



VMware vSphere® 6.5 の 新機能

テクニカル ホワイト ペーパー

目次

VMware vSphere 6.5 の新機能	4
VMware vCenter Server	4
移行	4
アプライアンス管理の強化	5
VMware vCenter High Availability	6
バックアップとリストア	8
vSphere Web Client	8
vSphere Client	9
コンテンツ ライブラリ	10
vSphere のホスト ライフサイクル管理の機能強化	10
vSphere Update Manager	10
VMware Tools と仮想ハードウェアのアップグレード	11
Windows ベース アーキテクチャも引き続きサポート	12
ホスト プロファイル	12
プロファイル管理の強化	12
運用に関する機能拡張	13
Auto Deploy	13
管理性の向上	13
パフォーマンスと耐障害性の向上	15
VMware Tools 10.1、10.0.12	15
署名付き ISO イメージ	15
レガシー ゲストと最新のゲストで異なる VMware Tools バージョンの使用	16
一般的なゲスト用の Tools のみ付属	16
ゲスト OS のより詳細な選択肢の提供	16
vSphere Web Client での VMware Tools のタイプとバージョンの詳細表示	16
VMware Tools インストーラーのアップデートの検出	17
vSphere の運用	17
運用管理	17
ログの監視	19
開発者向けインターフェイスと自動化インターフェイス	19
アプリケーション プログラミング インターフェイス (API)	19
vCenter Server Appliance API	19
仮想マシンの API	20
API を検出する新しい API Explorer	20
プロセスの改良	21
コマンド ライン インターフェイス	21
VMware vSphere PowerCLI	22

vSphere のコア モジュール	22
ストレージ モジュール	22
VMware Horizon モジュール	22
セキュリティ	23
仮想マシンの暗号化	23
vMotion の暗号化	24
セキュア ブートのサポート	25
仮想マシンのセキュア ブート	25
ESXi ホストのセキュア ブート	26
ログ機能の強化	27
仮想マシン サンドボックス	28
自動化	28
vSphere 6.5 の可用性の向上	29
Proactive HA	29
VMware vSphere High Availability による再起動のオーケストレーション	29
vSphere HA のアドミッション コントロールの強化	30
vSphere HA による NVIDIA GRID vGPU が構成された仮想マシンのサポート	31
VMware vSphere Fault Tolerance	31
リソース管理の強化	31
Predictive DRS	31
vSphere DRS のロード バランシング アルゴリズムの改良	32
vSphere DRS の追加オプション	32
ネットワークの使用率を認識する vSphere DRS (Network-aware DRS)	33
VMware vSphere Storage I/O Control におけるストレージ ポリシー ベースの管理 (SPBM) の使用	33
vSphere Integrated Containers	34
vSphere 6.5 のストレージの機能強化	35
アドバンスド フォーマット ドライブと 512e モード	35
UNMAP の自動化	35
LUN のスケーラビリティ	35
NFS 4.1 のサポート	36
ソフトウェア iSCSI のスタティック ルーティングのサポート	36
vSphere 6.5 のネットワークの機能強化	36
VMkernel ネットワーク アダプター専用のゲートウェイ	36
SR-IOV のプロビジョニング	36
ERSPAN のサポート	36
データパスの機能強化	37
まとめ	37
執筆者について	37

VMware vSphere 6.5 の新機能

VMware vSphere® 6.5 は、次世代のアプリケーションに対応する次世代のインフラストラクチャです。柔軟性と安全性に優れた強力な基盤を提供してビジネスの俊敏性を高め、クラウド コンピューティングへのデジタル トランスフォーメーションとデジタル エコノミーにおける成功を推進します。vSphere 6.5 は、1) 大規模環境の自動化と管理を可能にするシンプルなユーザー環境、2) データ、インフラストラクチャ、アクセスを保護するための包括的な組み込みのセキュリティ機能、3) あらゆるアプリケーションに対して最適な実行環境を提供するユニバーサル アプリケーション プラットフォームによって、既存のアプリケーションと次世代のアプリケーションの両方に対応します。vSphere 6.5 を使用することで、利用するクラウドやデバイスのタイプを問わずに、共通の運用環境でアプリケーションを実行、管理、接続、保護することが可能です。

このホワイトペーパーでは、vSphere 6.5 のさまざまなテクノロジー分野における 新機能と機能強化について説明します。詳細については、[VMware vSphere のドキュメント](#)を参照してください。

VMware vCenter Server

VMware vCenter Server® 6.5 には、多くの革新的な新機能があります。インストーラーが一新され、最新の操作感を提供します。また、Microsoft Windows、macOS、Linux の各オペレーティング システム (OS) で、プラグインを使用せずにインストーラを利用できるようになりました。vSphere 6.5 では、アプライアンス型の vCenter Server Appliance™ を大幅に強化しました。このため、vSphere 6.5 では、Windows ベースの vCenter Server ではなく、vCenter Server Appliance の使用をおすすめします。vCenter Server Appliance には次の独自の機能が実装されています。

- Windows ベースの vCenter Server からの移行ツール
- アプライアンス管理の強化
- ネイティブの高可用性機能
- ネイティブのバックアップとリストア

また、vSphere Web Client や、HTML5 ベースの vSphere Client の完全サポートなど、vCenter Server 6.5 では全般的に機能が強化されています。

移行

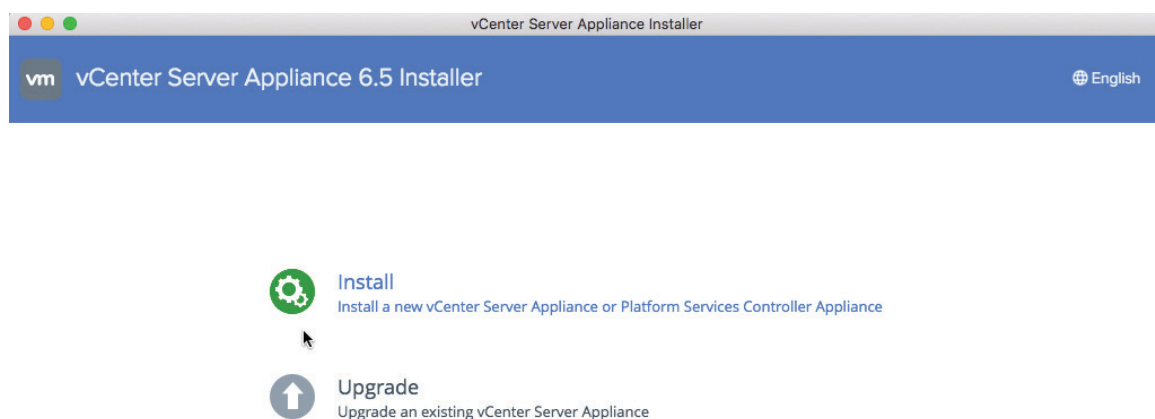


図 1: 移行やリストアも可能な最新の vCenter Server Appliance 6.5 インストーラー

インストーラーには移行ツールが組み込まれているため、vCenter Server Appliance 6.5 に容易に移行できます。この新バージョンの移行ツールは、以前の **vSphere 6.0 Update 2m** リリースと比較して、Windows vCenter Server 5.5 や 6.0 のサポートなど、いくつかの機能が強化されています。また、vCenter Server Appliance 6.5 には、VMware vSphere Update Manager™ が組み込まれています。このため、vSphere Update Manager 用の Windows Server を個別に管理することなく、vCenter Server Appliance に移行して、統合管理ができるようになりました。vCenter Server Appliance 6.0 にすでに移行しているお客様は、アップグレードすることで vSphere Update Manager のベースラインへの移行と vCenter Server Appliance 6.5 へのアップデートが可能です。移行の過程で、vCenter Server の設定、インベントリ、アラームのデータがデフォルトで移行されます。vSphere 6.5 では、移行対象データを次の 3 つから選択できます。

