[Local]** を選択します。
7. 使用するキーを選択して、**[Select]** をクリックします。証明書とキーのペアで使用するキーを暗号化するには、暗号化に使用するパスワードを **[Password]** ボックスに入力します。
8. **[インストール]** をクリックします。
9. 証明書キーのペアをダブルクリックし、**[証明書の詳細]** ウィンドウで、パラメーターが正しく構成されて保存されていることを確認します。

SSL 証明書キーペアの仮想サーバーへのバインド

SSL 証明書とそれに対応するキーをペアにしたら、証明書とキーのペアを SSL 仮想サーバーにバインドして、SSL 処理に使用できるようにする必要があります。セキュリティで保護されたセッションでは、クライアントコンピュー

ターとアプライアンス上の SSL ベースの仮想サーバーの間に接続を確立する必要があります。その後、仮想サーバーで着信トラフィックに対して SSL 処理が実行されます。したがって、アプライアンスで SSL 仮想サーバーを有効にする前に、有効な SSL 証明書を SSL 仮想サーバーにバインドする必要があります。

CLI を使用して、**SSL** 証明書キーペアを仮想サーバーにバインドします

コマンドプロンプトで次のコマンドを入力し、SSL 証明書とキーのペアを仮想サーバーにバインドして構成を確認します。

```
1 - bind ssl vsrver <vServerName> -certkeyName <string>
2 - show ssl vsrver <name>
3 <!--NeedCopy-->
```

例:

```
1 > bind ssl vsrver Vserver-SSL-1 -certkeyName CertKey-SSL-1
2
3
4
5
6 Done
7
8
9 > show ssl vsrver Vserver-SSL-1
10
11
12
13
14
15     Advanced SSL configuration for VServer Vserver-SSL-1:
16
17     DH: DISABLED
18
19
20     Ephemeral RSA: ENABLED Refresh Count: 0
21
22
23     Session Reuse: ENABLED Timeout: 120 seconds
24
25
26     Cipher Redirect: ENABLED
27
28
29     SSLv2 Redirect: ENABLED
30
31
32     ClearText Port: 0
33
34
35     Client Auth: DISABLED
36
```

```

37
38
39     SSL Redirect: DISABLED
40
41
42     Non FIPS Ciphers: DISABLED
43
44
45     SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
46
47
48
49
50
51 1) CertKey Name: CertKey-SSL-1 Server Certificate
52
53
54 1) Cipher Name: DEFAULT
55
56
57     Description: Predefined Cipher Alias
58
59
60 Done
61 <!--NeedCopy-->

```

GUI を使用して、**SSL** 証明書キーペアを仮想サーバーにバインドします

次の手順を実行します：

1. **[Traffic Management] > [SSL Offload] > [Virtual Servers]** の順に選択します。
2. 証明書とキーのペアをバインドする仮想サーバー（たとえば、[Vserver-SSL-1]）を選択して、**[Open]** をクリックします。
3. **[Configure Virtual Server (SSL Offload)]** ダイアログボックスの **[SSL Settings]** タブにある **[Available]** で、仮想サーバーにバインドする証明書とキーのペア（たとえば、[Certkey-SSL-1]）を選択して、**[Add]** をクリックします。
4. **[OK]** をクリックします。
5. 選択した証明書キーのペアが **[Configured]** 領域に表示されていることを確認します。

Outlook Web Access に対するサポートの構成

Citrix ADC アプライアンスで Outlook Web Access (OWA) サーバーを使用している場合は、OWA サーバー宛の HTTP 要求に特別なヘッダーフィールド「FRONT-END-HTTPS: ON」を挿入するようにアプライアンスを構成して、URL リンクが「<http://>」ではなく「<https://>」として生成されるようにします。

注：OWA サポートは、HTTP ベースの SSL 仮想サーバーと SSL サービスで有効にできます。TCP ベースの SSL 仮想サーバーと SSL サービスでは OWA をサポートできません。

OWA サポートを構成するには、次の操作を実行します。

- OWA サポートを有効にする SSL アクションを作成します。
- SSL ポリシーを作成します。
- ポリシーを SSL 仮想サーバーにバインドします。

OWA サポートを有効にする **SSL** アクションを作成します

Outlook Web Access (OWA) サポートを有効にする前に、SSL アクションを作成する必要があります。SSL アクションは SSL ポリシーにバインドされ、着信データがポリシーで指定された規則と一致すると実行されます。

CLI を使用して **OWA** サポートを有効にする **SSL** アクションを作成します

コマンドプロンプトで次のコマンドを入力し、OWA サポートを有効にする SSL アクションを作成して構成を確認します。

```
1 - add ssl action <name> -OWASupport ENABLED
2 - show SSL action <name>
3 <!--NeedCopy-->
```

