



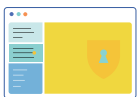
Progress LoadMaster 360

LoadMasterとアプリケーションの オーケストレーションと監視ダッシュボード

OVERVIEW

比類のないシンプルさ、柔軟性、価値

LoadMaster 360 を使用すると、重要なインフラストラクチャのアプリケーション配信を最適化できます。アプリケーション配信、高度なインシデント対応、WAFとのインターフェイス、アプリケーションとデバイスのテレメトリ、高度なライセンス、証明書管理をすべて単一のポータルから統合的に把握できます。



直感的でモダンなインターフェース

最適化されたワークフロー、視覚的に美しいデータモデリング、最新のUI



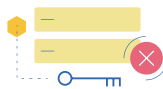
インシデント管理

コンテキストが豊富で重要アラートを使用して、問題が発生したときにタイムリーに対応できるように管理します。



WAFインサイト

WAFが実行されたあらゆる情報と結果を確認することができ、Webアプリケーションのセキュリティ防御の状態が確認できます。



証明書ライフサイクル管理と自動化

証明書とキーの管理を調整します。 期限切れの証明書について通知し、停止を防止します。



アプリケーション分析とテレメトリ

アプリケーションのパフォーマンス、健全性、セキュリティを監視するための包括的なダッシュボード。

ホストアプリケーションインフラストラクチャ – 何が可能か

- ・オーケストレーション
- ・監視
- ・SAAS
- ・クラウド、ハイブリッドクラウド
- ・インシデント管理
- ・アプリケーション認識
- ・証明書管理
- ・WAF Insight

Progress LoadMaster 360 とは

アプリケーション配信のパフォーマンス、セキュリティ、構成を管理します。ハードウェア環境においては、LoadMaster360 は、ユーザー向けのアプリケーションエクスペリエンス (AX) の単一のインターフェイスです。クラウド、仮想、アプリケーション全体で作業すると、期待どおりに動作し、あらゆる規模の組織に可能な限り最高のパフォーマンスを提供します。LoadMaster360 は、SaaS 製品であり、あらゆる規模の組織にさまざまな機能を提供します。

LoadMaster360 を使用すると、LoadMaster の大規模なインフラストラクチャをまとめて管理できます。単一のインシデントセンターで、進行中のすべての問題を全体的に確認しながら、通知に必要なメール アドレスに自動的に送信して対応することができます。アプリケーションとデバイスのテレメトリを使用すると、現在のトラフィックとパフォーマンスメトリック、履歴、および時間の経過に伴うヘルス状態を確認できます。また、LoadMaster360 は高度なライセンス機能も提供しており、ユーザーはデータセンター間で帯域幅を適切な方法で割り当てることができるため、いつでもどのようなアプリケーション配信要件にも対応できる柔軟性が得られます。

ソリューションエリア

直感的でモダンなインターフェース

素晴らしいデータモデリング機能： 視覚的に操作できるこのモダンなUIでワークフローを最適化できます。

インシデント管理

タイムリーな対応： コンテキストが豊富で重要アラートを使用して、問題が発生したときにタイムリーに対応できるように管理します。

証明書ライフサイクル管理と自動化

期限切れの証明書に関する通知を受信： 証明書と鍵の管理を調整し、停止を防止します。

アプリケーション分析とテレメトリ

包括的なダッシュボードにアクセスして、アプリケーションのパフォーマンス、健全性、セキュリティを監視します。

WAF Insight

WAFが実行したあらゆる情報と結果を確認することができ、Webアプリケーションのセキュリティ防御の状態が確認できます。

機能強化予定

ポリシー管理と施行(フェーズ II)

きめ細かなアクセス制御。構成のコンプライアンスと標準化、ドリフト検出

構成管理と展開の自動化(フェーズ II)