- 設定
- 設定、イベント、タスク
- 設定、イベント、タスク、パフォーマンス メトリック

データは、vSphere 5.5 または 6.0 でサポートされているデータベースから、組み込みの vPostgres データベースに移行されます。組み込みまたはリモートの環境で稼動している Microsoft SQL、Oracle、PostgreSQL の各データベースが対象となります。

アプライアンス管理の強化

vCenter Server Appliance 6.5 では、アプライアンス管理機能も強化されています。vCenter Server Appliance の管理インターフェイスは進化を続け、表示される設定データが増えています。CPU とメモリーの統計情報に加え、ネットワークとデータベースの統計情報、ディスク容量の使用状況、健全性のデータが表示されるようになりました。このため、コマンドライン インターフェイスを使用しなくても、大半の簡単な監視タスクや運用タスクを実行することができます。

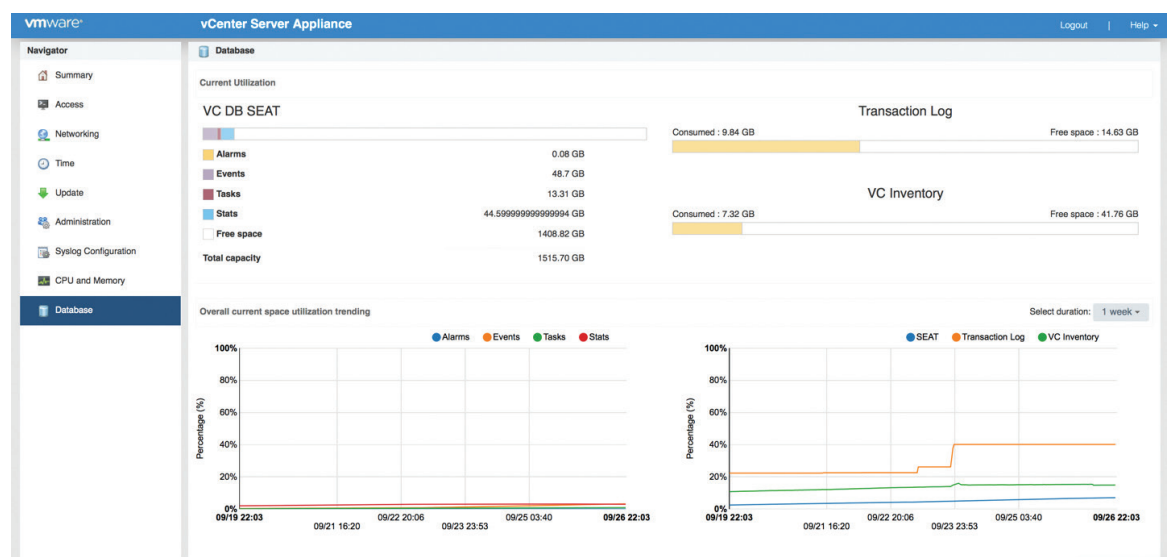


図 2 : vCenter Server Appliance の強化された管理インターフェイスに表示されるようになった vPostgres のデータ

vCenter Server または Platform Services Controller™ アプライアンスは、ポート 5480 を経由して vCenter Server Appliance の新しい管理インターフェイスにアクセスします。図 2 は、vCenter Server の新しいデータベース監視画面です。PostgreSQL データベースのディスク使用状況が詳細に表示されるため、空き容量不足に起因するクラッシュを防ぐことができます。データベースの容量が残り少なくなると、vSphere Web Client は新しいデフォルトの警告を表示して管理者に注意を促します。また、使用率が 95 % に達すると正常にシャットダウンするメカニズムも実装されているため、データベースの破損を防止できます。vCenter Server Appliance の強化された管理インターフェイスでは、Syslog を設定することもできます。

VMware vCenter High Availability

vCenter Server 6.5 には、vCenter Server Appliance のみで利用できるネイティブの高可用性ソリューションが新たに追加されました。このソリューションは、既存の vCenter Server インスタンスから複製されたアクティブ、パッシブ、ウィットネスの各ノードで構成されます。VMware vCenter® High Availability (vCenter HA) クラスタは、いつでも有効、無効、または破棄することができます。また、メンテナンス モードもあるため、計画的メンテナンスに起因する不要なフェイルオーバーを防止できます。

vCenter HA は、アクティブ ノードとパッシブ ノードの間で 2 種類のレプリケーションを使用します。vCenter Server データベースにはネイティブの PostgreSQL 同期レプリケーションを使用し、データベースを除く重要なデータにはファイル システムの非同期レプリケーション メカニズムを使用します。

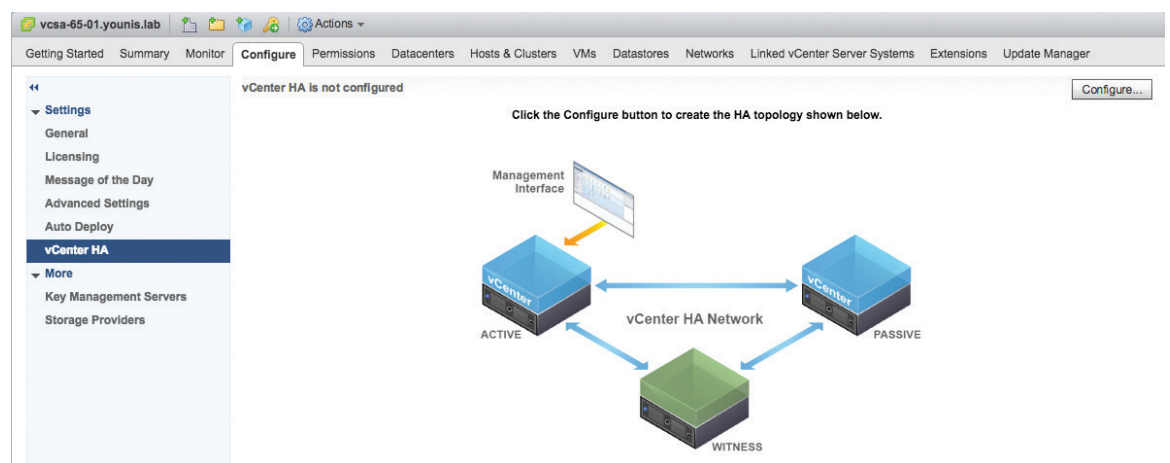


図 3：vCenter HA の設定ページ

vCenter HA は、「基本」と「詳細」の 2 つのワークフローで展開できます。基本ワークフローは、すべての vCenter HA ノードを同じクラスタで実行するほとんどのシナリオで使用できます。このワークフローは、その名のとおり非常にシンプルで、パッシブ ノードとウィットネス ノードを自動的に作成します。また、移行先のクラスタで VMware vSphere Distributed Resource Scheduler™ (vSphere DRS) が有効になっている場合は vSphere DRS の非アフィニティ ルールを作成し、VMware vSphere Storage DRS™ が有効になっている場合はこれを使用して初期配置を行います。このワークフローには柔軟性がある程度あり、ユーザーは、ノードごとに特定の移行先のホスト、データストア、ネットワークを選択できます。vCenter HA クラスタの運用を簡単に開始できます。もう 1 つの方法は、詳細ワークフローです。このワークフローは、アクティブ、パッシブ、ウィットネスの各ノードを、別々のクラスタ、vCenter Server インスタンス、またはデータセンターに展開する場合に使用できます。このプロセスでは、パッシブ ノード用とウィットネス ノード用に移行元の vCenter Server インスタンスを手動でクローン作成します。その後適切な IP アドレスを設定し、選択した場所にこれらのノードを配置する必要があります。基本ワークフローと比較すると複雑なプロセスですが、柔軟に設定することを希望するお客様に適しています。