例：

```
1 > add ssl action Action-SSL-OWA -OWASupport enabled
2
3
4
5
6 Done
7
8
9 > show SSL action Action-SSL-OWA
10
11
12 Name: Action-SSL-OWA
13
14
15 Data Insertion Action: OWA
16
17
18 Support: ENABLED
19
20
21 Done
22 <!--NeedCopy-->
```

GUI を使用して **OWA** サポートを有効にする **SSL** アクションを作成します

次の手順を実行します：

1. **[Traffic Management] > [SSL] > [Policies]** に移動します。
2. 詳細ペインで、**[Actions]** タブ、**[Add]** をクリックします。
3. **[Create SSL Action]** ダイアログボックスの **[Name]** ボックスに、「**Action-SSL-OWA**」と入力します。
4. **[Outlook Web Access]** で、**[Enabled]** を選択します。
5. **[Create]** をクリックしてから、**[Close]** をクリックします。
6. **[Action-SSL-OWA]** が **[SSL Actions]** ページに表示されていることを確認します。

SSL ポリシーを作成する

SSL ポリシーは、ポリシーインフラストラクチャを使用して作成します。各 SSL ポリシーには SSL アクションがバインドされ、アクションは、着信トラフィックがポリシーで設定された規則と一致すると実行されます。

CLI を使用して **SSL** ポリシーを作成します

コマンドプロンプトで次のコマンドを入力し、SSL ポリシーを作成して構成を確認します。

```
1 - add ssl policy <name> -rule <expression> -reqAction <string>
2 - show ssl policy <name>
3 <!--NeedCopy-->
```

例：

```
1 > add ssl policy Policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA
2
3 Done
4
5 > show ssl policy Policy-SSL-1
6
7 Name: Policy-SSL-1 Rule: ns_true
8
9 Action: Action-SSL-OWA Hits: 0
10
11 Policy is bound to following entities
12
13 1) PRIORITY : 0
14
15 Done
16 <!--NeedCopy-->
```

GUI を使用して SSL ポリシーを作成します

次の手順を実行します：

1. **[Traffic Management] > [SSL] > [Policies]** に移動します。
2. 詳細ペインで、**[Add]** をクリックします。
3. **[Create SSL Policy]** ダイアログボックスの **[Name]** ボックスに、SSL ポリシーの名前（たとえば、「Policy-SSL-1」）を入力します。
4. **[Request Action]** で、このポリシーに関連付ける既存の SSL アクション（たとえば、[Action-SSL-OWA]）を選択します。`ns_true` 汎用式により、成功した SSL ハンドシェイクトラフィックのすべてにこのポリシーが適用されます。特定の応答に対してのみポリシーを適用する必要がある場合は、より高い詳細レベルのポリシーを作成できます。詳細なポリシー式の設定について詳しくは、「[SSL アクションとポリシー](#)」を参照してください。
5. **[Named Expressions]** で、組み込みの汎用式 `ns_true` を選択し、**[Add Expression]** をクリックします。式 `ns_true` が [Expression] ボックスに表示されます。
6. **[Create]** をクリックしてから、**[Close]** をクリックします。
7. ポリシーを選択して、ペイン下部にある [Details] セクションを表示し、ポリシーが正しく構成されていることを確認します。

SSL ポリシーを SSL 仮想サーバーにバインドします

Outlook Web Access に SSL ポリシーを設定したら、Outlook 着信トラフィックをインターセプトする仮想サーバーにポリシーをバインドします。着信データが SSL ポリシーで構成された規則と一致すると、そのポリシーに関連付けられたアクションが実行されます。

CLI を使用して SSL ポリシーを SSL 仮想サーバーにバインドします

コマンドプロンプトで次のコマンドを入力し、SSL ポリシーを SSL 仮想サーバーにバインドして構成を確認します。

```
1 - bind ssl vserver <vServerName> -policyName <string>
2 - show ssl vserver <name>
3 <!--NeedCopy-->
```

例：

```
1 > bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1
2
3 Done
4
5 > show ssl vserver Vserver-SSL-1
6
7 Advanced SSL configuration for VServer Vserver-SSL-1:
8
```

```
9  DH: DISABLED
10
11  Ephemeral RSA: ENABLED
12
13  Refresh Count: 0
14
15  Session Reuse: ENABLED
16
17  Timeout: 120 seconds
18
19  Cipher Redirect: ENABLED
20
21  SSLv2 Redirect: ENABLED
22
23  ClearText Port: 0
24
25  Client Auth: DISABLED
26
27  SSL Redirect: DISABLED
28
29  Non FIPS Ciphers: DISABLED
30
31  SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
32
33  1) CertKey Name: CertKey-SSL-1 Server Certificate
34
35  1) Policy Name: Policy-SSL-1 Priority: 0
36
37  1) Cipher Name: DEFAULT Description: Predefined Cipher Alias
38
39  Done
40  <!--NeedCopy-->
```

