



Workload Optimization Manager 2.3.17 インストールとアップグレードガイド

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『INFORMATION PACKET』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティングシステムの UCB パブリック ドメインバージョンの一部として開発されたプログラムに適応したものです。全著作権所有。著作権©1981、カリフォルニア大学の評判。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、CISCO およびその供給者は、このマニュアルに適用できるまたは適用できないことによって、発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性が CISCO またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

Cisco は世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号については、シスコの Web サイトをご覧ください (www.cisco.com/go/offices)。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1110R)

Copyright © 2020 Cisco, all rights reserved

目次

| | |
|---|----|
| 対象紹介..... | 4 |
| タスク概要 | 5 |
| 最小要件..... | 7 |
| Workload Optimization Manager のインストール..... | 9 |
| VMware システムにインストール | 9 |
| Microsoft Hyper-V のインストール | 10 |
| AWS でのインストール | 10 |
| 一般構成タスク..... | 17 |
| (オプション) 静的 IP アドレスの指定 | 17 |
| (ベスト プラクティス) 時刻の同期 | 18 |
| (オプション) リモートの MariaDB 接続を Workload Optimization Manager インスタンスに構成する | 19 |
| (必須) ポート | 19 |
| (オプション) デフォルト以外のポートを開く | 20 |
| (必須) レポート用のカスタムポートのリスナーの構成..... | 20 |
| (オプション) セキュアなアクセスの適用 | 21 |
| (オプション) データベース ディスク使用量の電子メール通知を構成する | 24 |
| ライセンスのインストールおよび初回ログイン..... | 26 |
| WorkOptimization Manager License ライセンスをアップグレードする | 26 |
| シングル サインオン認証 | 28 |
| シングル サインオンの無効化 | 31 |
| シングル ログアウトのサポート | 32 |
| Workload Optimization Manager の新しいバージョンの更新..... | 33 |
| RHEL プラットフォームへのインストールと更新 | 36 |
| FAQ..... | 41 |



対象紹介

クラウドと仮想化環境の Intelligent Workload Automation Management ソリューションである Workload Optimization Manager をお選びいただきありがとうございます。このガイドは、仮想化環境に Workload Optimization Manager をインストールし、ライセンスをインストールし、リソースの管理を開始するのに必要な情報を提供します。

ご不明な点がございましたら、シスコ サポートまでお問い合わせください。

最後まで読んでいただき、ありがとうございました。

Workload Optimization Manager チーム



タスク概要

この『*Workload Optimization Manager* インストールガイド』には、以下のタスクを実行するための手順が記載されています。

| 次のことを行うことが必要な場合： | 実行または移動： |
|--|---|
| 新規 <i>Workload Optimization Manager</i> インストールを展開する。 | <ul style="list-style-type: none">■ <i>Workload Optimization Manager</i> のリリース ノートを確認します。■ 最小要件を満たしていることを確認してください。「最小要件」(7 ページ) を参照してください。■ 「<i>Workload Optimization Manager</i> のインストール」(9 ページ) のインストール手順を実行します。■ 必要に応じて設定構成を行います。「全般構成タスク」(17 ページ) を参照してください。■ 初回ログイン。「ライセンスのインストールおよび初回ログイン」(26 ページ) を参照してください。■ ライセンスをインストールします。「ライセンスのインストールおよび初回ログイン」(26 ページ) を参照してください。■ 必要に応じて SSO を構成します。「シングルサインオン認証」(28 ページ) を参照してください。■ <i>Workload Optimization Manager</i> インスタンスを引き続き使用します。『<i>Workload Optimization Manager</i> ユーザー ガイド』および『<i>Workload Optimization Manager</i> ターゲット構成ガイド』を参照してください。 |
| RHEL に新規 <i>Workload Optimization Manager</i> インストールを展開する。 | <ul style="list-style-type: none">■ <i>Workload Optimization Manager</i> のリリース ノートを確認します。■ 最小要件を満たしていることを確認してください。「RHEL とセットアップの要件」(36 ページ) を参照してください。■ 「RHEL プラットフォームへのインストールと更新」(36 ページ) のインストール手順を実行します。 |

| | |
|--|--|
| 次のことを行うことが必要な場合： | 実行するか次に移動： |
| ライセンスをアップグレードする。 | 「Workload Optimization Manager ライセンスのアップグレード」 (26 ページ) の指示に従ってください。 |
| 既存の Workload Optimization Manager インストールを更新する。 | <ul style="list-style-type: none"> ■ <i>Workload Optimization Manager</i> のリリース ノートを確認します。 ■ サポートされているハイパーバイザーまたは RHEL プラットフォームで Workload Optimization Manager を更新するための最小要件を満たしていることを確認します。 <ul style="list-style-type: none"> - 最小要件 (7 ページ)。 - RHEL とセットアップの要件 (36 ページ) ■ 次の更新手順のいずれかを実行します。 <ul style="list-style-type: none"> - Workload Optimization Manager の新規バージョンへの更新 (33 ページ) - RHEL 展開の更新 (39 ページ) ■ 必要に応じて、ライセンスをアップグレードします。「Workload Optimization Manager ライセンスのアップグレード」 (26 ページ) を参照してください。 ■ ログイン。 ■ Workload Optimization Manager インスタンスを引き続き使用します。『<i>Workload Optimization Manager ユーザー ガイド</i>』および『<i>Workload Optimization Manager ターゲット構成ガイド</i>』を参照してください。 |



最小要件

以下は Workload Optimization Manager の最小要件です。

| サポート対象テクノロジー | | ストレージ要件 | メモリ | CPU |
|---------------------------|--|--|-------|----------|
| VMware | vCenter バージョン 5.5、6.0、6.5、6.7 | 500GB 以上 | 32 GB | vCPU x 4 |
| Microsoft | Windows 2016、2008 R2、Hyper-V Server 2012、Hyper-V Server 2012 R2 とバンドルされた Hyper-V | 注意： ストレージの要件によってシンプロビジョニング可能です。 | | |
| Amazon Web Services (AWS) | | | | |

注:

最小要件は、環境内インベントリのサイズによって異なります。データストア、ホスト、VM、およびアプリケーションが多ければ多いほど、インストールを効果的に実行するのに必要なリソースが多くなります。他の管理ソフトウェアでは、低いリソースを持つ Workload Optimization Manager VM を実行するように推奨していることに注意してください。上記のガイドラインを使用して、Workload Optimization Manager に十分なリソースを提供してください。

価格調整を使用する場合は、Workload Optimization Manager で、Workload Optimization Manager インスタンスをホストする VM に割り当てられるメモリを次のように増やすことをお勧めします。

- 1 つ以上の請求グループに割り当てる価格調整の場合：
 - 最初の価格調整では、4GB 増設します。
 - 後続の価格調整のそれぞれについて、追加で 1 GB 増設します。

価格調整については、『*Workload Optimization Manager ユーザーガイド*』の「課金情報とコスト」を参照してください。

Workload Optimization Manager は、DHCP または静的 IP アドレス指定をサポートします。静的 IP アドレスを使用する方法の詳細については、[「\(オプション\) 静的 IP アドレスを指定する」 \(17 ページ\)](#) を参照してください。

ブラウザ要件

Workload Optimization Manager は、最も一般的に使用されている Web ブラウザ (Internet Explorer、Mozilla Firefox、Google Chrome、Apple Safari など) で動作します。

Web ブラウザは、JavaScript が有効になっている必要があります。

さらに、Workload Optimization Manager のユーザー インターフェイスに使用するブラウザは、Workload Optimization Manager インスタンスと 1 分以内に同期する必要があります。この同期を行わないと、Workload Optimization Manager に不正なメトリック値が表示される可能性があります。

また、Workload Optimization Manager のユーザー インターフェイスに GoogleChrome を使用している場合、レポートを表示するには、レポートをダウンロードする前に Chrome プレビュー モードをオフにする必要があります。



Workload Optimization Manager のインストール

Workload Optimization Manager を使い始めるときには、サポートされているハイパーバイザに使用可能なさまざまなダウンロードがあることに注意してください。これらのダウンロードはすべて同じ機能の Workload Optimization Manager の同じバージョンを配信しますが、異なるハイパーバイザプラットフォームでインストールおよび実行するようにパッケージングされています。

Red Hat を実行している VM のシスコソフトウェアをインストールできます ([「RHEL プラットフォームでインストールおよび更新する」 \(36 ページ\)](#) を参照してください)。

各インストールは、まったく同じ方法で仮想環境を管理します。選択したインストールは、企業のポリシーと標準規格によって異なります。このドキュメントでは、Workload Optimization Manager ダウンロードのそれぞれのインストール手順を説明します。選択したインストールは、Workload Optimization Manager で管理できる技術に影響がありません。どのタイプのマシンが Workload Optimization Manager をホストしているかに関係なく、クラウドプラットフォームおよびロードバランサターゲット経由で管理されているのと同じく、サポートされているハイパーバイザで実行されているすべてのワークロードを管理できます。

ここでは、新しい Workload Optimization Manager インスタンスをインストールする方法を説明します。現在のインストールを新しいバージョンに更新している場合、現在のインストールを更新する代わりに完全なインストールを実行する必要があります。[「Workload Optimization Manager の新しいバージョンへの更新」 \(33 ページ\)](#) を参照してください。

このセクションには、次のサポートされている仮想プラットフォーム用のインストール手順が含まれています。

- [VMware システムにインストール \(9 ページ\)](#)
- [Microsoft Hyper-V にインストール \(10 ページ\)](#)
- [AWS にインストール \(10 ページ\)](#)

Workload Optimization Manager を展開する時、それを名前に下線文字を含まない VM にインストールする必要があります。ホスト名を変更できない場合、[「ホスト名の制限を回避するには？」 \(43 ページ\)](#) で説明されている回避策を使用できます。

注:

IAM ロールを使用して AWS ターゲットを検出する場合、Workload Optimization Manager は AWS を展開する必要があり、IAM ロールに Workload Optimization Manager インスタンスを割り当てる必要があります。サポートが必要な場合は、テクニカルサポートにお問い合わせください。

VMware システムにインストール

この Workload Optimization Manager インスタンスのダウンロードは .OVA 1.0 の形式です。

Workload Optimization Manager をインストールする場合:

1. Workload Optimization Manager インストール パッケージをダウンロードします。
Workload Optimization Manager ダウンロード ページへのリンクについて、シスコから受信する電子メールを参照してください。
2. vCenter を使用して、VMware インフラストラクチャに OVA ファイルをインポートします。
3. Workload Optimization Manager アプライアンスを開始し、その IP アドレスを記録します。

ユーザーはアプライアンス IP アドレスに移動し、ブラウザで Web ユーザー インターフェイスを起動します。

4. 必要に応じて、アプライアンスに静的 IP アドレスを指定します。

環境に DHCP がない、または Workload Optimization Manager インスタンスに IP アドレスを付与する場合、[「\(オプション\) 静的 IP アドレスを指定する」 \(17 ページ\)](#) を参照してください。

5. Workload Optimization Manager インスタンスに必要な設定手順を実行します。

[「全般構成タスク」 \(17 ページ\)](#) を参照してください。

Microsoft Hyper-V のインストール

Workload Optimization Manager をインストールするには?