アーキテクチャ面では、vCenter HA は組み込みと外部の両方の Platform Services Controller の使用をサポートしています。シングル サインオン ドメイン内にほかの vCenter Server インスタンスや Platform Services Controller インスタンスがない場合は、組み込みの Platform Services Controller インスタンスを使用できます。逆に、拡張リンクモードの構成で vCenter Server インスタンスが複数ある場合は、外部の Platform Services Controller インスタンスが必要です。Platform Services Controller を外部に配置した構成で vCenter HA を使用する場合は、Platform Services Controller インスタンスの高可用性を確保するためにロード バランサを外部に配置する必要があります。Platform Services Controller レイヤーで高可用性を確保せずに vCenter HA を使用するメリットはほとんどありません。vSphere 6.5 の Platform Services Controller インスタンスでサポートされているロード バランサには、VMware NSX®、F5 BIG-IP LTM、Citrix NetScaler があります。

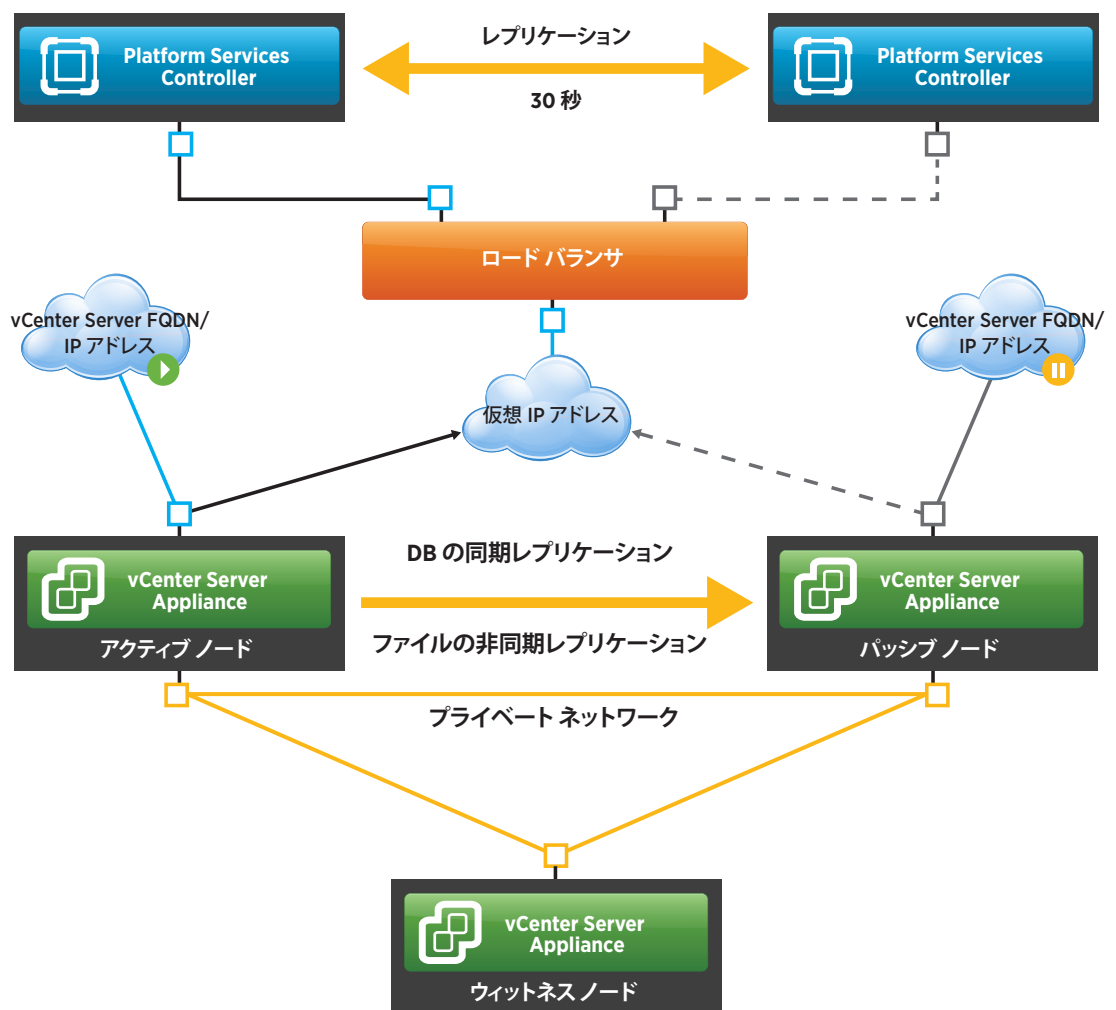


図 4：ロード バランサを使用した vCenter HA と Platform Services Controller HA のアーキテクチャ

ホスト障害などでノードが完全に失われた場合や、特定の重要なサービスが停止した場合に、フェイルオーバーが発生する可能性があります。vCenter HA の初期リリースでは、5 分程度の目標復旧時間（RTO）を予想していますが、これは基盤となるハードウェアの負荷、サイズ、機能に応じてわずかに変わる可能性があります。フェイルオーバー時には、フェイルオーバーが進行中であることを示す Web ページが一時的に表示されます。vCenter Server インスタンスがオンラインに戻ると、このページは vSphere Web Client のログイン ページに自動的に更新されます。フェイルオーバー時にアクティブではなかったユーザーは、再ログインを要求されない可能性があります。ただし、アクティブだったユーザーは一時的なスプラッシュ ページにリダイレクトされます。

新しいサービス ライフサイクル フレームワークである vMon により、Watchdog サービスも可用性が大幅に向上しています。vMon は、[vCenter Server 6.0 における Watchdog サービス](#) 5 つを唯一の正しい情報源としてまとめることで、vCenter Server サービスの管理と監視を簡素化します。vMon は、非常に複雑になることがあるサービスの依存関係を管理する際にも役立ちます。また、vCenter HA などの機能は、vMon を利用して別のノードにフェイルオーバーするタイミングを判断します。

バックアップとリストア

vCenter Server 6.5 の新機能として、vCenter Server Appliance のバックアップとリストアがネイティブでできるようになりました。詳細な設定が不要なこの新しい機能によって、ユーザーは vCenter Server や Platform Services Controller のアプライアンスを VAMI や API から直接バックアップできるようになります。バックアップ時には、SCP、HTTP (HTTPS)、FTP (FTPS) のいずれかのプロトコルを使用して、ユーザーが選択したストレージ デバイスに一連のファイルがストリーミングされます。このバックアップは、Platform Services Controller インスタンスが内部と外部のどちらに配置されているかに関係なく、vCenter Server Appliance インスタンスを完全にサポートします。

リストアのワークフローは、vCenter Server Appliance インスタンスまたは Platform Services Controller インスタンスを最初に展開またはアップグレードした ISO と同じ ISO から起動されます。新しい vCenter Server Appliance インスタンスが展開されたあと、選択したネットワーク プロトコルを使用してバックアップ ファイルを取り込みます。vCenter Server の UUID とすべての設定が維持されます。共通鍵暗号方式を使用してバックアップ ファイルを暗号化するオプションもあります。簡単なチェック ボックスと暗号化されたパスワードを使用してバックアップ セットが作成されたあと、リストア手順で同じパスワードを使用してバックアップ セットを復号化します。パスワードは可逆的暗号化を使用して保存されるわけではないので、パスワードを紛失した場合はバックアップ ファイルをリカバリできません。

vSphere Web Client

VMware は以前、[vSphere の次期リリースに C# クライアントが含まれないことを発表しました](#)が、vSphere 6.5 リリースがこれに該当します。VMware は、VMware PowerCLI™ や新しい vCenter Server REST API などのように、ツールを Web ベースまたは API ベースにする取り組みを進めています。

