Mirantis Kubernetes Engine

モダンなアプリケーションを安全にすばやく
環境を選ばずに構築・共有・実行する

2021.08.26

Mirantis Kubernetes Engine（MKE：旧Docker Enterprise／Universal Control Plane）は モダンなアプリケーションを構築・共有・実行するための唯一のコンテナプラットフォームです

MKEは開発と運用の協調性を高める機能を備え、Kubernetesを利用してコンテナを大規模に開発運用できる最もシンプルな方法です。あらゆる環境（パブリック・プライベート・マルチ・ハイブリッドクラウドなど）において、アプリケーションをすばやく本番環境用に整えます。
MKEでは、アプリケーションライフサイクルのさまざまな段階と、Kuberntesスタック全体を通して、MKEは迅速性・柔軟性・安全性を提供します。MKEを利用すれば、既存の知識やインフラストラクチャを活用して、モダンなアプリケーションの迅速な開発や、段階的なデリバリが可能になります。つまり、開発者の生産性の向上や、リリース頻度の向上に加え、コストの削減、そしてあらゆる環境におけるKubernetesスタックへの安全なパイプラインが実現するのです。

Mirantis Kubernetes Engineで実現できること

迅速性：シンプルな操作性と、ワークフローの効率化が、モダンなアプリケーションのより迅速な本番環境へのデリバリを可能にします。

- 開発者のオンボーディングの加速化・生産性向上・既存スキルの活用
- 開発者と運用者がMKEで共同作業することにより、両者のプロセスを簡略化・効率化
- 高度な専門知識いらずの、本番環境に適したKubernetesの迅速なデプロイ・管理・更新（オプション：Mirantis社によるKubernetesのリモートで完全に運用管理するサービスあり（注：英語のみ）

柔軟性：環境を選ばずにKubernetesを利用できます。

- 検証済みの安全なコンテナコンテンツをDocker Hubから利用し、さまざまなアプリケーションスタックとインフラストラクチャをサポート
- さまざまなデータセンターやクラウドで、さまざまなアーキテクチャとOSのアプリケーションを実行
- ベンダーロックインなくコスト削減できる、堅牢なオープンソース・テクノロジーのフルスタックをデプロイ

安全性：アプリケーションのライフサイクルとKubernetes全体におけるさまざまな段階において組織や業界の要件や規格を継続的に維持できるので、イノベーションのスピードを落とさずに高い安全性を提供します。

- 開発者の生産性に影響を与えずに、企業やアーキテクチャの標準に準拠
- すべてのアプリケーションの来歴を保証し、懸念事項を確実に分離
- 分散型でハイブリットな環境など、あらゆる組み合わせのインフラストラクチャにおいて安全性を確保できる、可搬性に優れたセキュリティモデルを実現
- 主要なオープンクラウドのエキスパート達によるサポートとマネージドサービスを活用し、完全にクラウドネイティブなスタックのセキュリティコンプライアンスと可能な限り最高のSLAを実現

構 築

既存のスキルを活用したままで、コンテナ化アプリケーションとマイクロサービスを安全な方法で迅速に開発できます。MKEはインストールも簡単なので、すばやく開発に着手できます。

As a Serviceモデル（オプション）

- Mirantis社のオープンソース専門家によるKubernetesのリモート管理サポート（注：英語のみ）
- 開発者はインフラ運用から解放され、開発業務に集中可能

アプリケーションの円滑なデプロイ

- どのようなアプリケーションでも同じようにUIまたはCLIでMKEにデプロイ可能
- 各コンテナを実行しているノードをUIまたはCLIで確認可能
- Kubernetes YAMLを用いてKubernetesにデプロイ可能
- Docker ComposeファイルでSwarmとKubernetesのどちらにもアプリケーションをデプロイ可能

CI/CDの統合によるワークフローの自動化

- Mirantis Secure Registry（MSR: 旧Docker Trusted Registry）のWebhookを用いて、CI/CDソリューションなどのサードパーティツールにリアルタイムに情報を送信することによるアプリケーションのテストとデリバリの高速化