このオーケストレーションプラットフォームで、LoadMasterのすべての構成とチューニングの側面を制御および自動化します。

ユーザビリティとエクスペリエンス

すべてのページ、ウィジェット、情報表示は、デザインと使いやすさを第一に考え、慎重にキュレーションされています。

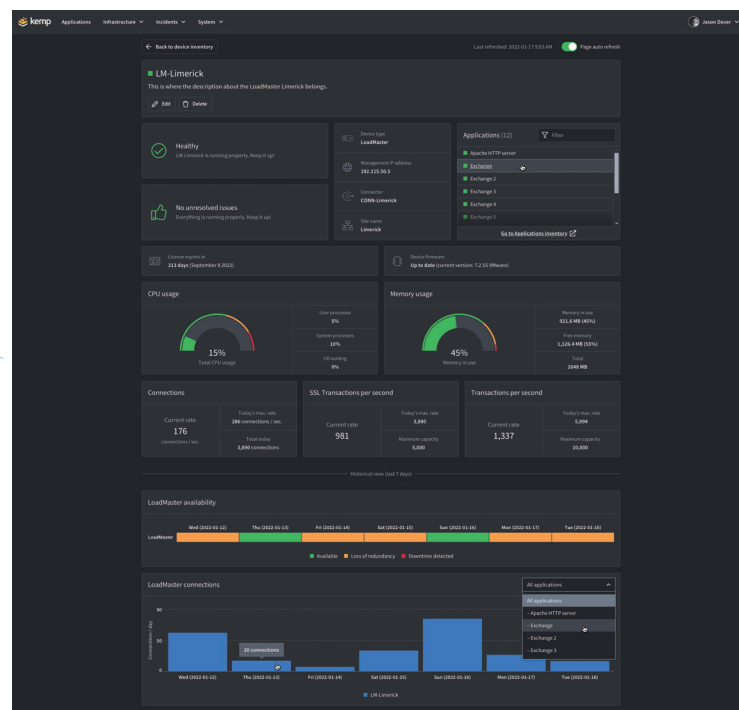
モダンなUI は、見た目に美しいインターフェースではありません。

読みやすさ、情報のフォーカス、シンプルな洗練さといった小さな要素が、私たちの理念を構成しています。



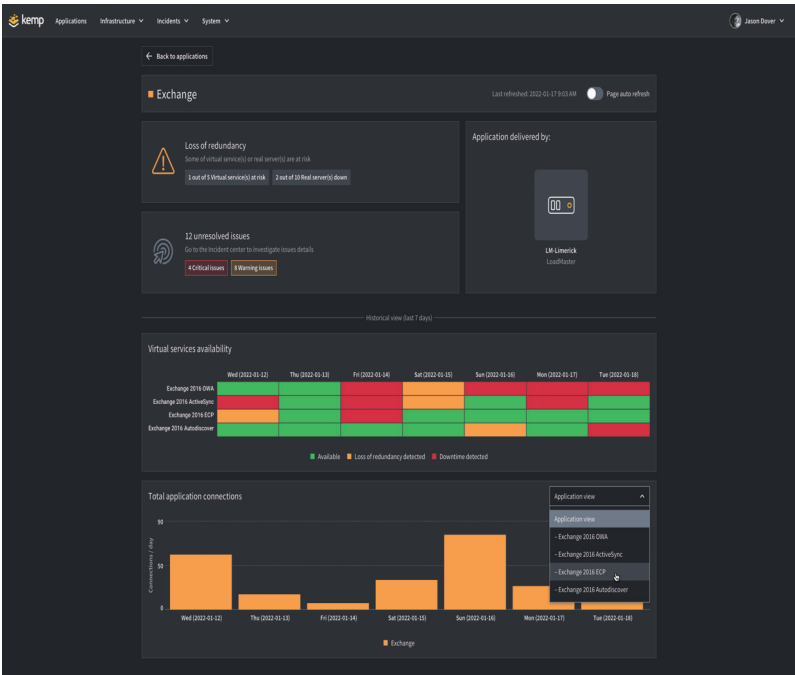
LoadMaster Insight

- LoadMaster の健全性をすばやく確認
- インシデントセンターからの未解決の問題
- ライセンスとサポートの監視
- パフォーマンスメトリック
- 時間の経過に伴う可用性