もっとも使用されているユーザー インターフェイスはおそらく vSphere Web Client です。このインターフェイスはこれまで同様に Adobe Flex プラットフォームを基盤としているため、使用するには Adobe Flash が必要です。VMware は、ユーザーの使用環境の改善に役立つ部分を特定するために継続的に取り組んできました。エンジニアリング部門は、過去 1 年間で何度か調査を行い、お客様がもっとも改善を求めている重要な部分を特定しました。

VMware は、これから示す効果的な部分を改善することで、vSphere Web Client のユーザーの使用環境全体を強化すると同時に、HTML5 ベースの vSphere Client の開発も進めていきます。はじめに、大部分の管理者がログイン時に最初にインベントリ ツリー ビューを開くため、ホーム画面ではなくインベントリ ツリーをデフォルトのビューにしました。お客様のフィードバックに基づいてホーム画面を再編成し、オプションのプラグインを、邪魔にならないように一番下に移動しました。もう 1 つの重要な変更点は、[Manage] タブの名前を [Configure] に変更したことです。このタブで実行できる操作を、名前から直感的に理解できるようになりました。また、管理者の要望に応え、一部の設定やワークフローの位置を変更しました。[Related Objects] タブを削除し、[Hosts]、[VMs]、[Datastores]、[Networks] に分けました。ユーザー インターフェイスをわかりやすくし、管理タスクを行うためのクリック回数を減らすことが目的です。

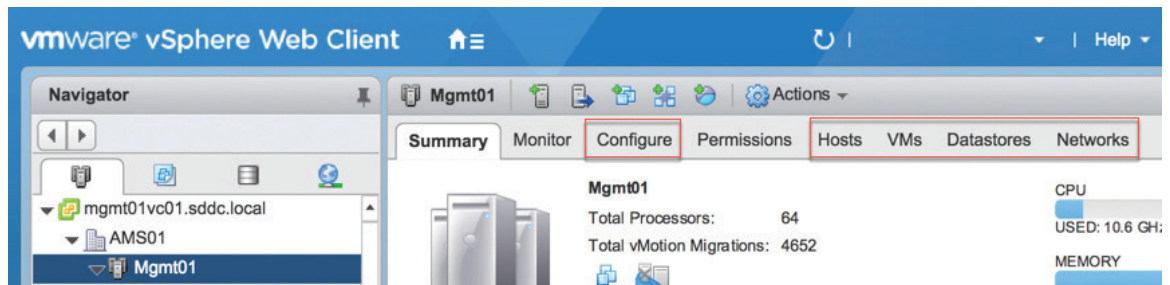


図 5 : [Related Objects] タブの分割を含む vSphere Web Client 6.5 の改善点

パフォーマンスの観点から、vSphere Web Client のユーザーの使用環境を改善するための取り組みを行いました。また、インベントリ ツリーに表示できる仮想マシンの台数が 100 倍になりました。ライブ更新機能も重要な機能強化の 1 つです。環境の運用状況をリアルタイムで表示する唯一の正しい情報源として vSphere Web Client を利用できるようになりました。自動タスク、ほかのサービスのタスク、ほかの管理者の操作を確認することができます。電源状態もリアルタイムで反映されるようになり、vSphere Web Client のユーザー使用環境が改善されました。

多くの一般的な管理タスクでプラグインが不要になりました。これは、vSphere Web Client だけでなく、vCenter Server Appliance の展開でも大きなメリットがあります。クライアント統合プラグイン (CIP) は、Web ブラウザー内のネイティブ機能に置き換わりました。vSphere 6.0 でこれまで CIP を必要としていた機能には、vCenter Server Appliance と Platform Services Controller アプライアンスのインストール、データストアへのファイルのアップロード、OVF と OVA の展開、コンテンツ ライブラリとの間のインポートとエクスポートがありました。

vSphere Web Client で Windows のパススルー認証やスマートカード ログインを使用する必要がある場合は、効率化された新しい拡張認証プラグインを使用できるようになりました。サービスの利用時にプラグインを必要とするユーザーは引き続き利用できますが、ほとんどの場合は必要ありません。プラグインの占有量と複雑さを大幅に軽減できるため、ブラウザーに依存する多くの問題が緩和されます。

vSphere Client

vSphere 6.5 では HTML5 ベースの vSphere Client が完全にサポートされており、これを vSphere Web Client と併用できます。この HTML5 vSphere Client は vCenter Server 6.5 (Windows とアプライアンスの両方) に組み込まれ、デフォルトで有効になっています。HTML5 vSphere Client は、まだ vSphere Web Client と同等の機能をすべて備えていませんが、管理者の日常的なタスクの多く、特に仮想マシンに関する機能を優先的に実装しています。また、フルタイムでの使用を可能にする機能も引き続き優先して実装されます。vSphere Web Client には、今後も <https://<vCenter Server の FQDN または IP アドレス >/vsphere-client> でアクセスできます。HTML5 vSphere Client には、<https://<vCenter Server の FQDN または IP アドレス >/ui> でアクセスできます。VMware は、vCenter Server の通常のリリース サイクルとは別に、HTML5 vSphere Client を定期的にアップデートする可能性があります。HTML5 vSphere Client は vCenter Server のほかの部分に影響を及ぼさずにアップデートできるため、お客様は HTML5 vSphere Client を常に最新の状態に維持できます。

新しい HTML5 vSphere Client のメリットを、次にいくつか示します。

- VMware の新しい Clarity UI 基準（ポートフォリオ全体で採用）に基づく、わかりやすく統一されたユーザー インターフェイス
- HTML5 をベースとする、ブラウザーやプラットフォームに依存しないアプリケーション
- ブラウザー プラグインのインストールや管理が不要
- vCenter Server 6.5 に統合され、完全にサポート
- 拡張リンク モードを完全にサポート
- Fling のユーザーがフィードバックでパフォーマンスを高く評価

HTML5 vSphere Client は 2016 年前半に [VMware Fling](#) として誕生しました。組み込みのフィードバック ツールを通じてお客様からたくさんのフィードバックが寄せられ、このフィードバックに基づいて、実装する新機能の優先順位を決めました。このツールは一般公開されるバージョンにも残る予定です。頻繁にはありませんが、Fling は今後もリリースされるため、最新の機能を試したいお客様は今後ともご利用いただけます。また、スタンドアロン アプライアンス形式が維持されるため、一般公開バージョンとの併用が可能です。ただし、ほかの VMware Fling と同様に、サポート対象外となります。

コンテンツ ライブラリ

vSphere 6.5 のコンテンツ ライブラリは、操作性が大きく向上しています。管理者は、コンテンツ ライブラリから ISO を直接マウントしたり、仮想マシンの展開時にゲスト OS のカスタマイズ仕様を適用したり、既存のテンプレートを更新したりできるようになりました。

パフォーマンス、復元性、スケーラビリティも向上しています。公開済みライブラリでのコンテンツの格納方法と同期方法は、最適化された新しい HTTP 同期オプションで制御します。このオプションを有効にすると、コンテンツは圧縮して格納されるため、拡張リンク モードを使用しない vCenter Server インスタンスとの間で短時間で同期できます。

