



HP Agile Manager

ソフトウェア・バージョン: 2.50

インストールおよび管理ガイド

ドキュメント・リリース日: 2016 年 2 月
ソフトウェア・リリース日: 2016 年 2 月

ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

すべてのサードパーティコードは、HPソフトウェアが管理しており、要求に応じて利用可能です。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2012-2016 Hewlett-Packard Development Company, L.P.

商標について

Adobe™は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft®およびWindows®は、米国におけるMicrosoft Corporationの登録商標です。

UNIX®は、The Open Groupの登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに更新されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。

<https://softwaresupport.hp.com>.

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの登録は、次のWebサイトから行なうことができます。<https://softwaresupport.hp.com> にアクセスして [Register] をクリックしてください。

サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。<https://softwaresupport.hp.com>

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、<https://softwaresupport.hp.com>にアクセスし、[Resister]をクリックしてください。

アクセスレベルの詳細については、次のWebサイトをご覧ください。

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HPソフトウェアソリューション、統合、およびベストプラクティス

HP Software Solutions Now (<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710>) サイトでは、HPEソフトウェアカタログに掲載のプロダクト間の連携や統合方法の閲覧、情報の交換、ビジネスニーズを満たすソリューションの検索を行うことができます。

Cross Portfolio Best Practices Library (<https://hpln.hpe.com/group/best-practices-hpsw>) では、さまざまなベストプラクティスドキュメントや資料を閲覧できます。

目次

Agile Manager によるこそ	7
概要	8
システム・アーキテクチャ	9
Agile Manager コンポーネント	9
基本設定の例	11
クラスタ設定の例	11
システム要件	13
最小ハードウェア要件	13
推奨ハードウェア要件	13
追加システム要件	14
Linux の前提条件	17
Linux のディスク容量要件	17
Linux サーバで必要になる権限	17
Oracle の前提条件	19
データベース要件	19
管理ユーザ権限の付与	20
メンテナンス完了後のユーザ権限	23
Oracle RAC サポートの有効化	23
インストールとアップグレード	25
プレインストール・チェックリスト	26
Agile Manager のインストール	27
クラスタ化されたシステムのインストール	38
Agile Manager のアンインストール	39
クラスタ化されたシステムのアップグレード	40
基本的な運用システムのアップグレード	44
ステージング環境を使用した Agile Manager のアップグレード	47
Agile Manager サービスの起動/停止	50
Agile Manager へのログイン	51
システムのセキュリティ保護	52
デプロイメントのセキュリティ保護	53
添付ファイルおよびダウンロードのセキュリティ保護	54

添付ファイルのセキュリティ保護	54
ダウンロードのセキュリティ保護	55
アプリケーション・サーバのセキュリティ保護	55
ネットワークと通信のセキュリティ保護	57
システム管理のセキュリティ保護	59
ユーザ認証のセキュリティ保護	60
ユーザ許可のセキュリティ保護	60
データの整合性	63
データ暗号化	64
データ・ロギング	65
アプリケーション・サーバでの SSL/TLS 設定	66
Apache Web サーバの統合 (例)	70
アプリケーション・サーバの管理	73
パスワードの変更	73
ヒープ・メモリ・サイズの変更	73
アプリケーション・サーバのポート番号の変更	74
データベースのシステム・パスワードの変更	74
システム・スキーマ・パスワードの変更	75
アプリケーション・サーバの管理ツール	76
トラブルシューティング	77
Agile Manager のシステム管理	79
アプリケーション・サーバの設定	80
最大データベース接続数の設定	80
同期負荷の分散	80
アプリケーション・ログ・ファイル	81
データベースの設定	83
サイトのアクティブ化	83
サイト・スキーマ・パスワードの変更	84
サイト・スキーマの復元	84
電子メール通知サーバの設定	85
ユーザ認証の設定	86
LDAP 認証の設定	86
LDAP ユーザ検索の設定	88
ユーザ・ライセンスの更新	89
システム管理者の定義とユーザ・パスワードのリセット	91
システム管理者	91
ユーザ・パスワード	91
一般的なシステム設定	92
詳細パラメータの設定	93
独自に定義できるシステム・パラメータ	94

フィードバックを送信95

Agile Manager によるこそ

Agile Manager は、アジャイル・プロジェクトを編成、計画、実行するためのアジャイル管理ソリューションです。単一のチーム、または複数の場所に分散したチームをエンタープライズ全体でサポートできます。Agile Manager は次のものを提供します。

- 容易なリリースとスプリントの計画、タスク割り当て、チームと個人のキャパシティ管理を可能にするドラッグアンドドロップ・インタフェース
- すべてのチーム・メンバーがプロジェクト全体の概況、作業のフロー、発生する可能性がある問題またはボトルネックをすぐに把握できるタスクとリリースの計画ボード
- 高度にカスタマイズ可能なダッシュボード、メトリック、および KPI を通じた進捗状況に関するリアルタイム・フィードバック(これにより、予測可能性を向上し、管理作業を最小化)
- ソース・コードやビルド情報を集計して、アプリケーション変更に対する意味のある解析情報を提示し、正確なリスク分析および詳細な情報を得た上での意思決定を可能にする、高度な開発分析

概要

このドキュメントでは、オンプレミス Agile Manager システムのコンポーネントとサポートされているアーキテクチャに加えて、アプリケーションのインストール手順、サーバの管理手順、システム管理タスクの実行手順について説明します。

Agile Manager の利用方法の詳細については、アプリケーションの[ヘルプ]メニューからアクセスできる、Agile Manager ヘルプセンターを参照してください。

本ドキュメントの内容

- 「[システム・アーキテクチャ](#)」(9ページ): 基本設定またはクラスタ設定でのシステム・コンポーネントについて説明します。
- 「[Linux の前提条件](#)」(17ページ): Linux アプリケーション・サーバの要件と関連する手順について説明します。
- 「[Oracle の前提条件](#)」(19ページ): Oracle データベース・サーバの要件と関連する手順について説明します。
- 「[インストールとアップグレード](#)」(25ページ): インストール、アップグレード、アンインストールの詳細な手順について説明します。
- 「[Agile Manager サービスの起動/停止](#)」(50ページ): Agile Manager サービスの開始と停止を行うコマンドの一覧を示します。
- 「[Agile Manager へのログイン](#)」(51ページ): インストールを完了してサーバを起動した後の Agile Manager と Agile Manager 管理サイトへのアクセス方法について説明します。
- 「[システムのセキュリティ保護](#)」(52ページ): Agile Manager システムのセキュリティ確保に関するベスト・プラクティスと手順について説明します。
- 「[アプリケーション・サーバの管理](#)」(73ページ): インストール後に実施する Linux サーバ管理のオプション手順について説明します。
- 「[トラブルシューティング](#)」(77ページ): インストール中にエラーが発生した場合にチェックする必要があるログ・ファイルについて説明します。
- 「[Agile Manager のシステム管理](#)」(79ページ): サーバ、ユーザ、およびその他のシステム設定を設定する方法について説明します。

システム・アーキテクチャ

本章では、サポートされている Agile Manager システム・アーキテクチャとシステム・コンポーネントについて説明します。

- [「Agile Manager コンポーネント」\(9ページ\)](#)
- [「基本設定の例」\(11ページ\)](#)
- [「クラスタ設定の例」\(11ページ\)](#)
- [「システム要件」\(13ページ\)](#)

Agile Manager コンポーネント

次の表では、Agile Manager システム・コンポーネントについてまとめています。

コンポーネント	説明
Agile Manager アプリケーション・サーバ	Agile Manager アプリケーションと Web サーバをホストし、Linux プラットフォーム上で実行します。
データベース・サーバ	次の Agile Manager スキーマを格納します。 <ul style="list-style-type: none">• システム管理スキーマ: Agile Manager システムに関連する情報(ユーザ設定やメール通知設定など)を格納します。• サイトスキーマ: ワークスペース、バックログ項目、リリース詳細など、すべてのサイト情報を格納します。 スキーマは Oracle サーバ上に存在します。詳細については、 「Oracle の前提条件」(19ページ) を参照してください。
ファイアウォール	オプション。セキュリティを高めるためには、Web ブラウザ(Agile Manager クライアント)と Agile Manager アプリケーション・サーバの間にファイアウォールを配置します。
LDAP サーバ	オプション。Agile Manager で直接ユーザを作成するのではなく、LDAP システム経由でユーザを認証する場合に使用します。 LDAP の設定は、インストール後に管理サイト経由で行います。詳細については、 「ユーザ認証の設定」(86ページ) を参照してください。
ロード・バランサ	クラスタ設定で使用します。 ロード・バランサを使用する場合、クライアント要求はロード・バランサに送信され、クラスタ内のサーバの可用性に従って分配されます。
メール・サーバ	ユーザにメール通知を送信する際に使用します。

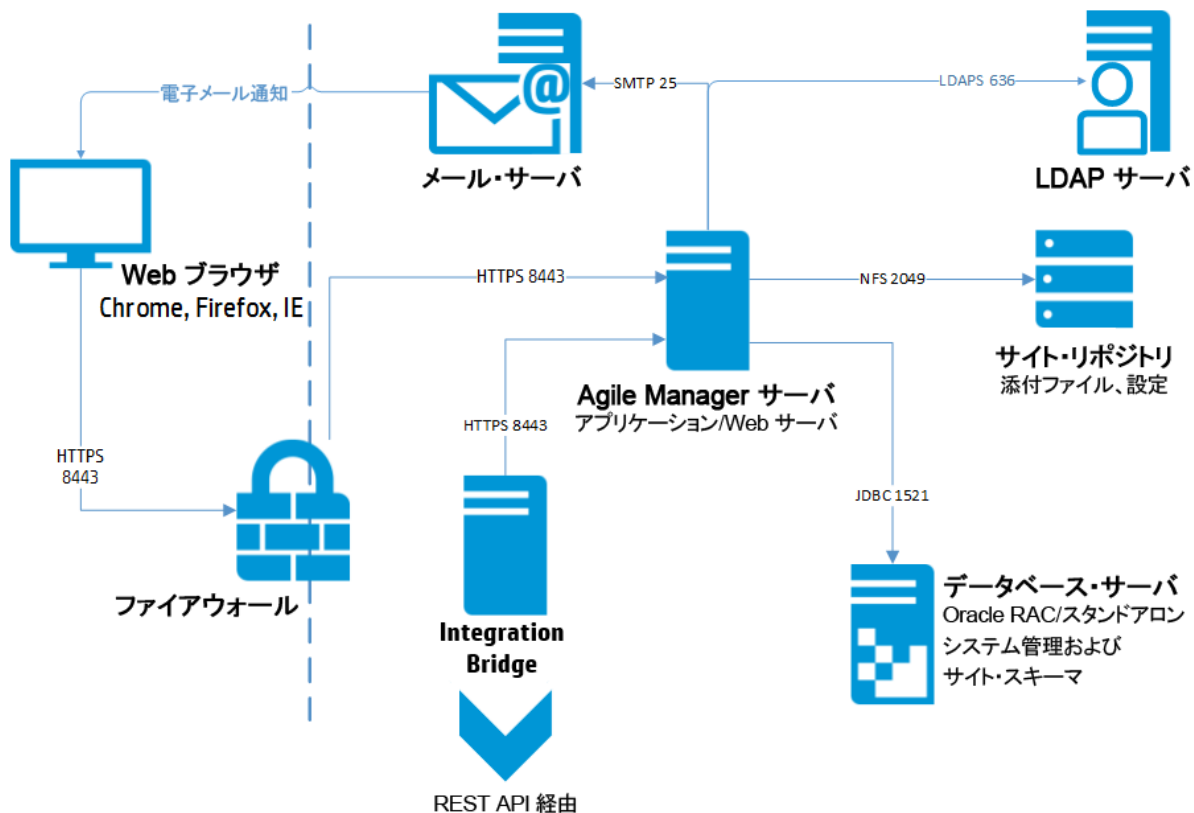
コンポーネント	説明
サイト・リポジトリ	<p>サイト・ファイル(添付など)を格納します。</p> <p>標準設定では、リポジトリはアプリケーション・サーバと同じマシン上にあります。これは小さなセットアップの場合に便利です。</p> <ul style="list-style-type: none">• 大規模な組織の場合, NAS(ネットワーク・アタッチト・ストレージ), SAN(ストレージ・エリア・ネットワーク), または専用マシンなどのストレージ・ソリューションにリポジトリをインストールすることが推奨されます。• クラスタ設定の場合, NAS, SAN, または専用マシンなどのストレージ・ソリューションにリポジトリをインストールすることが必要です。
Integration Bridge	オプション。NextGen Synchronizer で使用します。ALM との通信を OTA API 経由で行います。
Tanuki ラツパ	Agile Manager をインストールして制御できるようにする Java サービス・ラツパ。Agile Manager を監視する高度な障害検出ソフトウェアも含まれています。
Web ブラウザ	Agile Manager Web クライアントでは、Agile Manager のアプリケーションと管理サイトにアクセスできます。

注: システム・パフォーマンスを向上させるには、Agile Manager アプリケーション・オブジェクトとデータベース・サーバを別のマシンにインストールし、LAN ネットワーク経由で接続してください。

基本設定の例

基本的な Agile Manager 設定では、Agile Manager アプリケーション・サーバと Web サーバがインストールで組み込まれ、同じマシンにインストールされます。

次の図に、Agile Manager システムの基本設定を示します。



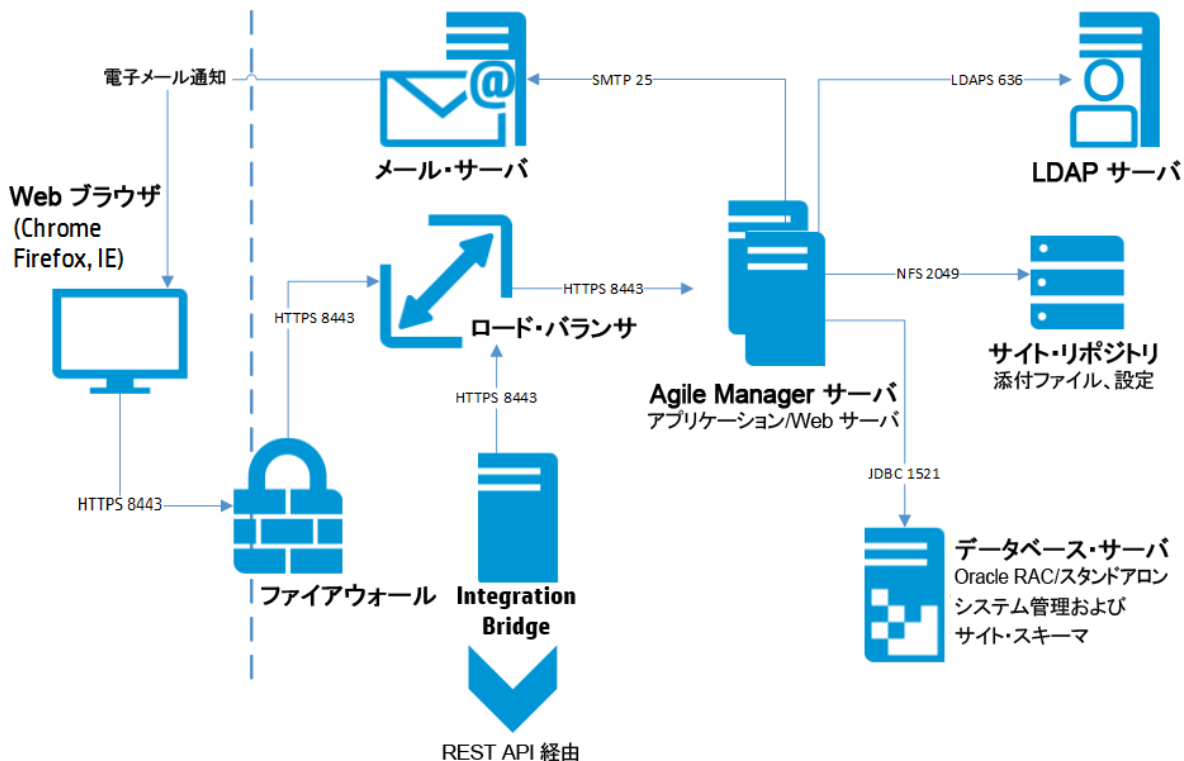
詳細については、「[Agile Manager コンポーネント](#)」(9ページ)および「[Agile Manager のインストール](#)」(27ページ)を参照してください。

クラスタ設定の例

Agile Manager ではクラスタ化がサポートされています。クラスタとはアプリケーション・サーバのグループで、あたかも 1 つのシステムであるかのように動作します。クラスタ内の各アプリケーション・サーバは、ノードと呼ばれます。

クラスタは、ミッションクリティカルなサービスを提供して最大のスケーラビリティを確保します。クラスタ内の負荷分散技法を使用して、クライアント要求を複数のアプリケーション・サーバにわたって分配し、多数のユーザにスケーリングしやすくします。

次の図に、Agile Manager システムのクラスタ設定を示します。



詳細については、「[Agile Manager コンポーネント](#)」(9ページ)および「[クラスタ化されたシステムのインストール](#)」(38ページ)を参照してください。

クラスタ化された環境では、次の事項を考慮してください。

クラスタの考慮事項	
オペレーティング・システムのバージョン	各ノードでは、すべてのパッチ、更新プログラム、または修正プログラムを含め、同じオペレーティング・システムのバージョンを使用する必要があります。
Agile Manager バージョン	各ノードでは、同じバージョンの Agile Manager を使用する必要があります。
システム管理データベース・スキーマ	すべてのノードは、システム管理データベース・スキーマをポイントする必要があります。
共有リソース	すべてのノードは次にアクセスできる必要があります。 <ul style="list-style-type: none"> すべてのデータベース・サーバ システム管理データベース・スキーマ サイト・リポジトリ <p>標準設定では、リポジトリはクラスタ内の最初のノードにあるため、その他すべてのノードは最初のノードにアクセスできる必要があります。リポジトリを専用マシンにインストールする場合、各ノードはそのマシンにアクセスする必要があります。</p>

システム要件

注: Agile Manager は, 必要なシステム要件を満たしている任意の仮想マシンにインストールできます。

本項には, 次の事項の詳細を記します。

- [最小ハードウェア要件](#) 13
- [推奨ハードウェア要件](#) 13
- [追加システム要件](#) 14

最小ハードウェア要件

注: 最小要件は, 同期も ALI も設定されていない基本的なシステムと用途に関して定義されています。

その他の設定の詳細については, [「推奨ハードウェア要件」\(13ページ\)](#)を参照してください。

コンポーネント	最小要件
アプリケーション・サーバ	<ul style="list-style-type: none">• デュアル・コア CPU• 4 GB のメモリ(RAM)• 最大 2 GB のヒープ• 空きディスク容量 16 GB 以上
データベース・サーバ	<ul style="list-style-type: none">• デュアル・コア CPU• 4 GB のメモリ(RAM)

推奨ハードウェア要件

推奨ハードウェア要件は, 次のシステム構成に対して別々に定義されます。

- [「基本設定の Agile Manager\(NextGen Synchronizer なし\)」\(14ページ\)](#)
- [「基本設定の Agile Manager\(NextGen Synchronizer あり\)」\(14ページ\)](#)
- [「クラスタ設定の Agile Manager\(NextGen Synchronizer あり\)」\(14ページ\)](#)

基本設定の Agile Manager(NextGen Synchronizer なし)

コンポーネント	最小要件
アプリケーション・サーバ	<ul style="list-style-type: none">クワッド・コア CPU8 GB のメモリ(RAM)最大 4 GB のヒープ空きディスク容量 16 GB 以上
データベース・サーバ	<ul style="list-style-type: none">8 コア CPU16 GB のメモリ(RAM)

基本設定の Agile Manager(NextGen Synchronizer あり)

コンポーネント	最小要件
アプリケーション・サーバ	<ul style="list-style-type: none">16 コア CPU16 GB のメモリ(RAM)最大 10 GB のヒープ空きディスク容量 16 GB 以上
データベース・サーバ	<ul style="list-style-type: none">12 コア CPU32 GB のメモリ(RAM)

クラスタ設定の Agile Manager(NextGen Synchronizer あり)

コンポーネント	最小要件
アプリケーション・サーバ	4 ノード(クラスタ化) 各ノードの要件 : <ul style="list-style-type: none">8 コア CPU12 GB のメモリ(RAM)最大 8 GB のヒープ空きディスク容量 16 GB 以上
データベース・サーバ	<ul style="list-style-type: none">16 コア CPU64 GB のメモリ(RAM)

追加システム要件

Agile Manager システムは、システム構成にかかわらず、次の要件をみたす必要があります。

- 「アプリケーション・サーバの TCP ポート要件」(15ページ)
- 「データベース・サイズの要件」(15ページ)
- 「サポートされている環境」(15ページ)
- 「クライアント・マシンの要件」(16ページ)

アプリケーション・サーバの TCP ポート要件

HTTP および HTTPS アクセスで使用される標準設定のポートは 8080 および 8443 です。

注: Linux で 1024 より上位のポート番号を使用するにはセキュリティ保護されたプロセスが必要です。

プロセスの権限を変更して、小さい番号のポートを使用するには、システム管理者に問い合わせてください。

データベース・サイズの要件

データベース・サーバ上のデータベースのサイズは次のように設定します。

設定	要件
ALI なし	初期サイズ 50 MB, 平均的なプロジェクトでは最終的に 1 GB 以上に達する可能性があります。
ALI あり	初期サイズ 5 GB。