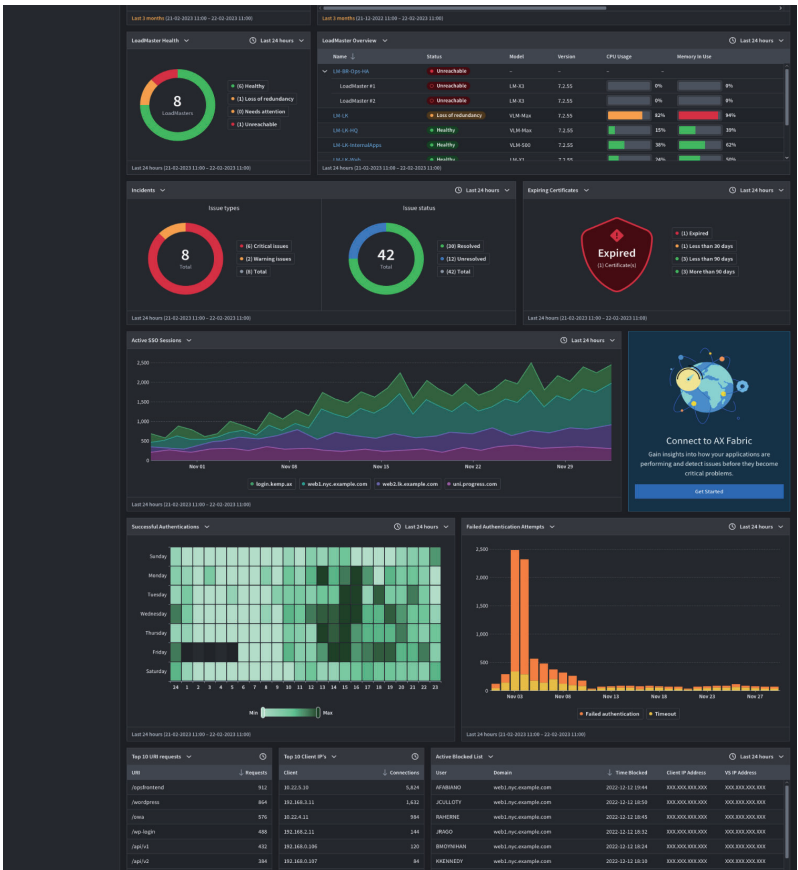
アプリケーションエクスペリエンス Insight

- ・現在の状態と過去の状態
- ・アプリケーションインシデント
- ・テレメトリ
- ・セキュリティインサイト
- ・HTTPレスポンスコードインサイト
- ・RTT と SRT メトリック