コンテンツ ライブラリは vCenter Server の一部であるため、vCenter Server 6.5 の新機能を利用します。これには、vCenter Server Appliance が提供する vCenter HA と vSphere 6.5 バックアップ / リストア サービスが含まれます。

vSphere のホスト ライフサイクル管理の機能強化

vSphere 6.5 では、VMware ESXi™ ホストのパッチ適用とアップグレード、設定管理の機能が大幅に強化されています。

vSphere Update Manager

ESXi ホストを最新の状態に保つ方法としては、引き続き vSphere Update Manager をおすすめします。vSphere 6.5 では、vSphere Update Manager が vCenter Server Appliance に完全に統合されたため、以前のアーキテクチャで必要だった別個の仮想マシン (VM)、オペレーティング システム ライセンス、データベース用の追加リソースは不要になります。統合された vSphere Update Manager では、vCenter Server Appliance に含まれる vPostgres を利用しますが、データは別のスキーマを使用して保存されます。

vSphere Update Manager のユーザー インターフェイスは完全に vSphere Web Client に統合されています。一部のワークフローが効率化され、日常的な運用が改善されました。たとえば、管理者は新しいチェック ボックスを使用して、修正ウィザードで変更されたオプションを保存し、その後の操作に反映することができます。

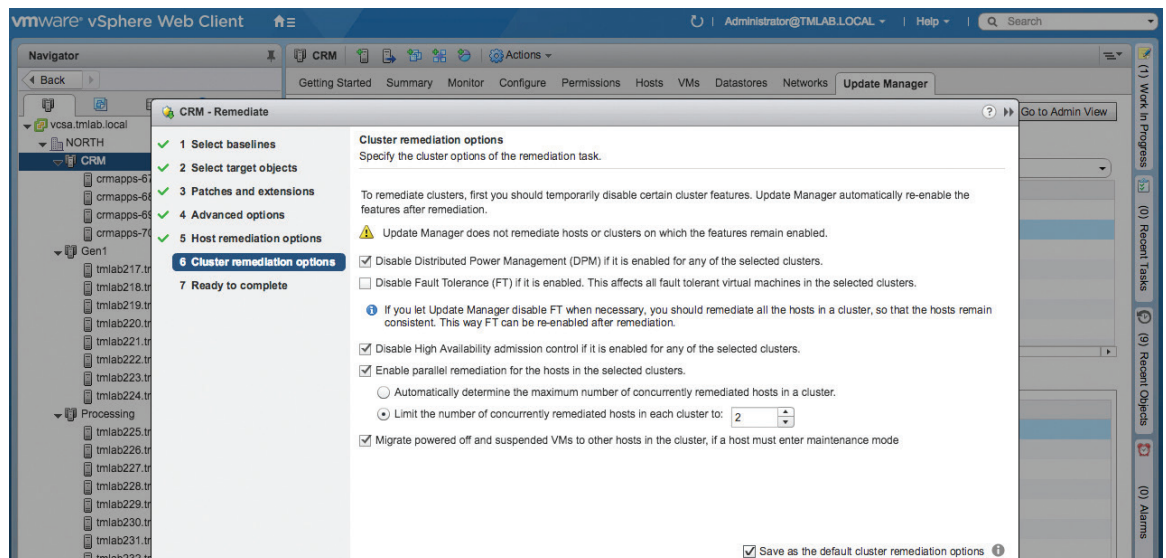


図 6：最新の修正ウィザード

vSphere Update Manager はデフォルトで有効になっているため、特に設定しなくてもすぐに使用できます。管理者はベースラインを作成し、既存のホストを ESXi 6.5 にアップグレードするか、ESXi のサポート対象バージョンにパッチを適用できます。

vCenter Server Appliance には、vCenter HA とアプライアンスのファイル ベースのバックアップという 2 つの新機能があり、これらを利用して vSphere Update Manager のダウンタイムを短縮できます（vCenter HA の耐障害性で冗長性を高め、アプライアンスのファイル ベースのバックアップで迅速にリカバリ）。

Windows ベースの vCenter Server から vCenter Server Appliance 6.5 への移行に関心があるお客様には、vCenter Server Appliance の移行ツールをご利用いただけます。

VMware Tools と仮想ハードウェアのアップグレード

vSphere Update Manager は、ESXi ホストのパッチ適用とアップグレードに加えて、VMware Tools™ や仮想マシンの互換性レベル、つまり仮想ハードウェアのアップデートにも使用できます。vSphere Update Manager 6.5 では、Linux 仮想マシンに関連して、この機能の次の 2 点が変更されました。

1 つ目の変更点は、vSphere に付属する VMware Tools（Tar Tools）を使用している Linux 仮想マシンが、VMware Tools のアップデート後に vSphere Update Manager によって不必要に再起動されなくなったことです。重要なストレージ、ネットワーク、その他のドライバはアップストリーム カーネルの一部として提供されるため、ほとんどの場合、VMware Tools のアップグレード後に Linux 仮想マシンを再起動する必要はありません。

2 つ目の変更点は、オペレーティング システム固有パッケージ（OSP）または Open VM Tools（OVT）のゲスト管理型 VMware Tools を使用している Linux 仮想マシンの場合、vSphere Update Manager を使用してその仮想ハードウェアをアップグレードできるようになったことです。これまで、vSphere Update Manager でアップグレードできたのは、Tar Tools を実行している仮想マシンのみでしたが、アップストリーム Linux ドライバの完成度が上がったため、この制約が緩和されました。

Windows ベース アーキテクチャも引き続きサポート

vCenter Server の展開モデルとしては vCenter Server Appliance をおすすめしますが、vCenter Server の Windows バージョンから移行する準備が整っていないお客様は、以前の vSphere Update Manager アーキテクチャを使用して運用を継続できます。vCenter Server がインストールされている仮想マシンとは別の Windows 仮想マシンに vSphere Update Manager 6.5 をインストールして、Windows ベースの vCenter Server に接続することはできませんが、vCenter Server Appliance と連携させて利用することはできません。

ホスト プロファイル

ホスト プロファイルは vSphere 4 で採用され、その後継続的に改善されてきました。このリリースでは、プロファイル自体の管理に加え、日常的な運用が大きく改善されています。

プロファイル管理の強化

vSphere Web Client に含まれるグラフィカル エディターがアップデートされ、使いやすい検索機能が加わりました。また、各設定要素をお気に入りとして登録して、簡単に利用できるようになりました。

さらに、設定を 1 つのプロファイルから 1 つまたは複数のプロファイルにコピーして差分を確認できる新しい機能により、管理者がホスト プロファイルの階層を作成できるようになりました。