サイズ要件は、プロジェクトに応じて異なります。サイズを左右するのは、システムで想定されるバックログ項目の数と、想定される 1 日あたりの変更の数です。

ALI の設定を計画する場合、サイズは 1 日当たりのビルド数、コミット数、およびファイル数によって左右されます。

サポートされている環境

オペレーティング・システム	Red Hat Enterprise Linux 6.2, 6.3, 6.4, または 6.5(64ビット) SUSE Linux Enterprise 11 サービス・パック 3
データベース	Oracle Database 11.2.0.4, Standard および Enterprise Edition Oracle Database 12.1.0.1, Enterprise Edition

注: PDB はサポートされていません。

クライアント・マシンの要件

サポートされているブラウザ	Chrome 23 以上 Firefox 16 以上 Internet Explorer 10 および 11 <div data-bbox="558 457 1375 579" style="background-color: #e6f2e6; padding: 5px;"><p>注: Internet Explorer で作業している場合, Chrome Frame プラグインが無効になっていることを確認してください。</p></div>
画面の解像度	1920x1080(推奨), 1680x1050(サポートされます)

Linux の前提条件

本章では、Linux アプリケーション・サーバの次の前提条件について説明します。

[「Linux のディスク容量要件」\(17ページ\)](#)

[「Linux サーバで必要になる権限」\(17ページ\)](#)

参照情報:

- [「システム要件」\(13ページ\)](#)
- [「Oracle の前提条件」\(19ページ\)](#)

Linux のディスク容量要件

サーバ・マシンが[「システム要件」\(13ページ\)](#)に列挙された Agile Manager のディスク容量の要件を満たしていることを確認します。

`/<ルート>/opt/hp` ディレクトリには、インストール後の Agile Manager のサイズ、および操作中に作成される任意のファイルを収容するのに十分な空き容量が最低限必要です。このディレクトリには、空き容量が約 5 GB 必要です。

ディスク容量を確認するには、次のコマンドを使用します。

```
df -h
```

Linux サーバで必要になる権限

Agile Manager を Linux サーバ・マシンにインストールするには、次の権限が必要です。

管理者のユーザ権限

- 管理者権限を持つローカル・ユーザまたはドメイン・ユーザとしてログオンする必要があります。
- ユーザ名に、ポンド記号 (#) またはアクセント記号付き文字 (ä, ç, ñ など) を含めることはできません。
- 標準設定では、Agile Manager インストーラには **root** ユーザが必要です。

セキュリティ上の理由から **root** ユーザを使用して Agile Manager をインストールできない場合、`sudo` 権限を持つ非 **root** ユーザとしてのインストールについて、システム管理者にお問い合わせください。

このユーザは、次の操作のアクセス許可が必要です。

- RPM パッケージのインストールの実行
- ローカル・ユーザの作成 (オプション。標準設定では、Agile Manager サービスを実行するユーザがインストール・プロセスで作成されます。必要な場合、この作成を禁止できます。詳細については、[「設定ウィザードの実行」\(28ページ\)](#)を参照してください)

- **su** コマンドによるユーザの切り替え
- HPALM を Linux の init システムのサービスとして登録

注: 一部の環境 (標準設定の SUSE など) では、**root** ユーザのパスワードを入力する必要があります。

ファイル・ディレクトリ権限

/opt/hp/agm ディレクトリおよびその下にあるすべてのファイルとフォルダに対する、完全な読み取り/書き込み権限が必要です。

ファイル・リポジトリがリモート・マシン上にある場合:

- ファイル・サーバ・マシン上で、ファイル・リポジトリ・ディレクトリを共有し、Agile Manager サービスを実行するユーザがファイルの所有者になるようにします。これは標準設定では **agml-user** です。詳細については、「[サービス・ユーザの名前の変更 \(オプション\)](#)」(28ページ)を参照してください。
- Agile Manager マシンまたは各 クラスタ・ノード上で、ファイル・リポジトリ・ディレクトリをポイントするマウント・ディレクトリを作成します。

Oracle の前提条件

本章では、Oracle データベース・サーバに必要な前提条件について説明します。

[「データベース要件」\(19ページ\)](#)

[「管理ユーザ権限の付与」\(20ページ\)](#)

[「Oracle RAC サポートの有効化」\(23ページ\)](#)


複数の Oracle インスタンスを使用して Oracle データベースの可用性とスケーラビリティを強化する場合、Oracle RAC を使用します。

参照情報:

- [「システム要件」\(13ページ\)](#)
- [「Linux の前提条件」\(17ページ\)](#)

データベース要件

Agile Manager を Oracle データベース・サーバに接続する前に、次のことを確認してください。

要件	説明
データベース接続	<ul style="list-style-type: none">• データベース・サーバへの接続 <p>Agile Manager とデータベース間の接続のセキュリティ確保の詳細については、「システム・コンポーネント間での SSL/TLS の使用」(57ページ)を参照してください。</p> <ul style="list-style-type: none">• DNS の解決 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> ヒント: DNS の解決をテストするには、データベース・サーバに対して ping を実行します。</div>
データベース・サイズ	<ul style="list-style-type: none">• ALI を使用しない場合: 初期サイズ 50 MB, 平均的なプロジェクトでは最終的に 1 GB 以上に達する可能性があります。• ALI を使用する場合: 初期サイズ 5 GB。
文字セット	<ul style="list-style-type: none">• データベース文字セットを AL32UTF8 に設定します。• 次のパラメータ値を設定します。 NLS_LENGTH_SEMANTICS=CHAR

要件	説明
データベースのカラムの長さの意味	<p>カラムの長さは、バイト数でなく、文字数に従って定義されている必要があります。</p> <p>注: Agile Manager は UNICODE 文字セットを使用しますが、この文字セットでは各文字に2バイト以上必要となることがあります。各カラムに必要な長さを確保するために、文字数でカラムの長さを定義してください。</p>
表領域の名前とサイズ	<ul style="list-style-type: none">表領域の名前： Default(標準設定) :qc_data Temporary(一時) :tempシステム管理データベース・スキーマを格納するための表領域の最小サイズ。初期要件は、次のとおりです。 qc_data: 20 MB temp: 50 MB表領域は、ロックしないでください。
クラスタ設定またはアップグレード	<p>Agile Manager をクラスタ設定の2番目のノードにインストールする場合や、アップグレード時には、以下が必要になります。</p> <ul style="list-style-type: none">Agile Manager をデータベース・サーバに接続するための、既存のデータベース・スキーマの名前とパーミッション。既存のリポジトリ上の完全な読み取り書き込み権限。前のシステム管理スキーマ・リポジトリ・パスへのアクセス権。Agile Manager ユーザには、このパスへの完全な読み取り書き込み権限が必要です。既存のスキーマの作成に使用された機密データ・パスフレーズ。

管理ユーザ権限の付与

データベースをインストールしているユーザは、Oracle で特定の管理タスクを実行するのに十分な権限を持っている必要があります。たとえば、これらのタスクには、Agile Manager サイト・ユーザ・スキーマの作成、プロジェクト間のデータのコピー、特定の表領域に十分なストレージがあるかどうかのチェックなどがあります。

注: セキュリティ上の理由で Oracle システム・ユーザを使用できない場合、Agile Manager のインストールに必要な特定の権限を持つ Agile Manager 管理者ユーザ (**agm_admin** など) をデータベース管理者が作成することをお勧めします。少ない権限で Agile Manager をインストールすることが必要な場合には、HP カスタマ・サポートまでお問い合わせください。

次のスクリプトを Oracle データベース・サーバ上で SYSDBA ユーザとして実行し、必要なデータベース管理のユーザとロールを付与します。

詳細については、「[ユーザ権限](#)」(22ページ)を参照してください。

```
--drop user agm_admin cascade;
--drop role agm_admin_role;
create user agm_admin identified by agm_admin
default tablespace qc_data
temporary tablespace temp
quota unlimited on qc_data;
grant CTXAPP to agm_admin WITH ADMIN OPTION;
create role agm_admin_role;
grant CREATE ANY SYNONYM to agm_admin_role;
grant agm_admin_role to agm_admin WITH ADMIN OPTION;
grant CREATE SESSION to agm_admin_role WITH ADMIN OPTION;
grant CREATE USER to agm_admin_role;
grant DROP USER to agm_admin_role;
grant CREATE TABLE to agm_admin_role WITH ADMIN OPTION;
grant CREATE VIEW to agm_admin_role WITH ADMIN OPTION;
grant CREATE TRIGGER to agm_admin_role WITH ADMIN OPTION;
grant CREATE SEQUENCE to agm_admin_role WITH ADMIN OPTION;
grant CREATE PROCEDURE to agm_admin_role WITH ADMIN OPTION;
grant SELECT ANY TABLE to agm_admin_role WITH ADMIN OPTION;
grant INSERT ANY TABLE to agm_admin_role;
grant SELECT ON DBA_FREE_SPACE to agm_admin_role;
grant SELECT ON SYS.DBA_TABLESPACES to agm_admin_role;
grant SELECT ON SYS.DBA_USERS to agm_admin_role;
grant SELECT ON SYS.DBA_REGISTRY to agm_admin_role;
grant SELECT ON SYS.DBA_ROLES to agm_admin_role;
```

ユーザ権限	
CREATE ANY SYNONYM WITH ADMIN OPTION (1)	<owner.> プレフィックスを使用せずに別のスキーマ内のオブジェクトを表示するために必要です。
CREATE PROCEDURE WITH ADMIN OPTION (1)	Agile Manager サイトのストアド・パッケージを作成するために必要です。Agile Manager では、パッケージを使用して、特定のテーブルの変更履歴が収集されます。
CREATE SEQUENCE WITH ADMIN OPTION (1)	Agile Manager プロジェクトのシーケンスを作成するために必要です。
CREATE SESSION WITH ADMIN OPTION (1)	Agile Manager データベース管理ユーザとしてデータベースに接続するために必要です。
CREATE TABLE WITH ADMIN OPTION (1)	この権限を新たに作成した Agile Manager サイト・ユーザ・スキーマに付与するために必要です。
CREATE TRIGGER WITH ADMIN OPTION (1)	Agile Manager プロジェクトのトリガを作成するために必要です。Agile Manager では、データベース・トリガを使用して、特定のテーブルの変更履歴が収集されます。
CREATE USER	新しい Agile Manager サイトの作成時に、新しいシステム・ユーザ・スキーマを作成するために必要です。
CREATE VIEW WITH ADMIN OPTION (1)	Agile Manager サイトのビューを作成するために必要です。
CTXAPP ROLE WITH ADMIN OPTION (1)	Agile Manager が Oracle テキスト検索機能を使用できるようにします。このロールは、Oracle テキスト検索コンポーネントがインストールされ、データベース・サーバ上で有効にされている場合にのみ存在します。
DROP USER	システム管理データベース・スキーマを削除するために必要です。
SELECT ANY TABLE WITH ADMIN OPTION (1) および INSERT ANY TABLE	サイトの復元時にパフォーマンスを向上させるために必要です。
SELECT ON DBA_FREE_SPACE (2)	新しいシステム管理データベース・スキーマまたは新しいサイトを作成する前に、データベース・サーバ上の空き領域をチェックするために必要です。
SELECT ON SYS.DBA_REGISTRY (2)	テキスト検索コンポーネントがデータベース・サーバ上にインストールされていることを確認するために必要です。
SELECT ON SYS.DBA_ROLES (2)	テキスト検索ロール (CTXAPP) がデータベース・サーバ上にインストールされていることを確認するために必要です。

ユーザ権限	
SELECT ON SYS.DBA_TABLESPACES (2)	新しいシステム管理データベース・スキーマまたは新しいサイトを作成する前に、データベース・サーバ上に存在する表領域のリストを収集するために必要です。
SELECT ON SYS.DBA_USERS (2)	特定のデータベース・サイト・ユーザの存在を確認するために必要です。たとえば、新しい Agile Manager サイトを作成する前に、Oracle CTXSYS ユーザの存在を確認したい場合があります。

注:

- (1) Agile Manager 管理者ユーザには、**Admin Option** 付きの権限が必要です。
- (2) **SELECT ON SYS.*** 権限は、テーブル所有者が直接、またはデータベース・アプリケーション・ロール経由で付与できます。これらの権限を毎回付与しないで済むように、このロールは Agile Manager 管理者ユーザに付与できます。このロールに推奨される名前は、**AGM_SELECT_ON_SYS_OBJECTS** です。

メンテナンス完了後のユーザ権限

- インストール、アップグレード、またはその他のメンテナンス手順の完了後には、権限をそのまま残しておくことをお勧めします。ADMIN オプションは削除できます。
- CREATE SESSION 権限は Agile Manager の日常の機能に必須ですが、この権限に対する ADMIN オプションは削除してもかまいません。
- 後でアップグレードやその他のメンテナンス手順を実行する際には、削除したすべての権限と ADMIN オプションを元に戻す必要があります。

Oracle RAC サポートの有効化

Oracle RAC を使用して Oracle データベースの可用性とスケーラビリティを強化し、複数のデータベース・インスタンスとやり取りできるようにします。

Agile Manager RAC サポートには、Oracle インスタンス間の負荷分散、および初期接続時に指定されたすべての Oracle RAC ノード間のフェールオーバが含まれています。

注: TAF(Transparent Application Failover: 透過的アプリケーション・フェイルオーバ)はサポートされていません。

Oracle インスタンスのクラッシュ後に要求を完了できないユーザは、動作している Oracle インスタンスで再度アクティビティを実行する必要があります。

Oracle RAC サポートを有効にするには、次の操作を実行します。

1. **tnsnames.ora** ファイルが Agile Manager サーバに保存されていることを確認します。
このファイルには、次の例のような Oracle データベース・アドレスが含まれている必要があります。
 - 「[ADDRESS サブセクション内のすべてのクラスタ・ノードを使用する RAC TNS エイリアス](#)」(24ページ)
 - 「[Single Client Access Name\(SCAN\) を使用する RAC TNS エイリアス](#)」(24ページ)
2. Agile Manager が参照する必要がある TNS サーバのアドレス(OrgRAC など)があることを確認します。

例:

ADDRESS サブセクション内のすべてのクラスタ・ノードを使用する RAC TNS エイリアス

この例では、負荷分散とフェールオーバー機能も使用しています。

```
OrgRAC =
(DESCRIPTION =
  (ADDRESS_LIST=
    (FAILOVER = on)
    (LOAD_BALANCE = on)
    (ADDRESS= (PROTOCOL = TCP)(HOST = server1)(PORT = 1521))
    (ADDRESS= (PROTOCOL = TCP)(HOST = server2)(PORT = 1521))
    (ADDRESS= (PROTOCOL = TCP)(HOST = server3)(PORT = 1521))
  )
  (CONNECT_DATA=
    (SERVICE_NAME = myrac.yourcompany.com)
  )
)
```

Single Client Access Name(SCAN) を使用する RAC TNS エイリアス

この例では、Oracle 11gR2 クライアントを有効にして、複数の IP アドレスの解決、クラスタ内の複数のリスナの反映、およびパブリック・クライアント接続の処理を行えるデータベースに接続します。

```
OrgRAC_Scan =
(DESCRIPTION =
  (ADDRESS_LIST=
    (FAILOVER = on)
    (LOAD_BALANCE = on)
    (ADDRESS= (PROTOCOL = TCP)(HOST = myrac-cluster-scan)(PORT = 1521))
  )
  (CONNECT_DATA=
    (SERVICE_NAME = myrac.yourcompany.com)
  )
)
```

RAC SCAN の使用方法の詳細については、Oracle ドキュメントを参照してください。

インストールとアップグレード

注: インストールまたはアップグレードの手順を開始する前に、「[プレインストール・チェックリスト](#)」(26ページ)を使用して必要なすべての詳細情報があることを確認してください。

このガイドでは、次のタイプのインストール手順について説明します。

スタンドアロンの初回インストール	Agile Manager をスタンドアロン・システム上に初めてインストールする場合は、直接「 Agile Manager のインストール 」(27ページ)に進んでください。
クラスタ・インストール	クラスタ化されたシステムをインストールする場合、クラスタ内の各ノード上に Agile Manager をインストールする必要があります。 「クラスタ化されたシステムのインストール」 (38ページ)から始めてください。
クラスタ化された運用システムのアップグレード	クラスタ化された運用システムをアップグレードする場合、クラスタ内の各ノード上で Agile Manager をアップグレードする必要があります。 「クラスタ化されたシステムのアップグレード」 (40ページ)から始めてください。
基本的な運用システムのアップグレード	運用システムを直接(ステージング・システムを使用せずに)アップグレードする場合、手順に従って、アップグレード固有の準備を実行する必要があります。 「基本的な運用システムのアップグレード」 (44ページ)から始めてください。
最初にステージング・システムを作成してアップグレード	ステージング・システムを使用してアップグレードする場合、アップグレードの前と途中で手動でファイルをコピーし、ステージング・システムをこれらのファイルに手動で接続する必要があります。 「ステージング環境を使用した Agile Manager のアップグレード」 (47ページ)から始めてください。

参照情報: [「Agile Manager のアンインストール」](#)(39ページ)

アップグレードのセキュリティの強化

特別な権限を持たない単純なユーザとして Agile Manager を実行する場合、以前のバージョンの Agile Manager では、その目的で使用する **agmuser** という名前のユーザを追加する必要がありました。

ユーザを追加した後にアップグレードを行う場合、アップグレード中に指示に従ってこの **agmuser** ユーザを削除できます。

アップグレードにより、**agml-user** という名前の独自の非ルート・ユーザがインストール・プロセスで作成されるようになりました。このユーザは、限られた権限が与えられており、Agile Manager サービスの実行を担当します。

- クラスタ設定を使用する場合は、アップグレード中に指示に従って、この名前のネットワーク・ユーザを作成し、共有リポジトリ・フォルダの所有者をこのユーザに変更する必要があります。
- **agmi-user** 以外のユーザ名を使用するには、デプロイ後にインストール・ファイルおよび設定ファイルを変更します。詳細については、「[サービス・ユーザの名前の変更\(オプション\)](#)」(28ページ)を参照してください。

注: アップグレードでは **agmi-user** という名前のユーザのみをサポートします。この名前を変更する場合は、その後のアップグレードでこれらの手順をもう一度実行する必要があります。

注意: **agmi-user** ユーザは内部用なので、ログインやスクリプトの実行などに明示的に使用しないでください。

プレインストール・チェックリスト

Agile Manager をインストールする前に、次のチェックリストをよく読んで内容を確認します。このチェックリストは、インストール・プロセス中に利用可能にしておく必要がある情報の概要を示しています。

注意: システムのセキュリティを保護するために、標準設定のパスワードは必ず変更してください。

サポートされているシステム環境の一覧については、「[システム要件](#)」(13ページ)を参照してください。

詳細とオプションのプレインストール手順については、「[Linux の前提条件](#)」(17ページ)および「[Oracle の前提条件](#)」(19ページ)を参照してください。

プレインストール・チェックリスト

クラスタ	クラスタ・ホスト名 クラスタ設定を使用している場合にのみ必要です。
暗号化パスワード	機密データ・パスフレーズ Default(標準設定): Seashells Grow Like Misty Tunas クラスタでは、すべてのノードで同じパスフレーズを使用します。 注: 電話サポートで使用するためにパスフレーズを記録しておいてください。

プレインストール・チェックリスト	
データベース・サーバ	<p>データベース: ホスト名, ポート, システム識別子 (SID), および管理者のユーザ名とパスワード。</p> <p>Oracle SID は, Oracle サーバのホスト・マシン上で特定の Oracle インスタンスを識別します。</p> <p>表領域: 標準設定の表領域の選択。</p>
システム管理	<p>システム管理</p> <p>システム管理パスワード。標準設定のパスワードは空です。インストール時にこのパスワードを変更できます。</p> <p>標準設定のシステム管理者ユーザ名は, sa です。これは変更できません。Agile Manager 管理サイト ([Configuration(設定)] > [Users(ユーザ)]) でシステム管理者として, 後でほかのユーザを定義できます。</p> <p>詳細については, 「システム管理者の定義とユーザ・パスワードのリセット」(91ページ)を参照してください。</p> <p>システム管理データベース・スキーマ</p> <p>システム管理データベース・スキーマのユーザ名とパスワード。</p> <p>標準設定のシステム管理データベース・スキーマ名は agm_siteadmin_db で, 標準設定のパスワードは tdtdtd です。インストール時にこれら両方の標準設定値を変更できます。</p>
ファイル・リポジトリ	<p>リポジトリ・パス</p> <ul style="list-style-type: none">標準設定では, リポジトリはデプロイメント・フォルダ内に設定されます。Agile Manager を実行するユーザは, リポジトリ・フォルダの所有者である必要があります。 <p>クラスタ設定では, このフォルダの所有者になる agml-user という名前のネットワークユーザを作成し, Agile Manager サービスを実行することをお勧めします。</p> <p>詳細については, 「クラスタ化されたシステムのインストール」(38ページ)を参照してください。</p>

Agile Manager のインストール

本項では, Agile Manager をインストールおよび設定する方法について説明します。

クラスタ化されたシステムにインストールするか, アップグレードする場合は, 先に次の項目を参照してください。

- 「[クラスタ化されたシステムのインストール](#)」(38ページ)
- 「[基本的な運用システムのアップグレード](#)」(44ページ)
- 「[ステージング環境を使用した Agile Manager のアップグレード](#)」(47ページ)
- 「[クラスタ化されたシステムのアップグレード](#)」(40ページ)

sudo 権限を持つ非 root ユーザとして Agile Manager をインストールする場合は、最初に「Linux サーバで必要になる権限」(17ページ)を参照してください。