代表的なユースケース

- レガシーなアプリケーションのモダナイズ
- マイクロサービス／クラウドネイティブなアプリケーション
- CI/CDやDevOpsの実装
- データサイエンス
- エッジコンピューティング
- クラウド移行
- デジタルトランスフォーメーション

共 有

MKEでは、世界最大のコンテナコンテンツライブラリであるDocker Hubと、安全なプライベートレジストリであるMSRをシームレスに活用できます。認証済みのコンテンツを特定し、安全に共有できます。

安全で分散型のイメージ管理

- イメージの安全な保管や、リポジトリに対する粒度の高いアクセス制御を行うMSR
- 複数の場所でイメージを利用可能にする必要がある分散型チームや本番環境向けに、MSRではリポジトリのミラーリングにより必要な場所にイメージを配置、またイメージのキャッシュ機能によりネットワーク帯域を節約。
- Docker Hubのコンテナコンテンツのうち、検証済みで安全なコンテンツを活用
- 多様なアプリケーションとインフラストラクチャをサポート

高可搬性

- アプリケーションごとにネットワーク・ストレージ・機密情報などを定義可能
- アプリケーションから設定情報や関連情報を分離できるので、再コーディングせずに異なるインフラストラクチャ上にデプロイでき、「私のマシンでは動作した」問題を徹底的に解消

イメージ署名・検証・セキュリティポリシー

- Mirantis Content Trust（旧Docker Content Trust）で、ネットワーク間を移動するイメージを中間者攻撃から保護
- ユーザはビルド時にイメージを暗号署名可能
- イメージを作成／変更したユーザを記録
- 本番環境へデプロイ前にセキュリティポリシーを適用

イメージスキャンと脆弱性モニタリング

- Mirantis Security Scanningにより、信頼性の高いアプリケーションのみが本番環境で実行可能（オプション機能）
- Mirantis Security Scanningは、WindowsイメージとLinuxイメージ内のコンポーネントをインデックス化し、既知のCVEデータベースと照合
- 新たな脆弱性が報告されると、該当するCVEレポートのコンポーネントと、イメージ内のコンポーネントのインデックスを照合し、迅速に脆弱性レポートを生成
- 管理者は特定の脆弱性スキャンの結果を制御可能
- スキャン実行時に脆弱性のあるイメージを可視化可能

実 行

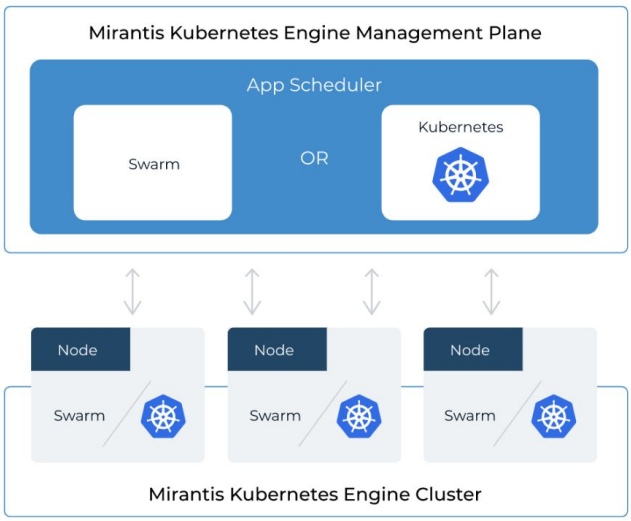
あらゆるクラウド上で実行できる一貫性のあるKubernetes環境で、モダンなアプリケーションを安全にデプロイ・管理します。

Kubernetesを使いやすく

- MKEに統合されているKubernetesは、CNCFが策定するKubernetesの動作仕様に準拠
- デフォルトで安全かつすぐに使えるKubernetesディストリビューション
- MKEを利用すれば、組織全体においてKubernetesがより簡単に、より安全に利用可能
- Kubernetesの専門知識は不要
- 熟達したユーザは、Kubernetes CLIによる高度な設定も可能