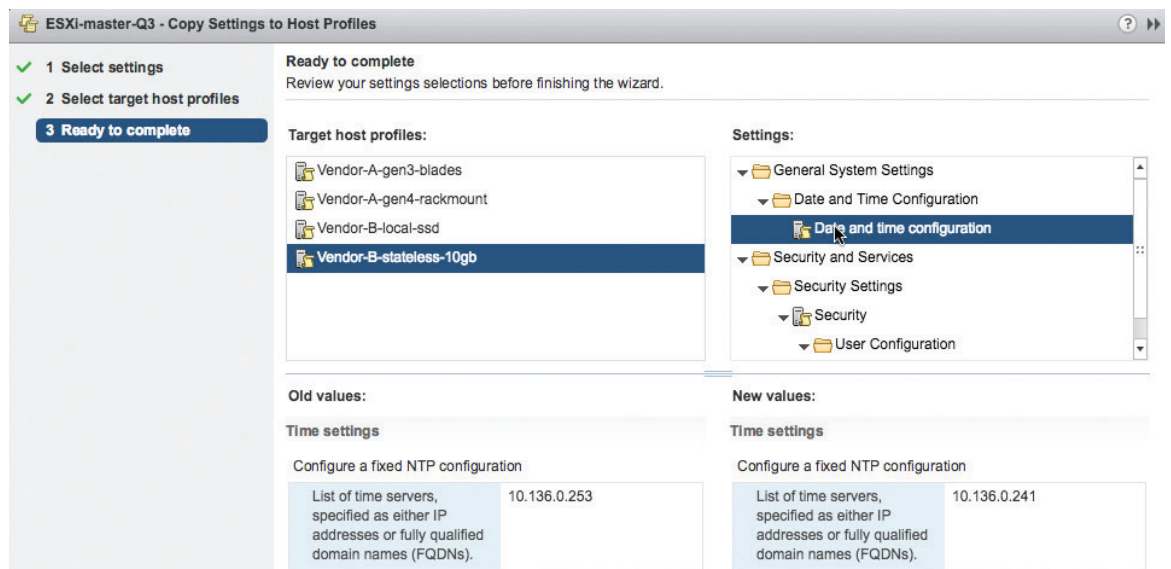
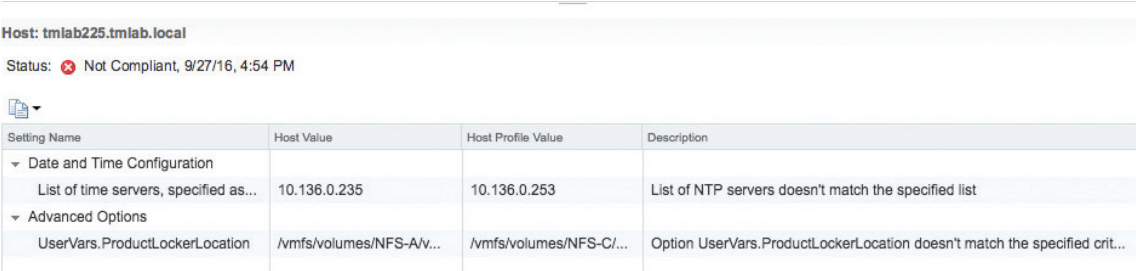


図 7：1 つのホスト プロファイルから 4 つのホスト プロファイルに設定をコピー

クラスタに複数の ESXi ホストが含まれる場合でも、固定 IP アドレスのように、各 ESXi ホストに異なる特性を設定できます。このように、ホストごとに値を設定するプロセスをホストのカスタマイズと呼びます。今回のリリースでは、CSV ファイルを使用して、複数のホストを含むグループの設定を管理できるようになりました。特に大規模環境の場合にこの機能は役立ちます。

運用に関する機能拡張

プロファイルの値とホストの実際の値を並べて詳細に比較できるため、コンプライアンスを詳しく確認できるようになりました。



Setting Name	Host Value	Host Profile Value	Description
▼ Date and Time Configuration			
List of time servers, specified as...	10.136.0.235	10.136.0.253	List of NTP servers doesn't match the specified list
▼ Advanced Options			
UserVars.ProductLockerLocation	/vmfs/volumes/NFS-A/v...	/vmfs/volumes/NFS-C/...	Option UserVars.ProductLockerLocation doesn't match the specified crit...

図 8：ホストとホスト プロファイルの設定値を示す詳細なコンプライアンス レポート

管理者は修正の前にチェックし、必要なホストのカスタマイズが行われているかどうか、また特定の設定を変更する際にメンテナンス モードにする必要があるかどうかを確認できます。

vSphere 6.5 では、設定の変更を反映するプロセスが大幅に最適化されています。メンテナンス モードを必要とする場合は vSphere DRS と連携し、メンテナンス モードを必要としない変更は並行して迅速に修正されます。

Auto Deploy

Auto Deploy は、業界標準の PXE テクノロジーを使用して、ローカル ディスクではなくネットワークから ESXi ホストを起動できる vSphere の機能です。ホストは、IP アドレスやホスト名など、さまざまな属性に基づく展開ルールを使用して、起動する ESXi イメージを判断します。展開ルールは vSphere の管理者が容易に更新できるため、単一のワークフローをあらゆるタイプの更新に使用して、パッチ適用やアップグレードを迅速に行うことができます。

管理性の向上

vSphere 6.5 では、全機能を備えた GUI が採用され、Auto Deploy が管理しやすくなりました。管理者が VMware PowerCLI を使用して展開ルールの作成や管理をしたり、ESXi イメージをカスタマイズしたりする必要はなくなりました。ただし、VMware PowerCLI を管理インターフェイスとして使用することも可能です。Auto Deploy の GUI を vSphere Web Client に表示するには、vCenter Server へのログイン時に Image Builder と Auto Deploy の両サービスが実行している必要があります。

新しい GUI の主要コンポーネントの 1 つに Image Builder があります。管理者は Image Builder を使用して ESXi イメージを VMware の公開リポジトリからダウンロードしたり、ESXi のイメージやドライバが含まれる zip ファイルをアップロードしたりできます。これらのイメージは、コンポーネントの追加や削除でカスタマイズしたり、必要に応じて ISO や zip にエクスポートして別の場所で使用したりできます。インターフェイスには比較ツールが含まれ、2 つのイメージの内容の違いを確認できます。

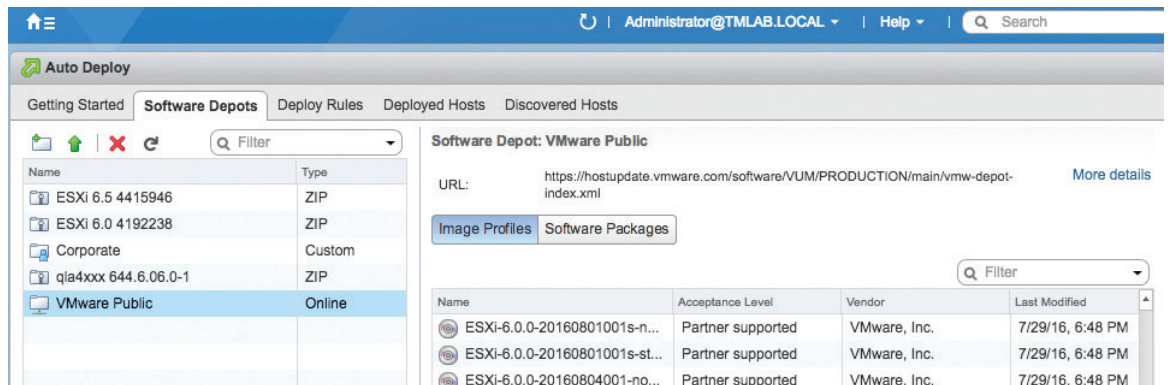


図 9 : Auto Deploy の [Software Depots] の GUI

新しい [Deployed Hosts] インターフェイス タブには、Auto Deploy を使用してプロビジョニングされたすべてのホストが一覧表示されます。このインターフェイスは、ホスト、イメージ、ホスト プロファイル、その他の属性の関連付けを確認する際の唯一の正しい情報源となります。また、管理者はこのインターフェイスを使用して各関連付けを対話形式でテスト、修正することもできます。これは展開ルールの編集後に通常必要な操作です。