インストール・プロセス中に問題が発生した場合の対処方法については、「トラブルシューティング」(77ページ)を参照してください。

注: Agile Manager をアンインストールした後で、前に使用していた同じ設定で再インストールする場合は、`qcConfigFile.properties.rpmsave` ファイルの名前を `qcConfigFiles.properties` に必ず変更してください。詳細については、「Agile Manager のアンインストール」(39ページ)を参照してください。

1. インストール・ファイルのデプロイ

rpm ファイルが格納されているディレクトリに移動し(`cd /home` など)、次のいずれかを実行します。

root ユーザとして	<pre>rpm --import keys/*.pub rpm -i Agile-Manager-ONPREM-<バージョン番号>.rpm</pre>
sudo ユーザとして	<pre>sudo rpm --import keys/*.pub sudo rpm -i Agile-Manager-ONPREM-<バージョン番号>.rpm</pre> <p>注: Agile Manager と sudo 権限の詳細については、「Linux サーバで必要になる権限」(17ページ)を参照してください。</p>

インストール・ファイルは、`/opt/hp/agm` 下にデプロイされます。

2. サービス・ユーザの名前の変更 (オプション)

標準設定では、Agile Manager は制限された権限を持つユーザを作成して、Agile Manager の実行に使用します。このユーザは `agml-user` という名前です。

このユーザ名を変更する場合は、次の手順を実行します。

- `/opt/hp/agm/conf/wrapper-user.conf` ファイルを参照して、編集用を開きます。
- 文字列 `agml-user` をサービス・ユーザの名前に置き換えます。これはローカル・ユーザまたは LDAP ユーザです。

Agile Manager はこの名前のユーザを作成します。ユーザを作成せずに、この名前の既存のユーザを使用するように Agile Manager に指示するには、手順 3 を参照してください。

注意: root をユーザ名として入力しないでください。

3. 設定ウィザードの実行

Agile Manager ファイルがデプロイされているディレクトリを開きます。

```
cd /opt/hp/agm
```

次のいずれかを実行します。

root ユーザとして	<code>./run_config.sh</code>
sudo ユーザとして	<code>sudo ./run_config.sh</code>

注:

- サービスの実行のために新規ユーザを作成せずに既存のユーザを使用するように Agile Manager に指示するには、`-noUserCreation` フラグを使用します。
`./run_config.sh -noUserCreation`
Agile Manager は、`/opt/hp/agm/conf/wrapper-user.conf` ファイルに定義されているユーザを使用します。
- Agile Manager をクラスタの 2 番目のノードにインストールしている場合、プライマリ・ノードまたは初回設定にのみ関連するステップの一部が表示されません。

Agile Manager 設定 ウィザードが開きます。

```
Welcome

Welcome to the HP Agile Manager Server Configuration Wizard.

The wizard will guide you through the steps of installing HP Agile Manager
on your computer.

Throughout the wizard, press Enter to accept the default selection, or type
your new selection. To exit the wizard, click Ctrl+C.
```

4. EULA を受け入れる

Agile Manager EULA が表示されます。EULA をよく読んで、その条項を受け入れて続行します。

```
-----
End User License Agreement

HP End User License Agreement - Enterprise Version

1. Applicability. This end user license agreement (the "Agreement") governs the
use of accompanying software, unless it is subject to a separate agreement
between you and Hewlett-Packard Company and its subsidiaries ("HP"). By
downloading, copying, or using the software you agree to this Agreement. HP
provides translations of this Agreement in certain languages other than
English, which may be found at: http://www.hp.com/go/SWlicensing.
```

5. 検出された設定の再利用

前に Agile Manager を設定している場合、以前の設定から検出された設定を保存できます。

```
Current Settings

The wizard has detected existing configuration settings on this computer.
Do you want to keep all current configuration settings?

[X] 1 - Yes, I want to keep all current settings
[ ] 2 - No, I want to reconfigure server settings

Press Enter to keep the current selection, or type selection number: [ ]
```

注: このステップは、`qcConfigFiles.properties` ファイルが `/opt/hp/agm/conf/` ディレクトリ内に存在している場合にのみ表示されます。

- クラスタをインストールしている場合、手順を開始する前に、このファイルを以前のインストールからコピーする必要があります。詳細については、「[クラスタ化されたシステムのインストール](#)」(38ページ)を参照してください。
- システムをアップグレードしている場合、前のバージョンの Agile Manager をアンインストールして、このファイルの名前を変更する必要があります。詳細については、「[基本的な運用システムのアップグレード](#)」(44ページ)を参照してください。

既存の設定を保持するか、またはクリアするかを選択します。[Yes(はい)]を選択すると、後続のウィザード・パラメータで既存の設定が標準設定として使用されます。任意の設定を変更することができます。

6. データベース・パラメータの入力

データベース・パラメータを接続文字列として入力するか、個別に入力するかを選択します。SSLを設定するには、以下に示すように、[Connection String(接続文字列)]を選択します。

```
Database Connection

[ ] 1 - Connection String
[X] 2 - Database Parameters
```

次に、接続データを文字列として入力するか、プロンプトごとに入力します。

データをパラメータとして入力するときには、次の各パラメータを入力した後に **ENTER** を押します。

パラメータ	説明
DB host name(DB ホスト名)	データベース・サーバのホスト名
DB port number(DB ポート番号)	データベース・サーバのポート番号。標準設定をそのまま使用できます。
Oracle SID(Oracle SID)	Oracle システム識別子。

ORA 設定ファイルを使用してデータベース・アドレスを定義する場合、この手順の接続文字列を使用します。

次に、ORAファイルとサービス名から作成された接続文字列の例を示します。

```
jdbc:mercury:oracle:TNSNamesFile=/<パス>;TNSServerName=<名前>
```

ここでは、次の意味があります。

- jdbc:mercury:oracle は必須です
- <パス> = tnsnames.ora ファイルのパス
- <名前> = TNS サーバの名前

Agile Manager と Oracle データベース間では、セキュア接続を設定できます。詳細については、「[システム・コンポーネント間での SSL/TLS の使用](#)」(57ページ)を参照してください。

この場合、この手順の接続文字列を使用して、次のパラメータを追加します。

パラメータ	説明
EncryptionMethod	SSL
TrustStore	クライアント証明書 (wallet) ファイルの完全パス。 例: /Wallets/client_wallet/ewallet.p12
TrustStorePassword	証明書を保護するために使用するパスワード。

次に、データベースへの SSL 接続に使用される接続文字列の例を示します。

```
jdbc:mercury:oracle://<DBHostname>:2484;sid=<SID>;EncryptionMethod=SSL;TrustStore=<certificate_folder>/ewallet.p12;TrustStorePassword=<password>
```

ここでは、次の意味があります。

- jdbc:mercury:oracle は必須です
- <DBHostname> = データベース・サーバのホスト名
- <SID> = Oracle システムの識別子
- certificate_folder = 証明書ファイルを含むフォルダ
- <password> = 証明書ファイルのキーストア・パスワード

7. データベース管理者のログイン情報の入力

```
Database Administrator Login
```

```
DB admin user name:
```

次の指定を行います。エントリごとに、**ENTER** を押します。

パラメータ	説明
DB admin user name(DB 管理者ユーザ名)	Agile Manager をデータベース・サーバに接続するために必要な管理権限を持つユーザの名前。
DB admin password(DB 管理者パスワード)	データベース管理者のパスワード。

8. データベース・スキーマ・オプションの選択

```
System Administration Database Schema

Select an option. See the Installation and Administration Guide for details
about each option.

[X] 1 - Create a new schema
[ ] 2 - Connect to existing schema/second node
[ ] 3 - Upgrade production
[ ] 4 - Create and upgrade staging

Type a number to change the selection or press Enter to continue:
```

表示されるオプションの1つを選択します。各オプションの詳細について知るには、次の関連するリンクをクリックしてください。

- [「Create a new schema\(新規スキーマの作成\)」](#)(32ページ)
- [「Connect to existing schema/second node\(既存のスキーマ/2番目のノードに接続\)」](#)(32ページ)
- [「Upgrade production\(運用システムのアップグレード\)」](#)(33ページ)
- [「Create and upgrade staging\(ステージングの作成とアップグレード\)」](#)(33ページ)
- **Create a new schema(新規スキーマの作成)**

新しいシステム管理データベース・スキーマを作成します。

注: 次の警告は無視できます: Schema differences were found(スキーマの相違が見つかりました)

この警告は、スキーマの拡張およびアップグレード機構の一環として生成されます。

- **Connect to existing schema/second node(既存のスキーマ/2番目のノードに接続)**

既存のシステム管理データベース・スキーマに接続できます。

このオプションは、主にクラスタ内で2番目のノードを設定している場合に関連します。このような場合、このオプションが有効になるのは、すべてのノードを同じバージョンでインストールしている場合のみです。

注意: クラスタのインストールまたはアップグレードを行う場合は、先に[「クラスタ化されたシ](#)

システムのインストール」(38ページ)または「クラスタ化されたシステムのアップグレード」(40ページ)を参照してください。

設定ウィザードの残りの部分では、機密データ・パスフレーズの定義を除いて、既存のデータをそのまま使用します。「機密データ・パスフレーズの入力」(35ページ)に進んだ後、「設定の確認」(37ページ)に進んでください。

- **Upgrade production(運用システムのアップグレード)**

既存のシステム管理データベース・スキーマのコピーを作成し、コピーをアップグレードして、既存の Agile Manager サイトに自動的に接続します。

注意: このオプションは、運用システムのアップグレードにのみ使用できます。

運用システムをアップグレードする前に別のシステムでアップグレードをテストする場合は、このオプションを選択しないでください。

「ステージング環境を使用した Agile Manager のアップグレード」(47ページ)を実行する場合は、「Create and upgrade staging(ステージングの作成とアップグレード)」(33ページ)を選択してください。

[**Upgrade production(運用システムのアップグレード)**]を選択した後は、プロンプトに従って次の手順を実行します。

- i. 古いシステム管理スキーマの名前とパスワードの値を入力するか、指定された値を受け入れます。
- ii. 新しいシステム管理スキーマの名前を入力します。

設定ウィザードの残りの部分では、機密データ・パスフレーズの定義を除いて、既存のデータをそのまま使用します。「機密データ・パスフレーズの入力」(35ページ)に進んだ後、「設定の確認」(37ページ)に進んでください。

- **Create and upgrade staging(ステージングの作成とアップグレード)**

既存のシステム管理データベース・スキーマのコピーを作成し、コピーをアップグレードしますが、Agile Manager サイトには接続しません。

このオプションでは、空のシステムが作成されます。このシステムは、運用環境をアップグレードする前のステージング環境として使用できます。

注意: このオプションは、「ステージング環境を使用した Agile Manager のアップグレード」(47ページ)の手順を実行する場合にのみ選択します。

[**Create and upgrade staging(ステージングの作成とアップグレード)**]を選択した後は、プロンプトに従って次の手順を実行します。

- i. 古いシステム管理スキーマの名前とパスワードの値を入力するか、指定された値を受け入れます。
- ii. 新しいシステム管理スキーマの名前を入力します。

設定ウィザードの残りの部分では、機密データ・パスフレーズの定義を除いて、既存のデータをそのまま使用します。「機密データ・パスフレーズの入力」(35ページ)に進んだ後、「設定の確認」(37ページ)に進んでください。

9. Oracle の一時表領域の情報の入力

一時表領域とは、内部データベース機能(大規模なソート・タスクなど)を円滑に実行するために一時的なテーブルが作成されるデータベースの場所です。

```
Oracle Tablespaces

Select the default and temporary tablespaces that will be used to store the
Agile Manager Server Site Administration database schema.

Temporary Tablespace:

[X] 1 - TEMP
```

ENTER を押して、標準設定の TEMP ディレクトリを選択します。

10. Oracle のデフォルト表領域の情報の入力

デフォルト表領域とは、データベース・オブジェクトが作成されるデータベースの場所です。

注: 2 番目のノードに Agile Manager をインストールしているか、システム管理データベースがすでに存在している場合、新しいシステム管理データベース・スキーマは、既存のスキーマと同じ表領域に作成されます。そのような場合は、「システム管理者ログイン情報の入力」(36ページ)に進んでください。

例として、スクリーンショットを以下に示します。出力内容はデータベースの構造によって異なります。

```
Default Tablespace:

[X] 1 - QC_DATA 7543MB
[ ] 2 - TDDATA 1654MB
[ ] 3 - TD 2778MB
[ ] 4 - USERS 8595MB

Type a number to change the selection, or click Enter to continue:
```

デフォルト表領域を選択します。

11. システム管理データベース・スキーマの詳細の入力

```
SA Schema Details

Schema name: [agm_siteadmin_db]
```

- a. システム管理データベース・スキーマの名前を入力するか、標準設定を受け入れます。
上記の[Upgrade production(運用システムのアップグレード)]を選択した場合、[New Schema Name(新規スキーマ名)]オプションが表示されます。システム管理データベース・スキーマのコピーのアップグレードの名前を入力します。

注: 既存のシステム管理データベース・スキーマをアップグレードして Agile Manager で使用する場合、アップグレード前に使用していた同じ名前を使用する必要があります。

- b. ウィザードによってパスワードの入力が求められ、標準設定として `tdtdtd` (暗号化済み) が提示されます。標準設定のパスワードを受け入れるか、新しいパスワードを入力して変更します。ウィザードによって設定が検証されます。

注意: 標準設定値の使用はセキュアではなく、推奨されません。暗号化された情報が権限のないアクセスに対してより攻撃を受けやすくなります。

- c. 上記の[Create a new schema(新規スキーマの作成)]を選択した場合、ライセンス・オプションが表示されます。
Agile Manager は試用版のインスタント・オン・ライセンスでインストールされます。このライセンスでコンカレント・ユーザと固定ユーザのどちらをサポートするかを選択します。

注: 標準設定のコンカレント・ライセンスを使用することを推奨します。

詳細については、「[ユーザ・ライセンスの更新](#)」(89ページ)を参照してください。

12. 機密データ・パスフレーズの入力

```
Security

Agile Manager Server encrypts confidential data, such as passwords to external
systems (DB, LDAP), and secures communication with other HP BTO applications.

Confidential Data Encryption

Enter a passphrase with at least 12 characters for secure storage of
confidential data.
Important: If you are installing a cluster of servers, make sure you enter the
same passphrase on all nodes.

Confidential data passphrase: [*****]
```

Agile Manager では、外部システム(DB, LDAP)に対するパスワードなどの機密データの暗号化および暗号化解除時に、このパスフレーズを使用します。このため、クラスタ化されたシステムを設定している場合、両方のノードで同じパスフレーズを使用する必要があります。

選択したパスフレーズは記録しておいてください。

標準設定値の `Seashells Grow Like Misty Tunas` の使用を選択することもできます。

注意: 標準設定値の使用はセキュアではなく、推奨されません。暗号化された情報が権限のないアクセスに対してより攻撃を受けやすくなります。

機密データ・パスフレーズ選択の際の考慮事項

考慮事項	詳細
パスワードは不変	設定ウィザードが完了したら、機密データ暗号化パスフレーズを変更またはリセットできなくなります。
パスワード構文	パスフレーズは大文字と小文字が区別されます。 パスフレーズは、先頭または末尾に空白を設定できません。 パスフレーズには、英数字しか含めることができません。
アップグレード時	システム管理データベーススキーマのバージョンをアップグレードする場合、前のインストールで使用したのと同じパスフレーズを入力する必要があります。 標準設定では、ウィザードによって暗号化されたパスワードが提示されます。
クラスタへのインストール	Agile Manager をクラスタにインストールする場合、すべてのノードに同じパスフレーズを使用する必要があります。

13. システム管理者ログイン情報の入力

```
Site Administrator User

Type the password to be used when logging in to Agile Manager Administration.
Note: The default administrator user name is 'sa'. To add or change
administrators, after the configuration is complete, log in to the Agile
Manager Administration.

Password:
```

sa ユーザが Agile Manager 管理サイトへのログインに使用するパスワードを定義します。ウィザードによってパスワードの再入力求められます。

注意: 標準設定のパスワード値の使用はセキュアではなく、推奨されません。暗号化された情報が権限のないアクセスに対してより攻撃を受けやすくなります。

注: 標準設定の管理者ユーザ名は、**sa** です。この値は変更できません。

14. ファイル・リポジトリ・パスの入力

```
File Repository Path

File repository path: [/opt/hp/agm/repository]
```

標準設定のパスを受け入れるか、新しいパスを入力します。



ヒント: このパスの定義に関するガイドラインについては、「[ファイル・リポジトリ](#)」(27ページ)を参照してください。

15. アプリケーション・サーバのポートが空いていることの確認

```
Application Server

Advanced Options

Server HTTP Port: [8080]
```

標準設定(8080)を受け入れるか、新しいポートを入力します。

注: このポート番号を変更する場合、Linux で 1024 より上位のポート番号を使用するにはセキュリティ保護されたプロセスが必要です。

プロセスの権限を変更して、小さい番号のポートを使用するには、システム管理者に問い合わせてください。

16. 設定の確認

```
Installation Summary

To confirm the following configuration, Select "Continue". To modify any of the settings, Select "Back"
```

表示される情報を確認します。[**Continue(続行)**]を選択して設定を適用します。

17. 設定の完了

```
Finish

The wizard settings were successfully set.

To start the server, run "/opt/hp/agm/wrapper/HPALM start".
```

プロンプトに従ってサーバを起動します。詳細については、「[Agile Manager サービスの起動/停止](#)」(50ページ)を参照してください。

注: サーバを初めて起動したときに、Agile Manager 用の新しいデータベース・スキーマが作成されます。このスキーマの名前は、`t1_sa_main_db` です。

18. サービスが起動したら、Agile Manager または Agile Manager システム管理サイトにログインして続行します。詳細については、「[Agile Manager へのログイン](#)」(51ページ)を参照してください。
- セキュリティに関するベスト・プラクティスと手順については、「[システムのセキュリティ保護](#)」(52ページ)を参照してください。
- 他のサーバおよびシステムの管理の詳細については、「[アプリケーション・サーバの管理](#)」(73ページ)および「[Agile Manager のシステム管理](#)」(79ページ)を参照してください。

インストール後の注意事項:

- 設定ウィザードによって作成された次のファイルは移動しないでください。
`/opt/hp/agm/repository/qc/repid.txt`
`/opt/hp/agm/conf/qcConfigFile.properties`
- いくつかの設定は、ウィザードの実行後に変更できます。詳細については、「[アプリケーション・サーバの管理](#)」(73ページ)を参照してください。

クラスタ化されたシステムのインストール

本項では、クラスタ化された Agile Manager システムを設定する際の基本的な手順について説明します。

開始する前に、サーバ・ノードが Linux と Oracle サーバの前提条件を満たしていることを確認してください。詳細については、「[Linux の前提条件](#)」(17ページ)および「[Oracle の前提条件](#)」(19ページ)を参照してください。

1. 共有ネットワーク・ユーザの作成

NIS ユーザや LDAP ユーザなどのネットワーク・ユーザを作成します。これらのユーザは、すべてのノードでアクセス可能な共有リポジトリの所有者として使用され、Agile Manager サービスを実行する場合にも使用されます。

注: このユーザに `agml-user` という名前を付けることをお勧めします。異なる名前を使用する場合は、必ず「[Agile Manager システム・ファイルでの共有ネットワーク・ユーザの変更 \(オプション\)](#)」(39ページ)を実行してください。

2. 共有ファイル・リポジトリの作成およびマウント

共有リポジトリフォルダを作成し、前の手順で作成したユーザを所有者として定義します。

たとえば、次のコマンドを実行します。`chown agml-user -R /opt/hp/agm/repository`

- 各ノードでこのリポジトリをマウントします。マウントでは、キャッシュ機構を使用しないでください。詳細については、ネットワーク管理者にお問い合わせください。
 - すべてのノードで、同じマウント名を使用して共有ファイル・サーバをマウントする必要があります。すべてのノードで次のマウント名を使用することをお勧めします。`/opt/hp/agm/repository`
- すべてのノード上のインストール・ファイルをデプロイ
詳細については、「[インストール・ファイルのデプロイ](#)」(28ページ)を参照してください。
 - Agile Manager システム・ファイルでの共有ネットワーク・ユーザの変更 (オプション)
共有ネットワークユーザに `agm1-user` という名前を付けることをお勧めします。
このユーザに異なる名前を使用する場合は、Agile Manager を設定する前に**すべてのノード**のシステム・ファイルを変更します。詳細については、「[サービス・ユーザの名前の変更 \(オプション\)](#)」(28ページ)を参照してください。
 - 最初のノードでの Agile Manager の設定
詳細については、「[設定ウィザードの実行](#)」(28ページ)を参照してください。リポジトリ・パスを定義する場合、前に作成した共有フォルダを入力します。
 - 他のすべてのノードでの Agile Manager の設定
 - `/opt/hp/agm/conf/qcConfigFile.properties` ファイルを、最初のノードから他のすべてのノード上の同じフォルダにコピーします。
 - 他の各ノード上で Agile Manager 設定ウィザードを実行します。
設定中は、次のオプションの選択以外は、どの設定も変更しないでください。
 - Keep all current settings(現在の設定をすべて保持)
 - Connect to an existing schema/second node(既存のスキーマ/2番目のノードに接続)
詳細については、「[設定ウィザードの実行](#)」(28ページ)および「[Connect to existing schema/second node\(既存のスキーマ/2番目のノードに接続\)](#)」(32ページ)を参照してください。
 - 設定が完了したら、Agile Manager を起動します。
 - インストールの確認
Agile Manager 管理サイトにアクセスします。[Servers(サーバ)] > [Application(アプリケーション)] ページで、すべてのアプリケーション・サーバが正しく表示されることを確認します。
詳細については、「[Agile Manager へのログイン](#)」(51ページ)を参照してください。
 - Agile Manager から送信される電子メールで使用する外部 URL を設定します。
この手順は、通知電子メール用の電子メール・サーバを設定する場合のみ関係します。詳細については、「[電子メールで使用する外部 URL を設定します。](#)」(85ページ)を参照してください。