選択可能なオーケストレーション

- MKEは同じクラスタ上でSwarmとKubernetesの両者を同時に実行できる唯一のプラットフォーム
- LinuxとWindowsのノードに対し、双方のオーケストレータを選択できる柔軟性
- オートスケール・Container Storage Interface (CSI)のサポート・Kubernetesネイティブなアクセス制御・ストレージの保護など、Kubernetesが有する新たな機能を順次更新(MKEに搭載しているKubernetesの最新バージョンなど、詳細情報は販売店にお問い合わせください)



ライフサイクル管理の自動化

- クラスタ管理ツールを用いて、簡単なCLIコマンドを使用し、CNCF認定のKubernetes環境を容易にデプロイ・スケール・バックアップ・リストア・アップグレード
- ベアメタル・OpenStack・AWS・Azure・VMwareや、クラウド(パブリック/プライベート/ハイブリッド/マルチクラウドを含む)などあらゆる環境に、MKEを自動でインストールおよび設定可能

クラスタの透過的なアップグレード

- アプリケーションへの影響を軽減するため、クラスタにブルー・グリーンアップグレードを実施可能
- インフラソフトウェアのライフサイクルを、より少ないリスクかつ、より高い粒度で制御

統合されたネットワークとルーティング

- SwarmやKubernetesにデプロイしたアプリケーションは、“すぐに使えて交換可能な” ネットワークとルーティングのソリューションにアクセス可能
- デフォルトでインストールされている拡張性の高いネットワークとルーティングのソリューションであるProject Calicoは、好みのKubernetes CNIプラグインソリューションに交換可能
- Swarmにデプロイしたアプリケーション用のInterlockアーキテクチャに基づく、強力なアプリケーション層のルーティングとロードバランシング

ローリングアップデート

- ローリングアップデートにより、ダウンタイムなしでアップデートや新機能のデプロイが可能
- パフォーマンスメトリクスによって進捗状況を監視
- 必要に応じて迅速なロールバックも可能

Web UI

- SwarmとKubernetesどちらも、ユーザ・コンテナ・サービス・ネームスペース・コントローラ・ロードバランサ・ネットワーク・ボリューム・シークレット・ノードなど、すべてのシステムコンポーネントを、Web UIから一括管理

すぐに使えるダッシュボード

- 強力なヘルスステータスダッシュボードによる、ノードとコンテナのより詳細なメトリクス
- 障害発生時の迅速なトラブルシューティング
- 問題特定のための、クラスタレベル・ポッドレベル・コンテナ固有のメトリクスの表示と履歴の追跡
- クラスタメトリクスを外部のPrometheusサーバにエクスポートすることで、ローカルでの管理やモニタリングに利用可能

クラスタやアプリケーションの一括管理が行えるMKEのweb UI

アクセス制御の強化

- 組織のLDAP/AD、SAML 2.0によるSSO、PKI証明書に基づく認証をMKEに統合
- アプリケーション・ノード・シークレット・ネットワーク・ボリュームなどすべてのシステムコンポーネントに対する役割と責任範囲を管理
- MKEで事前設定済みのロールを利用することも、あるいは組織の既存プロセスに合わせたカスタムロールを作成することも可能

ノードのRBAC

- 特定のユーザやチームに、特定のノードへのアクセスを許可することで、物理的に隔離されたレイヤーを追加提供
- SwarmのリソースコレクションとKubernetesのネームスペースの両方に適用することで、ITサービス組織向けの "Bring Your Own Node (自分のノードを持ち込む)" サービスモデルが可能

アプリケーションのヘルスチェック

- サービスのヘルスチェックによる信頼性と安定性の向上
- 必要であれば、タイムリーなヘルスチェックや調整を行うために、ヘルスチェックの実行頻度をUIまたはDockerfileで設定可能

柔軟なOSの選択肢

- さまざまなLinuxディストリビューション (CentOS・Oracle Linux・RHEL・SLES・Ubuntu)
- Windows Server 2019