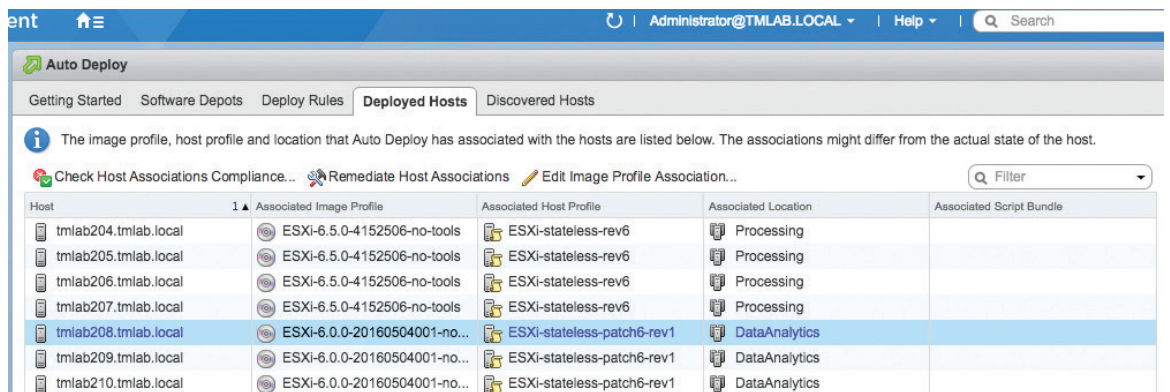


図 10 : Auto Deploy の [Deployed Hosts] の GUI

Auto Deploy から起動される未割り当ての新しいホストは、指示を待つ間、[Discovered Hosts] タブに集められます。対話形式の新しいワークフローを使用すると、展開ルールを作成せずにホストをプロビジョニングできます。このワークフローを使用してプロビジョニングされたホストも、パターン ベースの展開ルールでオンラインになったホストとともに、[Deployed Hosts] に一覧表示されます。

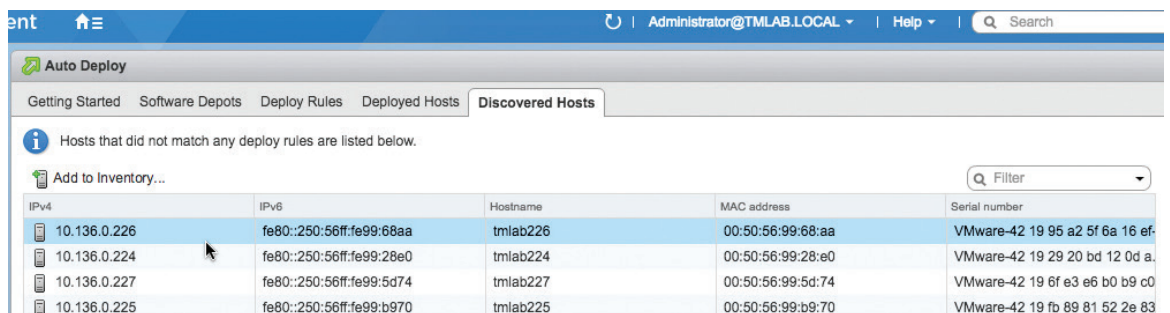


図 11 : Auto Deploy の [Discovered Hosts] の GUI

新しいスクリプトバンドル機能では、Auto Deploy で起動された ESXi ホスト上で自作のスクリプトを実行できるため、カスタム連携やその他の特殊な設定タスクが可能です。スクリプトは、ESXi と互換性がある shell や Python などのスクリプト言語で記述し、tar gzip (tgz) アーカイブにバンドルする必要があります。新しい VMware PowerCLI コマンドレット (Add-ScriptBundle) を使用して Auto Deploy サーバーにスクリプトバンドルをアップロードしたあと、ホストプロファイルやクラスタなどのほかのアイテムとともに、新しい展開ルールまたは既存の展開ルールと関連付ける必要があります。

パフォーマンスと耐障害性の向上

スケーラビリティが、これまでのリリースと比べて大幅に向上しています。Auto Deploy ではこれまでより数倍のホストを同時に起動できるようになりました。正確な数値については、『vSphere 6.5 の構成の上限』を参照してください。

アーキテクトが、フロントエンドのキャッシュ層を設計して vCenter Server Appliance からトラフィックをオフロードする場合、Auto Deploy 6.5 は業界標準のリバースプロキシキャッシュセットの取り込みを促進し、これをホストの起動時にラウンドロビン方式で使用しようとしています。使用可能なプロキシを Auto Deploy で利用できるようにするには、新しい VMware PowerCLI コマンドレット (Add-ProxyServer) を使用します。アクセスできるプロキシがない場合、ホストは vCenter Server Appliance から ESXi イメージを直接起動するデフォルトの動作に戻ります。この機能は、高可用性よりもパフォーマンスの最適化を目的としています。vSphere データセンターでホストを適切に設定してオンラインにするには、ホストの起動時に vCenter Server Appliance と Auto Deploy サービスが使用可能である必要があります。

Auto Deploy は、vSphere Update Manager と同様に、システムが停止した場合にネイティブの vCenter HA によって迅速にフェイルオーバーされます。より深刻な災害からリカバリできるように、Auto Deploy の設定は新しい vCenter Server Appliance のファイルベースのバックアップ機能にも取り込まれます。展開ルール、設定、SSL 証明書を含む Auto Deploy の完全な状態を、新しい VMware PowerCLI コマンドレット (Export-AutoDeployState) を使用して手動でエクスポートし、安全に保管することができます。

Auto Deploy は、VMware OEM パートナーが提供する最新のサーバーを使用しているお客様のために、BIOS と UEFI の両方のハードウェアをサポートするようになりました。通常の undionly.kpxe ではなく snponly64.efi iPXE エージェントを起動するように UEFI サーバーに正しく指示するためには、DHCP サーバーが設定されている必要があります。Auto Deploy 6.5 は、IPv4 と IPv6 の両方の環境で動作します。

VMware Tools 10.1、10.0.12

vSphere 6.5 には、VMware Tools の最新バージョンが含まれます。これは、仮想マシンのパフォーマンスの最適化と管理性の向上に役立つ、ゲスト内のドライバやエージェントの集合です。vSphere と VMware Tools のいくつかの新機能が連携して、ワークロードの全体的な管理が改善されています。

署名付き ISO イメージ

VMware Tools のインストーラーは ISO イメージとして配布され、各仮想マシンにマウントしてインストールまたはアップグレードできます。ESXi 6.5 では、これらの ISO イメージを読み取るたび暗号を使用して検証する新しいセキュリティレイヤーが採用されています。この検証を円滑化するため、VMware Tools のディストリビューションに、適切な署名を含むファイルが追加されています。

レガシー ゲストと最新のゲストで異なる VMware Tools バージョンの使用

VMware Tools 10.1 は、OEM がサポートするゲスト OS のみで利用できます。各ベンダーでサポートされていないゲストには、VMware Tools バージョン 10.0.12 が提供されます。このバージョンが今後機能強化される予定はありません。ゲスト OS のサポート分類の詳細については、[VMware ナレッジベースの記事 2097459](#) を参照してください。

一般的なゲスト用の Tools のみ付属

ESXi 6.5 には、一般的に使用されているゲスト OS 用の VMware Tools が含まれています。その他のゲスト用の Tools は、My VMware からダウンロードできます。同様に、同じゲスト用の VMware Tools のアップデートは、必要に応じて vSphere Update Manager を通じて配布されます。

VMware Tools のバージョン	vSphere に付属	ダウンロードのみ
10.1	Windows Vista 以降 Linux glibc2.5 以降	Solaris FreeBSD Mac OS X 10.11 以降
10.0.12	Windows Vista より前	Windows 2000 より前 Mac OS X 10.11 より前 Linux glibc2.5 より前 NetWare

表 1: VMware Tools 10.1、10.0.12 の分離

ゲスト OS のより詳細な選択肢の提供

前述した VMware Tools の 2 つのバージョンに対応するため、ゲスト OS の特定のファミリー向けに VMware Tools 10.1 と 10.0.12 の ISO イメージが用意されています。これにより、一部のゲストでより細かく属性を設定できるようになりました。