1. Workload Optimization Manager インストールパッケージをダウンロードします。

Workload Optimization Manager ダウンロード ページへのリンクについて、シスコから受信する電子メールを参照してください。

2. .zip ファイルを展開し内容をコピーして、Hyper-V サーバに（またクラスタ共有ボリュームかローカルハードドライブのどちらかに）仮想マシンイメージを含みます。

3. Hyper-V マネージャの仮想マシン インポート ウィザードを使用して、環境内に仮想マシンをインポートします。

4. 仮想ネットワーク アダプタが正しい仮想ネットワークに接続されていることを確認します。

5. Workload Optimization Manager インスタンスに十分なメモリが必要です。

シスコでは、Workload Optimization Manager インスタンスに静的メモリを使用することを推奨します。ただし、インスタンスに静的または動的なメモリを指定することができます。

インスタンスの **[プロパティ]** で、インスタンスの **[ハードウェア設定]** に移動します。

- 静的メモリについては、最低 32 G の**仮想マシンのメモリ**を設定します。
- 動的メモリについては、**スタートアップメモリ** および**最小メモリ**を 32 GB にします。

6. Workload Optimization Manager アプライアンスを開始し、その IP アドレスを記録します。

ユーザーはアプライアンス IP アドレスに移動し、ブラウザで Web ユーザー インターフェイスを起動します。

7. 必要に応じて、アプライアンスに静的 IP アドレスを指定します。

環境に DHCP がない、または Workload Optimization Manager インスタンスに IP アドレスを付与する場合、[「\(オプション\) 静的 IP アドレスを指定する」 \(17 ページ\)](#) を参照してください。

8. Workload Optimization Manager インスタンスに必要な設定手順を実行します。

[「全般設定タスク」 \(17 ページ\)](#) を参照してください。

注:

Workload Optimization Manager インスタンスの設定には、ネットワークに接続されていない NIC が含まれています。インスタンスをインストールすると、Hyper-V マネージャを使用して、ネットワーク VLAN 設定を設定し、クラスタのネットワークの要件に合わせます。

AWS でのインストール

AWS インストールの場合、Workload Optimization Manager を Amazon Machine Image (AMI) としてインストールします。このインストールを実行するには、展開が次のような Workload Optimization Manager と Amazon のベスト プラクティスに従っていることを確認してください。

- EBS データ ボリューム スナップショットの自動スケジューリングと実行

AWS はこれらのスナップショットを毎日実行し、ユーザーが作成した S3 バケットに 14 日間保存します。

- EBS ボリューム暗号化

Workload Optimization Manager は、セキュリティ グループを使用して、HTTPS を介した Workload Optimization Manager インスタンスへのアクセスのみを許可することをお勧めします。

- 認証のための Identity and Access Management (IAM) インスタンス プロファイル (インスタンス ロール) のセットアップと使用

ワークロード最適化マネージャーは、アクセスキーよりもインスタンスロールを推奨します。インスタンス ロールは、コンプライアンス目的で管理するのがより簡単であり、AWS SDK によってネイティブにサポートされています。

さらに、Workload Optimization Manager は、次の場所に示された手順に従って、インスタンス ロールのクロスアカウント アクセスを有効にすることをお勧めします。 <https://aws.amazon.com/blogs/security/how-to-enable-cross-account-access-to-the-aws-management-console/>
- HA/リカバリ目的で自動拡張を利用する

AWS 自動拡張を使用して、Workload Optimization Manager は、インスタンスが常に実行されていることを確認します。このインストールを実行すると、CloudFormation テンプレートによってこれらのベスト プラクティスが確実に順守されます。

CloudFormation テンプレートを使用したインストール

このテンプレートは、CentOS を実行し、Workload Optimization Manager インスタンスをホストする VM の起動を指示します。このテンプレートにより、展開が Workload Optimization Manager と Amazon のベスト プラクティス両方に従うことが保証されます。

CloudFormation テンプレートを使用して Workload Optimization Manager をインストールするには：

1. Workload Optimization Manager CloudFormation テンプレートをダウンロードします。
CloudFormation テンプレートにアクセスするには、テクニカル サポートにお問い合わせください。
2. テンプレートを変更して、AWS 環境に応じてパラメーターを設定します。
詳細については、[「CloudFormation テンプレートの概要」 \(12 ページ\) を確認してください](#)。
3. AWS コンソールにログインし、CloudFormation サービスを選択します。
4. 新しいスタックを作成します。
テンプレートの入力を求められたら、次の手順に従います。
 - a. [テンプレートを Amazon S3 にアップロード (Upload a template to Amazon S3)] をクリックします。
 - b. ダウンロードして変更したテンプレートを選択します。
 - c. [次へ (Next)] をクリックします。
5. [詳細の指定 (Specify Details)] ページで、スタック情報を入力します。
スタック名を入力し、画像サイズを選択します。[Next] をクリックします。

注:

シスコでは m5.xlarge インスタンス タイプを推奨していますが、m5.large、m5.2xlarge、m4.xlarge、m4.large、m4.2xlarge、r4.xlarge、r4.2xlarge、r5.xlarge、r5.2xlarge、i2.xlarge、i3.xlarge、c4.2xlarge、c5.2xlarge を使用することもできます。

6. [オプション (Options)] ページで、必要なタグを入力します。
たとえば、Key-Value ペアのデフォルト値を変更して、データの定期的なバックアップを設定します。
タグを追加したら、[次へ] をクリックします。
タグは、セキュリティのニーズやビジネス要件などに基づいてインスタンスをグループ化するための便利な方法です。詳細については、<https://aws.amazon.com/answers/account-management/aws-tagging-strategies/> を参照してください。
7. [レビュー (Review)] ページで、選択が正しいことを確認します。
選択内容を確認したら、[作成 (Create)] をクリックします。

(オプション) セキュリティ グループの作成

注:

CloudFormation テンプレートを介して Workload Optimization Manager をインストールすると、そのインストールによってこのステップが自動的に実行されます。

CloudFormation テンプレートを使用せずに Workload Optimization Manager をインストールする場合、シスコではセキュリティグループを作成して Workload Optimization Manager インスタンスに対してのみ HTTPS へのアクセスを制限し、このグループを Workload Optimization Manager インスタンスに接続することをお勧めします。

セキュリティ グループの詳細については、Amazonのドキュメントを参照してください。を参照してください。 http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

CloudFormation テンプレートの概要

このセクションでは、CloudFormation テンプレートの一部について、テンプレートを準備するときに役立つ可能性のある追加の説明を提供します。

このスニペットは、CloudFormation テンプレートの構造を作成し、テンプレートの残りの部分で使用されます。

Metadata:

Instances:

Description: Your Turbonomic instance is created with an encrypted EBS Volume. If you create an encrypted volume and don't specify this property, AWS CloudFormation uses the default master key.

'AWS::CloudFormation::Designer':

5979b605-17c1-4e1a-9158-ae132fb86736:

size:

width: 60

height: 60

position:

x: 30

'y': -20

z: 1

embeds: []

ef20cdef-19a0-4d61-9f16-0108bb0330e1:

size:

width: 60

height: 60

position:

x: 150

'y': 10

z: 1

embeds: []

dependson:

- ea836120-be24-44ab-bd80-e2c9749fad84

- b4bc499e-9882-4ab9-9c37-e165e51fe589

ea836120-be24-44ab-bd80-e2c9749fad84:

size:

width: 60

height: 60

position:

x: -60

'y': 210

z: 1

embeds: []

b4bc499e-9882-4ab9-9c37-e165e51fe589:

size:

width: 60

height: 60

position:

x: 180

'y': 210

z: 1

embeds: []

```

dependson:
  - ea836120-be24-44ab-bd80-e2c9749fad84
isrelatedto:
  - ea836120-be24-44ab-bd80-e2c9749fad84
6e649c64-891f-4e11-a83a-2df5cf26d0b5:
  source:
    id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
  target:
    id: ea836120-be24-44ab-bd80-e2c9749fad84
  z: 2
7c216255-250c-4574-9bcf-fb02673b306e:
  source:
    id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
  target:
    id: b4bc499e-9882-4ab9-9c37-e165e51fe589
  z: 2
84fca9b5-0bb0-4a88-b0e3-c74af6b00b80:
  source:
    id: b4bc499e-9882-4ab9-9c37-e165e51fe589
  target:
    id: ea836120-be24-44ab-bd80-e2c9749fad84
  z: 2

```

次のスニペットは、許可されるデブ展開テンプレートを設定し、後でテンプレートで使用する VPC ID を定義します。

Parameters:

InstanceTypeParameter:

Type: String

Default: m4.xlarge

AllowedValues:

- m4.large
- m4.xlarge
- m4.2xlarge

Description: 'Enter m4.large, m4.xlarge, or m4.2xlarge. Default is m4.xlarge.'

VpcIdParameter:

Type: 'List<AWS::EC2::VPC::Id>'

Description: VpcId of your existing Virtual Private Cloud (VPC)

ConstraintDescription: must be the VPC Id of an existing Virtual Private Cloud.