Agile Manager のアンインストール

- Agile Manager をインストールしたのと同じユーザ (`root` または `agmadmin sudo` ユーザ) としてサーバ・マシンにログインします。
- Agile Manager をアンインストールします。`rpm -e Agile-Manager`

注意: 標準設定では、以下のファイルおよびディレクトリはマシンから削除されません。

- **conf, log, repository**, および **wrapper** ディレクトリ
- **webapps/qcbin/WEB-INF/siteadmin.xml** ファイル

これらのファイルおよびディレクトリはアップグレード時に使用されます。この後にアップグレードする予定がある場合は、これらのファイルを削除しないでください。

注: Agile Manager をアンインストールすると、**qcConfigFile.properties** ファイルの名前が **qcConfigFile.properties.rpmsave** に変更されます。このファイルは、前回設定ウィザードを実行したときに定義した値を格納しています。

前に使用したのと同じ値を使用して Agile Manager を再インストールする場合、再インストールする前に、このファイルの名前を **qcConfigFile.properties** に変更する必要があります。

3. (オプション) Agile Manager のすべての痕跡をマシンから削除するには、インストール・ディレクトリ内に残っているすべてのファイルとデプロイメント・パスを削除します。
 - **conf** ディレクトリを削除すると、設定ウィザードの次回実行時に値を手動で追加する必要があります。
 - **repository** ディレクトリを削除すると、すべてのサイト・リポジトリも削除されます。データベースは指定して削除しない限り、保持されます。

クラスタ化されたシステムのアップグレード

本項では、クラスタ設定で Agile Manager をアップグレードする方法について説明します。基本的なスタンドアロン・システムのアップグレードの詳細については、「[基本的な運用システムのアップグレード](#)」(44ページ)を参照してください。

運用システムをアップグレードする前に別のシステムでアップグレードをテストする場合には、「[ステージング環境を使用した Agile Manager のアップグレード](#)」(47ページ)を代わりに参照してください。

本項の内容

1. 「[前提条件](#)」(41ページ)
2. 「[最初のノードでのみ実行する手順](#)」(41ページ)
3. 「[最初のノード以外のすべてのノードで実行する手順](#)」(43ページ)

注: アップグレード中にユーザが Agile Manager にログインしていた場合、アップグレードが完了してから作業を続行するには、ブラウザの表示の更新が必要になる可能性があります。

前提条件

1. システム要件とサーバの前提条件の確認

前のバージョン以降に変更があった場合、サーバ・ノードがLinuxとOracleサーバの前提条件を満たしていることを確認してください。詳細については、次を参照してください。

- [「システム要件」\(13ページ\)](#)
- [「Linuxの前提条件」\(17ページ\)](#)
- [「Oracleの前提条件」\(19ページ\)](#)

2. Agile Managerの停止

すべてのノード上でAgile Managerサービスを停止します。`/opt/hp/agm/wrapper/HPALM stop`

注: SUSE環境にインストールされたAgile Manager 2.20からアップグレードした場合、サービスを開始または停止した後に、存在しないフォルダに関する警告が表示される場合があります。この警告は無視してかまいません。

最初のノードでのみ実行する手順

1. agmuser ユーザの削除 (オプション)

以前に `agmuser` という名前の単純なユーザを作成し、特別なアクセス許可なしでAgile Managerを実行した場合は、ここでこのユーザを削除できます。現在のインストールによって、サービス・ユーザとして使用されるユーザが `agml-user` という名前で作成されます。

このユーザに異なる名前を使用する場合、あるいは既存のユーザをAgile Managerに使用させる場合は、インストールおよび設定中に適切な手順に従います。詳細については、[「サービス・ユーザの名前の変更 \(オプション\)」\(28ページ\)](#)を参照してください。

2. 共有リポジトリへのアクセスのための共有ネットワーク・ユーザの作成

- a. NIS ユーザやLDAP ユーザなどのネットワーク・ユーザを作成します。これらのユーザは、すべてのノードでアクセス可能な共有リポジトリの所有者として使用され、Agile Managerサービスを実行する場合にも使用されます。

注: このユーザに `agml-user` という名前を付けることをお勧めします。

このユーザに異なる名前を使用する場合は、インストールおよび設定手順中に変更します。詳細については、[「Agile Manager システム・ファイルでの共有ネットワーク・ユーザの変更 \(オプション\)」\(43ページ\)](#)を参照してください。

- a. このネットワーク・ユーザを共有リポジトリ・フォルダの所有者として定義します。例:
`chown -R agml-user /mnt/sharedfolder`

3. データのバックアップ

- アップグレードを行う前にデータベース・スキーマとサイト・リポジトリをバックアップします。



注意: サイトをバックアップする前に、非アクティブにしておくことを強くお勧めします。

サイトがまだアクティブな状態で、バックアップを実行する必要がある場合、最初にデータベースをバックアップしてから、ファイル・システムをバックアップしてください。データベースをバックアップしてから、可能な限りすみやかにファイル・システムをバックアップすることもお勧めします。

- 次のシステム・ファイルをバックアップするために、`/opt/hp` ディレクトリの外に保存します。
 - `/opt/hp/agm/server/conf/jetty.xml`
 - `/opt/hp/agm/java/jre/lib/security/cacerts`(SSL/TLS 設定のみ)
- **[Max DB Connections(最大 DB 接続数)]**の値を変更してある場合は、現在の値を記録しておきます。アップグレードでは標準設定値が復元されるため、変更はすべて失われます。この値は、Agile Manager システム管理サイトの **[Servers(サーバ)]** > **[Application(アプリケーション)]** タブで定義されています。詳細については、[「最大データベース接続数の設定」\(80ページ\)](#)を参照してください。

4. SSL/TLS を設定している場合は、`server.keystore` ファイルの特定やバックアップを行います。

`jetty.xml` ファイルを開き、`server.keystore` が保存される場所を決定します。

このファイルが `/opt/hp/agm` ディレクトリ、またはそのサブディレクトリに保存されている場合は、ファイルをバックアップするために `/opt/hp` ディレクトリの外に保存します。

5. 新しいバージョンの Agile Manager をインストールします。

インストール・パッケージにある rpm ファイルとキー・ファイルを `tmp` フォルダなどのアクセス可能なフォルダにコピーします。

rpm ファイルが格納されているディレクトリに移動し (`cd /home` など)、次のいずれかを実行します。

root ユーザとして	<pre>rpm --import keys/*.pub rpm -U AGM-ONPREM<バージョン番号> .rpm</pre>
sudo ユーザとして	<pre>sudo rpm --import keys/*.pub sudo rpm -U AGM-ONPREM<バージョン番号> .rpm</pre>

インストール・ファイルは、`/opt/hp/agm` 下にデプロイされます。

6. バックアップ・ファイルの復元

以前にバックアップした次のファイルを復元します。

- `/opt/hp/agm/server/conf/jetty.xml`
- `/opt/hp/agm/java/jre/lib/security/cacerts`(SSL/TLS 設定のみ)
- `server.keystore`(SSL/TLS 設定の場合のみ、必要に応じて)

注意: 2.40 より前のバージョンからアップグレードしている場合: 以前のリリースで `wrapper.conf` ファイルの `wrapper.java.maxmemory` プロパティを変更した場合, この変更を `/opt/hp/agm/conf/wrapper-install.conf` ファイルに手動で移行してください。

7. Agile Manager システム・ファイルでの共有ネットワーク・ユーザの変更 (オプション)

共有ネットワークユーザに `agm1-user` という名前を付けることをお勧めします。

このユーザに異なる名前を使用する場合は, Agile Manager を設定する前に**すべてのノードのシステム・ファイル**を変更します。詳細については, 「[サービス・ユーザの名前の変更 \(オプション\)](#)」(28ページ)を参照してください。

8. 設定ウィザードの実行および設定の完了

詳細については, 「[設定ウィザードの実行](#)」(28ページ)を参照してください。

次の設定を除いて, 前のインストールで使用したものと**同じ設定の詳細**を使用します。

[**System Administration Database Schema (システム管理データベーススキーマ)**] 画面で, [**Upgrade production (運用システムのアップグレード)**] を選択します。詳細については, 「[Upgrade production \(運用システムのアップグレード\)](#)」(33ページ)を参照してください。

注意: 運用システムをアップグレードする前に別のシステムでアップグレードをテストする場合は, このオプションを選択しないでください。アップグレードをテストする場合は, 「[ステージング環境を使用した Agile Manager のアップグレード](#)」(47ページ)から始めてください。

注: 新しいアップグレードしたスキーマの名前をメモします。他のノードをアップグレードするときにこの名前が必要になります。

最初のノード以外のすべてのノードで実行する手順

- [**Max DB Connections (最大 DB 接続数)**] の値を変更してある場合は, 現在の値を記録しておきます。アップグレードでは標準設定値が復元されるため, 変更はすべて失われます。
この値は, Agile Manager システム管理サイトの [**Servers (サーバ)**] > [**Application (アプリケーション)**] タブで, 各サーバに対して定義されています。詳細については, 「[最大データベース接続数の設定](#)」(80ページ)を参照してください。
- 新しいバージョンの Agile Manager をインストールします。**
インストール・パッケージにある rpm ファイルとキー・ファイルを `tmp` フォルダなどのアクセス可能なフォルダにコピーします。
rpm ファイルが格納されているディレクトリに移動し (`cd /home` など), 次のいずれかを実行します。

root ユーザとして	<pre>rpm --import keys/*.pub rpm -U AGM-ONPREM<バージョン番号> .rpm</pre>
sudo ユーザとして	<pre>sudo rpm --import keys/*.pub sudo rpm -U AGM-ONPREM<バージョン番号> .rpm</pre>

インストール・ファイルは、`/opt/hp/agm` 下にデプロイされます。

3. 最初のノードから他のすべてのノードへのファイルのコピー

最初のノードから他のすべてのノードの同じ場所に次のファイルをコピーします。

- `/opt/hp/agm/server/conf/jetty.xml`
- `/opt/hp/agm/java/jre/lib/security/cacerts`(SSL/TLS 設定のみ)
- `server.keystore`(SSL/TLS 設定の場合のみ、必要に応じて)。このファイルを `jetty.xml` ファイルで定義されている場所にコピーします。
- `/opt/hp/agm/conf/qcConfigFile.properties`
- `/opt/hp/agm/conf/wrapper-install.conf`
- `/opt/hp/agm/conf/wrapper-user.conf`

4. 設定ウィザードの実行および設定の完了

詳細については、「[設定ウィザードの実行](#)」(28ページ)を参照してください。

次の設定を除いて、前のインストールで使用したものと同一設定の詳細を使用します。

[**System Administration Database Schema**(システム管理データベーススキーマ)]画面で、[**Connect to an existing schema/second node**(既存のスキーマ/2番目のノードに接続)]を選択します。

詳細については、「[Connect to existing schema/second node](#)(既存のスキーマ/2番目のノードに接続)」(32ページ)を参照してください。

5. 最大 DB 接続数の更新(オプション)

以前に[**Max DB Connections**(最大 DB 接続数)]の値を変更した場合は、アップグレード後に標準設定値が復元されます。

Agile Manager システム管理サイトにログインし、[**Servers**(サーバ)] > [**Application**(アプリケーション)]ページで、クラスタ内の各サーバに対して値を変更します。

詳細については、「[最大データベース接続数の設定](#)」(80ページ)を参照してください。

注: アップグレードの完了後に、通知電子メール用の電子メールサーバを設定する場合は、それらの電子メールで使用する外部 URL も設定します。

詳細については、「[電子メールで使用する外部 URL を設定します。](#)」(85ページ)を参照してください。

基本的な運用システムのアップグレード

本項では、基本的なスタンドアロン構成で Agile Manager をアップグレードする方法について説明します。

- クラスタ化されたシステムのアップグレードの詳細については、「[クラスタ化されたシステムのアップグレード](#)」(40ページ)を参照してください。
- ステージング環境として使用するブランクシステムをまず作成してアップグレードする場合は、「[ステージング環境を使用した Agile Manager のアップグレード](#)」(47ページ)を参照してください。

注: アップグレード中にユーザが Agile Manager にログインしていた場合、アップグレードが完了してから作業を続行するには、ブラウザの表示の更新が必要になる可能性があります。

1. システム要件とサーバの前提条件の確認

前のバージョン以降に変更があった場合、サーバ・ノードが Linux と Oracle サーバの前提条件を満たしていることを確認してください。詳細については、次を参照してください。

- 「システム要件」(13ページ)
- 「Linux の前提条件」(17ページ)
- 「Oracle の前提条件」(19ページ)

2. Agile Manager の停止

Agile Manager サービスを停止します。/opt/hp/agm/wrapper/HPALM stop

注: SUSE 環境にインストールされた Agile Manager 2.20 からアップグレードした場合、サービスを開始または停止した後に、存在しないフォルダに関する警告が表示される場合があります。この警告は無視してかまいません。

3. データのバックアップ

- アップグレードを行う前にデータベース・スキーマとサイト・リポジトリをバックアップします。

注意: サイトをバックアップする前に、非アクティブにしておくことを強くお勧めします。

サイトがまだアクティブな状態で、バックアップを実行する必要がある場合、最初にデータベースをバックアップしてから、ファイル・システムをバックアップしてください。データベースをバックアップしてから、可能な限りすみやかにファイル・システムをバックアップすることもお勧めします。

- 次のシステム・ファイルをバックアップします。
 - /opt/hp/agm/server/conf/jetty.xml
 - /opt/hp/agm/java/jre/lib/security/cacerts(SSL/TLS 設定のみ)
- [Max DB Connections(最大 DB 接続数)]の値を変更してある場合は、現在の値を記録しておきます。アップグレードでは標準設定値が復元されるため、変更はすべて失われます。この値は、Agile Manager システム管理サイトの[Servers(サーバ)] > [Application(アプリケーション)]タブで定義されています。詳細については、「最大データベース接続数の設定」(80ページ)を参照してください。

4. SSL/TLS を設定している場合は、server.keystore ファイルの特定や移動を行います。

jetty.xml ファイルを開き、server.keystore が保存される場所を決定します。

このファイルが /opt/hp/agm ディレクトリ、またはそのサブディレクトリに保存されている場合は、server.keystore ファイルをバックアップします。

5. 新しいバージョンの Agile Manager をインストールします。

インストール・パッケージにある rpm ファイルとキー・ファイルを tmp フォルダなどのアクセス可能なフォル

ダにコピーします。

rpm ファイルが格納されているディレクトリに移動し(cd /home など), 次のいずれかを実行します。

root ユーザとして	rpm --import keys/*.pub rpm -U AGM-ONPREM<バージョン番号> .rpm
sudo ユーザとして	sudo rpm --import keys/*.pub sudo rpm -U AGM-ONPREM<バージョン番号> .rpm

インストール・ファイルは、/opt/hp/agm 下にデプロイされます。

6. agmuser ユーザの削除 (オプション)

以前に **agmuser** という名前の単純なユーザを作成し、特別なアクセス許可なしで Agile Manager を実行した場合は、ここでこのユーザを削除できます。現在のインストールによって、サービス・ユーザとして使用されるユーザが **agml-user** という名前で作成されます。

このユーザに異なる名前を使用する場合、あるいは既存のユーザを Agile Manager に使用させる場合は、インストールおよび設定中に適切な手順に従います。詳細については、「[サービス・ユーザの名前の変更 \(オプション\)](#)」(28ページ)を参照してください。

7. バックアップ・ファイルの復元

以前にバックアップした次のファイルを復元します。

- /opt/hp/agm/server/conf/jetty.xml
- /opt/hp/agm/java/jre/lib/security/cacerts (SSL/TLS 設定のみ)
- server.keystore (SSL/TLS 設定の場合のみ、必要に応じて)

注意: 2.40 より前のバージョンからアップグレードしている場合: 以前のリリースで **wrapper.conf** ファイルの **wrapper.java.maxmemory** プロパティを変更した場合、この変更を /opt/hp/agm/conf/wrapper-install.conf ファイルに手動で移行してください。

8. 設定ウィザードの実行および設定の完了

詳細については、「[設定ウィザードの実行](#)」(28ページ)を参照してください。

設定ウィザードを実行する場合は、次の例外を除き、前回のインストールと同じ設定詳細を使用します。

- [**System Administration Database Schema (システム管理データベーススキーマ)**] 画面で、[**Upgrade production (運用システムのアップグレード)**] を選択します。詳細については、「[Upgrade production \(運用システムのアップグレード\)](#)」(33ページ)を参照してください。

注意: 運用システムをアップグレードする前に別のシステムでアップグレードをテストする場合は、このオプションを選択しないでください。アップグレードをテストする場合は、「[ステージング環境を使用した Agile Manager のアップグレード](#)」(47ページ)を参照してください。

- 以前にアプリケーションのポートを 1024 より小さい番号に変更した場合、Linux で 1024 より上位のポート番号を使用するにはセキュリティ保護されたプロセスが必要であることを注意してください。

このポート番号を変更するか、システム管理者に問い合わせるプロセスの権限を変更し、小さい番号のポートを使用してください。詳細については、「[アプリケーション・サーバのポートが空いていることの確認](#)」(37ページ)を参照してください。

9. 最大 DB 接続数の更新(オプション)

以前に[**Max DB Connections(最大 DB 接続数)**]の値を変更した場合は、アップグレード後に標準設定値が復元されます。Agile Manager システム管理サイトにログインし、[**Servers(サーバ)**] > [**Application(アプリケーション)**] ページで値を変更します。

詳細については、「[最大データベース接続数の設定](#)」(80ページ)を参照してください。

ステージング環境を使用した Agile Manager のアップグレード

Agile Manager システムをアップグレードする際には、まずステージング環境として使用するブランクシステムを新しいバージョンで作成することをお勧めします。

このためには、別のアプリケーション・サーバが必要です。別のデータベース・サーバを使用することもできます。

1. システム管理スキーマとサイト・スキーマの両方を、ステージング・データベース・サーバに手動でコピーします。

これらのスキーマの名前は、システム管理サイトの[**Servers(サーバ)**] > [**Database(データベース)**] タブの[**General Information(一般情報)**]の下にあります。詳細については、「[データベースの設定](#)」(83ページ)を参照してください。

2. ステージング・アプリケーション・サーバで、Agile Manager をデプロイします。詳細については、「[インストール・ファイルのデプロイ](#)」(28ページ)を参照してください。
3. インストール時に、Agile Manager サービスを実行するための **agml-user** という名前のユーザが作成されます。

このユーザに異なる名前を使用する場合、あるいは既存のユーザを Agile Manager に使用させる場合は、インストールおよび設定中に適切な手順に従います。詳細については、「[サービス・ユーザの名前の変更\(オプション\)](#)」(28ページ)を参照してください。

4. リポジトリをステージング・アプリケーション・サーバに手動でコピーします。

リポジトリのパスは、システム管理サイトの[**Servers(サーバ)**] > [**Database(データベース)**] タブの[**General Information(一般情報)**]の下にあります。詳細については、「[データベースの設定](#)」(83ページ)を参照してください。

ステージング・アプリケーション・サーバで、`/opt/hp/agm/conf/qcConfigFile.properties` ファイルの `repositoryPath` プロパティが、リポジトリの正しい場所を指していることを確認します。

`qcConfigFile.properties` ファイルにこのプロパティが存在しない場合、手動で追加し、正しい場所を設定します。

5. ステージング・アプリケーション・サーバで、設定ウィザードを実行します。詳細については、「[設定ウィザードの実行](#)」(28ページ)を参照してください。

設定ウィザードの実行中は、次の値を除いて標準設定値をそのまま使用します。

ウィザード画面	入力または選択する値
[Database Connection(データベース接続)]および[Database Administrator Login(データベース管理者ログイン)]	ステージング・データベース・サーバの詳細を入力します。これらは元の値と同じ場合も異なる場合もあります。 詳細については、「データベース・パラメータの入力」(30ページ)および「データベース管理者のログイン情報の入力」(31ページ)を参照してください。
System Administration Database Schema(システム管理データベース・スキーマ)	[Create and upgrade staging(ステージングの作成とアップグレード)]を選択します。 詳細については、「Create and upgrade staging(ステージングの作成とアップグレード)」(33ページ)を参照してください。

- 手順に従って設定ウィザードを完了し、Agile Manager を起動します。詳細については、「Agile Manager サービスの起動/停止」(50ページ)を参照してください。

注: このプロセスが終了すると、Agile Manager は標準設定のポート(8080)を使用します。必要な場合、Agile Managerを起動する前に、「アプリケーション・サーバのポート番号の変更」(74ページ)の手順を実行します。

- システム管理サイトにアクセスし、「Restore Site Schema(サイトスキーマの復元)」のオプションを使用して、コピーしたサイト・スキーマにステージング環境を接続します。詳細については、「サイト・スキーマの復元」(84ページ)を参照してください。

別の場所へのインストールのデプロイ

インストール・ファイルのデプロイは、Agile Manager のインストールまたはアップグレードの最初のステップです。

標準設定では、インストール・ファイルは、`/opt/hp/agm` の下にデプロイされます。これは推奨される場所です。

別の場所にデプロイする必要がある場合は、`--prefix` オプションで場所を指定します。

例:

```
rpm -i --prefix /opt/MyInstallPath Agile-Manager-ONPREM- <バージョン番号> .rpm
```