柔軟なインフラストラクチャの選択肢

- 仮想マシン・ベアメタル、AWSやMicrosoft Azureなど主要なクラウドプロバイダに簡単にインストール可能
- スムーズに動作するよう最適化・テスト済み

さらに安全なコンテナプラットフォームを維持するための多数の機能

FIPS 140-2に準拠したDocker Engine

- MCR（旧エンタープライズ版Docker Engine）の暗号モジュールは、米国の規制産業の要件であるFIPS140-2に準拠

通信の暗号化

- 自動的な相互TLS認証により、システム内通信をデフォルトで暗号化し保護
- SwarmとKubernetesネットワークの暗号化は、IPsecトンネルによりすべてのホスト間通信を保護

ノードアイデンティティの暗号化

- 悪意のあるノードがクラスタに追加されることを防ぐため、組み込みのルート認証局（CA）が自動で認証をローテーションし、システムの安全とオンライン状態を維持
- 外部CAをサポートし、ローテーション頻度を設定可能

シークレット管理の統合

- APIキーや認証情報などのシークレットを暗号化して安全に保存し、それらを必要とするアプリケーションサービスのみに転送
- WindowsとLinuxベースのコンテナどちらでも、アプリケーションサービス用のシークレットを簡単に作成・管理・展開

詳細な監査ログ

- クラスタとレジストリの両者にわたって詳細なイベントログを記録
- イベントログでは、セキュリティインシデント後の分析や特定のコンプライアンスの準拠のために、必要なユーザ・行動・タイムスタンプを記録し、完全な監査証跡を取得

SwarmのGroup Managed Service Accounts（gMSA）

- gMSAのサポートにより、Active Directory認証が必要なWindows Serverアプリケーションの対応範囲が拡大
- SwarmではDocker Configで認証情報を作成し、gMSAを使いやすく自動化可能

エンタープライズサポートと認定パートナーのエコシステム

MKEはエンタープライズに最適な製品です

定期的なリリースとメンテナンス

- 定期的なリリースにより、デプロイとアップグレードを事前に計画可能
- 各リリースのソフトウェアメンテナンス期間は24か月。詳細：https://docs.mirantis.com/mke/3.4/compat-matrix.html
- ソフトウェアメンテナンス期間中は、セキュリティパッチのほか、サポート対象のすべてのバージョンにホットフィックスをバックポートを提供

ソースコードのサポートと運用管理サービス

- Mirantisのクラウド専門家チームと共に構築をしたチームによるSLAに基づいたサポートサービス。
- 完全なKubernetesスタックのサポート。
- サポートサービス各種プラン
  - OpsCare（運用管理サービス）※英語
  - ProdCare（24時間365日）※英語
  - LabCare（平日10時-18時）※日本語

専門家による支援サービス

- 数多くの顧客企業と協業するMirantis社が培った実践的な方法論に基づき、技術面にとどまらないソリューションアーキテクチャエンゲージメントを提供
- 技術実装のみならず、レガシーシステムのコンテナ化の道のりを加速
- 業務に関わる人々やプロセスを考慮したアプローチ・サービス・トレーニング・導入サポートなどを提供

認証コンテナ

- Independent Software Vendors（ISV）が、自社のソフトウェアをMKE用のコンテナとしてパッケージ化し配布
- これらのコンテナはベストプラクティスに基づいて構築・テスト・スキャン・レビュー済み
- Mirantis社とISVからのサポートサービス有り

Mirantis社認定インフラストラクチャ

- Mirantis社認定インフラストラクチャであるAWS・Azure・vSphereにMKEをデプロイするための模範的なアプローチを提供。
- リファレンスアーキテクチャとエコシステムソリューション要項の提供により、MKEの自動ライフサイクル管理機能を補完。

認証プラグイン

- テクノロジーパートナーが、ネットワークプラグインとボリュームプラグインをMKE向けコンテナとしてパッケージ化し配布
- これらのコンテナはベストプラクティスに基づいて構築され、一連のAPIコンプライアンステストに合格し、スキャンおよびレビュー済み
- Mirantis社とプラグイン提供者によるサポートサービス有り