次のスニペットは、さまざまな AWS リージョンをマッピングして、Workload Optimization Manager インスタンスがデフォルトのリージョンに展開されていることを確認します。

注:

リージョンごとに利用可能な AMI のリストは定期的に変更されます。Workload Optimization Manager の AMI の最新リストを取得するには、AWS Marketplace にアクセスし、AWS 認証情報を使用してログインします。[手動起動 (Manual Launch)] タブをクリックします。次に、Workload Optimization Manager の最新バージョンを選択して、リージョンと AMIID を表示します。テンプレートで使用するために、リージョンと AMI ID を記録します。

Mappings:

RegionMaptoAMI:

us-east-2:

AMI:

- "ami-366f4e53"

us-east-1:

AMI:

```
- "ami-7ae9c16c"
us-west-1:
AMI:
- "ami-898fa2e9"
us-west-2:
AMI:
- "ami-f656428f"
ap-south-1:
AMI:
- "ami-f23f419d"
ap-northeast-2:
AMI:
- "ami-76f02f18"
ap-southeast-1:
AMI:
- "ami-756fe316"
ap-southeast-2:
AMI:
- "ami-f32d3d90"
ap-northeast-1:
AMI:
- "ami-e834208f"
ca-central-1:
AMI:
- "ami-28cd724c"
eu-central-1:
AMI:
- "ami-72eb4d1d"
eu-west-1:
AMI:
- "ami-1d7b607b"
eu-west-2:
AMI:
- "ami-eb61778f"
sa-east-1:
AMI:
- "ami-cce289a0"
```

次のスニペットは、Workload Optimization Manager セキュリティグループを作成します。これにより、Workload Optimization Manager インスタンスへのアクセスが HTTPS のみに制限されます。

Resources:

```
TurbonomicSecurityGroup:
Type: AWS::EC2::SecurityGroup
Properties:
GroupName: TurbonomicSecurityGroup
GroupDescription: Creates and limits access to Turbonomic instance through port 443 only
VpcId:
Ref: VpcIdParameter
SecurityGroupIngress:
- IpProtocol: tcp
FromPort: '443'
ToPort: '443'
CidrIp: 0.0.0.0/0
Metadata:
```

```

    'AWS::CloudFormation::Designer':
      id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
  DependsOn:
    - Turbonomic

```

次のスニペットは、Workload Optimization Manager インスタンスの次の項目を設定します。

- インスタンスのサイズ
- インスタンスのリージョン
- アクセス、バックアップ、暗号化などのブロックストレージプロパティ
- セキュリティグループ

注:

DeleteOnTermination はデフォルトでは false に設定されます。これにより、EC2 インスタンスが後で終了した場合でも、データが保持されます。

```

Turbonomic:
  Type: 'AWS::EC2::Instance'
  Properties:
    InstanceType:
      Ref: InstanceTypeParameter
    ImageId:
      'Fn::FindInMap':
        - RegionMaptoAMI
        - Ref: 'AWS::Region'
        - AMI
    BlockDeviceMappings:
      - DeviceName: /dev/sdi
        Ebs:
          VolumeType: gp2
          DeleteOnTermination: false
          VolumeSize: 150
          Encrypted: true
    EbsOptimized: true
    InstanceInitiatedShutdownBehavior: stop
  Metadata:
    'AWS::CloudFormation::Designer':
      id: ea836120-be24-44ab-bd80-e2c9749fad84

```

次のスニペットは、1 の自動スケーリンググループを作成します。これにより、Workload Optimization Manager EC2 インスタンスが常に実行されます。

```

TurbonomicAutoScalingGroup:
  Type: 'AWS::AutoScaling::AutoScalingGroup'
  Properties:
    AvailabilityZones:
      - !GetAtt Turbonomic.AvailabilityZone
    InstanceId:
      Ref: Turbonomic
    Cooldown: '1800'
    MinSize: '1'
    MaxSize: '1'
    DesiredCapacity: '1'
    HealthCheckType: EC2
    HealthCheckGracePeriod: 900

```

```
Metadata:
  'AWS::CloudFormation::Designer':
    id: b4bc499e-9882-4ab9-9c37-e165e51fe589
DependsOn:
  - Turbonomic
```

次のスニペットは、毎日のバックアップに必要な S3 バケットを作成します。

```
TurbonomicS3BackupBucket:
  Type: 'AWS::S3::Bucket'
  Properties:
    AccessControl: AuthenticatedRead
    BucketName: turbonomic-s3-volume-backup-bucket
  Metadata:
    'AWS::CloudFormation::Designer':
      id: 5979b605-17c1-4e1a-9158-ae132fb86736
```




一般構成タスク

Workload Optimization Manager インスタンスをインストールした後、次の設定タスクを実行します。

- (オプション) 静的 IP アドレスを指定します。
- (ベスト プラクティス) システム クロックを同期し、時間サーバーを構成します。
- (オプション) リモート MariaDB 接続を構成します。
- (必須) Workload Optimization Manager が必要とするポートでネットワーク通信が開いていることを確認します。
- (オプション) Workload Optimization Manager VM でデフォルト以外のポートを開き、ターゲットからの通信を可能にします。
- (必須) レポート用のカスタム ポートのリスナーを構成します。
- (オプション) 信頼できる証明書をインストールして、セキュアなアクセスを実施します。
- (オプション) データベース ディスク使用量の電子メール通知を構成します。

(オプション) 静的 IP アドレスの指定

多くのインストールでは、動的 IP アドレスの割り当てに DHCP を使用します。仮想マシンの IP 設定で静的アドレスを指定することもできます。

静的 IP アドレスを指定する必要がある場合のみ、次の方法のいずれかを選択します。

- Workload Optimization Manager から `ipsetup` スクリプトを使用します。
- 静的 IP アドレスを手動でこのトピックで説明されているように構成します。

ipsetup スクリプト

Workload Optimization Manager は、このタスクをサポートする `ipsetup` スクリプトを提供します。

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
次のデフォルトのクレデンシャルを使用します。
 - ユーザー名: `root`
 - パスワード: `vmturbo`
2. セッションが開いたら `ipsetup`、コマンドでスクリプトを実行します。

手動による静的 IP アドレスの設定

静的 IP アドレスを指定するには、次の手順を実行します。

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
次のデフォルトのクレデンシャルを使用します。
 - ユーザー名：root
 - パスワード：vmturbo
2. 接続エディタを開きます。
 - a. nmtui コマンドを実行します。
これにより、NetworkManager にユーザー インターフェイスが開きます。
 - b. **[接続の編集 (Edit a connection)]** をクリックしてエディタを開きます。
3. 新しい接続を追加します。
画面の **[追加]** をクリックして、[新規接続] ダイアログ ボックスを開きます。
4. イーサネット接続を追加します。
 - a. オプションのリストから **[イーサネット (Ethernet)]** を選択し、次の情報を入力します（指定された値は例です）。
 - プロファイル名：eth0
 - デバイス：eth0
 - IPv4 構成：Manual
 - **[表示 (Show)]** をクリックし、環境に応じてサブ設定を完了します。
 - b. **[OK]** をクリックして、構成リストに戻ります。
5. 作成した接続が存在することを確認します。
6. **[終了 (Quit)]** をクリックしてコマンドラインに戻ります。
7. ネットワーク サービスを再起動します。

```
service network restart
```

ネットワーク サービスが正常に再起動します。
8. マシンがアクセス可能であり、静的 IP アドレスが正しいことを確認します。

```
ifconfig eth0
```

この手順は、Quit インスタンスの IP アドレスに適用されます。この IP アドレスを使用して Web ユーザー インターフェイスにアクセスできます。

(ベスト プラクティス) 時刻の同期

同じネットワークにあるデバイスとともに、Workload Optimization Manager インスタンスの時計を同期することが重要です。Workload Optimization Manager では通常夜間に定期的なデータ メンテナンスを実行するため、パフォーマンス上、シスコでは利用するタイムゾーンに Workload Optimization Manager システム クロックを設定することをお勧めします。Network Time Protocol デーモンを使用して (ntpd)、Workload Optimization Manager システム クロックを設定します。

注:

yast オプションを使用して NTP サービスを設定しないでください。NTP を設定するには、以下の手順を使用します。yast タイムゾーンユーティリティには NTP を設定するオプションがありますが、この yast オプションを使用しないでください。

NTP サーバを構成するには：

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
2. ntp 構成ファイルを開きます。
たとえば、次のコマンドを実行します。vi /etc/ntp.conf
3. タイム サーバーを指定する行を見つけます。
4. これらのタイム サーバー行を、タイム サーバーの完全修飾ドメイン名に置き換えます。

もっとも安全なアプローチは、通常タイム サーバーの IP アドレスを提供することです。タイム サーバーが 1 つしかない場合は、2 回目のサーバー エントリを削除できます。

5. ファイルを保存します。

6. NTP デーモンが有効になっていることを確認してください。

NTP デーモンはデフォルトで有効になっている必要があります。デーモンを有効にするには、以下の `systemctl enable ntpd` コマンドを使用します。

7. NTP デーモンが動作していません。

実行: `systemctl status ntpd`

8. 時間が正しいことを確認してください。

`date` コマンドを実行します。次のような結果が表示されます。

```
Thu Oct 18 14:25:45 CST 2018
```

(オプション) リモートの MariaDB 接続を Workload Optimization Manager インスタンスに構成する

リモートクライアントが Workload Optimization Manager インスタンスの MariaDB データベースへ接続できるようにする場合、ローカルホストバインドアドレス (127.0.0.1) を Workload Optimization Manager インスタンスの IP アドレスに置換できます。リモートクライアント接続を MariaDB データベースに設定するには、次の手順を実行します。

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。

次のデフォルトのクレデンシャルを使用します。

- ユーザー名: root
- パスワード: vmturbo

2. `bind+addr` 構成ファイルを開きます。

たとえば `vi /etc/my.cnf.d/bind-addr.cnf`、コマンドを使用します。

3. `bind_address` パラメーターを Workload Optimization Manager インスタンスの IP アドレスに設定します。

次に例を示します。 `bind_address=10.10.10.123`

4. ファイルを保存します。

5. MariaDB サービスを再起動します。

`systemctl restart mariadb` コマンドを実行します。

(必須) ポート

ネットワーク通信のポートが開いていることを確認します。

Workload Optimization Manager は、次のポートを使用します。

| ポート: | サポート: |
|------|---|
| 80 | HTTP 経由で受信ブラウザ接続 |
| 443 | <ul style="list-style-type: none"> ■ HTTPS 経由で受信ブラウザ接続 ■ プロアクティブなサポート (Workload Optimization Manager 問題のサポート チケットを自動的に生成) |