GUI を使用して **SSL** ポリシーを **SSL** 仮想サーバーにバインドします

次の手順を実行します：

1. **[Traffic Management] > [SSL Offload] > [Virtual Servers]** の順に選択します。
2. 詳細ペインで仮想サーバー（たとえば、[Vserver-SSL-1]）を選択して、**[Open]** をクリックします。
3. **[Configure Virtual Server (SSL Offload)]** ダイアログボックスで **[Insert Policy]** をクリックし、SSL 仮想サーバーにバインドするポリシーを選択します。必要に応じて、**[Priority]** ボックスをダブルクリックして、新しい優先度を入力することもできます。
4. **[OK]** をクリックします。

一目でわかる機能

April 25, 2022

Citrix ADC の機能は、特定のニーズに対応するために、個別に構成することも、組み合わせて構成することもできます。一部の機能は複数のカテゴリに当てはまりますが、多数の Citrix ADC 機能は、一般に、アプリケーションスイッチングおよびトラフィック管理機能、アプリケーションアクセラレーション機能、アプリケーションセキュリティおよびファイアウォール機能、およびアプリケーション可視性機能として分類できます。

各機能进行处理する順序については、「[機能の処理順序](#)」を参照してください。

アプリケーションスイッチングとトラフィック管理機能

April 25, 2022

以下は、アプリケーションスイッチングとトラフィック管理機能です。

SSL オフロード

Web サーバーから SSL 暗号化および解読を透過的にオフロードして、コンテンツ要求の処理用にサーバーのリソースを解放します。SSL はアプリケーションのパフォーマンスにとって大きな負担となり、多くの最適化方法が無効になることがあります。SSL オフロードおよび SSL アクセラレーションでは、Citrix Request Switching 技術のすべての利点を SSL トラフィックに適用できるため、エンドユーザーのパフォーマンスを低下させることなく、Web アプリケーションのセキュリティ保護されたデリバリーを実現できます。

詳しくは、「[SSL オフロードおよびアクセラレーション](#)」を参照してください。

アクセス制御リスト

着信パケットとアクセス制御リスト (ACL: Access Control List) を比較します。パケットが ACL 規則と一致した場合は、規則で指定されたアクションがパケットに適用されます。一致しない場合は、デフォルトアクション (ALLOW) が適用され、パケットは通常どおりに処理されます。アプライアンスが着信パケットと ACL を比較されるようにするには、ACL を適用する必要があります。すべての ACL はデフォルトで有効になっていますが、Citrix ADC アプライアンスが着信パケットを ACL と比較するためには、管理者が ACL を適用する必要があります。ルックアップテーブルに含める必要がなくても保持すべき ACL がある場合は、それを無効にしてから ACL を適用する必要があります。ADC アプライアンスは、着信パケットを無効な ACL と比較しません。

詳しくは、「[アクセス制御リスト](#)」を参照してください。

負荷分散

負荷分散の決定は、ラウンドロビン、最小接続数、加重最小帯域幅、加重最小パケット数、最小応答時間、および URL、ドメインソース IP、宛先 IP に基づくハッシュなど、さまざまなアルゴリズムに基づいて行われます。TCP と UDP プロトコルの両方がサポートされているので、Citrix ADC アプライアンスはこれらのプロトコルに基づくすべてのトラフィック（たとえば、HTTP、HTTPS、UDP、DNS、FTP、NNTP、および一般的なファイアウォールトラフィック）を負荷分散することができます。また、ADC アプライアンスは、ソース IP、Cookie、サーバー、グループ、または SSL セッションに基づくセッションパーシステンスを維持できます。サーバー、キャッシュ、ファイアウォール、およびその他のインフラストラクチャデバイスが正常に動作して適切なコンテンツがユーザーに提供されるように、カスタムの Extended Content Verification (ECV) を適用できます。また、ping、TCP、または HTTP URL を使用してヘルスチェックを実行したり、Perl スクリプトによるモニターを作成したりできます。

高度な WAN 最適化を提供するには、データセンターで展開されている CloudBridge アプライアンスを Citrix ADC アプライアンスで負荷分散することができます。これにより、帯域幅と同時セッションの数を大幅に改善できます。