インストール・ファイルは、指定したフォルダの下に `agm` フォルダにデプロイされます。

詳細については、「インストール・ファイルのデプロイ」(28ページ)を参照してください。

注意: Agile Manager をアップグレードする場合、常に前のインストールと同じフォルダにアップグ



レードしてください。例: `rpm -U --prefix /opt/MyInstallPath Agile-Manager-ONPREM-<バージョン番号>.rpm`

Agile Manager サービスの起動/停止

アクション	コマンド (root または sudo で)
サービスの起動	root で: /opt/hp/agm/wrapper/HPALM start sudo で: sudo /opt/hp/agm/wrapper/HPALM start
サービスの停止	root で: /opt/hp/agm/wrapper/HPALM stop sudo で: sudo /opt/hp/agm/wrapper/HPALM stop
サービスの再起動	root で: /opt/hp/agm/wrapper/HPALM restart sudo で: sudo /opt/hp/agm/wrapper/HPALM restart

Agile Manager と sudo 権限の詳細については、[「Linux の前提条件」\(17ページ\)](#)を参照してください。

注:

- サーバを初めて起動したときに、Agile Manager 用の新しいデータベース・スキーマが作成されます。このスキーマの名前は、**t1_sa_main_db** です。
- SUSE 環境にインストールされた Agile Manager 2.20 からアップグレードした場合、サービスを開始または停止した後に、存在しないフォルダに関する警告が表示される場合があります。この警告は無視してかまいません。

リブート後に Agile Manager サービスを起動

標準設定では、Agile Manager はシステムのブート時に起動します。

この登録を削除するには、次のコマンドを実行します。	root で: /opt/hp/agm/wrapper/HPALM remove sudo で: sudo /opt/hp/agm/wrapper/HPALM remove
この登録に戻すには、次のコマンドを実行します。	root で: /opt/hp/agm/wrapper/HPALM install sudo で: sudo /opt/hp/agm/wrapper/HPALM install

Agile Manager へのログイン

インストールが完了したら、Agile Manager 管理サイトを使用して Agile Manager システムを管理します。Agile Manager で直接サイトとユーザを管理します。

Agile Manager	http://<サーバ>:<ポート>/agm/login
Agile Manager 管理サイト	http://<サーバ>:<ポート>/agm/admin

リバース・プロキシ経由で Agile Manager にアクセスする場合は、サーバ・アドレスとしてプロキシ・アドレスを使用します。詳細については、「[Apache Web サーバの統合 \(例\)](#)」(70ページ)を参照してください。

Agile Manager でインストールされる標準設定のユーザは、sa ユーザです。インストール中に sa ユーザのパスワードを定義しました(「[システム管理者ログイン情報の入力](#)」(36ページ)を参照)。

Agile Manager の豊富な機能セットを十分に活用するには、ヘルプセンタ(ヘッダで②をクリック)にアクセスするか、[Hewlett Packard Enterprise Software forums and blogs](#) でディスカッションに参加します。

注:

- Agile Manager ヘルプセンターは、Agile Manager と一緒にインストールされます。Agile Manager 内からヘルプにアクセスするには、[ヘルプ]②メニューを使用するか、次のパスで開きます。
http://<サーバ>:<ポート>/agm/agmdocs/Default.htm
- アップグレードを実行していて、設定ウィザードで[**Create and upgrade staging(ステージングの作成とアップグレード)**]を選択した場合は、Agile Manager にはアクセスできません。先に「[Agile Manager のインストール](#)」(27ページ)を実行してください。

システムのセキュリティ保護

Agile Manager プラットフォームは、セキュア・アーキテクチャの構成要素になるように設計されていて、潜在的なセキュリティ脅威に対処することができます。

本章では、Agile Manager デプロイメントのセキュリティを強化するベスト・プラクティスと推奨される手順について説明します。

Agile Manager にアクセスするには、サポートされている最新バージョンのブラウザの使用を強くお勧めします。これにより、古いバージョンのブラウザでの既知のセキュリティ上の欠陥を回避できます。サポートされるブラウザおよびブラウザのバージョンのリストについては、『Agile Manager ユーザーズ・ガイド』を参照してください。

注: エンタープライズのセキュリティ要件は、絶えず進化しています。本章で扱われていない追加のセキュリティ要件がある場合は、本ガイドの改訂版に追加するべき要件についてご提案ください。

セキュリティ問題の報告: <https://h41268.www4.hp.com/live/index.aspx?qid=11503>

最新の Agile Manager セキュリティ情報へのアクセス/セキュリティ・アラートの登録:
<https://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive?ac.admitted=1389784040189.876444892.199480143>

本章の内容

- 「デプロイメントのセキュリティ保護」(53ページ)
- 「添付ファイルおよびダウンロードのセキュリティ保護」(54ページ)
- 「アプリケーション・サーバのセキュリティ保護」(55ページ)
- 「ネットワークと通信のセキュリティ保護」(57ページ)
- 「システム管理のセキュリティ保護」(59ページ)
- 「ユーザ認証のセキュリティ保護」(60ページ)
- 「ユーザ許可のセキュリティ保護」(60ページ)
- 「データの整合性」(63ページ)
- 「データ暗号化」(64ページ)
- 「データ・ロギング」(65ページ)
- 「Apache Web サーバの統合 (例)」(70ページ)

さらに、アプリケーション・サーバ、LDAP サーバ、および SMTP サーバでの SSL/TLS 接続を設定できません。データベース・サーバへのセキュア接続はサポートされていません。

詳細については、次を参照してください。

- 「アプリケーション・サーバでの SSL/TLS 設定」(66ページ)
- 「LDAP サーバでの SSL/TLS 設定」(87ページ)
- 「SMTP サーバで SSL/TLS を設定します(オプション)。」(85ページ)

標準設定では、Agile Manager をインストールするデータベース・ユーザは、Oracle で特定の管理タスクを実行するのに十分な権限を持っている必要があります。詳細については、「[管理ユーザ権限の付与](#)」(20ページ)を参照してください。少ない権限で Agile Manager をインストールするには、HP カスタマ・サポートまでお問い合わせください。

デプロイメントのセキュリティ保護

Agile Manager は、Java 2 Enterprise Edition (J2EE) テクノロジーに基づくエンタープライズ規模のアプリケーションです。J2EE テクノロジーは、エンタープライズ・アプリケーションのデザイン、開発、アセンブリ、およびデプロイメントに対するコンポーネントベースのアプローチを提供します。

Agile Manager は、インストール中に Agile Manager が作成した非ルート・ユーザを使用して実行されます。標準設定では、このユーザは、**agml-user** という名前です。Agile Manager サービスのみを実行する限られた権限が与えられています。ユーザ名は変更でき、新規ユーザを作成せずに既存のユーザを使用するように Agile Manager に指示することもできます。

Agile Manager は、基本設定またはクラスタ設定で設定できます。上記どちらの設定のセキュリティも、次の方法で強化してください。

デプロイメントのセキュリティ保護方法	
SSL/TLS	<p>基本設定 : Agile Manager Jetty の SSL/TLS を有効にし、必須にします。</p> <p>クラスタ設定 : ロード・バランサ上の Agile Manager 仮想 IP に対して SSL/TLS を必須にします。</p> <p>詳細については、次を参照してください。</p> <ul style="list-style-type: none">「アプリケーション・サーバでの SSL/TLS 設定」(66ページ)「LDAP サーバでの SSL/TLS 設定」(87ページ)「電子メール通知サーバの設定」(85ページ) <p>注 : データベース・サーバへのセキュア接続はサポートされていません。</p>
リバース・プロキシ	<p>Agile Manager サーバの前面にリバース・プロキシをインストールし、リバース・プロキシ・サーバで SSL/TLS を設定します。</p> <p>詳細については、「リバース・プロキシ・アーキテクチャ」(58ページ)および「Apache Web サーバの統合 (例)」(70ページ)を参照してください。</p> <p>Apache とのすべての通信で SSL/TLS を有効にする方法の詳細については、http://httpd.apache.org/docs/current/ssl/ssl_howto.html (英語サイト) を参照してください。</p> <p>注 : リバース・プロキシを設定する場合は、Agile Manager から送信される電子メールで使用する外部 URL も設定します。詳細については、「電子メールで使用する外部 URL を設定します。」(85ページ)を参照してください。</p>

デプロイメントのセキュリティ保護方法

ファイアウォール	クライアントとその他の Agile Manager コンポーネントとの間でファイアウォールを使用します。 アプリケーション・サーバで、Agile Manager が使用する HTTP ポート (8080) または HTTPS ポート (8443) 以外の、すべての着信トラフィックへのアクセスをブロックします。
----------	--

参照情報: [「ネットワークと通信のセキュリティ保護」\(57ページ\)](#)

一般的な考慮事項とベスト・プラクティス

- アプリケーション、Exchange、データベース、および LDAP の各サーバ間の信頼境界を十分にレビューし、コンポーネント間のホップ数を最小化します。また、SSL/TLS を使用して、このような境界をまたがる位置にあるサーバへのアクセスのセキュリティを確保することをお勧めします。
- Agile Manager デプロイメント・コンポーネント間にファイアウォールがある場合、ベンダの推奨事項に従って適切な設定を行います。
- クライアントとサーバ上で信頼されたルート証明機関の証明書更新を定期的に行い、デジタル・コード署名で使用される発行者証明書が信頼できることを確認します。

注: 標準設定では、Agile Manager アプリケーション・サーバでは SSL/TLS が有効になっていません。ロード・バランサまたはリバース・プロキシを問わず、フロント・エンド・サーバで SSL/TLS が必須になるように設定することをお勧めします。

現時点では、Agile Manager からデータベース・サーバへのセキュアなチャネルはサポートされていません。

添付ファイルおよびダウンロードのセキュリティ保護

このトピックでは、次の内容について説明します。

- [「添付ファイルのセキュリティ保護」\(54ページ\)](#)
- [「ダウンロードのセキュリティ保護」\(55ページ\)](#)

添付ファイルのセキュリティ保護

Agile Manager 管理サイトを使用して、ユーザがエンティティ添付としてアップロードできるファイルのタイプとファイル・サイズを制限します。管理サイトで、**[Configuration(設定)] > [General(一般)]** ページを参照し、次のオプションを定義します。

- **Maximum upload file size (MB)(最大アップロード・ファイル・サイズ(MB))**
- **Maximum aggregated size for all attachments (MB)(すべての添付ファイルの最大合計サイズ(MB))**
- **Blocked file extensions files types(ブロックするファイルの拡張子)**

詳細については、「[添付ファイル設定の定義](#)」(92ページ)を参照してください。



注意:

添付ファイルには危険なコンテンツが含まれている可能性があり、ダウンロードして開く際には注意が必要です。

Agile Manager のサーバ・マシンとクライアント・マシンの両方に割り当てられたファイル・ストレージに対して、ウイルス対策を導入することを強く推奨します。

ダウンロードのセキュリティ保護

NextGen Synchronizer の Integration Bridge は、Agile Manager と ALM の同期をサポートします。

初めて Integration Bridge をインストールする場合、Agile Manager から手動でダウンロードします。その後のアップグレードは自動で行われ、ブリッジのダウンロード、認証の検証、およびインストールのアップグレードが行われます。

詳細については、『Agile Manager 同期ガイド』を参照してください。

社内のルールで自動ダウンロードが禁止されている場合、OPB_ENABLE_AUTO_UPGRADE パラメータを N に設定することで、自動アップグレードを無効にできます。詳細については、「[詳細パラメータの設定](#)」(93ページ)を参照してください。

この場合、Agile Manager の新規バージョンに Integration Bridge へのアップグレードが含まれていれば、既存のすべての同期ブリッジは、手動でアップグレードされるまで、実行が停止されます。

アプリケーション・サーバのセキュリティ保護

Agile Manager のインストール・プロセスでは、最低限の権限を持つ **agml-user** という名前のローカル・ユーザが作成されます。このユーザは、サーバにはログインできないユーザで、セキュリティ目的でのみ使用されます。

- Agile Manager サービスは、**agml-user** ユーザの権限を使用して実行します。
- **agml-user** は、最低限のディレクトリ・セットの所有者で、サーバの運用に必要です。他のすべてのディレクトリの所有者は **root** ユーザです。

その他の手順

アプリケーション・サーバのセキュリティを保護するために、次の追加手順を実行します。

- Agile Manager アプリケーション・サーバで SSL/TLS を設定する場合、アクセス制限のある非公開のディレクトリにキーストアを保持します。Java キーストアはパスワードで保護されていますが、パスワードが標準設定値の **changeit** から変更されていない限り、脆弱性があります。詳細については、「[アプリケーション・サーバでの SSL/TLS 設定](#)」(66ページ)を参照してください。
- **jetty.xml** ファイルに入力されるパスワードを、常にわかりにくくします。詳細については、<http://www.eclipse.org/jetty/documentation/current/configuring-security-secure-passwords.html> (英語サイト)を参照してください。
- 標準設定のパスワード(標準設定の **sa** ユーザ・パスワードや機密データ・パスフレーズなど)の変更を求められたら、必ずそのパスワードを変更します。
- 電子メール・サーバを設定する場合は、Agile Manager が、Agile Manager へのリンクを含む電子メールをユーザに送信します。これらの電子メールでは、実際のマシン名が公開される場合があります。このような電子メールの例として、ユーザが Agile Manager から直接別のユーザにエンティティを送信する場合や、新しいユーザがログインを促すようこそメールを受信する場合などがあります。実際のマシン名を隠すには、システム管理サイトの[**Advanced Parameters (詳細パラメータ)**]ページで **EXTERNAL_BASE_URL** 詳細パラメータを追加します。電子メールに表示する外部 URL の値を定義します。

例 : `http://my-load-balancer-domain:8080/`

注: URL の末尾に `agm` を追加しないでください。

詳細については、「[電子メール通知サーバの設定](#)」(85ページ)および「[詳細パラメータの設定](#)」(93ページ)を参照してください。

アプリケーション・サーバのセキュリティに関する FAQ

質問	回答
アプリケーション・リソースは、アプリケーション管理者のみがアプリケーション・リソース設定ファイルの変更を可能にする権限セットで保護されていますか?	はい。Agile Manager アプリケーション・サーバ・マシン上の特定のディレクトリにアクセスできる権限を持つユーザのみが、Agile Manager の設定ファイルを変更できません。
Agile Manager では、設定ファイルがユーザ・データと同じディレクトリに格納されませんか?	管理者は、Agile Manager 管理サイトを使用して、リポジトリとログ・ファイルの場所を変更し、ユーザ・データと設定ファイルが同じ場所に保存されるのを回避できます。 [Servers(サーバ)] > [Database(データベース)] ページのリポジトリ・パス、および [Servers(サーバ)] > [Application(アプリケーション)] ページのログ・ファイル・パスを変更します。 詳細については、「 データベースの設定 」(83ページ)および「 アプリケーション・サーバの設定 」(80ページ)を参照してください。

質問	回答
Agile Manager は、適切な操作には不要な権限で実行しませんか？	はい。権限は常時レビューされ、必要な権限のみが要求されます。

ネットワークと通信のセキュリティ保護

Agile Manager システム・コンポーネント間の通信のセキュリティを保護するには、次の対策をお勧めします。

- [「システム・コンポーネントの分離とセキュリティ保護」\(57ページ\)](#)
- [「システム・コンポーネントの分離とセキュリティ保護」\(57ページ\)](#)
- [「システム・コンポーネントの分離とセキュリティ保護」\(57ページ\)](#)
- [「システム・コンポーネントの分離とセキュリティ保護」\(57ページ\)](#)
- [「リバース・プロキシを使用する利点 : 」\(58ページ\)](#)
- [「セキュアな通信チャネル」\(59ページ\)](#)

システム・コンポーネントの分離とセキュリティ保護

- Web サーバ、アプリケーション・サーバ、ロード・バランサ、およびデータベース・サーバを分離します。
- LDAP サーバと Oracle データベースのセキュリティ・ガイドラインに従います。
- 低い権限で SNMP サーバと SMTP サーバを実行します。

システム・コンポーネント間での SSL/TLS の使用

SSL/TLS プロトコルは、クライアントとサーバ間の接続のセキュリティを確保します。セキュア接続を必要とする URL は、HTTP ではなく、HTTPS で始まります。Agile Manager では SSLv3 と TLSv1 がサポートされています。

詳細については、[「アプリケーション・サーバでの SSL/TLS 設定」\(66ページ\)](#)を参照してください。

注：標準設定では、Agile Manager アプリケーション・サーバでは SSL/TLS が有効になっていません。ロード・バランサまたはリバース・プロキシを問わず、フロント・エンド・サーバで SSL/TLS が必須になるように設定することをお勧めします。

アプリケーション・サーバとデータベース・サーバが同じファイアウォールの背後にない場合、SSL を使用して 2 台のサーバ間の通信のセキュリティを保護できます。

データベース・サーバ側の操作 (詳細については、Oracle ドキュメントを参照) :

1. TCPS ポートを開くようにデータベースを設定します。
2. サーバとクライアントの証明書を作成します。

Agile Manager 側の操作 :

1. クライアント証明書 (Wallet と呼ばれる) を Agile Manager コンピュータ上の安全な場所にコピーします。
2. Agile Manager のインストール中に、データベース・パラメータを入力する場合、クライアント証明書へのパスと証明書のパスワードを含めます。詳細については、「[データベース・パラメータの入力](#)」(30ページ)を参照してください。

ファイアウォールを使用する DMZ アーキテクチャ

DMZ アーキテクチャでは、追加ネットワークがシステムに追加され、内部ネットワークを外部ネットワークから分離できます。ファイアウォールを使用して、Agile Manager のクライアントとサーバ間を完全に分離し、直接アクセスを回避します。

一般的な DMZ 実装がいくつかあります。このガイドでは、DMZ とリバース・プロキシをバックツーバックのトポロジ環境で実装する方法について説明します。

注: アプリケーション・サーバでファイアウォールを使用する場合、着信トラフィック用に指定されたポート (jetty ポート) を開いたままにしておく必要があります。標準設定ではこのポートは **8080** で、セキュアな接続を使用している場合は **8443** です。

リバース・プロキシ・アーキテクチャ

Agile Manager は、リバース・プロキシとセキュアなリバース・プロキシ・アーキテクチャを完全にサポートします。

リバース・プロキシは、クライアントと Web サーバ間に配置されたサーバです。クライアント・マシンにとっては、リバース・プロキシは、クライアントの HTTP(S) 要求に対応する標準の Web サーバのようなもので、追加の設定は不要です。

クライアントは Web コンテンツ要求をリバース・プロキシに送信し、リバース・プロキシはそれを Web サーバに転送します。Web サーバは、リバース・プロキシ経由で順番に応答します。ただし、その応答は、Web サーバからでなくリバース・プロキシから送信されたかのようにクライアントには見えます。

リバース・プロキシは、外部クライアントとのすべての通信を通じて要塞ホストとして機能し、外部クライアントからアドレスできる唯一のマシンであり、残りの内部ネットワークを覆い隠します。

リバース・プロキシの設定方法の例については、「[Apache Web サーバの統合 \(例\)](#)」(70ページ)を参照してください。

リバース・プロキシを使用する利点 :

- アプリケーション・サーバを内部ネットワークの別のマシン上に配置できます。
- DMZ プロトコルは変換されません。着信と発信のプロトコルが同一です。ヘッダの変更だけが行われます。
- リバース・プロキシへの http(s) アクセスのみが許可されます。これにより、ステートフル・パケット・インスペクション・ファイアウォールによる通信保護が強化されます。
- リバース・プロキシへの http(s) アクセスのみが許可されます。これにより、ステートフル・パケット・インスペクション・ファイアウォールによる通信保護が強化されます。
- リバース・プロキシ上のリダイレクト要求の静的かつ制限付きセットを定義できます。
- 認証方法や暗号化など、ほとんどの Web サーバ・セキュリティ機能にアクセスできます。
- サーバ IP アドレスおよび内部ネットワーク・アーキテクチャをスクリーニングできます。

- NAT ファイアウォールがサポートされます。
- ファイアウォール内で開いている必要があるポート数が最小限で済みます。
- メンテナンスが容易です。必要に応じてパッチをリバース・プロキシに追加できます。
- Web サーバにアクセスできるクライアントは、リバース・プロキシのみです。
- リバース・プロキシは、他の要塞ソリューションに比べて高いパフォーマンスを提供します。

セキュアな通信チャネル

Agile Manager は次のセキュア・チャネルをサポートします。

- **クライアント/アプリケーション・サーバ**: 一般的に、信頼はクライアント上でのみ必要になります。これは、Agile Manager アプリケーション・サーバのサーバ証明書を発行した機関に対する信頼です。
- **アプリケーション・サーバ/LDAP サーバ**: Agile Manager 管理サイトの **[Configuration(設定)] > [Authentication(認証)]** ページで LDAP 設定を実行します。詳細については、[「LDAP 認証の設定」\(86ページ\)](#)を参照してください。
- **アプリケーション・サーバ/メール・サーバ**: メール・サーバを定義する際には、セキュアなポートを指定します。
- **リバース・プロキシまたはロード・バランサ/アプリケーション・サーバ**: SSL/TLS を使用して Agile Manager アプリケーション・サーバを設定します。

リバース・プロキシまたはロード・バランサ上で、Agile Manager サーバへのセキュアな接続 (<https://<サーバ>:8443/agm> など)を使用します。