Workload Optimization Manager インスタンスとのブラウザ接続について、ポート 80 または 443 のどちらかを使用する必要があります。

注:

Workload Optimization Manager で使用するさまざまなターゲットは、Workload Optimization Manager との通信を可能にするために、それらのターゲットでポートを開く必要がある場合があります。詳細とデフォルトポートのリストについては、『*Workload Optimization Manager* ターゲット構成ガイド』の「ポート構成」を参照してください。

(オプション) デフォルト以外のポートを開く

ターゲットがデフォルト以外の非標準ポートを使用している場合、Workload Optimization Manager VM でポートを開き、ターゲットからの通信を可能にできます。ポートを開くには、SELinux audit2allow 診断ツールを使用します。audit2allow ツールが監査ログからアクセスベクトルキャッシュ (AVC) メッセージを解析し、モジュールを作成して (semodule)、ポートへのアクセスを許可します。

デフォルト以外の非標準ポートを開くには、次の手順を実行します。

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
2. SELinux コマンドを実行可能な一時ディレクトリに変更します (たとえば、/tmp/selinux)。
3. モジュール、マイアプリを作成します。

audit2allow オプションで -M コマンドを使用します。

```
audit2allow -M myapp < /var/log/audit/audit.log
```

4. カーネルにモジュールをロードします。

```
semodule -i myapp.pp
```
5. ポートへのアクセスを再テストします。

(必須) レポート用のカスタムポートのリスナーの構成

会社のポリシーにより要求されているカスタムポート番号を使用していて、レポートが例外により失敗する場合は Error Generating Report、ポート 443 でローカルホストインターフェイスアドレス (127.0.0.1) のリスナーを構成する必要があります。

リスナーを構成するには、次の手順を実行します。

1. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。

次のデフォルトのクレデンシャルを使用します。

- ユーザー名: root
- パスワード: vmturbo

2. Apache ssl.conf ファイルを開きます。

たとえば vi /etc/httpd/conf.d/ssl.conf、コマンドを使用します。

3. 構成ファイルで、リスナーセクションを検索します。

次のコードを探します。

```
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
```

4. ポート 443 にローカルホストインターフェイスアドレス (127.0.0.1) のリスナーを追加します。

この例では、カスタムポート 1443 がすでに存在すると仮定します。ポート 443 にリスナーが追加されていることに注意してください。

```
# When we also provide SSL we have to listen to the
```

```
# the HTTPS port in addition.
#
Listen 1443 https
Listen 127.0.0.1:443 https
```

5. `ssl.conf` ファイルの `VirtualHost` セクションを確認してください。

- ポート 443 の元の `VirtualHost` セクションがまだ存在する場合は、それが次の `VirtualHost` セクションと一致することを確認してください。
- 元の `VirtualHost` セクションがカスタム ポート用に変更されている場合は `ssl.conf`、ファイルの最上部でリスナー用に次の `VirtualHost` セクションを追加します。

重要事項：

カスタム ポートに使用されるのと同じキー ペアをリスナーに使用する必要があります。

```
<VirtualHost 127.0.0.1:443>
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SSLHonorCipherOrder On
SSLCipherSuite HIGH:!NULL:!MD5:!DSS:!3DES
SSLProtocol -all +TLSv1.2
SSLCipherSuite ALL:+HIGH:!ADH:!EXP:!SSLv2:!SSLv3:!DSS:!3DES:!MEDIUM:!LOW:!NULL:!aNULL
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

6. 書き込みし `ssl.conf`、ファイルを終了します。

esc を押して `:wq!` と入力し、**Enter** キーを押します。

7. `http` サービスを再起動します。

```
service http restart
```

(オプション) セキュアなアクセスの適用

会社のポリシーにより信頼できる証明書が必要な場合、`Workload Optimization Manager` により既知の証明機関から信頼できる証明書をインストールすることができます。

1. 証明書を要求します。

a. `Workload Optimization Manager` インスタンスへの SSH ターミナルセッションを開きます。

デフォルトのクレデンシャルは次のとおりです。

- ユーザー名：`root`
- パスワード：`vmturbo`

- b. 秘密キーを保存する `/private` ディレクトリに変更します。
`cd /etc/pki/tls/private`
- c. 秘密キー ファイルを作成するコマンドを実行します。
`openssl genrsa -out turbonomic.key 2048`
- d. CSR を生成するために使用される情報が含むファイルを作成します。
`vi certsignreq.cfg`
- e. ファイルでは、次のコードを挿入しフィールドを指定します。

```
[req]
ts = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[dn]
C=<country, 2 letter code>
L=<city>
O=<company>
OU=<organizational unit name>
CN=<FQDN>
emailAddress=<email address>

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = <FQDN>
DNS.2 = <server's short name>
DNS.3 = <server's IP address>
```

注:

[CN] フィールドに、Workload Optimization Manager インスタンスの完全修飾ドメイン名を指定します。

代理ユーザー名は、Workload Optimization Manager インスタンスにアクセスする別の方法です。代行ユーザー名 ([alt_names]) セクションに、DNS.1 フィールドの値は必須です。[DNS.1] フィールドに、Workload Optimization Manager インスタンスの完全修飾ドメイン名を指定します。DNS.2 と DNS.3 のフィールドの値はオプションです。必要に応じて、複数の DNS.<n> フィールドを追加できます。

次に例を示します。

```

root@turbonomic:/etc/pki/tls/private
[root@turbonomic private] vim certsignreq.cfg

ts = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[dn]
C=US
ST=New York
L=White Plains
O=Turbonomic
OU=Educational Services
CN=demo.turbonomic.com
emailAddress= <first.lastname>@turbonomic.com

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = demo.turbonomic.com
DNS.2 = demo
DNS.3 = my.ip.add.ress
  
```

- f. 書き込みし、ファイルを終了します。
esc を押して `:wq!` と入力し、**Enter** キーを押します。
 - g. 証明書要求ファイルを作成します。
 コマンドを実行します:

```
openssl req -new -sha256 -nodes -out turbonomic.csr -key turbonomic.key -config certsignreq.cfg
```
 - h. ローカル マシンに証明書要求ファイルを転送します。
 リモート マシンの証明書要求ファイル (`turbonomic.csr`) へのパスは、`/etc/pki/tls/private` です。
 - i. このファイルを証明機関に送信します。
 証明機関は証明書を作成するためにこのファイルを使用します。
 認証局から DER と Base64 の間のエンコーディングを選択できる場合は、**Base64** を選択してください。
2. 証明書ファイルの名前を変更します。
 証明機関 (CA) から証明書ファイルを受信するときに、証明書ファイルの名前を確認します。
 名前を `turbonomic.crt` に変更します。
 中間証明書のバンドルについて、証明機関 (たとえば、GoDaddy または Symantec) はセキュリティ上の理由により、ルート証明書にプロキシとして中間証明書を使用する場合があります。その場合、証明書チェーンバンドルも受信します。その場合、証明書チェーンにも `.crt` 拡張子 (例: `<intermediate>.crt`) が付けられた名前をつけます。
 3. 証明書をアップロードします。
 Workload Optimization Manager インスタンスの `/etc/pki/tls/certs` ディレクトリに上記の証明書ファイルをします。
 4. 証明書を適用します。
 - a. Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
 デフォルトのクレデンシャルは次のとおりです。
 - ユーザー名: `root`
 - パスワード: `vmturbo`
 - b. `ssl.conf` ファイルのバックアップ ファイルを作成します。

```
cp /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf-LOCALHOST
```
 - c. `ssl.conf` ファイルを開きます。

```
vi /etc/httpd/conf.d/ssl.conf
```
 - d. 新しいキーと `crt` ファイルのファイルパスを指定するため、`ssl.conf` ファイルを編集します。
 - `localhost.crt` を新しい証明書名に置換します (`turbonomic.crt`) 。
 - `# Server Certificate`

- ```

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

```
- また localhost.key、を新しいキー ファイル名に置換します (turbonomic.key) 。
 

```

Server Private Key
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

```
  - 中間証明書を受信した場合 server-chain.crt、を新規の中間ファイル名 (<intermediate>.crt) に置換します。
 

```

Server Certificate Chain
SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

```
- e. 書き込みし ssl.conf ファイルを終了します。  
**esc** を押して :wq! と入力し、**Enter** キーを押します。
- f. httpd サービスを再起動します。  

```

service httpd restart

```
5. (オプション) セキュアな LDAP を設定します。
- a. LDAPS をサーバから CER のファイルに SSL 証明書情報を保存します。  
 たとえば、証明書プロパティを表示し、**[名前を付けて保存]** または **[エクスポート]** をクリックして CER ファイルを作成します。
  - b. システムから Workload Optimization Manager アプライアンスに .CER ファイルを転送します。  
 たとえば、デフォルト証明書 (root/vmturbo) を持つ SCP (secure copy) コマンドを使用して、CER ファイルを Workload Optimization Manager インスタンスの /tmp ディレクトリにコピーします。
  - c. Workload Optimization Manager インスタンスで、.CER ファイルを /anchors ディレクトリにコピーします。  
 たとえば rootca.cer、ファイルを /usr/share/pki/ca-trust-source/anchors/ ディレクトリにコピーします。
  - d. ルートとして update-ca-trust コマンドを実行します。  
 これは自動的に内蔵 cacerts jks を更新し、追加オプションの必要なく、curl で使用される適切な場所に証明書を置きます。
  - e. Tomcat サービスを再起動します。  

```

service tomcat restart

```

## (オプション) データベース ディスク使用量の電子メール通知を構成する

データベースがダウンしたとき、またはストレージの使用率が80%を超えたときに電子メールで通知するように、Workload Optimization Manager を構成できます。この通知を構成するには、最初に構成を初期化するスクリプトを実行します。次に、ディスク消費量の定期的なチェックを設定するために、Workload Optimization Manager がサーバー上で提供するスクリプトを実行する cron ジョブを設定します。

この通知のワンタイム構成を実行するには、次のようにします。

1. 通知スクリプトの1つを実行します。  
 構成を初期化するには、提供されているスクリプトのいずれかを実行できます。それから、次のコマンドのいずれかを実行します。
  - /srv/tomcat/script/appliance/turbo\_check\_db.sh
  - /srv/tomcat/script/appliance/turbo\_check\_disk.sh
2. スクリプトでプロンプトが表示されたら、情報を入力します。  
 スクリプトは次のプロンプトを表示します。