詳しくは、「[負荷分散](#)」を参照してください。

トラフィックドメイン

トラフィックドメインを使用すると、単一の Citrix ADC アプライアンス内にいくつかの論理 ADC パーティションを作成できます。トラフィックドメインを使用すると、異なるアプリケーション用にネットワークトラフィックを分離できます。トラフィックドメインを使用すると、リソース間のやり取りが行われない分離環境を複数作成できます。特定のトラフィックドメインに属しているアプリケーションは、そのドメイン内のエンティティおよびプロセストラフィックとのみ通信します。あるトラフィックドメインに属しているトラフィックは、別のトラフィックドメインの境界を越えることはできません。そのため、アドレスが同じドメイン内で重複していない限り、アプライアンスで重複する IP アドレスを使用できます。

詳しくは、「[トラフィックドメイン](#)」を参照してください。

ネットワークアドレス変換

ネットワークアドレス変換 (NAT) では、Citrix ADC アプライアンスを通過する IP パケットの送信元/宛先 IP アドレスや TCP/UDP ポート番号が変更されます。Citrix ADC アプライアンスで NAT を有効にすると、プライベートネットワークのセキュリティが強化されます。また、データが NetScaler を通過するときにプライベートネットワークの送信元 IP アドレスが変更されるため、インターネットなどのパブリックネットワークからプライベートネットワークが保護されます。

Citrix ADC アプライアンスでは、次の種類のネットワークアドレス変換がサポートされます。

INAT: 受信 NAT (Inbound NAT: INAT) では、Citrix ADC アプライアンスで構成された IP アドレス（通常はパブリックアドレス）がサーバーの代わりに接続要求を待機します。アプライアンスがそのパブリック IP アドレスで要求パケットを受信した場合、Citrix ADC は、宛先 IP アドレスをサーバーのプライベート IP アドレスに置き換えます。

つまり、アプライアンスはクライアントとサーバー間のプロキシとして機能します。INAT 構成には、Citrix ADC アプライアンスの IP アドレスとサーバーの IP アドレスの間の 1 対 1 の関係を定義する INAT 規則が含まれます。

RNAT: 逆ネットワークアドレス変換 (Reverse Network Address Translation: RNAT) では、サーバーによって開始されたセッションについて、Citrix ADC アプライアンスは、サーバーが生成したパケットの送信元 IP アドレスをアプライアンスで設定された IP アドレス (種類: SNIP) に置き換えます。これにより、サーバーが生成したパケットでサーバーの IP アドレスがさらされるのを防止します。RNAT 構成には、条件を指定する RNAT 規則が含まれます。アプライアンスは、条件に一致するパケットに対して RNAT 処理を実行します。

ステートレス **NAT46** 変換: ステートレス NAT46 は、セッション情報を Citrix ADC アプライアンスに保持せずに、IPv4 パケットと IPv6 パケットを相互に変換することにより、IPv4 ネットワークと IPv6 ネットワーク間の通信を実現します。ステートレス NAT46 構成には、IPv4-IPv6 INAT 規則と NAT46 IPv6 プレフィックスが含まれます。

ステートフル **NAT64** 変換: ステートフル NAT64 機能は、セッション情報を Citrix ADC アプライアンスに保持しながら、IPv6 パケットと IPv4 パケットを相互に変換することにより、IPv4 クライアントと IPv6 サーバー間の通信を実現します。ステートレス NAT64 構成には、NAT64 規則と NAT64 IPv6 プレフィックスが含まれます。

詳しくは、「[ネットワークアドレス変換の構成](#)」を参照してください。

マルチパス **TCP** のサポート

Citrix ADC アプライアンスは、マルチパス TCP (MPTCP) をサポートします。MPTCP は、ホスト間で使用可能な複数のパスを識別および使用して TCP セッションを保持する TCP/IP プロトコル拡張機能です。TCP プロファイルで MPTCP を有効にして仮想サーバーにバインドする必要があります。MPTCP が有効な場合、仮想サーバーは MPTCP ゲートウェイとして機能し、クライアントとの MPTCP 接続を、サーバーとの間で保持している TCP 接続に変換します。

詳しくは、「[MPTCP \(Multi-Path TCP\)](#)」を参照してください。

コンテンツ スイッチ

ポリシーを切り替えるコンテンツの構成に基づいて要求を送信するサーバーを決定します。ポリシールールは、IP アドレス、URL、HTTP ヘッダーに基づいて設定できます。これにより、そのときのユーザー、使用されているエージェントの種類、ユーザーが要求したコンテンツなど、ユーザーとデバイスの特性に基づいて、スイッチを決定することができます。