システム管理のセキュリティ保護

Agile Manager サイトは、Agile Manager 管理サイトを使用して管理します。

- システム管理者のパスワードは、初期セットアップ時に([「システム管理者ログイン情報の入力」\(36ページ\)](#)を参照)、またはセットアップ後に Agile Manager 管理サイトで変更し、管理サイトのセキュリティを確保します。管理サイトを使用して、他のシステム管理者を指定します。
システム管理者とパスワードを管理するには、**[Configuration(設定)] > [User(ユーザ)]** 管理ページを参照してください。システム管理者には強力なパスワードを使用します。詳細については、[「ユーザ認証のセキュリティ保護」\(60ページ\)](#)を参照してください。
- Agile Manager 設定領域 (**[Site(サイト)] > [Users(ユーザ)]**) でユーザ権限を変更することで、サイトのカスタマイズを制限します。詳細については、Agile Manager ヘルプセンターを参照してください。
- ユーザ・アクションをデバッグするには、ログ・レベルを **[Debug(デバッグ)]** に設定します。デバッグを終了したら、ログ・レベルを必ず前の値に戻してください。詳細については、Agile Manager 管理サイト (**[Servers(サーバ)] > [Application(アプリケーション)]**) および [「アプリケーション・サーバの設定」\(80ページ\)](#)を参照してください。
- ライセンスを更新したら、ライセンス・ファイルをセキュアな場所に格納して、不正アクセスを防ぎます。詳細については、[「ユーザ・ライセンスの更新」\(89ページ\)](#)を参照してください。

詳細については、[「Agile Manager へのログイン」\(51ページ\)](#)および [「Agile Manager のシステム管理」\(79ページ\)](#)を参照してください。

ユーザ認証のセキュリティ保護

Agile Manager は、次の認証方法をサポートします。

- **Create users directly in Agile Manager(Agile Manager で直接ユーザを作成)**:このオプションは、セキュリティ保護されていません。セキュアなアクセスには、外部 LDAP 認証を使用してください。
- **LDAP authentication(LDAP 認証)**:LDAP3 をサポートしている任意の LDAP プロバイダからユーザをインポートします。

認証の設定は、Agile Manager 管理サイト([Configuration(設定)] > [Authentication(認証)])で行います。Agile Manager 設定領域([Site(サイト)] > [Users(ユーザ)])で、サイト管理者がユーザを追加またはインポートします。

詳細については、「[Agile Manager へのログイン](#)」(51ページ)、「[ユーザ認証の設定](#)」(86ページ)、および Agile Manager ヘルプセンターを参照してください。

ユーザ認証のセキュリティ保護に関する FAQ

質問	回答
Agile Manager では、企業ポリシーに準拠するアカウント・パスワードを要求できますか?	LDAP 認証は、パスワード・ポリシーのサポートを保証するソリューションであり、お勧めします。
Agile Manager はどの LDAP プロバイダをサポートしていますか?	Agile Manager は、LDAP3 プロトコルをサポートしている任意の LDAP プロバイダで動作します。
セッション管理とセッション・ロックアウト機構について説明してください。 検証が失敗した場合、Agile Manager はどのように応答しますか?ユーザはロックアウトされますか?設定できますか?	Agile Manager は、セッションをユーザ・レベルで管理します。無操作状態でのタイムアウトは、システム管理者が Agile Manager 管理サイト([Site Configuration(サイト設定)] > [General(一般)])を使用して設定できます。 LDAP 設定のみ:一連の不正なログインを試行したユーザは、Agile Manager から 30 分間ロックアウトされます。

ユーザ許可のセキュリティ保護

Agile Manager リソースへのユーザ・アクセスは、ユーザのロールと権限に基づいて許可されます。

Agile Manager にアクセスする前に、ユーザを Agile Manager に追加またはインポートして、アクティブにする必要があります。利用可能なライセンスがある限り、ユーザは自動的にアクティブになります。

ユーザには、次の任意のロールを割り当てることができます。

ロール名	説明	設定場所
System Administrator (システム管理者)	<p>Agile Manager オンプレミス・システム管理サイトにアクセスして読み取りと書き込みが行えます。</p> <p>標準設定では、Agile Manager アプリケーションでの権限は何も与えられていません。</p>	<p>システム管理の [Configuration(設定)] > [Users(ユーザ)] ページ。</p> <p>詳細については、「システム管理者の定義とユーザ・パスワードのリセット」(91ページ)を参照してください。</p>
サイト管理者	<p>[サイト] 設定ページと [ワークスペース] > [ユーザ] 設定ページに対する読み取り/書き込みアクセス権が与えられています。</p> <p>サイト管理者は、サイト・ユーザがアクセスできるワークスペースを制限できます。</p>	<p>[サイト] > [ユーザ] 設定ページ。</p>
ワークスペース管理者	<p>すべてのアプリケーション・ページと機能に加え、[ワークスペース] および [統合] 設定領域に対する読み取り/書き込みアクセス権が与えられています。</p> <p>ワークスペース管理者は、ワークスペース・ユーザがアクセスできるアプリケーションを制限できます。</p>	<p>[サイト] > [ユーザ] 設定ページ、または [ワークスペース] > [ユーザ] 設定ページ。</p>

ロール名	説明	設定場所
<p>チーム・メンバ</p>	<p>ユーザは、アクセス権限を持つアプリケーションに関連する項目のみを表示できます。</p> <p>アクセス権限を持つアプリケーションについて、すべてのアプリケーション・ページと機能に対する読み取り/書き込みアクセス権が与えられています。ただし、次の場合を除きます。</p> <ul style="list-style-type: none"> ワークスペース管理者は、他のユーザが作成した項目をチーム・メンバが削除できないようにする権限を設定できます。 <p>[他のユーザが作成したバックログ項目の削除をチーム・メンバに許可] オプションをクリアすると、チーム・メンバは自分が作成者のテーマ、フィーチャー、およびバックログ項目のみ削除できます。標準設定では、このオプションが選択されており、チーム・メンバは任意の項目を削除できます。</p> <p>チーム・メンバは、設定を問わずタスクを選択でき、作成者を問わず受け入れテストが行えます。</p> <ul style="list-style-type: none"> チーム・メンバには作成者フィールドに対して読み込み専用アクセス権のみが与えられています。このフィールドはワークスペース管理者のみが変更することができます。 	<p>[サイト] > [ユーザ] 設定ページ、または [ワークスペース] > [ユーザ] 設定ページ。</p>
	<ul style="list-style-type: none"> チーム・メンバには、グリッド・ページ上の公開お気に入り、公開ダッシュボードのお気に入り、および公開ダッシュボードのギャラリーに対して閲覧アクセス権のみが与えられています。これらの項目の作成、更新、または削除は行えなくなります。 また、チーム・メンバは次の設定のみ変更できます。 <ul style="list-style-type: none"> チームが担当するスプリントでの1日あたりの作業時間と作業日の変更([リリース バックログ]のバケットからのみ変更可能)。 ALI設定の変更。 	

ロール名	説明	設定場所
表示者	<p>すべてのバックログ項目、グリッド・ページ、および[スプリント クロージャ]ページに対する読み取り専用アクセス権が与えられています。また、バックログ項目をウォッチして、ステータス更新についての通知を受信することができます。</p> <p>さらに、次の権限が与えられています。</p> <ul style="list-style-type: none"> グリッド・ページ上の非公開お気に入りに対する読み取り書き込みアクセス。 [不具合管理]ページでの非公開バケットの作成。 ダッシュボードに対する読み取りアクセス権、および非公開ダッシュボードの項目とお気に入りに対する読み取り書き込みアクセス権。 	[サイト] > [ユーザ] 設定ページ、または [ワークスペース] > [ユーザ] 設定ページ。
統合管理者	<p>NextGen Synchronizerを設定する[統合]設定領域に対する読み取り書き込みアクセス権が与えられています。</p>	[サイト] > [ユーザ] 設定ページ、または [ワークスペース] > [ユーザ] 設定ページ。
Integration Bridge	<p>Agile Manager と Integration Bridge 間の通信を管理します。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>注:</p> <ul style="list-style-type: none"> セキュリティ上の理由から、このユーザには他のロールは割り当てられません。 このロールは、後方互換性のためにのみサポートされます。 これは、Agile Manager ユーザ資格情報を使用して、まだ Agile Manager に接続している既存の Integration Bridge に使用されます。 </div>	[サイト] > [ユーザ] 設定ページ。

サイト・ユーザとワークスペース・ユーザの定義、および ALI の詳細については、Agile Manager ヘルプセンターを参照してください。

データの整合性

データの整合性は重大なセキュリティ要件であり、データ・バックアップ手順はこの要件の不可欠の部分です。Agile Manager にはバックアップ機能はありません。バックアップは、Oracle データベース管理者の責任です。

システムのバックアップ時には、次のことを考慮してください。

- バックアップは、アップグレードなどの重大なアクションの前に特に重要です。
Agile Manager 管理サイト([Servers(サーバ)] > [Database Server(データベースサーバ)])を使用すると、サイトを特定のバックアップ・ファイルの状態に復元できます。詳細については、「[データベースの設定](#)」(83ページ)を参照してください。
- バックアップ・ファイルは、権限のないアクセスを避けるために、業界のベスト・プラクティスに従って正しく格納する必要があります。
- データ・バックアップでは、大量のリソースが使用されます。ピーク需要時にはバックアップの実行を避けることを強くお勧めします。

注：データベースをバックアップする場合、同じシステム状態を反映させるために、ファイル・リポジトリも同時にバックアップするようにしてください。

データ暗号化

Agile Manager は、次のタイプの暗号化をサポートしています。

- **Agile Manager 暗号化** : Agile Manager は、機密の資格情報を暗号化した状態でデータベース内に格納します。
機密データの例としては、Agile Manager が使用するデータベース・サーバに対する資格情報、Agile Manager の統合先のLDAPサーバとSMTPサーバに対する資格情報、ユーザ・データを含むマシンの資格情報などがあります。
Agile Manager は次のセキュリティ設定を使用しています。
JCE crypto source, Symmetric block cipher, 3DES engine, 192 key size
LW crypto source, Symmetric block cipher, AES engine, 256 key size
- **パスワードの暗号化** : ユーザ・パスワードは格納されません。パスワードのハッシュ版のみが格納されます。
- **透過的なデータ暗号化 (TDE)** : Agile Manager は、Oracle データベースの TDE で動作することが保証されています。
- **フル・ディスク暗号化 (FDE)** : FDE は、すべてのシステム・コンポーネント(データベース、サーバ、リポジトリ・サーバ、クライアント・マシンなど)に対してサポートされています。

注意：TDE または FDE の実装は、システム・パフォーマンスに影響を与える可能性があります。詳細については、暗号化を提供しているベンダにお問い合わせください。

暗号化に関する FAQ

質問	回答
Agile Manager は、アカウント・パスワードを承認された暗号化形式で送信しますか？	Agile Manager と LDAP サーバで SSL/TLS を有効にして、アカウント・パスワード送信のセキュリティを確保することを強くお勧めします。 詳細については、「 Agile Manager のインストール 」(39ページ)および「 LDAP 認証の設定 」(86ページ)を参照してください。
Agile Manager は、アカウント・パスワードを承認された暗号化形式で格納しますか？	ユーザ・パスワードは一切格納されず、ハッシュ版のみが格納されます。 内部システム・パスワードは、AES 256 で格納されます。
Agile Manager は、Federal Information Processing Standard (FIPS) 140-2 検証済み暗号モジュールと乱数ジェネレータを使用して、暗号化、キー交換、デジタル署名、ハッシュ機能を実装しますか？	Agile Manager が使用する暗号化プロバイダは、FIPS で検証されていません。
どんなベース製品とサービス認証方法が提供されますか？	Agile Manager は、次の認証方法をサポートするように設定できます。 <ul style="list-style-type: none">ユーザ名/パスワードLDAP 認証 詳細については、「 ユーザ認証のセキュリティ保護 」(60ページ)を参照してください。
Agile Manager には、標準設定のベンダ提供パスワードなどのセキュリティパラメータが埋め込まれていますか？	はい。標準設定のパスワードは、インストールおよび設定時に変更できます。 インストールと設定の詳細については、「 Agile Manager のインストール 」(27ページ)を参照してください。

データ・ロギング

Agile Manager には、次のタイプのログが用意されています。

[「アプリケーション・ログ」](#)(65ページ)

[「エンティティ・ログ」](#)(66ページ)

アプリケーション・ログ

アプリケーション・ログ・ファイルは、Agile Manager 管理サイト(**[Servers(サーバ)]** > **[Application(アプリケーション)]**) に設定されているログ・レベルに応じてすべてのシステム・イベントをレポートできます。ログ・データを保持する期間は設定可能で、標準設定は制限なしです。

詳細については、「[アプリケーション・サーバの設定](#)」(80ページ)を参照してください。

エンティティ・ログ

既存のエンティティ(不具合やユーザ・ストーリーなど)に対する変更は、エンティティ履歴としてデータベースに格納されます。エンティティ履歴は、Agile Manager の[詳細]ページから表示できます。

エンティティ履歴は、エンティティ自身が削除されない限り、保持されます。このため、バックログ項目を完全に削除する代わりに、専用のリリース、フィーチャー、テーマに割り当てることをお勧めします。管理者はテーマとフィーチャーをアーカイブすることにより、これらをバックログ・グリッドやグラフから削除することもできます。

詳細については、Agile Manager ヘルプセンターを参照してください。

注: ユーザの責任において、保護されていない機密データを通常の Agile Manager エンティティ・フィールドに挿入しないようにする必要があります。

ログ・ファイルに関する FAQ

質問	回答
Agile Manager は、知る必要がある情報へのアクセスと主要なアプリケーション・イベントを監査しますか?	この情報は、アプリケーション・ログ・ファイルまたは Agile Manager エンティティ履歴から取得できます。
Agile Manager は、データ・コンテンツのユーザによる最終変更の日時を表示しますか?	この情報は、Agile Manager エンティティ履歴で利用可能です。
Agile Manager は、データへのアクセスおよびデータへの変更のトランザクション・ログの作成をサポートしますか?	この情報は、ログ・レベルに応じてアプリケーション・ログで見つけることができます。

アプリケーション・サーバでの SSL/TLS 設定

次の手順では、Agile Manager アプリケーション・サーバで Agile Manager への Secure Socket Layer (SSL) または Transport Layer Security (TLS) 接続を設定する方法について説明します。

参照情報: [「LDAP サーバでの SSL/TLS 設定」\(87ページ\)](#)および[「電子メール通知サーバの設定」\(85ページ\)](#)。

注意: この手順は、Agile Manager のインストール後にのみ実行する必要があります。詳細については、[「Agile Manager のインストール」\(27ページ\)](#)を参照してください。

1. Agile Manager のインストール時と同じユーザ(**root**または **agmadmin sudo ユーザ**)でサーバ・マシンにログインします。
2. このサーバの名前に対して発行されたサーバ証明書(java キーストア形式)を取得します。この中には、秘密キーとその発行元の証明機関が含まれている必要があります。
証明書を **/opt/hp/agm/server/conf/** フォルダにコピーし、名前を **server.keystore** に変更します。

別の方法として、運用目的でない場合にのみ、次のようにして自分自身でこの証明書を作成できます。

次のコマンドを順次実行します(ここで、<サーバ> は Agile Manager アプリケーション・サーバの完全修飾名です)。

```
cd ~  
export SERVER_DN="CN=<サーバ>,OU=X,O=Y,L=Z,S=XY,C=YZ"  
export KSDEFAULTS="-storepass changeit"  
export KEYINFO="-keyalg RSA"  
  
/opt/hp/agm/java/jre/bin/keytool -genkey -alias tomcat -dname $SERVER_DN  
$KSDEFAULTS -keystore server.keystore $KEYINFO -keypass changeit  
  
cp ~/server.keystore /opt/hp/agm/conf/server.keystore  
  
/opt/hp/agm/java/jre/bin/keytool -export -alias tomcat -file temp_  
server.cer $KSDEFAULTS -keystore server.keystore  
  
/opt/hp/agm/java/jre/bin/keytool -import -keystore  
/opt/hp/agm/java/jre/lib/security/cacerts $KSDEFAULTS -alias tomcat -file  
temp_server.cer
```

3. すべてのユーザが Agile Manager からログアウトしたことを確認し、Agile Manager サービスを停止します。/opt/hp/agm/wrapper/HPALM stop
4. /opt/hp/agm/server/conf/ ディレクトリに移動して **jetty.xml** ファイルを開きます。

Configure 要素の下に、次のセクションを追加します。

注: ベスト・プラクティスとして、次のセクションに太線を含めることを推奨します。これにより、Agile Manager での特定の暗号アルゴリズムとプロトコルの使用が制限され、最もセキュアなプロトコルと暗号だけが使用されます。

この操作の前に、Java Cryptography Extension (JCE) Unlimited Strength ポリシー・ファイルを[ダウンロード](#)し、AES-256 などの十分な強度の暗号を取得します。

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html> からこれらのファイルをダウンロードします。

2 つの JAR ファイルを展開し、次の場所にコピーします。<Agile Manager のインストール・フォルダ>/java/jre/lib/security

```
<New id="sslContextFactory"  
class="org.eclipse.jetty.http.ssl.SslContextFactory">  
  <Set name="ExcludeProtocols">  
    <Array type="java.lang.String">
```

```
        <Item>SSLv3</Item>
      </Array>
    </Set>
  </New>

<Call name="addConnector">
  <Arg>
    <New class="org.eclipse.jetty.server.ssl.SslSocketConnector">
      <Arg><Ref id="sslContextFactory" /></Arg>
      <Set name="host"><Property name="jetty.host" /></Set>
      <Set name="Port">8443</Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="keystore">/opt/hp/agm/conf/server.keystore</Set>
      <Set name="password">changeit</Set>
      <Set name="keyPassword">changeit</Set>
      <Set
name="truststore">/opt/hp/agm/java/jre/lib/security/cacerts</Set>
      <Set name="trustPassword">changeit</Set>
      <Set name="IncludeCipherSuites">
        <Array type="java.lang.String">
          <Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
          <Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
          <Item>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</Item>
          <Item>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</Item>
        </Array>
      </Set>
    </New>
  </Arg>
</Call>
```

5. 追加されたセクションで、次の手順を実行します。
 - ポート番号を変更する場合、**8443**を新しいポート番号に置き換えます。
 - 標準設定のキーストア・パスワードを変更した場合(推奨)は、**changeit**を新しいパスワードに置き換えます。
6. (オプション)パスワードを暗号化するには、次の手順を実行します。
 - a. 次のコマンドを実行します。`/opt/hp/agm/java/jre/bin/java -cp " ./opt/hp/agm/server/lib/*:/opt/hp/agm/server/lib/ext/" org.eclipse.jetty.http.security.Password <パスワード>`

たとえば、次のコマンドを実行するとします。

```
/opt/hp/agm/java/jre/bin/java -cp
" ./opt/hp/agm/server/lib/*:/opt/hp/agm/server/lib/ext/"
org.eclipse.jetty.http.security.Password changeit
```

出力は次のようになります。

```
changeit
OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0
MD5:b91cd1a54781790beaa2baf741fa6789
```

- b. **jetty.xml** ファイルで、プレーン・テキスト・パスワードを **OBF** と **MD5** のプレフィックスを含む暗号化された出力で置き換えます。
7. SSL/TLS 接続が動作することを確認したら、Agile Manager アプリケーション・サーバへの HTTP 以外のアクセスを無効にします。**jetty.xml** ファイルで、次のセクションを探し、セクションの先頭に `<!--`、末尾に `-->` を配置してコメントアウトします。

例：

```
<!--
<Call name="addConnector">
  <Arg>
    <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
      <Set name="host"><Property name="jetty.host" /></Set>
      <Set name="port"><Property name="jetty.port" default="8080"/></Set>
      <Set name="maxIdleTime">30000</Set>
      <Set name="Acceptors">2</Set>
      <Set name="statsOn">false</Set>
      <Set name="confidentialPort">8443</Set>
      <Set name="lowResourcesConnections">20000</Set>
      <Set name="lowResourcesMaxIdleTime">5000</Set>
    </New>
  </Arg>
</Call>
-->
```

注：実際の **jetty.xml** ファイルのこのセクションは若干異なっている可能性があります。

8. **jetty.xml** ファイルを保存します。
9. Agile Manager サービスを再起動します。 `/opt/hp/agm/wrapper/HPALM restart`
10. ポート 8443 または新しいポート番号 (上記の手順で変更した場合) を使用して、Agile Manager に接続します。説明に従って、次の URL を使用して Agile Manager に接続します。

Agile Manager	https://<サーバ>:<ポート>/agm/login
Agile Manager 管理サイト	http://<サーバ>:<ポート>/agm/admin

Apache Web サーバの統合 (例)

外部認証をサポートするか、セキュリティを向上させるには、Agile Manager アプリケーション・サーバをセキュアなリバース・プロキシの背後に配置します。詳細については、「[リバース・プロキシ・アーキテクチャ](#)」(58 ページ)を参照してください。

本項では、これを行う1つの方法について説明します。具体的には、要求を Agile Manager アプリケーション・サーバにリダイレクトするように Apache Web サーバを設定します。

注: Apache Web サーバをプロキシ HTTP モードで動作するように設定します。Apache HTTP サーバのバージョン 2.4 を使用することをお勧めします。

1. Apache Web サーバが停止していることを確認します。
2. <Apache ホーム・ディレクトリ>\conf ディレクトリに移動します。
3. `httpd.conf` ファイルを開きます。
4. 次の LoadModule コマンドをコメント解除または追加します。

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
```

注: 上記のモジュールが Apache のインストール・ディレクトリにすべて存在することを確認します。

5. 次のセクションをファイルの末尾に追加します(後述の注を参照)。