```

[root@turbonomic appliance] ./turbo_check_db.sh
Configuration file does not exist.
Creating default configuration file.

```



```

Database name (Default: vmtdb):
Database user (Default: root):
Database password:
Database port (Default: 3306):
Email address to send notifications to:

```

通知を受信する電子メールアドレスを入力します。

スクリプトを実行すると、指定した設定を保存する構成ファイルが作成されます。

30分ごとに実行される定期チェックを設定するには、**crontab** ファイルに次の行を追加します。

```

*/30 * * * * /srv/tomcat/script/appliance/turbo_check_db.sh >/dev/null 2>&1
*/30 * * * * /srv/tomcat/script/appliance/turbo_check_disk.sh >/dev/null 2>&1

```

**cron** ジョブを設定した後、データベースがダウンした場合、またはディスク使用量が 80% を超えた場合、スクリプトは初期構成で指定した受信者に電子メールアラートを送信します。さらに、スクリプトはアラートをログファイルに書き込みます。/var/log/tomcat/monitor.log



# ライセンスのインストールおよび初回ログイン

開始する前に、別の電子メールで送信されたフルライセンス キー ファイルまたはトライアル ライセンス キー ファイルがあることを確認してください。Workload Optimization Manager のインストールにアップロードできるように、ライセンスファイルをローカルマシンに保存します。

Workload Optimization Manager を初めて使用するには、以下のステップを実行します。

1. インストールされている Workload Optimization Manager インスタンスの IP アドレスを Web ブラウザに入力して接続します。
2. Workload Optimization Manager へログインします。
  - **USERNAME** administrator のデフォルトのクレデンシャルを使用します。
  - **PASSWORD** のパスワードを入力します。
  - パスワードをもう一度入力して、**REPEAT PASSWORD**を確認します。
  - **【構成 (CONFIGURE)】** をクリックします。
3. 使用状況データと分析を有効にするかどうかを決定します。  
**【はい (AGREE)】** または **【いいえ (No)】** をクリックします。  
この設定は後でいつでも変更できます。詳細については、『*Workload Optimization Manager ユーザガイド*』の「管理タスク」を参照してください。
4. Workload Optimization Manager のインストールのセットアップを続行します。  
**【開始 (LET'S GO)】** をクリックします。
5. **【ライセンスの入力】** スライドアウトを開きます。  
**【ライセンスのインポート (IMPORT LICENSE)】** をクリックします。
6. ライセンス キー ファイルをアップロードします。
  - a. **【ライセンスの入力】** スライドアウトで、次の方法のいずれかを使用してライセンスをアップロードすることができます。
    - **【ライセンスの入力 (Enter License)】** スライドアウトにライセンス キーのファイルをドラッグします。
    - ライセンス キー ファイルを参照します。  
.xml or .lic ファイルのみをアップロードしてください。
  - b. **【保存 (SAVE)】** をクリックします。

## WorkOptimization Manager License ライセンスをアップグレードする

ライセンスを購入してトライアルバージョンからフルバージョンにアップグレードする場合、またはライセンスを購入してインストールにより多くのワークロード容量を追加する場合、電子メールメッセージで新しいライセンスが表示されます。Workload Optimization Manager のインストールにアップロードできるように、ライセンスファイルをローカルマシンに保存します。

ライセンスをインストールするには、次の手順を実行します。

1. ライセンス設定ページに移動します。  
[設定 (Settings)] > [ライセンス (License)] を選択します。
2. [ライセンスの入力] スライドアウトを開きます。  
[ライセンスのインポート (IMPORT LICENSE)] をクリックします。
3. ライセンス キー ファイルをアップロードします。
  - a. [ライセンスの入力] スライドアウトで、次の方法のいずれかを使用してライセンスをアップロードすることができます。
    - [ライセンスの入力 (Enter License)] スライドアウトにライセンス キーのファイルをドラッグします。
    - ライセンス キー ファイルを参照します。  
.xml or .lic ファイルのみをアップロードしてください。
  - b. [保存 (SAVE)] をクリックします。

新しいライセンスをインストールすると、追加のワークロードの容量が自動的に使用可能になります。



# シングルサインオン認証

会社のポリシーがシングルサインオン (SSO) 認証をサポートしている場合、Workload Optimization Manager によりセキュリティアサーションマークアップ言語 (SAML) 2.0 を使用して、SSO 認証を有効にします。

高レベルでは、プロセスが含まれます。

- 複数の外部グループまたは SSO に最低でも 1 個の外部グループを作成します。『*Workload Optimization Manager ユーザーガイド*』の「ユーザーアカウントの管理」を参照してください。
- Workload Optimization Manager を設定して SAML ID プロバイダ (IdP) に接続します。[「シングルサインオンの構成」\(28 ページ\)](#) を参照してください。

SSO が有効になっているときに、SSO クレデンシャルを使用して Workload Optimization Manager インスタンスにログインします。ログインにローカルまたは Active Directory (AD) クレデンシャルを使用しないでください。ID プロバイダ (IdP) により認証が実行されます。

## 注:

SSO を有効にすると、Workload Optimization Manager は設定した IdP から認証のみを承認します。Workload Optimization Manager REST API 経由のリモート要求では SSO を使用しないでください。

エンドユーザー認証に Workload Optimization Manager REST API と SSO を同時に使用する場合は、SSO を構成するときに SAML\_ENABLE ポリシーを設定することで実行できます ([「シングルサインオンの構成 \(28 ページ\)」](#) を参照)。[SAML\\_ENABLE](#) ポリシーを設定すると、アプリケーションへのエンドユーザー認証が IdP に委任され、ローカルで定義されたユーザーの監査済みクラスが RESTAPI 統合で使用できるようになります。

もう 1 つの選択肢は、SAML\_ONLY セキュリティ ポリシーです。SAML\_ONLY ポリシーを設定すると、すべての認証が IdP に委任されます。セキュリティ上の理由から、SAML\_ONLY ポリシーが構成されている場合、RESTAPI 要求は実行されません。

## 前提条件

開始する前に、IdP が SSO 用に設定されていることを確認してください。独自仕様または公開 IdP を使用できます。パブリック Okta IdP の設定例については、[「IdP の一般的な設定とは？」\(44 ページ\)](#) を参照してください。

## シングルサインオンの設定

シングルサインオンを設定するには、これらの手順を実行します。

1. (必須) 複数の外部グループまたは SSO に最低でも 1 個の外部グループを作成します。

**重要事項：**

SSO が有効になっている場合、Workload Optimization Manager は SSO IdP を介したログインのみを許可します。Workload Optimization Manager のインストールに移動するたびに、ユーザーは認証のために SSO ID プロバイダー (IdP) にリダイレクトされてから、Workload Optimization Manager のユーザーインターフェイスが表示されます。

Workload Optimization Manager のインストールで SSO を有効にする前に、Workload Optimization Manager の管理者権限を持つ SSO ユーザーを少なくとも 1 人設定する必要があります。そうしないと、SSO を有効にした後、Workload Optimization Manager で SSO ユーザーを設定できなくなります。管理者として SSO ユーザーを認証するには、**外部認証**を使用して次のいずれかを実行します。

- 管理者承認を持つ 1 人の SSO ユーザーを設定します。  
外部ユーザーを追加します。ユーザー名は、IdP で管理されているアカウントと一致する必要があります。
- 管理者承認を持つ SSO ユーザー グループを設定します。  
外部グループを追加します。グループ名は IdP でユーザー グループと一致する必要があり、そのグループは少なくとも 1 人のメンバーが必須です。

SSO への複数の外部グループまたは外部ユーザーの作成については、『*Workload Optimization Manager ユーザー ガイド*』の「ユーザー アカウントの管理」を参照してください。

2. (必須) NTP サーバーが構成されており、Workload Optimization Manager インスタンスのシステム時刻が正しいことを確認してください。

手順については、[\(ベスト プラクティス\) 時刻の同期 \(18 ページ\)](#) を参照してください。

3. Workload Optimization Manager インスタンスへの SSH ターミナル セッションを開きます。
4. IdP からメタデータをダウンロードします。
5. メタデータを調べます。

メタデータを、[「IdP メタデータの例」 \(30 ページ\)](#) で提供されているサンプルと比較します。

メタデータに例に記載されていないオプションの属性タグが含まれている場合、それらはサポートされていないため、これらのオプションの属性タグを削除する必要があります。

6. Saml.xml ファイルに IdP メタデータのインポートします。
  - a. saml.xml ファイルを作成します。  

```
vi /srv/tomcat/data/config/saml.xml
```
  - b. /srv/tomcat/data/config/saml.xml ファイルに IdP メタデータのインポートします。
  - c. ファイルを保存します。
7. Tomcat 設定ファイルを変更します。
  - a. Tomcat 設定ファイルを開きます。  

```
vi /etc/tomcat/tomcat.conf
```
  - b. CATALINA\_OPTS 変数を設定します。  
次のいずれかを選択します。
    - SAML\_ONLY：SAML 認証のみを許可します。Workload Optimization Manager REST API 統合はサポートされていません。
    - SAML\_ENABLE：SAML 認証を許可し、Workload Optimization Manager REST API 統合（ローカルおよび LDAP 認証）をサポートします。

次に例を示します。CATALINA\_OPTS="-Dadmin.policy.localusers=SAML\_ONLY"

- c. ファイルを保存します。
8. プロパティ ファイルをコピーします。  

```
cp /srv/tomcat/data/config/saml.template.properties /srv/tomcat/data/config/saml.properties
```
9. プロパティ ファイルを変更します。
  - a. Saml.properties ファイルを開きます。  

```
vi /srv/tomcat/data/config/saml.properties
```
  - b. IDP.entityId プロパティを IdP のオーディエンス制限プロパティと同じ値に設定します。  
次に例を示します。IDP.entityId=urn:test:turbo:markharm