アプリケーションセキュリティ Insight

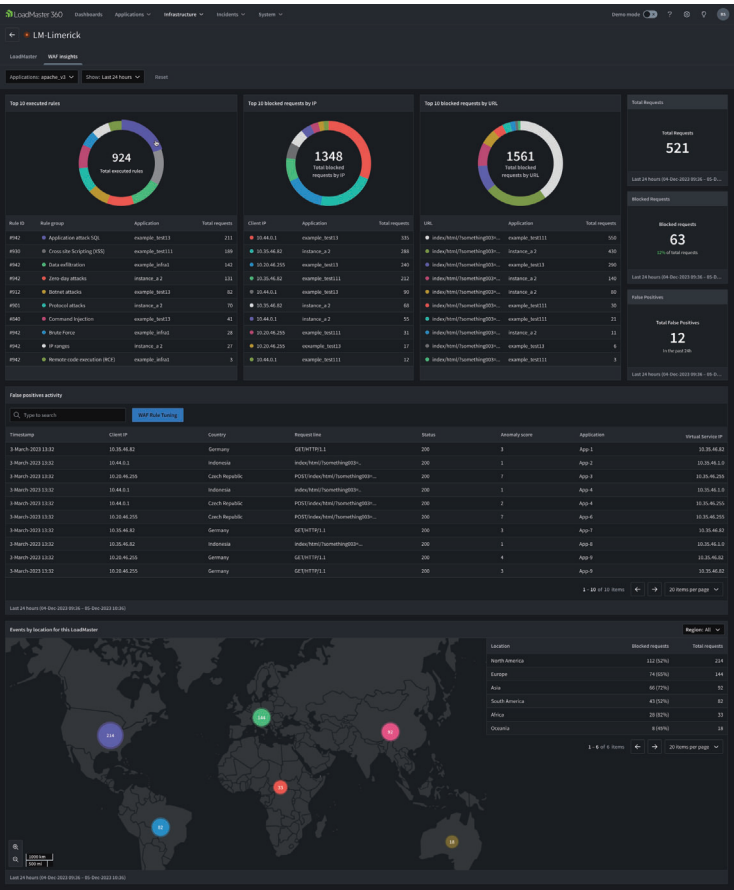
- ・証明書の洞察
- ・アクティブなSSOセッション
- ・成功した認証ヒートマップ
- ・失敗した認証
- ・アクティブな認証ブロックリスト
- ・上位10 件の URI
- ・上位10 件のクライアント IP



WAF Insight

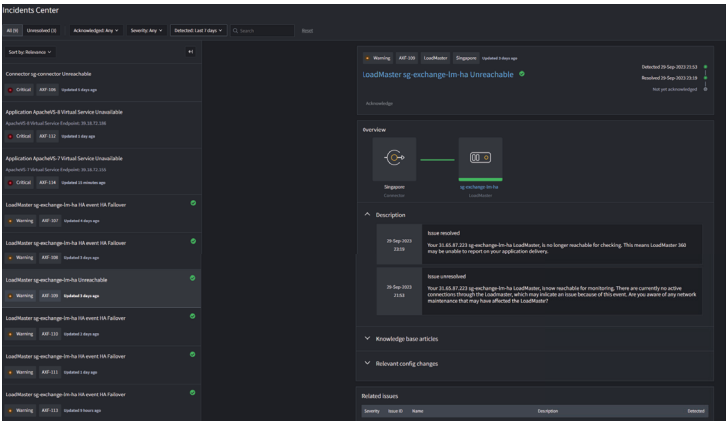
LoadMaster360 の新しい拡張 Webアプリケーションファイアウォール (WAF) 機能により、セキュリティに関する洞察が向上し、WAF の構成と調整に必要な時間が最小限に抑えられます。AI 駆動型の誤検知識別とスマート ルール調整により、ユーザーは具体的なガイダンスに従ってセキュリティの脅威を識別し、正当なアプリケーショントラフィックから誤検知を除外できます。

- スマートなルール調整により構成プロセスを改善
- 環境とアプリケーションに関する専門的なセキュリティ情報を取得
- LoadMaster WAF のパフォーマンスを把握