```
# Turn off support for true Proxy behavior as we are acting as a reverse
proxy
ProxyRequests Off

# Turn off VIA header as we know where the requests are proxied
ProxyVia Off

# Set the permissions for the proxy
<Proxy *>
AddDefaultCharset off
```

```
Order deny,allow
Allow from all
</Proxy>
# Turn on Proxy status reporting at /status
# This should be better protected than:Allow from all
ProxyStatus On
<Location /status>
SetHandler server-status
Order Deny,Allow
Allow from all
</Location>
# Configuring mod_proxy_http
# To connect to servlet container with HTTP protocol, the
# ProxyPass directive can be used to send requests received on a
# particular URL to a Jetty instance.
ProxyPreserveHost off
ProxyPass /qcbn http://<サーバ>:<ポート>/qcbn
ProxyPassReverse /qcbn http://<サーバ>:<ポート>/qcbn
ProxyPass /agm http://<サーバ>:<ポート>/agm
ProxyPassReverse /agm http://<サーバ>:<ポート>/agm
# Rewrite rule trailing slash must be used in the VirtualHost
# sectionLoadModule rewrite_module modules/mod_rewrite.so
RewriteEngine On
```

注:

- <サーバ> は、Agile Manager アプリケーション・サーバの完全修飾ホスト名と置き換えてください。
- ポート番号とプロトコルは必要に応じて変更してください。

6. 変更内容をファイルに保存します。
7. Apache Web サーバを再起動します。

[「Agile Manager へのログイン」\(51ページ\)](#)に記載された URL を使用し、URL 内の Apache 用ポートを通じて Agile Manager に接続します。

注: 通知電子メール用の電子メールサーバを設定する場合は、それらの電子メールで使用する外部 URL も設定します。

詳細については、[「電子メールで使用する外部 URL を設定します。」\(85ページ\)](#)を参照してください。

アプリケーション・サーバの管理

本章には、Agile Manager アプリケーション・サーバの管理、および一般的な Java 管理ツールに関する情報が記載されています。

- [「パスワードの変更」\(73ページ\)](#)
- [「ヒープ・メモリ・サイズの変更」\(73ページ\)](#)
- [「アプリケーション・サーバのポート番号の変更」\(74ページ\)](#)
- [「アプリケーション・サーバの管理ツール」\(76ページ\)](#)

注: リポジトリを移動する必要がある場合もあります。移動する場合は、Agile Manager に設定されているリポジトリ・パスを変更する必要がある場合があります。Agile Manager 管理サイト([\[Servers\(サーバ\)\]](#)) > [\[Database\(データベース\)\]](#))の [\[Restore Site Schema\(サイトスキーマの復元\)\]](#) オプションを使用します。詳細については、[「サイト・スキーマの復元」\(84ページ\)](#)を参照してください。

パスワードの変更

各種システム・コンポーネントへの接続に使用するパスワードは、時間の経過に伴って変更されます。このようなパスワード定義を Agile Manager システムで変更するには、次の手順を実行します。

- [「データベースのシステム・パスワードの変更」\(74ページ\)](#)
- [「システム・スキーマ・パスワードの変更」\(75ページ\)](#)
- [「サイト・スキーマ・パスワードの変更」\(84ページ\)](#)

ヒープ・メモリ・サイズの変更

Agile Manager をインストールしたら、必要に応じて、ヒープ・メモリ・サイズを変更します。たとえば、同時ユーザー・セッションの数が増えた場合、ヒープ・サイズを増やしたい場合があります。

注:

- 最大ヒープ・サイズは、最大メモリ(RAM)サイズを超えることはできません。
- 32ビット・オペレーティング・システムを実行しているマシン上では、ヒープ・メモリ・サイズは 1024 MB を超えることができません。

1. すべてのユーザが Agile Manager からログアウトしたことを確認し、Agile Manager サービスを停止します。`/opt/hp/agm/wrapper/HPALM stop`
2. Agile Manager デプロイメント・パスで、`/opt/hp/agm/conf/wrapper-install.conf` ファイルを開きます。

3. 必要に応じて、`wrapper.java.maxmemory` の値を変更します。
4. Agile Manager サービスを再起動します。`/opt/hp/agm/wrapper/HPALM restart`

アプリケーション・サーバのポート番号の変更

Agile Manager をインストールしたら、必要に応じて、アプリケーション・サーバのポート番号を変更します。

アプリケーション・サーバの標準設定のポートが、同じマシンで実行中の別のアプリケーションによって使用されている可能性があります。

その場合、ポートを使用しているアプリケーションを探して停止するか、Agile Manager サーバのポートを変更できます。

標準設定のポートは、**8080** または **8443**(セキュアな接続の場合) です。

注: このポート番号を変更する場合、Linux で 1024 より上位のポート番号を使用するにはセキュリティ保護されたプロセスが必要です。プロセスの権限を変更して、小さい番号のポートを使用するには、システム管理者に問い合わせてください。

1. すべてのユーザが Agile Manager からログアウトしたことを確認し、Agile Manager サービスを停止します。`/opt/hp/agm/wrapper/HPALM stop`
2. `/opt/hp/agm/server/conf/jetty.xml` ファイルに移動します。
3. `jetty.port` の値を変更します。
4. Agile Manager サービスを再起動します。`/opt/hp/agm/wrapper/HPALM restart`

データベースのシステム・パスワードの変更

データベースのシステム・パスワードは、定期的に変更してシステムのセキュリティを確保します。変更時は、Agile Manager で定義されているパスワードも同様に変更します。

1. すべてのユーザが Agile Manager からログアウトしたことを確認し、Agile Manager サービスを停止します。`/opt/hp/agm/wrapper/HPALM stop`
2. 設定ウィザードを再度実行します。詳細については「[Agile Manager のインストール](#)」(27ページ)を参照してください。

インストール時には、現在の設定をすべて保持し、次の変更のみを行います。

ウィザード・ページ	選択オプション
Current Settings(現在の設定)	[Keep all current settings(現在の設定をすべて保持)]を選択します。 例
Database Administrator Login(データベース管理者のログイン)	プロンプトが表示されたら、新しいパスワードを入力します。 詳細

ウィザード・ページ	選択オプション
System Administration Database Schema(システム管理データベース・スキーマ)	[Connect to existing schema/second node(既存のスキーマ/2番目のノードに接続)]を選択します。 詳細

3. Agile Manager を起動します。詳細については、「[Agile Manager サービスの起動/停止](#)」(50ページ)を参照してください。
4. サービスが起動したら、「[Agile Manager へのログイン](#)」(51ページ)に進みます。

システム・スキーマ・パスワードの変更

システム・スキーマへのアクセスに使用するパスワードは、定期的に変更してシステムのセキュリティを確保します。変更時は、Agile Manager で定義されているパスワードも同様に変わります。

1. すべてのユーザが Agile Manager からログアウトしたことを確認し、Agile Manager サービスを停止します。`/opt/hp/agm/wrapper/HPALM stop`
2. 設定ウィザードを再度実行します。詳細については「[Agile Manager のインストール](#)」(27ページ)を参照してください。

インストール時には、現在の設定をすべて保持し、次の変更のみを行います。

ウィザード・ページ	選択オプション
Current Settings(現在の設定)	[Keep all current settings(現在の設定をすべて保持)]を選択します。 例
System Administration Database Schema(システム管理データベース・スキーマ)	[Connect to existing schema/second node(既存のスキーマ/2番目のノードに接続)]を選択します。 詳細
SA Schema details(SA スキーマの詳細)	プロンプトが表示されたら、新しいパスワードを入力します。 詳細

3. Agile Manager を起動します。詳細については、「[Agile Manager サービスの起動/停止](#)」(50ページ)を参照してください。
4. サービスが起動したら、「[Agile Manager へのログイン](#)」(51ページ)に進みます。

アプリケーション・サーバの管理ツール

Agile Manager アプリケーション・サーバは、Java ベースです。Agile Manager サーバを効率的に管理するには、次の Java ツールをお勧めします。

ツール	アドレス
jconsole	<p>http://docs.oracle.com/javase/8/docs/technotes/guides/management/jconsole.html (英語 サイト)</p> <p>リモート・プロセスを使用して jconsole に接続するには、次の URL 構文を使用します。</p> <pre>service:jmx:rmi://<サーバ>:29601/jndi/rmi://<サーバ>:9999/server</pre> <p>このコンソールを公開しない場合、サーバ上の関連するポート(29601と9999)を閉じる必要があります。</p>
jstack	<p>http://download.oracle.com/javase/1.5.0/docs/tooldocs/share/jstack.html (英語 サイト)</p>
jmap	<p>http://download.oracle.com/javase/1.5.0/docs/tooldocs/share/jmap.html (英語 サイト)</p>
jvisualvm	<p>http://download.oracle.com/javase/6/docs/technotes/tools/share/jvisualvm.html (英語 サイト)</p>

トラブルシューティング

Agile Manager のインストールまたはアップグレード中に問題が発生した場合、次のログ・ファイルのエラーをチェックしてください。

ログ	パス
インストールと設定	/opt/hp/agm/log/InstallationLog_<日時>.html
システム管理データベース・スキーマの作成	/opt/hp/agm/log/sa

エラー: An Agile Manager installation already exists (Agile Manager インストールがすでに存在します)

既存の Agile Manager インストールをアンインストールして、そのすべての痕跡をサーバ・マシンから削除します。その後、Agile Manager のインストールを再度試行します。



注意: Agile Manager サーバの実行中にログ・ファイルが削除された場合、サーバを再起動するまで再作成されません。

詳細については、「[Agile Manager のアンインストール](#)」(39ページ)を参照してください。

エラー: Agile Manager server isn't started because RMI port is in use (RMI ポートが使用中のため、Agile Manager サーバが起動しません)

このような場合、**wrapper.log** ファイルにエラーが出力されます。

例:

```
INFO | jvm 5 | 2014/07/15 14:00:09.497 | WrapperSimpleApp Error: Caused by: java.rmi.server.ExportException: Port already in use: 29601; nested exception is:  
INFO | jvm 5 | 2014/07/15 14:00:09.497 | java.net.BindException: Address already in use
```

回避策: 次のいずれかを行います。

- ポートを使用している Linux プロセスを解放します。
- Agile Manager が使用する RMI ポートを変更します。詳細については、「[アプリケーション・サーバのポート番号の変更](#)」(74ページ)を参照してください。

エラー: Couldn't flush system prefs (システム設定をフラッシュできませんでした)

Agile Manager 2.10 から Agile Manager 2.50 にアップグレードした場合、**wrapper.log** に次のようなエラーが含まれます。Couldn't flush system prefs(システム設定をフラッシュできませんでした)

修正方法：

1. `/opt/hp/agm/wrapper/wrapper.conf` ファイルをバックアップします。
2. 同じフォルダの `wrapper.conf.rpmnew` ファイルの名前を `wrapper.conf` に変更します。
3. 設定ウィザードを再実行します。今回は、設定ウィザードの[**System Administration Database Schema(システム管理データベーススキーマ)**]画面で、[**Connect to an existing schema/second node(既存のスキーマ/2番目のノードに接続)**]を選択します。

詳細については、「[Agile Manager のインストール](#)」(27ページ)および「[Connect to existing schema/second node\(既存のスキーマ/2番目のノードに接続\)](#)」(32ページ)を参照してください。

注：前に `wrapper.conf` ファイルの `wrapper.java.maxmemory` プロパティを変更した場合、この変更を `/opt/hp/agm/conf/wrapper-install.conf` ファイルに手動で移行してください。

Agile Manager のシステム管理

『Agile Manager インストールおよび管理ガイド』の本項は、サーバ、ユーザ、その他のシステム設定を管理する必要があるシステム管理者を対象としています。

注: 本項で説明する機能は Agile Manager 管理サイトでのみ利用可能です。

管理サイトへアクセスするには、ユーザが Agile Manager システム管理者として定義されている必要があります。アクセスの詳細については、「[Agile Manager へのログイン](#)」(51ページ)を参照してください。


管理ホーム・ページには、Agile Manager サイトを設定する前に実施する必要がある設定のチェックリストがあります。



緑のチェック・マークは、設定手順が完了していることを示します。



青の編集アイコンは、設定情報が必須であることを示します。

管理サイトの各ページでは、変更の保存や、最後の保存以降の変更を元に戻すことができます。ツールヒント  にマウス・カーソルを置くと、各フィールドの詳細が表示されます。

このPDF版 オンラインヘルプについて

本ドキュメントのこの項はオンラインヘルプのPDF版です。このPDFは、ヘルプ情報から複数のトピックを簡単に印刷したり、オンラインヘルプをPDF形式で閲覧できるようにするために提供されています。このコンテンツは本来、オンラインヘルプとしてWebブラウザで閲覧することを想定して作成されているため、トピックによっては正しいフォーマットで表示されない場合があります。また、インタラクティブトピックの一部はこのPDF版では提供されません。これらのトピックは、オンラインヘルプから正しく印刷することができます。

機能の紹介

• アプリケーション・サーバの設定	80
• データベースの設定	83
• 電子メール通知サーバの設定	85
• ユーザ認証の設定	86
• ユーザ・ライセンスの更新	89
• システム管理者の定義とユーザ・パスワードのリセット	91
• 一般的なシステム設定	92
• 詳細パラメータの設定	93

アプリケーション・サーバの設定

タブ: [Servers(サーバ)] > [Application(アプリケーション)]

このページには、左で選択したアプリケーション・サーバのデータが表示されます。複数のアプリケーション・サーバを使用したクラスタ設定の場合は、そのサーバに関連するデータを設定して表示するサーバを選択します。

クラスタ設定の詳細については、「[クラスタ設定の例](#)」(11ページ)を参照してください。

最大データベース接続数の設定

[Max DB Connections(最大 DB 接続数)]の値を変更し、選択したアプリケーション・サーバからデータベースへの最大同時接続数を設定します。

標準設定値は **100** です。

注:

- 変更した値を有効にするにはサーバを再起動する必要があります。
- この値は、アップグレード後に標準設定値に再設定されます。この値を変更してからアップグレードした場合、アップグレード完了後に再び値を変更する必要があります。

同期負荷の分散

クラスタ化されたシステムで NextGen Synchronizer を使用している場合、自動同期によってメインの Agile Manager サーバに余分な負荷が生じるのを防ぐことができます。

同期プロセスを処理しない Agile Manager ユーザ・アクティビティ用のノードを指定することで、サーバの負荷を分割できます。この場合でも、すべてのノードのデータは引き続き同期されます。

次の操作を実行します。

1. Agile Manager ユーザ・アクティビティ専用使用するノードで、次の手順を実行します。

[Servers(サーバ)] > [Application(アプリケーション)] タブで、[**Disable NextGen Synchronizer processes(NextGen Synchronizer プロセスの無効化)**]を選択します。

注: 変更を有効にするには、この設定を変更した後でサーバを再起動する必要があります。

2. [Configuration(設定)] > [Advanced Parameters(詳細パラメータ)] タブで、次の手順を実行します。
 - a. OPB_AGM_SERVER_URL という名前のシステム・パラメータを追加します。
 - b. パラメータの値を、同期プロセスを実行するノードにアクセスするための URL に設定します。これは、Agile Manager ノードの URL またはロード・バランサの URL です。
次の形式を使用します。http(s)://<サーバのホスト名または IP アドレス>:<ポート>/agmこれにより、Integration Bridge がダウンロードされたときに、標準設定で同期を処理する Agile Manager ノードにアクセスするように設定されます。



ヒント: `server-connection.conf` ファイルは、Integration Bridge とともにダウンロードされます。このファイルには、ブリッジが Agile Manager にアクセスするために使用する URL とサイト ID が含まれています。

3. NextGen Synchronizer プロセスを無効にしたノードから前にダウンロードした、すべての Integration Bridges を変更する必要があります。
Integration Bridge は、標準設定でダウンロード元のノードにアクセスするように設定されています。これが同期プロセスを実行するノードと通信するようにするには、次の手順を実行します。
 - a. <HP Integration Bridge のインストール・フォルダ>\product\conf フォルダ(Linux の場合、スラッシュを反転)に移動します。
 - b. `server-connection.conf` ファイルを編集用を開きます。
 - c. `agm.base.url` プロパティで、ホスト名/IP アドレスを、関連する Agile Manager ノードまたはロード・バランサのホスト名/IP アドレスで置き換えます。
 - d. ブリッジを再起動します。

アプリケーション・ログ・ファイル

次の標準 log4j ファイルが Agile Manager によって生成され、アプリケーション・サーバに保存されます。

<code>agm.logger.txt</code>	Agile Manager アプリケーションで発生したイベントを記録します。 <code>/opt/hp/agm/log/qc</code> ディレクトリに格納されます。
<code>sa.logger.txt</code>	管理サイトで発生したイベントを記録します。 <code>/opt/hp/agm/log/sa</code> ディレクトリに格納されます。
<code>PublicApiAudit.logger.txt</code>	公開 API REST 呼び出しを記録します。呼び出しを実行したユーザーのユーザー名も含まれます。 <code>/opt/hp/agm/log/qc</code> ディレクトリに格納されます。
<code>PublicApi.logger.txt</code>	特定の公開 API セッション中に発生したイベントを記録します。 <code>/opt/hp/agm/log/qc</code> ディレクトリに格納されます。

標準設定値

標準設定:

- どちらのファイルでも、ログ・レベルは WARN に設定されます。
- ログ・ファイルのサイズは 10000 KB に制限されています。これを超えると、連番を付けた別のファイルに現在のログ・エントリがコピーされます。新しいログ・ファイルが作成されるたびに連番が更新され、指定した最大ファイル数に達するまでファイルが作成されます。
- 一度に 10 個のログ・ファイルを保持できます。現在のログ・ファイル 1 個と、過去のエントリのログ・ファイル 9 個になります。

特定のパラメータの標準設定値の詳細については、以下の表を参照してください。

ログの設定

ログの設定は、**log4j.properties** ファイルの中の値を変更して行えます。このファイルは、アプリケーション・サーバの **/opt/hp/agm/webapps/qcbin/WEB-INF/classes** ディレクトリにあります。

注: アプリケーション・ログ・サーバ名はページ上部に一覧表示されます。クラスタ環境で作業している場合、左のリストからサーバ名を選択します。

ログ設定を変更した後で、サーバを再起動する必要はありません。

以下のログ変数を設定します。

パラメータ	説明
Log level(ログ・レベル)	ファイルの最初の行に定義します。 Default(標準設定): WARN 注: ログ・レベルを [Debug(デバッグ)] に変更した場合は、デバッグの終了後に必ず元に戻してください。
FileAppender	ログ・ファイルが最大設定サイズに達したときに、それぞれのファイル名に付加するアペンダを定義します。 Default(標準設定): RollingFileAppender(log4j の標準値)
FileAppender.File	ログ・ファイルの場所と名前を定義します。 Default(標準設定): \${log.folder}qc/agm.logger.txt
FileAppender.MaxFileSize	ログ・ファイルの最大サイズを定義します。 Default(標準設定): 10,000 KB

パラメータ	説明
FileAppender. MaxBackupIndex	保持するログ・ファイルの最大数(過去のエントリを保存するファイルを含む)を定義します。最大数に達すると、最も古いエントリがシステムから削除されます。 Default(標準設定): 10 ファイル
FileAppender.layout	ログ・ファイルのレイアウトと構成を定義します。 Default(標準設定): PatternLayout(log4jの標準値)
FileAppender.layout. ConversionPattern	ログ・ファイルに表示するデータを定義します。 Default(標準設定): log4jの標準値と、次のカスタム属性があります。 <ul style="list-style-type: none">• file: イベントが格納されたファイル。• class: イベント・クラス。• method: イベント・メソッド。• build: イベントが発生したビルド。

データベースの設定

タブ: [Servers(サーバ)] > [Database(データベース)]

データベース・サーバの詳細は Agile Manager のインストールおよび設定中に設定され、本ページで説明するデータのほとんどは読み取り専用です。データベース設定の詳細については、「[データベース・パラメータの入力](#)」(30ページ)を参照してください。

サイトがアップグレードなどのメンテナンス中の場合は、メンテナンスの詳細が[**Site Status(サイトステータス)**]領域の[**Maintenance Status(メンテナンスステータス)**]フィールドに表示されます。このフィールドはメンテナンス中のみ表示されます。



注意: ユーザが Agile Manager に接続している間は、このページでアクションを実行しないでください。

管理サイトを使用して、次の処理を実行できます。

- 「[サイトのアクティブ化](#)」(83ページ)
- 「[サイト・スキーマ・パスワードの変更](#)」(84ページ)
- 「[サイト・スキーマの復元](#)」(84ページ)

サイトのアクティブ化

設定済みパスワードの編集やサイトのアップグレードといったメンテナンス作業中は、サイトは非アクティブになります。

メンテナンス完了時に[Site Status(サイト ステータス)]の下にある[Activate(アクティブ化)]をクリックすると、サイトが再度アクティブになります。

サイト・スキーマ・パスワードの変更

サイト・スキーマへのアクセスに使用するパスワードを更新した場合は、Agile Manager で設定したパスワードも同様の編集が必要になります。

[Database User Credentials(データベース ユーザ資格情報)]領域で、[Edit Password(パスワードの編集)]をクリックします。新しいパスワードを入力した後、確認のために再度入力します。

注:


- [Edit Password(パスワードの編集)]をクリックすると、パスワードの変更が完了していない場合でも、サイトが非アクティブになります。サイトを再度アクティブにするには[Activate(アクティブ化)]をクリックしてください。
- サイト・スキーマ・パスワードの変更は、システム・スキーマ・パスワードの更新とは異なります。詳細については、「[システム・スキーマ・パスワードの変更](#)」(75ページ)を参照してください。

サイト・スキーマの復元

古いバージョンのデータベースとリポジトリを使用して、サイトを前の状態に復元します。この操作により、現在 Agile Manager で設定されているデータベース([Servers(サーバ)]>[Database(データベース)]ページの[General Information(一般情報)]の下に一覧表示)が置き換えられます。

注意:

- Agile Manager からは、一度に1つのサイトにしかアクセスできません。つまり、サイト・スキーマを復元すると、現在 Agile Manager で表示されているデータにはすべてアクセスできなくなります。反対に、このデータには復元したスキーマからのみアクセスできるようになります。
 - サイトを復元するには、同じデータベース・サーバ上にホストされ、現在のバージョンでの定義と同じ資格情報を持つスキーマを使用する必要があります。
 - まったく新しいシステム管理スキーマを利用している場合に既存のサイト・スキーマを復元すると、管理スキーマのデータはアップグレード後に使用できなくなります。Agile Manager で認証されるユーザのユーザ・パスワードやユーザのAvatar写真も同様です。
 - LDAP 認証のユーザのユーザ・ログインには、まったく影響はありません。
 - Agile Manager が直接認証するユーザは、パスワードを一切入力せずにログインできるようになります。
 - Avatar写真のリセットは、すべてのユーザに必要なになります。
- 詳細については、「[基本的な運用システムのアップグレード](#)」(44ページ)を参照してください。

ページ上部の  [Restore Site Schema(サイトスキーマの復元)] をクリックし、復旧するサイトのスキーマとリポジトリの情報を入力します。

電子メール通知サーバの設定

タブ: [Servers(サーバ)] > [Mail(メール)]

Agile Manager からユーザに通知を送信できるように SMTP メールサーバを設定する必要があります。

1. [Mail server(メールサーバ)] ドロップダウンから [SMTPServer(SMTP サーバ)] を選択します。
2. サーバ名とサーバのポート番号を指定します。
3. メールサーバで SMTP 認証が必要な場合、[Enable connection to an SMTP server that requires authentication(認証が必要な SMTP サーバへの接続を有効にする)] を選択し、認証の詳細を入力します。

注: SMTP サーバ上で SSL/TLS を設定することを計画している場合は、認証詳細の設定が必要です。

4. SMTP サーバで SSL/TLS を設定します(オプション)。

セキュリティで保護された SMTP メールサーバに接続するには、次の手順を実行します。


- a. [Enable SSL support(SSL サポートを有効にする)] を選択します。
- b. 証明書のトラスト・ストアを Agile Manager アプリケーション・サーバで事前に設定します。
多くの場合、標準設定のトラスト・ストアが使用されます。標準設定のトラスト・ストアは `/opt/hp/agm/java/jre/lib/security/cacerts`、標準設定のパスワードは `changeit` です。
SMTP サーバ証明書の信頼性を確立するには、keytool ユーティリティを使用して Java トラスト・ストアに証明書をインポートします。keytool ユーティリティは `/opt/hp/agm/java/jre/bin` ディレクトリにあります。

例