```

KoZIHvcNAQkBFglpbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAE
ugxQGqHAXpjVQZwsO9n8l8bFCoEevH3AZbz7568XuQm6MK6h7/O9wB4C5oUYddemt5t2Kc8GRhf3
BDXX5MVZ8G9AUpG1MSqe1CLV2J96rMnwMIJsKerXR01LYxv/J4kjktpOC389wmcy2fE4RbPoJne
P4u2b32c2/V7xsJ7UEjPPSD4i8l2QG6qsUkx3AyNsjo89PekMfm+Iu/dFKXkdjwXZXPxaL0HrNW
PTpzek8NS5M5rvF8yaD+eElzS0I/HicHbPOVvLal0JZYn/f4bp0XJkxZJz6jF5DvBkwIs8/Lz5GK
nn4XW9Cqjk3equSCJPo5o1Msj8vlLrJYVarqhwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC26kYe
LgqjIkF5rvxB2QzTgcd0LVzX0uiVVTZr8Sh5714jJqbDoIgvaQQRxRSQzD/X+hcmhuwdp9s8zPHS
JagtUJXiywNtrzbF6M7ltrWB9sdNrqc99dlgOVRr0Kt5pLTLale5kkq7dRaQoOIVIJhX9wgynaAK
HF/SL3mHUytjXggs88AAQa8JH9hEpwG2srN8EsizX6xwQ/p92hM2oLvK5CSMwTx4VBuGod70EOwp
6TalURLQh6jCCOCWRuZbbz2T3/sOX+sibC4rLlIlfyTkcUopF/bTSdWwknORskK4dBekFcvN9N+C
p/qaHYcQd6i2vyor888DLHDPXhSKWhpG
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://dev-771202.oktapreview.com/app/ibmdev771202_turbo2_1/exkexl6xc9MhzqiC30h7/sso/sam
1"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="htt
ps://dev-771202.oktapreview.com/
app/ibmdev771202_turbo2_1/exkexl6xc9MhzqiC30h7/sso/saml"/>
</md:IDPSSODescriptor>
</md:EntityDescriptor>

```

## シングル サインオンの無効化

いずれかの理由で SSO を使用今後使用しない場合、Workload Optimization Manager インストールで無効にできます。シングルサインオンを無効にするには、これらの手順を実行します。

- Workload Optimization Manager インスタンスへの SSH ターミナルセッションを開きます。
- CATALINA\_OPTS 変数を無効にする Tomcat 設定ファイルを変更します。
  - Tomcat 設定ファイルを開きます。
 

```
vi /etc/tomcat/tomcat.conf
```
  - コメント文字を挿入または CATALINA\_OPTS 変数の行を削除します。
 

次に例を示します。# CATALINA\_OPTS="-Dadmin.policy.localusers=SAML\_ONLY"
  - ファイルを保存します。
- ローカル マシンの Tomcat 設定ディレクトリに移動します。
 

ディレクトリは、次のとおりです。/srv/tomcat/data/config
- Tomcat 設定ディレクトリからファイルを削除します。
 

次を削除します。

  - メタデータ ファイル：/srv/tomcat/data/config/saml.xml
  - SAML 構成ファイル：/srv/tomcat/data/config/saml-security.xml
  - SAML プロパティ ファイル：/srv/tomcat/data/config/saml.properties
- Tomcat サービスを再起動します。
 

```
service tomcat restart
```

6. 設定が正しいことを確認します。
  - a. Workload Optimization Manager のユーザー インターフェイスに移動します。

認証のため、IdP にはリダイレクトされません。デフォルトの Workload Optimization Manager ログイン画面にリダイレクトされます。
  - b. ローカルのアカウントまたはアクティブ ディレクトリ (AD) アカウントでログインします。

## シングル ログアウトのサポート

SSO 機能を使用している場合、Workload Optimization Manager セキュリティ アサーション マークアップ 言語 (SAML) 2.0 によって提供されるシングル ログアウト機能をサポートしています。SSO が有効になっている Workload Optimization Manager セッションで **[ログアウト (Logout)]** をクリックする時、SAML 2.0 シングル ログアウト機能では Workload Optimization Manager セッション、ブラウザ セッション、Id プロバイダー (IdP) セッション、同じ IdP セッションに接続されている他のサービス プロバイダー (SP) のセッションを終了します。

この機能を使用する場合は、セキュリティ管理者に問い合わせて設定してください。

要件は次のとおりです。

- Single Logout 設定を IdP で有効にする必要があります。
- IdP では Workload Optimization Manager SAML キー ストアの証明書を信頼する必要があります。

IdP を有効にしていない、またはシングル ログアウトをサポートしない場合、IdP から手動でログアウトし、Workload Optimization Manager から完全にログアウトする必要があります。

**[ログアウト (Logout)]** をクリックせずにブラウザを閉じる場合や、ブラウザセッションがタイムアウトする場合、Workload Optimization Manager または IDP セッションが有効であるならば再びログインすることができます。





# Workload Optimization Manager の新しいバージョンの更新

当社は Workload Optimization Manager のすべての側面を革新し改善するよう引き続き取り組んでいきます。これは、Workload Optimization Manager の新しいバージョンを定期的にリリースすることを意味します。新しいバージョンが使用可能かどうかを定期的に確認する必要があります。

新しいバージョンが利用可能になったら、新しいバージョンをインストールするだけでなく、既存のインストールされたサーバを適切に更新することも重要です。最初に Workload Optimization Manager をインストールしたとき、高度なデータ収集と分析プロセスを行うことができます。インストールの内部には、仮想環境全体のパフォーマンス データを保持する統合データベースが存在します。Workload Optimization Manager は、右サイジング、傾向予測、その他の分析を行うこの履歴データを使用します。つまり、Workload Optimization Manager にとってデータベースは重要であり、時間の経過とともにより重要になっていきます。Workload Optimization Manager のインストールを適切に更新すると、データベースを継続して使用できるようになります。

Workload Optimization Manager インストールを更新するには：

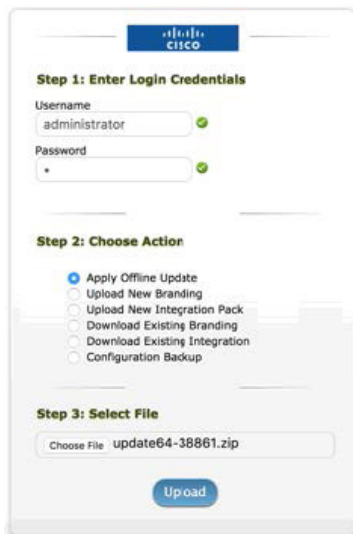
1. Workload Optimization Manager VM に十分なディスク容量があるかどうかを確認します。  
サーバのディスク容量使用状況を確認するには、SSH を Workload Optimization Manager インスタンスに root として実行します（デフォルトのパスワードは vmturbo です）。次のコマンドを発行します。df -kh  
更新を実行するには、少なくとも 5 GB のディスク空き領域が必要です。必要な量はデータベースのサイズによって異なり、データベースを完全にコピーするため、データベースのパーティションに十分な領域が必要です。たとえば、大規模な環境と大規模なデータベースがある場合、必要な容量の適切な概算は 15 GB です。
2. 現在の Workload Optimization Manager VM のスナップショットを保存します。  
更新する前に、Workload Optimization Manager VM を適切にシャットダウン（電源オフではない）し、スナップショットを実行する必要があります（または VM のクローン）。これにより、更新中に問題が発生した場合に、信頼性の高い復元ポイントが確保できます。スナップショットを作成したら、VM をオンラインに戻します。
3. オフライン インストールパッケージをダウンロードします。  
<http://www.cisco.com> に移動して、Workload Optimization Manager の最新の更新パッケージを見つけます。ローカルマシンにパッケージをダウンロードします。戻ることができる場所にダウンロードを保存します。
4. Workload Optimization Manager の更新ページが開かれます。  
次の URL から、Workload Optimization Manager の [更新 (Update)] ページに移動できます。  
[https://YOUR\\_WOM\\_URL\\_or\\_IP/update.html](https://YOUR_WOM_URL_or_IP/update.html).たとえば、アドレスから Workload Optimization Manager を表示する場合は、10.10.222.333ブラウザを <https://10.10.222.333/update.html>. に移動します。
5. [更新] ページにログインします。



デフォルトの Workload Optimization Manager 管理者アカウントにクレデンシャルを割り当てます。

- ユーザー：administrator
- パスワード：このアカウントに設定したパスワード

6. 更新パッケージをアップロードして、オフライン更新を適用します。



- [オフライン更新を適用する (Apply Offline Update)] アクションを選択します
- 適用する更新パッケージを選択します  
[ファイルの選択] をクリックして、ローカルマシンに保存した更新パッケージを参照します。
- [アップロード (Upload)] をクリックして、更新パッケージを適用します

7. ブラウザのデータを消去し、ブラウザを更新してください。

クラシック UI を使用する場合は、フラッシュ キャッシュも消去する必要があります。詳細については、[ローカル Adobe Flash キャッシュをクリアする必要があるケースは？ \(41 ページ\)](#) を参照してください。

ブラウザのデータを消去してブラウザを更新すると、Workload Optimization Manager の機能に完全にアクセスできるようになります。ただし、現在の分析データに依存する機能は、完全なマーケット サイクル（通常は 10 分）が経過するまで利用できません。たとえば、保留中のアクションのリストには、完全なマーケット サイクルが終了するまでアクションは表示されません。

8. 新しいバージョンを確認してください。

[設定 (Settings)] > [更新 (Updates)] に移動し、[バージョン情報 (About)] をクリックします。

9. (オプション) リモート クライアント接続を許可します。

手順については、[を参照してください。](#)

**リンクが切れています! (オプション) リモートの MariaDB 接続をインスタンスに設定します。**

10. 他のユーザーに、ブラウザ データを消去し、Workload Optimization Manager ブラウザ セッションを更新するように通知します。

他のユーザーがクラシック UI を使用している場合は、フラッシュ キャッシュも消去する必要があります。詳細については、[ローカル Adobe Flash キャッシュをクリアする必要があるケースは？ \(41 ページ\)](#) を参照してください。

**重要事項：**

ソフトウェアの更新が完了し、Workload Optimization Manager のユーザー インターフェイスがブラウザで更新されるまで、Workload Optimization Manager VM を再起動しないでください。更新が完了しないと思われる場合、シスコ サポート 担当者にご連絡ください。

Workload Optimization Manager は、更新を段階的に適用します。ソフトウェアは、特定の構成ファイルとともにすぐに更新します。更新プロセスにより Workload Optimization Manager サーバをできるだけ早く再起動します。

一部のバージョンでは、更新によりデータベースの再構築を行う必要があります。これはお客様の環境とデータベースのサイズによって、時間のかかる可能性があります。クイック サーバ再起動を有効にするため、サーバの実行中に、更新によりバックグラウンドでこの再構成を実行します。Workload Optimization Manager は環境内の管理されますが、履歴データへのアクセスが完了できない可能性があります。たとえば、データベースの再構築が完了するまでレポートを表示することができません。



# RHEL プラットフォームへのインストールと更新

Cisco delivers a server tha象 Vx86アーキテクチャの VM にインストールされた RedHat Linux (RHEL) 7.xプラットフォーム上のこれは、管理ポリシーで RHEL が必要な環境をサポートするためです。

## 注:

Workload Optimization Manager のもっとも一般的な配信は、CentOS を OS として実行する x86 アーキテクチャを使用する VM 上にあります。CentOS の配信には、必要なすべてのコンポーネントが含まれています。CentOS プラットフォームへのアップグレードが必要になった場合、シスコはプラットフォームの更新を含む新しい配信をリリースします。このセクションでは、RHEL を実行している VM でのあまり一般的でない展開について説明します。RHEL プラットフォームの場合、プラットフォームを最新の状態に保つ責任があります。

## RHEL の要件およびセットアップ

新規インストールを実行する場合でも、既存の Workload Optimization Managerインストールを更新する場合でも、プラットフォームが最新であることを確認する必要があります。

さらに、実行する Workload Optimization Manager のバージョンに対応する openJDK バージョンを実行する必要があります。現在の Workload Optimization Manager バージョンには、openJDK1.8 が必要です。

シスコは、RHELVm に対して次のセットアップの推奨事項を作成します。

- VMには4つのvCPUと32GBのRAMが必要です。
- OSカーネルのブートパーティションを作成して、500MBにする必要があります。
- VMストレージ要件は500GB以上です。ストレージ要件によってシンプロビジョニング可能です。
- 次の目的でLVMボリュームを作成する必要があります。
  - パーティションスキームに関するRedHatの推奨事項に従ったスワップパーティション。
  - スワップパーティションのサイズは、割り当てられたRAMサイズと一致する必要があります (たとえば、32GBのRAMと32GBのスワップパーティション)
  - /var/log/ に保存するシステムログ用に30GB
  - /tmp/ のシステム一時ストレージ用に20GB
  - ルートパーティション (/) への製品インストール用に50GB
  - 残りのスペース (約380GB) を /var/lib/mysql のデータベースに使用します。

さらに、VMは次の前提条件を満たしている必要があります。

- OSプラットフォームはRHEL7.xです。
- ファイアウォールは、ポート80および443での接続を許可するように構成されています。
- unzipユーティリティをインストールする必要があります。
- VMの名前にアンダースコア文字は含まれていません。ホスト名を変更できない場合、[「ホスト名の制限を回避するには？」 \(43ページ\)](#)で説明されている回避策を使用できます。

- 次の DejaVu フォントがインストールされています。

- dejavu-fonts-common
- dejavu-sans-fonts
- dejavu-sans-mono-fonts
- dejavu-serif-fonts

フォントを確認するには、次のコマンドを使用します。