詳しくは、「[コンテンツスイッチ](#)」を参照してください。

広域サーバー負荷分散 (**Global Server Load Balancing: GSLB**)

NetScaler のトラフィック管理機能を拡張して、分散インターネットサイトとグローバル企業に対応します。設置場所が、複数のネットワークの場所や 1 箇所の複数のクラスターに分散していても、NetScaler は可用性を維持し、それらの間でトラフィックを分散します。インテリジェントな DNS 決定を行って、ダウンまたは過負荷状態のサイト

にユーザーが割り当てられるのを防ぎます。近接ベースの GSLB 方式が有効な場合、NetScaler は、さまざまなサイトからクライアントのローカル DNS サーバー (LDNS) までの距離に基づいて、負荷分散の決定を行うことができます。距離ベースの GSLB 方式の最大の長所は、最も近い使用可能なサイトが選択されて、応答時間が短くなることです。

詳しくは、「[グローバルサーバー負荷分散](#)」を参照してください。

動的ルーティング

ルーターが、隣接するルーターからトポロジ情報、ルート、および IP アドレスを自動的に取得できるようにします。動的ルーティングが有効な場合、対応するルーティングプロセスはルート更新をリスンして、ルート情報を提供します。ルーティングプロセスはパッシブモードにすることもできます。ルーティングプロトコルを利用して、アップストリームルーターは Equal Cost Multipath 手法を使用し、2 台のスタンドアロン NetScaler 装置にホスティングされた同一の仮想サーバーに、トラフィックを負荷分散することができます。

詳しくは、「[動的ルートの構成](#)」を参照してください。

リンク負荷分散

複数の WAN リンクを負荷分散して、リンクフェールオーバーを提供し、ネットワークのパフォーマンスをさらに最適化して、ビジネスの継続性を保証します。インテリジェントなトラフィック制御とヘルスチェックを行って、アップストリームルーター間で効率的にトラフィックを分散することにより、ネットワーク接続の高い可用性を維持します。ポリシーとネットワーク状態に基づいて、着信トラフィックと送信トラフィックの両方をルーティングする最適な WAN リンクを特定し、高速な障害検出とフェールオーバーによって、WAN やインターネットリンク障害からアプリケーションを保護します。

詳しくは、「[負荷分散のリンク](#)」を参照してください。

TCP 最適化

TCP プロファイルを使用すると、TCP トラフィックを最適化できます。TCP プロファイルでは、NetScaler 仮想サーバーによる TCP トラフィックの処理方法を定義します。管理者は、組み込みの TCP プロファイルを使用するか、カスタムプロファイルを作成することができます。TCP プロファイルを定義した後、そのプロファイルを 1 つまたは複数の仮想サーバーにバインドできます。

TCP プロファイルで有効にできる主要な最適化機能のいくつかは次のとおりです。

- TCP Keep-Alive - リンクが切断されるのを防ぐために、指定された間隔で通信先の動作状態をチェックします。
- SACK (Selective Acknowledgment: 選択的確認応答) - 特に LFN (Long Fat Network: 広帯域高遅延ネットワーク) において伝送のパフォーマンスを向上させます。
- TCP ウィンドウスケールリング—LFN 経由の効率的なデータ転送を可能にします。

TCP プロファイルについて詳しくは、「[TCP プロファイルの構成](#)」を参照してください。

CloudBridge Connector

Citrix OpenCloud フレームワーク

の基本機能である Citrix NetScaler CloudBridge Connector は、クラウド拡張型のデータセンターの構築に使用されるツールです。OpenCloud Bridge により、ネットワークを再構成することなく、クラウド上の 1 つまたは複数の Citrix ADC アプライアンスまたは NetScaler 仮想アプライアンスをネットワークに接続することができます。クラウドがホストするアプリケーションは、組織内の単一ネットワーク上で実行されているかのように動作します。OpenCloud Bridge の主な目的は、企業がアプリケーションをクラウドに移行しながら、コストやアプライアンス障害のリスクを削減できるようにすることにあります。また、OpenCloud Bridge は、クラウド環境のネットワークセキュリティを向上します。OpenCloud Bridge は、クラウドインスタンス上の Citrix ADC アプライアンスまたは NetScaler 仮想アプライアンスを LAN 上の Citrix ADC アプライアンスまたは NetScaler 仮想アプライアンスに接続するレイヤー 2 ネットワークブリッジです。接続は、GRE (Generic Routing Encapsulation) プロトコルを使用するトンネルを介して確立されます。GRE プロトコルは、さまざまなネットワークプロトコルからのパケットをカプセル化し、別のプロトコル経由で転送するメカニズムを提供しています。IPSec (Internet Protocol Security: インターネットプロトコルセキュリティ) プロトコルは、OpenCloud Bridge のピア間の通信を確保します。