```
keytool -import -alias <自分の SMTP CA> -trustcacerts -file <SMTP CA 証明書> -keystore /opt/hp/agm/java/jre/lib/security/cacerts
```

- c. 中間の証明機関がある場合は、その証明書もインポートします。

注: SMTP サーバ上で暗号化接続を使用すると、SMTP ポートが変わることがあります。ポートを確認し、必要に応じて変更してください。

5. 変更を保存します。ページ上部の [Save(保存)] をクリックします。
6. 暗号化された接続を使用している場合は、証明書をインポートした後に Agile Manager を再起動します。詳細については、「[Agile Manager サービスの起動/停止](#)」(50ページ)を参照してください。
7. 設定をテストします。ページ上部の [Test Send Mail(メール送信テスト)]  をクリックします。
テストメールの送信先電子メールアドレスを入力し、[Test(テスト)] をクリックします。
8. 電子メールで使用する外部 URL を設定します。

電子メール・サーバを設定する場合は、Agile Manager が、Agile Manager へのリンクを含む電子メールをユーザに送信します。これらの電子メールでは、実際のマシン名が公開される場合があります。

このような電子メールの例として、ユーザが Agile Manager から直接別のユーザにエンティティを送信する場合や、新しいユーザがログインを促すようこそメールを受信する場合があります。

実際のマシン名を隠すには、システム管理サイトの **[Advanced Parameters(詳細パラメータ)]** ページで **EXTERNAL_BASE_URL** 詳細パラメータを追加します。電子メールに表示する外部 URL の値を定義します。

例 : `http://my-load-balancer-domain:8080/`

注: URL の末尾に `agm` を追加しないでください。

詳細については、「[詳細パラメータの設定](#)」(93ページ)を参照してください。

参照情報:

- 『HP Agile Manager インストールおよび管理ガイド』「[アプリケーション・サーバでの SSL/TLS 設定](#)」(66ページ)
- 「[LDAP サーバでの SSL/TLS 設定](#)」(87ページ)

ユーザ認証の設定

タブ: [Configuration(設定)] > [Authentication(認証)]

Agile Manager は次のタイプの認証をサポートします。

タイプ	説明
Agile Manager 認証	標準設定では、Agile Manager にユーザが追加されて直接認証されます。 [Agile Manager]を選択して Agile Manager 設定領域 ([サイト] > [ユーザ]) にそのまま進み、個々のユーザを追加します。このページには、Agile Manager サイト管理者のみがアクセスできます。 詳細については、Agile Manager ヘルプセンターを参照してください。
LDAP 認証	ユーザは、社内 LDAP システムからインポートされ、LDAP システムで認証されます。 LDAP ユーザは、自分のシステム・プロファイルに設定されている電子メール・アドレスとコンピュータのパスワードを使用して Agile Manager にログインします。 詳細については、「 LDAP 認証の設定 」(86ページ)を参照してください。

LDAP 認証の設定

注: Agile Manager は、セキュア・ソケット (SSL) を使用した LDAP 通信転送もサポートしています。

す。これにより、ユーザの資格情報(パスワード)がネットワーク上で保護されていない状態で送信されることはありません。

LDAP サーバでの SSL/TLS 設定

SSL/TLS 経由で LDAP を使用するには、次の設定を行う必要があります。

LDAP サーバの設定	<p>LDAP サーバで事前に次の設定を行う必要があります。</p> <ul style="list-style-type: none">• SSL/TLS を有効にします。• セキュリティで保護されたポートを定義します。標準設定では、Agile Manager は 636 番ポートを使用します。• サーバ証明書をインストールします。 <p>さらに、LDAP 証明書を発行した証明機関(CA)のルート証明書(およびすべての中間証明書)を取得します。</p>
Agile Manager サーバの設定	<p>証明書のトラスト・ストアを Agile Manager アプリケーション・サーバで事前に設定します。</p> <p>多くの場合、標準設定のトラスト・ストアが使用されます。標準設定のトラスト・ストアは <code>/opt/hp/agm/java/jre/lib/security/cacerts</code>、標準設定のパスワードは <code>changeit</code> です。</p> <p>LDAP サーバ証明書の信頼性を確立するには、keytool ユーティリティを使用して Java トラスト・ストアに証明書をインポートします。keytool ユーティリティは <code>/opt/hp/agm/java/jre/bin</code> ディレクトリにあります。</p> <p>例:</p> <pre>keytool -import -alias <自分の LDAP CA> -trustcacerts -file <LDAP CA 証明書> -keystore /opt/hp/agm/java/jre/lib/security/cacerts</pre> <p>中間の証明機関がある場合は、その証明書もインポートします。</p>

注: 証明書を追加した後に、Agile Manager を再起動してから、SSL/TLS を介して LDAP サーバに接続する必要があります。詳細については、「[Agile Manager サービスの起動/停止](#)」(50ページ)を参照してください。

参照情報:


- 「[アプリケーション・サーバでの SSL/TLS 設定](#)」(66ページ)
- 「[SMTP サーバで SSL/TLS を設定します\(オプション\)](#)」(85ページ)

LDAP 認証を設定するには、次の手順を実行します。

1. [LDAP]を選択し、次の領域に示すフィールドを使用して Agile Manager が LDAP システムに接続するように設定します。

特定のフィールドに関する詳細な説明が必要な場合は、マウス・カーソルをツールヒント(?)の上に移動します。

LDAP 設定	説明
Authentication Settings(認証設定)	LDAP サーバ URL, ディレクトリの認証タイプなどの一般的な認証データ。 [Directory Provider URL(ディレクトリプロバイダ URL)]フィールドを SSL/TLS 用に設定する場合、次の構文を使用します。 <ul style="list-style-type: none"> • ldaps://<サーバ名>:<ポート> • ldap://<サーバ名>:<ポート> (LDAP サーバが SSL/TLS を使用するように設定されていない場合) [Test connection(テスト接続)]をクリックして LDAP サーバとの接続をテストします。
Base Settings(基本設定)	ユーザ取り込み元のディレクトリ・ノードの詳細、取り込むユーザ、一度に取り込むユーザ数。 [Result record limit(結果レコードの制限)]の値に、Agile Manager に一度にインポートするユーザ数を設定します。 同時に多数のユーザをインポートすると、時間がかかる可能性があります。
Field Mappings and Search Types(フィールド・マッピングおよび検索タイプ)	LDAP フィールドを Agile Manager フィールドにマッピングし、サポートする LDAP 検索を定義します。 電子メール・アドレス以外のログイン ID を使用する場合は、適切な LDAP フィールドを[Alternative Login ID(代替ログイン ID)]フィールドに入力します。 検索定義の詳細については、 「LDAP ユーザ検索の設定」(88 ページ) を参照してください。

2. 認証設定と基本設定の両方を検証するには、ページ上部の[**Test LDAP Settings(LDAP 設定のテスト)**]  をクリックします。
3. LDAP 設定を定義したら、Agile Manager 設定領域に進み、ユーザをインポートします([**サイト**] > [**ユーザ**])。このページには、Agile Manager サイト管理者のみがアクセスできます。

詳細については、Agile Manager ヘルプセンターを参照してください。

LDAP ユーザ検索の設定

[**Field Mappings and Search Types(フィールド マッピングおよび検索タイプ)**]の下で、各フィールドに対して有効にする検索タイプを選択します。次のいずれかを選択します。

オプション	説明
Contains(包含)	検索文字列と結果が完全には一致しない結果が返されます。 たとえば、フルネームのフィールドに対して[Contains(包含)]を選択して John を検索すると、John Doe, Johnny Smith, John Carter といったユーザが返されます。Jon という名前のユーザは返されません。
Equals(一致)	結果と完全に一致する検索文字列を指定する必要があります。 たとえば、フルネームのフィールドに対して[Equals(一致)]を選択すると、 John Doe といったユーザのフルネームを検索文字列として指定する必要があります。John だけの検索では John Doe は結果として返されません。
None(除外)	すべての検索でこのフィールドが無視されます。 たとえば、電話番号のフィールドに対して[None(除外)]を選択すると、管理者がユーザを電話番号で検索できなくなります。


ユーザ・ライセンスの更新

タブ: [Configuration(設定)] > [Licenses(ライセンス)]

Agile Manager は標準設定の **インスタント・オン** ライセンスでインストールされます。このライセンスは、100 ユーザで 30 日間使用できます。ユーザを追加する場合や、最初の 30 日が経過した後に Agile Manager にアクセスする場合は、ライセンスを追加購入してください。

HP から提供される **.dat** ライセンス・ファイルでシステムを更新することで、ライセンスを追加できます。ライセンスを更新したら、ライセンス・ファイルをセキュアな場所に格納して、不正アクセスを防ぎます。

.dat ファイルの準備が出来たら、次の手順を実行します。

1. ページ上部の[**+Update Licenses(ライセンスの更新)**]をクリックします。
2. **.dat** ファイルを見つけて選択します。
3.  [**Refresh(更新)**]をクリックして更新後のライセンス数をテーブルで確認します。

ユーザ数とライセンス数の調節

ライセンス数以上のユーザを追加またはインポートすると、これらのユーザは**非アクティブ**なユーザとして追加されます。ユーザ・ライセンスは、Agile Manager 設定領域([**サイト**] > [**ユーザ**])でユーザをアクティブまたは非アクティブにすることで数を調節します。このページには、Agile Manager サイト管理者のみがアクセスできます。

詳細については、Agile Manager ヘルプセンターを参照してください。

クラスタ設定でのライセンスのインストール

クラスタ設定で作業している場合、1つのノードにライセンスをインストールしても、そのライセンスが他のノードにも自動的にインストールされるとは限りません。

このような場合、ライセンスをインストールしていないノードから(ロード・バランサを経由せずに) Agile Manager 管理サイトに直接アクセスして、ライセンスを同様に更新します。ライセンスを適用するために、このノードを再起動します。

コンカレント・ライセンス

コンカレント・ライセンスは、同時にログインしているユーザのプールに適用されます。

最初のインストール時に、管理者は、コンカレント・**インスタント・オン**・ライセンスをインストールするか、固定ユーザ・**インスタント・オン**・ライセンスをインストールするかを選択できます。後者は、特定のユーザにのみ適用されます。

コンカレント・ライセンスの使用を計画している場合、最初に**インスタント・オン**・コンカレント・ライセンスを選択することを推奨します。

- 固定ユーザ・ライセンスとコンカレント・ライセンスを購入できますが、同じシステム上で両方のタイプのライセンスを使用することはできません。システム上で1つのタイプの購入済みライセンスをインストールしたら、別のタイプのライセンスをインストールすることはできません。
- インスタント・オンおよび評価用固定ユーザ・ライセンスは、購入したコンカレント・ライセンスによってオーバーライドすることができます。その逆も可能です。

詳細については、「[ライセンスの種類](#)」(90ページ)を参照してください。

ライセンスの期限切れ

有効期限付きライセンスが失効すると、そのライセンスでアクティブになっているユーザがすべて非アクティブになります(詳細については「[ライセンスの種類](#)」(90ページ)を参照)。引き続き Agile Manager を使用する場合はライセンスを追加購入してください。

非アクティブになるユーザにシステム管理者が含まれる場合、現在有効な別のライセンスがインストールされているかどうかの確認が Agile Manager で行われます。インストールされている場合は、そのライセンスにシステム管理者が移行され、Agile Manager を引き続き使用できます。

システム管理者は、Agile Manager のオンプレミス・システム管理サイトにアクセスできます。詳細については、「[システム管理者](#)」(91ページ)を参照してください。

ライセンスの種類

タイプ	説明
インスタント・オン	Agile Manager の試用版をダウンロードすると提供される初期ライセンス。100 ユーザで 30 日間使用可能です。
評価	指定した数のユーザが限られた期間内で使用できる評価用ライセンス。 さらに時間をかけて Agile Manager を評価する必要がある場合に、標準設定の インスタントオン ・ライセンスを置き換える目的で使用します。

タイプ	説明
永続的	特定数のユーザが無期限の期間内で使用できる購入ライセンス。ユーザ数を増やすにはライセンスを追加購入してください。
期限付き	特定数のユーザが限られた期間内で使用できる購入ライセンス。 この期間の終了後に引き続き Agile Manager を使用する場合や、ユーザを追加する場合は、ライセンスを追加購入する必要があります。

システム管理者の定義とユーザ・パスワードのリセット

タブ: [Configuration(設定)] > [Users(ユーザ)]

システム管理者

サイトに個々のユーザを追加するか、LDAP システムからユーザをインポートした後、特定のユーザを追加のシステム管理者として定義します。

システム管理者には、Agile Manager 管理サイトの読み取り書き込みアクセス権が与えられています。Agile Manager アプリケーションでは、システム管理者の特別な権限は標準設定されていません。

注: まず Agile Manager 設定領域 ([Site(サイト)] > [Users(ユーザ)]) でユーザの追加またはインポートを行ってから、ユーザをシステム管理者として定義する必要があります。このページには、Agile Manager サイト管理者のみがアクセスできます。

詳細については、Agile Manager ヘルプセンターを参照してください。

- ユーザをシステム管理者として定義するには、ユーザの行を選択して、[Set as System Administrator(システム管理者に設定)] をクリックします。
- 特定のユーザからシステム管理者のロールを削除するには、ユーザの行を選択して、[Remove from System Administrators(システム管理者から削除)] をクリックします。
- [Filter(フィルタ)] ボックスに氏名またはログイン名の全体または一部や電話番号を入力して、特定のユーザを検索できます。

ユーザ・パスワード

このページを使用して、(LDAP システム経由ではなく) Agile Manager で直接認証されるユーザのパスワードをリセットします。

1. グリッドでユーザを選択し、[Reset User Password(ユーザパスワードのリセット)] をクリックします。
2. 新しいパスワードを入力し、確認します。

一般的なシステム設定

タブ: [Configuration(設定)] > [General(一般)]

セキュリティ設定の定義

[Security(セキュリティ)]で、次の項目を設定します。

- **inactivity session timeout(無操作状態でのセッションのタイムアウト)**: 非アクティブなユーザを Agile Manager からログアウトさせるまでの時間(分)を指定します。

注: ユーザがログアウトするまで、最大 15 分の余分な遅延がある場合もあります。

この設定に対する変更は、ユーザがログアウトしてから再度ログインするまで有効になりません。

- **Allow 'sa' user to log in with AGM credentials(sa ユーザによる AGM 資格情報でのログインの許可)**: 標準設定の sa ユーザが、LDAP 設定にかかわらず、Agile Manager の資格情報を使用してログインすることを許可するかどうかを指定します。

この設定は、LDAP 認証が設定されているにもかかわらず、sa ユーザが LDAP システムに存在しない場合に使用されます。

注意:

- sa ユーザでないシステム管理者が存在する場合、このオプションを無効にすると、後で再び有効にすることはできません。
- sa ユーザが唯一のシステム管理者であるか、唯一のサイト管理者である場合、このオプションは無効にできません。

System Administrators(システム管理者) は [Users(ユーザ)] 管理サイト・ページで設定します。詳細については、「[システム管理者](#)」(91ページ)を参照してください。

サイト管理者(Site Administrators) は Agile Manager 設定領域([サイト] > [ユーザ])で設定します。詳細については、Agile Manager ヘルプセンターを参照してください。

添付ファイル設定の定義

添付ファイルとしてアップロードできるファイルのタイプの制限を定義します。次のものがあります。

- Maximum file size for each file uploaded(アップロードされるファイルの最大ファイル・サイズ)
- Maximum aggregated size for all attachments in the site(サイト内のすべての添付ファイルの最大合計サイズ)
- Blocked file extension types(ブロックするファイルの拡張子)

カスタム・フィールド設定の定義

管理者は、次のエンティティ・タイプに対してカスタム・フィールドを作成できます: テーマ、フィーチャー、ユーザ・ストーリー、不具合、バックログ項目(ユーザ・ストーリーと不具合の両方に適用)

次の制限を定義します:

- The maximum number of custom fields allowed in your site per entity type.(サイトで設定できるエンティティ・タイプあたりのカスタム・フィールドの最大数。)

標準設定 : 12

最大数 : 40

注:

- サイト管理者はこの割り当てをサイト・レベルとワークスペース・レベルに分割できます。詳細については、『Agile Manager ユーザーズ・ガイド』の「カスタム・フィールドの最大数」を参照してください。
- テーマ、フィーチャー、ユーザ・ストーリーに対して定義したカスタム・フィールドの合計数は、合わせて 40 を超えることができません。
このため、カスタム・フィールドの最大数を 14 以上に増やすと、3 つのすべてのエンティティ・タイプで同時にこの最大数に到達することができなくなります。

- The maximum number of values allowed per list field.(リスト・フィールドごとに許可される値の最大数。)

標準設定 : 20

最大数 : 100

レポート設定の定義

時系列のダッシュボード・グラフ用に、Agile Manager が日次データを集計する時間を定義します。

注: 変更した値を有効にするにはサーバを再起動する必要があります。

詳細パラメータの設定

タブ: [Configuration(設定)] > [Advanced Parameters(詳細パラメータ)]

詳細パラメータは、システムの標準設定の動作を変更するシステム・パラメータです。

通常、システム・パラメータは、HP カスタマ・サポートに指示された場合のみ定義してください。

- **+**[Add Parameter(パラメータの追加)] をクリックします。パラメータの名前と値のほか、オプションで説明を入力します。

注: スペースと次の特殊文字は、パラメータの名前に使用できません。

[\ ! @ # \$ % ^ & * () = + | < , > / ? { [] ~ " ; :]

- パラメータはカラムでソートします。または、パラメータの名前、値、説明の一部と一致する任意のテキストでフィルタ処理することもできます。

独自に定義できるシステム・パラメータ

- **PRODUCT_GROUP_FUSE**: サイトで定義できるワークスペースの数 (標準設定 = 100。400 より大きい値に設定しないことを推奨します)。
- **OPB_AGM_SERVER_URL**: Integration Bridge が Agile Manager にアクセスする際に使用する URL。詳細については、[「アプリケーション・サーバの設定」\(80ページ\)](#)を参照してください。
- **OPB_ENABLE_AUTO_UPGRADE**: Integration Bridge を自動的にアップグレードできるかどうかを指定します。

標準設定では、Integration Bridge は自動的にアップグレードされます。アップグレードを無効にするには、このパラメータを N に設定します。詳細については、[「添付ファイルおよびダウンロードのセキュリティ保護」\(54ページ\)](#)を参照してください。

フィードバックを送信



インストールおよび管理ガイドを使用してお気づきになった点をお知らせください。

電子メールの宛先: docteam@hpe.com