```
rpm -qa | grep dejavu
```

DejaVu フォントがインストールされていない場合は、[「フォントを追加してRHELプラットフォームのレポートを有効にする方法」 \(42ページ\) の手順を実行します。](#)

(オプション) RHEL プラットフォームが SELinux を使用している場合は、以下が設定されていることを確認してください。

- Apache と Tomcat 間の通信を許可するように SELinux を構成します。

1. /etc/selinux/config ファイルを編集します。ファイルで SELINUX=permissive、を検索して SELINUX=enforcing に設定します。

2. RHEL オペレーティングシステムを再起動します。

```
systemctl reboot
```

3. Apache と Tomcat 間の通信を有効にします。

次のコマンドを実行します。

```
setsebool -P httpd_can_network_connect=1
```

- policycoreutils-python-2.2.5-11.el7\_0.1.x86\_64 パッケージをインストールします。

次のコマンドを実行します。

```
yum provides /usr/sbin/semanage
```

```
yum install policycoreutils-python
```

## ブラウザ要件

Workload Optimization Manager は、最も一般的に使用されている Web ブラウザ (Internet Explorer、Mozilla Firefox、Google Chrome、Apple Safari など) で動作します。

Web ブラウザは、JavaScript が有効になっている必要があります。

さらに、Workload Optimization Manager のユーザー インターフェイスに使用するブラウザは、Workload Optimization Manager インスタンスと 1 分以内に同期する必要があります。この同期を行わないと、Workload Optimization Manager に不正なメトリック値が表示される可能性があります。

また、Workload Optimization Manager のユーザー インターフェイスに GoogleChrome を使用している場合、レポートを表示するには、レポートをダウンロードする前に Chrome プレビュー モードをオフにする必要があります。

## RHEL VM へのインストール

Workload Optimization Manager の RHEL 展開を作成するには、RHEL 7.x を実行する VM を作成し、Workload Optimization Manager の更新をダウンロードして、必要なコンポーネントをインストールします。さらに、VM のディレクトリ構造を変更し、データベース構成ファイルを変更して、必要なサービスを起動する必要があります。

1. RHEL7.x オペレーティングシステムを実行する VM を作成します。

2. Workload Optimization Manager 製品を RHELVM にインストールします。

オフライン更新を構成して、Workload Optimization Manager の初期バージョンをインストールできます。

- a. Workload Optimization Manager の更新パッケージについては、シスコの担当者にお問い合わせください。

- b. パッケージを RHEL サーバー上の /tmp ディレクトリに保存します。

- c. 必要なオフライン更新バージョンを特定したら、root 権限を持つ shell を開き、次のコマンドを実行します。<cwom\_update\_package\_name.zip> は、オフライン更新パッケージの名前です。

```
cd /tmp
unzip <cwom_update_package_name.zip>
cp /tmp/cisco_temp.repo /etc/yum.repos.d/
```

3. その他の必要なコンポーネントをインストールします。

コンポーネントをインストールするには、この順番で次のコマンドを実行します。

a. apache/mod\_ssl

```
yum install mod_ssl
```

b. Java ランタイム環境

インストールしている **Workload Optimization Manager** のバージョンと一致する JRE バージョンをインストールする必要があります。この例は、JRE1.8 のインストールを示しています。

```
yum install java-1.8.0-openjdk
update-alternatives --config java
```

コマンドで、インストールしたばかりのバージョンに対応する Java のバージョンを選択します（「[RHEL とセットアップの要件](#)」（36 ページ）を参照）。

c. Workload Optimization Manager バンドル

```
yum install cwom-bundle --nogpgcheck
```

4. 正しいファイル構造を設定します。

次のコマンドを実行して、必要なディレクトリ構造を設定します。

```
ln -s /srv/www/htdocs /srv/www/html
rmdir /var/www/cgi-bin
rmdir /var/www/html
ln -s /srv/www/cgi-bin /var/www/cgi-bin
ln -s /srv/www/htdocs /var/www/html
rm -rf /var/lib/tomcat6/ /var/lib/tomcat/
ln -s /srv/tomcat6/ /var/lib/
ln -s /srv/tomcat/ /var/lib/
mkdir -p /var/lib/mysql/tmp
chown mysql:mysql /var/lib/mysql/tmp
mkdir /var/lib/wwwrun
chown -R apache.apache /var/lib/wwwrun
```

5. Workload Optimization Manager バンドルにインストールされたデータベースを初期化します。

次のコマンドを実行します。

```
cd /srv/rails/webapps/persistence/db/
./initialize_all.sh
```

6. 関連するサービスを開始します。

VM を再起動するか、次のコマンドを実行してサービスを開始できます。

```
service tomcat start
service httpd start
```

7. VM と VM をホストする物理マシンの間で時刻が同期されていることを確認します。

NTP サービスが実行されていることを確認します。

VMware vSphere によって管理されているホストの場合、VM の **[ゲスト時間とホストの同期 (Synchronize Guest Time With Host)]** オプションを無効にします。この設定は、**[オプション (Options)] > [VMware ツール (VMware Tools)] > [詳細 (Advanced)]** にあります。

8. /cgi-bin ディレクトリのコンテキストを変更して、cgi スクリプトの実行を有効にします。

次のコマンドを実行します。

```
semanage fcontext -a -t httpd_sys_script_exec_t "/srv/www/cgi-bin(/.*)?"
restorecon -Rv /srv/www/cgi-bin/
```

9. http と https を firewalld に追加して、http(s) 通信を有効にします。  
次のコマンドを実行します。

- a. /etc/firewalld/zones/public.xml ファイルを編集します。  
パブリックゾーン セクションの設定を変更します。次に例を示します。

```
<zone>
<short>Public </short>
<description>For use in public areas. You do not trust the other
computers on networks to not harm your computer. Only selected
incoming connections are accepted. </description>
<service name="dhcpv6-client"/>
<service name="ssh"/>
<service name="http"/>
<service name="https"/>
</zone>
```

- b. Firewalld をリロードします。  
firewall-cmd --complete-reload

- c. firewalld サービスを再起動します。  
systemctl restart firewalld

10. (オプション) リモート MariaDB クライアント接続を許可します。

- a. bind-addr 構成ファイルを開きます。  
たとえば vi /etc/my.cnf.d/bind-addr.cnf、コマンドを使用します。
- b. bind\_address パラメーターを Workload Optimization Manager インスタンスの IP アドレスに設定します。  
次に例を示します。bind\_address=10.10.10.123
- c. ファイルを保存します。
- d. MariaDB サービスを再起動します。  
systemctl restart mariadb コマンドを実行します。

**注:**

リモート MariaDB クライアント接続を許可する場合は、必ず /etc/firewalld/zones/public.xml ファイルに行  
<service name="mysql"/> を追加してください。

11. (オプション) SSO 認証を設定します。手順については、[「シングルサインオン認証」 \(28 ページ\)](#) を参照してください。

## 既存のRHEL 展開の更新

RHEL プラットフォームに Workload Optimization Manager を展開した後、新しいバージョンの Workload Optimization Manager が利用可能になったら、そのインストールを更新できます。

**注:**

DejaVu フォントがインストールされており、JDK バージョンが新しい Workload Optimization Manager バージョンと互換性があることを確認する必要があります。詳細については、[「RHELとセットアップの要件」 \(36 ページ\)](#) を参照してください。

# オフライン更新

以下の手順を実行します。

1. 新しいオフライン成果物をダウンロードして、/tmp ディレクトリに解凍します。<cwom\_update\_package\_name.zip> は、オフライン更新パッケージの名前です。