詳しくは、「[CloudBridge](#)」を参照してください。

DataStream

NetScaler DataStream 機能は、送信中の SQL クエリに基づいて要求を分散することで、データベース層で要求の割り振りを実行するインテリジェントなメカニズムを提供します。

データベースサーバーの前に NetScaler を導入すれば、アプリケーションサーバーまたは Web サーバーからのトラフィックを最適に分散することができます。管理者は、SQL クエリの情報と、データベース名、ユーザー名、文字セット、およびパケットサイズに基づいて、トラフィックをセグメント化できます。

負荷分散を構成して、負荷分散アルゴリズムに基づいて要求を割り振ることができます。または、ユーザー名、データベース名、コマンドパラメーターなどの SQL クエリパラメーターに基づくコンテンツスイッチを構成して、スイッチ条件を詳細に設定できます。さらに、モニターを構成してデータベースサーバーの状態を監視することもできます。

Citrix ADC アプライアンスの高度なポリシーインフラストラクチャには、要求の評価と処理に使用できる式が含まれています。高度な式により、MySQL データベースサーバーに関連付けられたトラフィックが評価されます。高度なポリシーの要求ベースの式 (MYSQL.CLIENT および MYSQL.REQ で始まる式) を使用すると、コンテンツスイッチ仮想サーバーのバインドポイントで要求スイッチの意思決定を行うことが可能になり、応答ベースの式 (MYSQL.RES で始まる式) を使用すると、ユーザー設定のヘルスモニターへのサーバー応答を評価することができます。

注: DataStream は、MySQL と MS SQL のデータベースでサポートされています。

詳しくは、「[DataStream](#)」を参照してください。

アプリケーションの速度向上機能

April 21, 2022

- AppCompress

gzip 圧縮プロトコルを使った HTML とテキストファイルに対する透過的圧縮一般的な 4: 1 の圧縮率で、データセンターの帯域幅要件が、最大 50% 削減されます。また、ユーザーのブラウザに渡す必要があるデータ量が削減されるため、エンドユーザーの応答時間が大幅に短縮されます。

- キャッシュリダイレクト

リバースプロキシ、透過プロキシ、またはフォワードプロキシのキャッシュファームに対するトラフィックのフローを管理します。すべての要求を検査して、キャッシュ不能な要求を特定し、固定接続を介してそれらを発信元のサーバーに直接送信します。キャッシュ不能な要求を発信元の Web サーバーヘインテリジェントにリダイレクトすることによって、Citrix ADC アプライアンスはキャッシュリソースを解放し、キャッシュヒット率を上げながら、これらの要求に対する全体的な帯域幅消費と応答遅延を削減します。

詳しくは、「[キャッシュリダイレクト](#)」を参照してください。

- AppCache

静的および動的コンテンツの両方に対して、高速インメモリ HTTP/1.1 および HTTP/1.0 準拠の Web キャッシュを提供し、Web コンテンツとアプリケーションデータデリバリーを最適化します。このオンボードキャッシュは、着信要求がセキュリティで保護されたり、データが圧縮されたりしている場合でも、着信アプリケーション要求の結果を保存し、データを再利用して、同じ情報に対する今後の要求に対応します。オンボードキャッシュから直接データを提供することによって、静的および動的コンテンツ要求をサーバーに送信する必要がなくなるので、アプライアンスはページの再生成時間を削減できます。

詳しくは、「[統合キャッシュ](#)」を参照してください。

- TCP バッファリング

サーバーの応答をバッファリングして、そのクライアントの速度でクライアントに応答を提供し、より高速にサーバーをオフロードするので、Web サイトのパフォーマンスが向上します。

アプリケーションセキュリティとファイアウォール機能

April 25, 2022

以下は、セキュリティとファイアウォールの機能です。

サービス不能 (DoS) 攻撃に対する防御

悪意ある分散型サービス不能 (DDoS: Distributed Denial of Service) 攻撃や、そのほかの悪意ある攻撃をサーバーに達する前に検出して阻止し、ネットワークおよびアプリケーションのパフォーマンスに悪影響を及ぼさないようにします。Citrix ADC アプライアンスは適正なクライアントを特定して、その優先度を引き上げ、疑わしいクライアントが不相应に大量のリソースを消費してサイトをダウンすることがないようにします。アプライアンスは、次のような種類の悪意ある攻撃に対するアプリケーションレベルの保護を提供します。