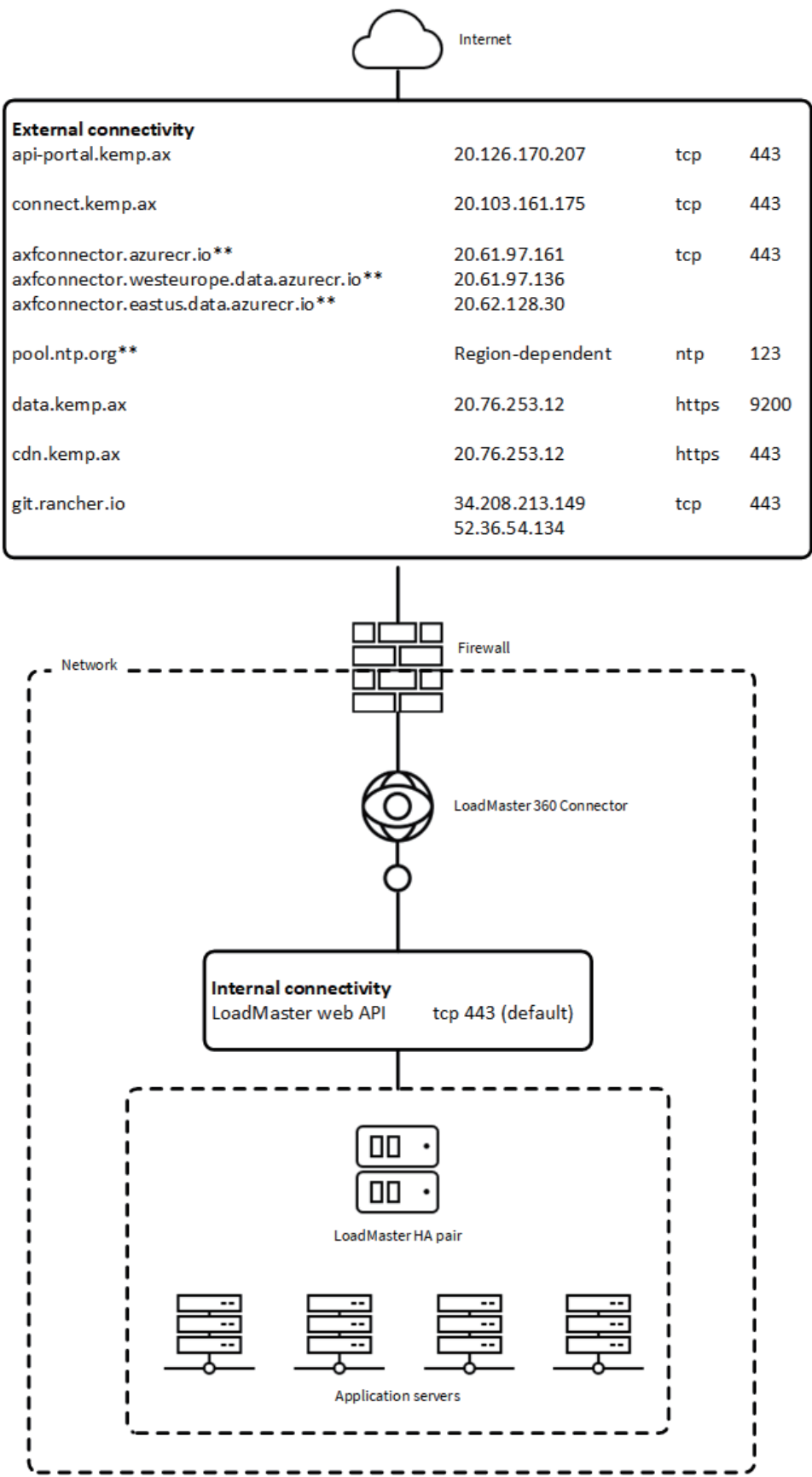


インシデント対応

- LoadMaster360 は、管理対象のロードマスター、アプリケーション、リアルサーバーを常に監視します
- 解決タイムライン
- 何が起こったのか、どのように解決するのかをユーザーに伝えるシンプルなビュー
- 外部通知用の通信チャンネル
- 前回の発生ヒートマップ



LoadMaster360 の構成図



ファイアウォールと接続要件

LoadMaster 360 を使用する前に、満たす必要のある接続要件がいくつかあります。これらの要件により、管理対象デバイスからデータが正常に収集および提示され、問題が検出されたときに報告されることが保証されます。

LoadMaster 360 を使用するには、ネットワークに少なくとも 1 つの Connector を展開して、アプリケーション配信インフラストラクチャを監視する必要があります。この Connector は、ネットワーク メトリックを LoadMaster 360 に報告します。

これを有効にするには、Connector から LoadMaster 360 への通信を許可する必要があります。この通信には、HTTPS トラフィックの送信が必要です。この送信通信を有効にするには、適切なファイアウォールルールが必要です。