```
rm -rf /tmp/cisco
cd /tmp
unzip <cwom_update_package_name.zip>
```

2. これらのコマンドを実行して、インストールされているコンポーネントを更新します。

```
yum clean all
cd /tmp/cisco
yum -y localupdate x86_64/* i586/* | tee /var/lib/wwrun/manual_cisco_update.txt
```

3. ブラウザのデータを消去し、ブラウザを更新してください。

クラシック UI を使用する場合は、フラッシュ キャッシュも消去する必要があります。詳細については、[ローカル Adobe Flash キャッシュをクリアする必要があるケースは？ \(41 ページ\)](#) を参照してください。

ブラウザのデータを消去してブラウザを更新すると、Workload Optimization Manager の機能に完全にアクセスできるようになります。ただし、現在の分析データに依存する機能は、完全なマーケット サイクル（通常は10分）が経過するまで利用できません。たとえば、保留中のアクションのリストには、完全なマーケット サイクルが終了するまでアクションは表示されません。

4. バージョンを確認してください。

[設定 (Settings) ] > [更新 (Updates) ] に移動し、[バージョン情報 (About) ] をクリックします。

5. (オプション) リモート MariaDB クライアント接続を許可します。

- a. bind-addr 構成ファイルを開きます。

たとえば vi /etc/my.cnf.d/bind-addr.cnf、コマンドを使用します。

- b. bind\_address パラメーターを Workload Optimization Manager インスタンスの IP アドレスに設定します。

例: bind\_address=10.10.10.123

- c. ファイルを保存します。

- d. MariaDB サービスを再起動します。

systemctl restart mariadb コマンドを実行します。

6. 他のユーザーに、ブラウザ データを消去し、Workload Optimization Manager ブラウザ セッションを更新するように通知します。

他のユーザーがクラシック UI を使用している場合は、フラッシュ キャッシュも消去する必要があります。詳細については、[ローカル Adobe Flash キャッシュをクリアする必要があるケースは？ \(41 ページ\)](#) を参照してください。





## FAQ

Workload Optimization Manager でもっとも価値ある経験を得るため、もっともユーザーが経験しているインストールの問題を収集しました。詳細について質問があれば、Workload Optimization Manager テクニカル サポートに連絡します。

### Workload Optimization Manager クライアントを実行するために特別なソフトウェアが必要ですか？

クラシック UI を使用する場合、ブラウザに最新の Flash プラグインをインストールしていることを確認します。URL にアクセスすると空白のページに移動する場合、Flash プラグインがインストールされていない可能性があります。

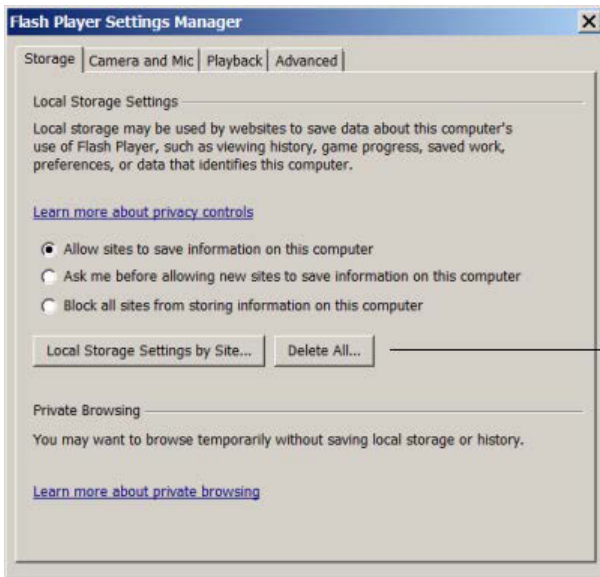
### ローカル Adobe Flash キャッシュをクリアするタイミングは？

Workload Optimization Manager インスタンスを更新した後にクラシック UI を使用する場合、Flash のキャッシュをクリアする必要があります。Flash のキャッシュをクリアすることで、Workload Optimization Manager ユーザー インターフェイスは、ブラウザで完全に更新されます。キャッシュをクリアするには、システムにローカルで Flash 設定を開くか、次の Adobe サイトから設定マネージャにアクセスできます。

[http://www.macromedia.com/support/documentation/en/flashplayer/help/settings\\_manager07.html](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html)

システムでローカル設定マネージャを開くには、次をクリックします。

- Windows : [スタート (Start) ] > [設定 (Settings) ] > [コントロール パネル (Control Panel) ] > [Flash Player]
- Macintosh : [システム設定 (System Preferences) ] > [Flash Player]
- Linux Gnome : [システム (System) ] > [設定 (Preferences) ] > [Adobe Flash Player]
- Linux KDE : [システム設定 (System Settings) ] > [Adobe Flash Player]



Click **Local Storage Settings by Site** to clear just the Operations Manager appliance, or click **Delete All** clear the cache for all sites that have run on your computer.

## Workload Optimization Manager によって作成された推奨事項の一部を実行できないのはなぜですか？

Workload Optimization Manager の推奨を自動化するには、設定ポリシーについての完全な情報に関する『*Workload Optimization Manager ユーザー ガイド*』を確認してください。ポリシーは [設定] > [ポリシー] にあります。

Workload Optimization Manager は、次のアクションモードをサポートしています。

- 無効 — アクションを推奨または実行しません。
- 推奨 — アクションを推奨することで、ユーザーは指定のハイパーバイザを使用するか、他の方法で実行できます。
- 手動 — アクションを推奨しオプションを提供して、ユーザー インターフェイスを介してアクションを実行します。
- 自動 — Workload Optimization Manager によりアクションを自動的に実行します。

一部のアクションはデフォルトで推奨または無効に設定されています。これらのアクションの実行を有効にするには、手動または自動を変更する必要があります。

その他のアクションは、Workload Optimization Manager では実行できません。これらのアクションはオプションとして、無効または推奨のみがあります。

## RHEL プラットフォームのレポートを有効にする フォントを追加するには？

DejaVu フォントがインストールされているかどうかを確認するには、コマンドを使用します。

```
rpm -qa | grep dejavu
```

DejaVu フォントがインストールされていない場合は、次の手順に従います。

1. DejaVu フォントをインストールするには、ルート権限を持つシェルを開き、この YUM コマンドを実行します。

```
yum install -y dejavu-fonts-common dejavu-sans-fonts dejavu-sans-mono-fonts dejavu-serif-fonts
```

2. 新しい設定ファイルを作成します。  
`vi /etc/fonts/local.conf`
3. このコードを `/etc/fonts/local.conf` ファイルにコピーします。

```
<?xml version='1.0'?>
<!DOCTYPE fontconfig SYSTEM 'fonts.dtd'>
<fontconfig>
<alias>
 <family>serif</family>
 <prefer><family>Utopia</family></prefer>
</alias>
<alias>
 <family>sans-serif</family>
 <prefer><family>Utopia</family></prefer>
</alias>
<alias>
 <family>monospace</family>
 <prefer><family>Utopia</family></prefer>
</alias>
<alias>
 <family>dialog</family>
 <prefer><family>Utopia</family></prefer>
</alias>
<alias>
 <family>dialoginput</family>
 <prefer><family>Utopia</family></prefer>
</alias>
</fontconfig>
```

4. ファイルを保存します。

## アンダースコア文字を含むホスト名の制限を回避するには?

デフォルトで、Apache は名前に下線文字があるホスト名をサポートします。Workload Optimization Manager を展開する時、その名にそれらの文字を含まない VM にインストールする必要があります。ホスト名に下線文字を含む場合、ユーザー インターフェイスを開こうとすると Apache は 400 個以上のエラーが返されます。

ホスト名を変更できない場合、Apache 設定ファイルを変更して、回避策としてレガシ動作を有効にできます。これを行うには、次の手順を実行します。

1. デフォルト クレデンシャルを使用して、セキュアなシェルを Workload Optimization Manager マシンで開きます：`root/vmturbo`。
2. Apache 設定ファイルを開きます。  
`vi /etc/httpd/conf/httpd.conf`
3. `HttpProtocolOptions` の安全でない設定を有効にします。
  - a. コマンド文字を削除して、`HttpProtocolOptions` の安全でない設定を有効にします。
  - b. コメント文字を挿入して、`HttpProtocolOptions` の厳密な設定を無効にします。  
次に例を示します。

```
HttpProtocolOptions unsafe
HttpProtocolOptions strict
```

4. ファイルを保存します。
5. httpd サービスを再起動します。

```
service httpd restart
```

## What IdP の一般的な設定とは?

シングルサインオン (SSO) の構成を開始する前に、IdP が SSO 用に設定されていることを確認する必要があります。IdP を設定するときに役立つ可能性のあるパブリック OktaIdP の一般的な設定を次に示します。

| SAML 設定：全般           |                                          |
|----------------------|------------------------------------------|
| 設定                   | 例                                        |
| シングルサインオン URL        | https://10.10.10.123/vmturbo/saml/SSO    |
| 受信者 URL              | https://10.10.10.123/vmturbo/saml/SSO    |
| 宛先 URL               | https://10.10.10.123/vmturbo/saml/SSO    |
| 聴衆の制限                | urn:test:turbo:markharm                  |
| デフォルトのリレー状態          |                                          |
| 名前 ID の形式            | Unspecified                              |
| アプリケーション ユーザー名       | Okta で管理されているアカウントのユーザー名                 |
| 応答                   | Signed                                   |
| アサーション署名             | Signed                                   |
| Signature Algorithm  | RSA_SHA256                               |
| デジタルアルゴリズム           | SHA256                                   |
| アサーションの暗号化           | Unencrypted                              |
| SAML シングル ログアウト      | Enabled                                  |
| シングルログアウト URL        | https://10.10.10.123/vmturbo/rest/logout |
| SP 発行者               | turbo                                    |
| 署名証明書                | Example.cer (CN=apollo)                  |
| authnContextClassRef | PasswordProtectedTransport               |
| オーナー強制認証             | Yes                                      |
| SAML 発行者 ID          | http://www.okta.com/\$ (org.externalKey) |