- SYN フラッド攻撃
- パイプライン攻撃
- ティアドロップ攻撃
- ランド攻撃
- 帯域枯渇攻撃
- ゾンビ接続攻撃

アプライアンスは、これらの接続へのサーバーリソースの割り当てを禁止して、これらの種類の攻撃を積極的に防御します。これによって、これらのイベントに関連するパケットが原因でサーバーに大きな負担がかかることがないようにします。

アプライアンスは、ICMP 率の制限と積極的な ICMP パケットチェックを使用して、ICMP ベースの攻撃からもネットワークリソースを保護します。強力な IP 再構築を実行して、さまざまな疑わしい、間違った形式のパケットをドロップし、サイトトラフィックにアクセス制御リスト (ACL: Access Control List) を適用して保護機能を強化します。

詳しくは、「[HTTP サービス不能攻撃に対する防御](#)」を参照してください。

コンテンツフィルタリング

レイヤー 7 レベルで、Web サイトを悪意のある攻撃から保護します。アプライアンスは、HTTP ヘッダーに基づくユーザー構成の規則に従って、各着信要求を検査し、ユーザーが構成したアクションを実行します。アクションとして、接続の再設定、要求のドロップ、ユーザーのブラウザーへのエラーメッセージの送信などを設定できます。これにより、不要な要求を除去して、サーバーが攻撃にさらされる危険性を減らすことができます。

この機能は、HTTP GET と POST 要求を分析して、既知の不正なシグニチャを排除できるので、HTTP ベースの攻撃からサーバーを防御できます。

詳しくは、「[コンテンツフィルタリング](#)」を参照してください。

レスポnder

高度なフィルタリングのように機能し、アプライアンスからクライアントへの応答を生成するために使用できます。この機能の一般的な用途は、リダイレクト応答、ユーザー定義応答、およびリセットの生成です。

詳しくは、「[レスポnder](#)」を参照してください。

リライト

HTTP ヘッダーと本文のテキストを変更します。再書き込み機能を使用して、HTTP 要求または応答に HTTP ヘッダーを追加したり、個別の HTTP ヘッダーを変更したり、HTTP ヘッダーを削除したりできます。また、要求と応答の HTTP ボディを変更することもできます。

アプライアンスは、要求を受信したり応答を送信したりするときに書き換え規則をチェックして、適切な規則を要求や応答に適用してから Web サーバーまたはクライアントコンピューターに渡します。

詳しくは、「[書き換え](#)」を参照してください。

優先度によるキューイング

ユーザー要求に優先度を付けて、要求ボリュームのサージ中に、最も重要なトラフィックが最初に処理されるようにします。要求 URL、Cookie、またはその他のさまざまな要因に基づいて、優先度を設定できます。アプライアンスは、構成された優先度に基づいて 3 層のキューに要求を入れて、サージ中やサイト攻撃中でも、ビジネスクリティカルなトランザクションをスムーズに処理できるようにします。

詳しくは、「[優先度によるキューイング](#)」を参照してください。

サージ保護

サーバーへのユーザー要求のフローを調整し、サーバー上のリソースへ同時にアクセスできるユーザー数を制御して、サーバーの容量に達した場合には、追加の要求をキューに入れます。接続を確立できるレートを制御することによって、アプライアンスは、サーバーに渡される要求のサージをブロックし、サイトがオーバーロード状態になるのを防ぎます。

詳しくは、「[サージ保護](#)」を参照してください。

Citrix Gateway

1 Citrix Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data **while** allowing users to work from anywhere. It gives IT administrators a single point of control and tools to help ensure compliance with regulations and the highest levels of information security across and outside the enterprise. At the same time, it empowers users with a single point of access—optimized **for** roles, devices, and networks—to the enterprise applications and data they need. This unique combination of capabilities helps maximize the productivity of today's **mobile workforce**.

詳しくは、「[Citrix Gateway](#)」を参照してください。

アプリケーションファイアウォール

保護された各 Web サーバーと、その Web サーバー上の Web サイトに接続するユーザー間のトラフィックをフィルター処理して、クロスサイトスクリプティング攻撃、バッファオーバーフロー攻撃、SQL インジェクション攻撃、強制的ブラウズなど、ハッカーやマルウェアによる悪用からアプリケーションを保護します。アプリケーションファイアウォールは、Web サーバーセキュリティに対する攻撃や、Web サーバーリソースの悪用の形跡がないかどうか、すべてのトラフィックを調べて適切なアクションを実行し、これらの攻撃を未然に防ぎます。