Connector が展開されると、管理対象 LoadMaster からのメトリックの監視と収集が Connector によって行われます。これを有効にするには、HTTPS RESTful API が使用されます。これには、Connector から LoadMaster の管理インターフェイス (通常はポート 443) への HTTPS 通信が必要です。これに加えて、LoadMaster は UDP ポート 514 を使用して syslog メッセージを Connector に送信します。

接続元	接続先	Public IP Address	プロトコル	ポート
Connector	LoadMaster360 api-portal.kemp.ax	20.126.170.207	HTTP(S) TCP	443
Connector	NTP Pool pool.ntp.org	これらのIPアドレスは地域によって異なります	NTP UDP	123
Connector	LoadMaster		HTTP(S) TCP	443
LoadMaster	Connector		Syslog	514
Connector	connect.kemp.ax	20.103.161.175	TCP	443
Connector	axfconnector.azurecr.io axfconnector.westeurope.data.azurecr.io axfconnnector.eastus.data.azurecr.io	20.61.97.161 20.61.97.136 20.62.128.30	TCP	443
Connector	data.kemp.ax	20.76.253.12	HTTP(S)	9200
Connector	cdn.kemp.ax	20.76.253.12	HTTP(S)	443
Connector	git.rancher.io	34.208.213.149 52.36.54.134	TCP	443

LoadMaster360 Connector

LoadMaster と LoadMaster360 を統合する LoadMaster360 Connector を導入する必要があります。
LoadMaster360 Connector は下記の仮想環境で動作します。



ESXi, vCenter, vSphere



(Beta)



Microsoft Hyper-V (弊社は VMware 仮想マシンを推奨します。)

LoadMaster360 Connector のシステム要件

CPU	メモリー	ディスク	コメント
2.4GHz クアッドプロセッサ以上	最低 4GB	小規模環境：64GB 中規模環境：256GB 大規模環境：512GB	デフォルトでシステムログ、ESP/WAF のログを保存するためにそれぞれ 7GB のスペースを使用します。ログ保存スペースは拡張できます。

＊LoadMaster360 Connector は LoadMaster360 から生成されます。

LoadMaster360 ライセンス体系

LoadMaster360 のライセンスはアセット単位に使用許諾します。

製品情報

製品番号 (SKU)	製品説明
LM360starter1Y	10 アセットまで /90 日間のデータ保存 Application Health, Performance and Security Insight
LM360Asset10	追加 10 アセット
LM360-PLP1Y	1 年サブスクリプション更新

アセットとは (Asset)

LoadMaster 台数もしくは LoadMaster HA ペア数、それに基づいて算出され使用許諾されるアプリケーショングループ、仮想サービス数のことをいいます。

算出方法

例 1：1 台の LoadMaster もしくは 1 ペアの LoadMaster HA を所有している場合：

Asset 数 $10 - 1 = 9$ 個のアプリケーショングループ数

1 アプリケーショングループあたり 15 の仮想サービスが使用許諾されます。

$15 \text{ 仮想サービス} \times 9 \text{ 個のアプリケーショングループ数} = \text{LoadMasrt 1 台に最大 135 の仮想サービスが許諾されます。}$

例 2：5 台の LoadMaster もしくは 5 ペアの LoadMaster HA を所有している場合：

Asset 数 $10 - 5 = 5$ 個のアプリケーショングループ数

1 アプリケーショングループあたり 15 の仮想サービスが使用許諾されます。

$15 \text{ 仮想サービス} \times 5 \text{ 個のアプリケーショングループ数} = \text{LoadMaster 5 台全体に最大 75 の仮想サービスが許諾されます。}$

＊LoadMaster の台数が増えると、最終的にアプリケーショングループ数、仮想サービス数が減ります。
アプリケーショングループ数、仮想サービス数を増やしたい場合は、製品番号 LM360Asset10 を使用して 10 Asset 増やすことができます。