詳しくは、「[アプリケーションファイアウォール](#)」を参照してください。

アプリケーションの可視性機能

April 21, 2022

- NetScaler Insight Center

NetScaler Insight Center は、Web および HDX (ICA) トラフィックにおけるエンドツーエンドのユーザーエクスペリエンスの視覚化を提供する高パフォーマンスのコレクターです。NetScaler ADC アプライアンスによって生成された HTTP および ICA AppFlow レコードを収集し、レイヤー 3 からレイヤー 7 の統計情報をカバーする分析レポートを作成します。NetScaler Insight Center は、直前 5 分間のリアルタイムデータおよび直前 1 時間、1 日間、1 週間、1 か月間について収集された履歴データを詳細に分析します。

HDX (ICA) 分析ダッシュボードでは、HDX ユーザー、アプリケーション、デスクトップ、およびゲートウェイレベルの情報をドリルダウンできます。同様に、HTTP 分析では、Web アプリケーション、アクセスされた URL、クライアント IP アドレス、サーバー IP アドレス、およびその他のダッシュボードの概観を表示します。管理者は、ユースケースに合わせて、これらのダッシュボードからドリルダウンして問題点を明らかにできます。

- AppFlow を使用した拡張されたアプリケーションの可視性

Citrix ADC アプライアンスは、データセンター内のすべてのアプリケーショントラフィックを一元的に制御します。これは、アプリケーションパフォーマンスの監視、分析、およびビジネスインテリジェンスアプリケーションにとって有効なフローとユーザーセッションレベルの情報を収集します。AppFlow は、RFC 5101 で定義されたオープンな IETF (Internet Engineering Task Force: インターネット技術標準化委員会) 標準である IPFIX (Internet Protocol Flow Information eXport) 形式を使用して、この情報を送信します。IPFIX (Cisco 社製 NetFlow の標準化バージョン) は、ネットワークフロー情報を監視するために幅広く使用されています。AppFlow は、新しい情報要素を定義してアプリケーションレベルの情報を表現します。

トランスポートプロトコルとして UDP を使用して、AppFlow はフローレコードと呼ばれる収集されたデータを 1 つまたは複数の IPv4 コレクターに送信します。コレクターはフローレコードを集約し、リアルタイムレポートまたは履歴レポートを生成します。

AppFlow は、HTTP、SSL、TCP、および SSL_TCP フローのトランザクションレベルでの可視性を実現します。監視対象のフロータイプのサンプリングとフィルタリングを行うことが可能です。

アプリケーショントラフィックのサンプリングとフィルタリングを行うことで監視するフロータイプを制限する場合は、AppFlow を仮想サーバー向けに有効化できます。AppFlow では、仮想サーバーの統計情報も提供しています。

また、AppFlow を特定のサービス向けに有効化してアプリケーションサーバーを表現し、そのアプリケーションサーバーへのトラフィックを監視することもできます。

詳しくは、「[AppFlow](#)」を参照してください。

- ストリーム分析

Web サイトやアプリケーションのパフォーマンスは、最も頻繁に要求されるコンテンツの配信をどのように最適化するかにより決まります。キャッシュや圧縮などの方法は、クライアントへのサービス配信の高速化に役立ちますが、最も頻繁に要求されるリソースを特定し、それらのリソースをキャッシュまたは圧縮できるようにする必要があります。Web サイトやアプリケーショントラフィックに関するリアルタイム統計を集計すれば、最も頻繁に使用されるリソースを特定できます。リソースごとのアクセス頻度や消費帯域幅などの統計によって、サーバーパフォーマンスとネットワーク使用率を改善するために、それらのリソースをキャッシュまたは圧縮する必要があるかどうかを判断できます。応答時間やアプリケーションへの同時接続数などの統計は、サーバー側のリソースを強化する必要があるかどうかを判断するのに役立ちます。

Web サイトやアプリケーションが頻繁に更新されない場合、統計データを収集する製品を使用して、その統計を手動で分析し、コンテンツの配信を最適化できます。ただし、最適化を手動で行わない場合や、Web サイトまたはアプリケーションのコンテンツが動的に生成される場合、統計データを収集するだけでなく、その統計に基づいてリソースの配信を自動的に最適化できるインフラストラクチャが必要です。Citrix ADC アプライアンスでは、この機能はストリーム分析機能によって提供されます。この機能は単一の Citrix ADC アプライアンス上で実行され、定義した条件に従ってリアルタイム統計を収集します。Citrix ADC ポリシーと共に使用すると、この機能によって自動的なリアルタイムトラフィックの最適化に必要なインフラストラクチャも提供されます。

詳しくは、「[アクション分析](#)」を参照してください。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).