この変更のもっとも顕著な例が CentOS です。vSphere 6.5 では、CentOS ゲストを CentOS 7、CentOS 6、CentOS 4/5 から選択できるようになりました。旧リリースでは、これらのバージョンがすべて 1 つの選択肢となっていました (CentOS 4/5/6/7)。管理者はゲスト OS のタイプを編集するか、新しい仮想マシン設定オプション `tools.hint.imageName` を使用して、適切な ISO イメージをこれらの仮想マシンにマウントできます。

vSphere Web Client での VMware Tools のタイプとバージョンの詳細表示

VMware Tools のバージョンを指定する形式は 2 つあります。1 つは 10.0.7 などの人が理解できる数値で、もう 1 つは 10247 などの内部コードです。vSphere 6.5 では、この両方の形式のバージョン番号に加え、ゲスト OS にインストールされている VMware Tools のタイプ (MSI、OSP、OVT、Tar Tools) が vSphere Web Client に表示されるようになりました。

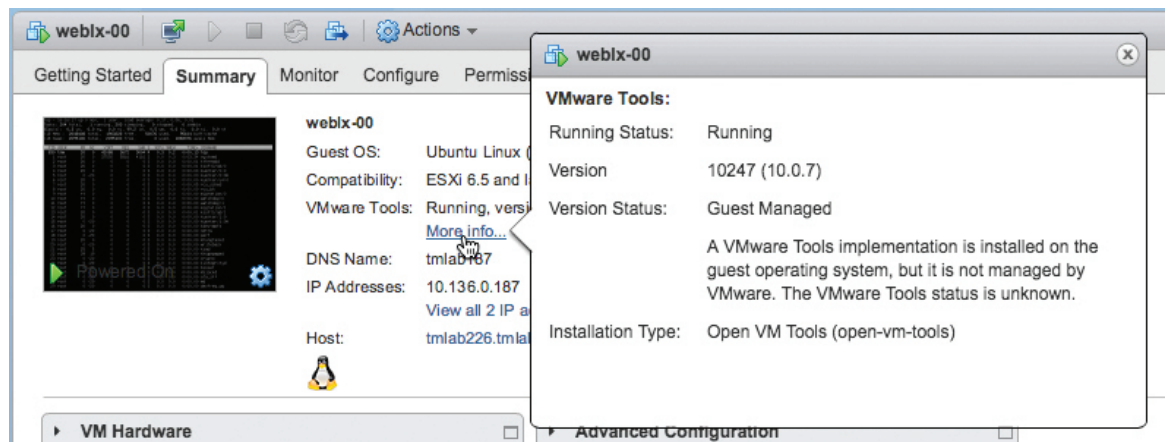


図 12：VMware Tools の詳細なバージョンとデータ タイプの表示

VMware Tools インストーラーのアップデートの検出

各 ESXi ホストは、VMware Tools インストール ISO イメージを含むローカル リポジトリまたは共有リポジトリを使用します。これまで、仮想マシンは電源投入時または移行時にのみ、VMware Tools のアップデートの有無を確認していました。vSphere 6.5 では、この確認が 5 分間隔で行われるようになりました。VMware Tools の新しいインストールイメージが見つかった場合は、アップデートが使用可能であることを示すアラートが仮想マシンに表示されます。

vSphere の運用

運用管理

vSphere の特定のエディション¹には、VMware vRealize® Operations Manager™ が含まれます。vSphere 6.5 のリリースでは、vRealize Operations Manager もバージョン 6.4 にアップデートされました。今回のアップデートには新しいダッシュボード、ダッシュボードの機能強化、その他の重要な機能が数多く含まれており、管理者は迅速かつ効率的に根本原因を判断できます。

vRealize Operations Manager には、多数のダッシュボードがデフォルトで用意されており、それぞれに環境の特定の部分が表示されます。vRealize Operations Manager 6.4 には、[Operations Overview]、[Capacity Overview]、[Troubleshoot a VM] の 3 つの新しいダッシュボードがあります。[Operations Overview] には、インベントリの概要、クラスタの更新、全体的なアラート量に加え、CPU の競合、メモリーの競合、ディスクの遅延が発生している上位 15 台の仮想マシンを示すウィジェットなど、関連する環境に関する情報が表示されます。[Capacity Overview] には、合計キャパシティ、CPU 数に使用されているキャパシティ、RAM、ストレージ ベースのメトリックなどの情報が表示されます。また、再利用可能なキャパシティに関する追加情報や使用率の分布も表示されます。[Troubleshoot a VM] ダッシュボードには、各仮想マシンに関する情報がまとめて表示されます。アラートや関係に加え、需要、競合、親クラスタの競合、親データストアの遅延に関するメトリックなどが表示されます。

¹ vSphere ライセンスの各エディションの詳細については、<http://www.vmware.com/jp/products/vsphere.html#compare> を参照してください。

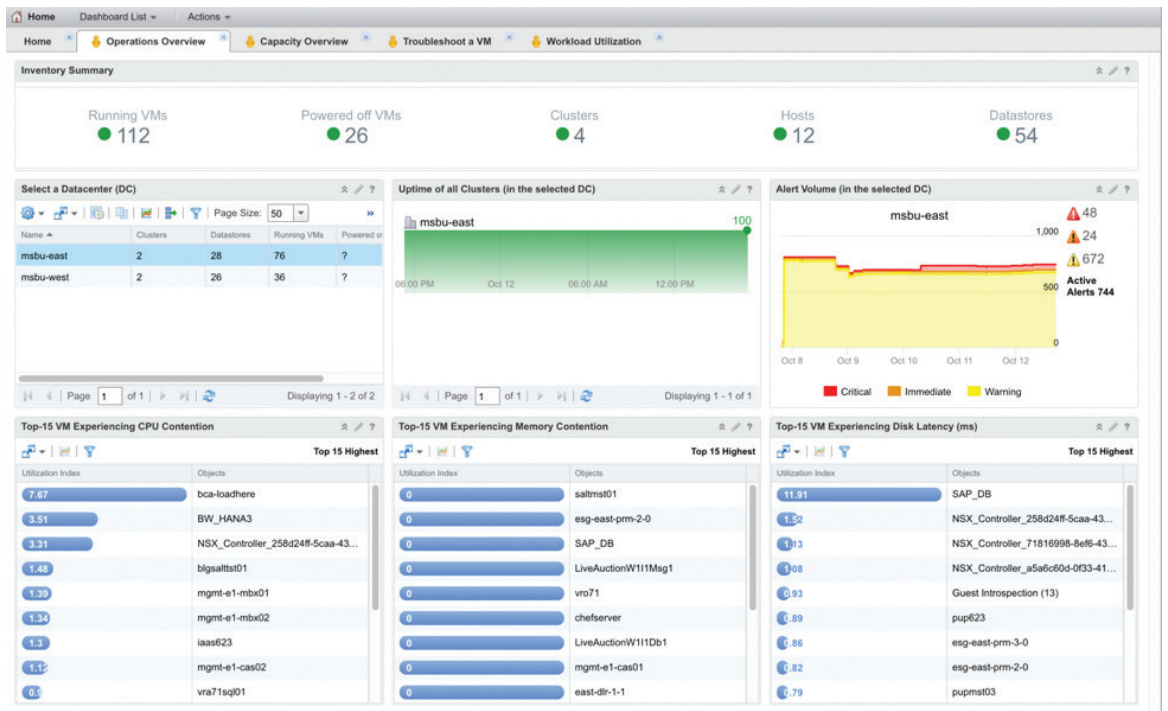


図 13: vRealize Operations Manager 6.4 の新しい [Operations Overview] ダッシュボード

vRealize Operations Manager 6.4 のダッシュボード以外の機能強化として、オブジェクトごとの新しいビューがあります。この新しいビューは、前回のバージョンで追加されたホーム ダッシュボードに似ていますが、ホーム ダッシュボードには選択されたオブジェクトのみが表示されます。この新しいビューに表示される情報には、アクティブ アラート、主要なプロパティ、主要なパフォーマンス指標 (KPI) のメトリック、関係に関するその他のデータが含まれます。

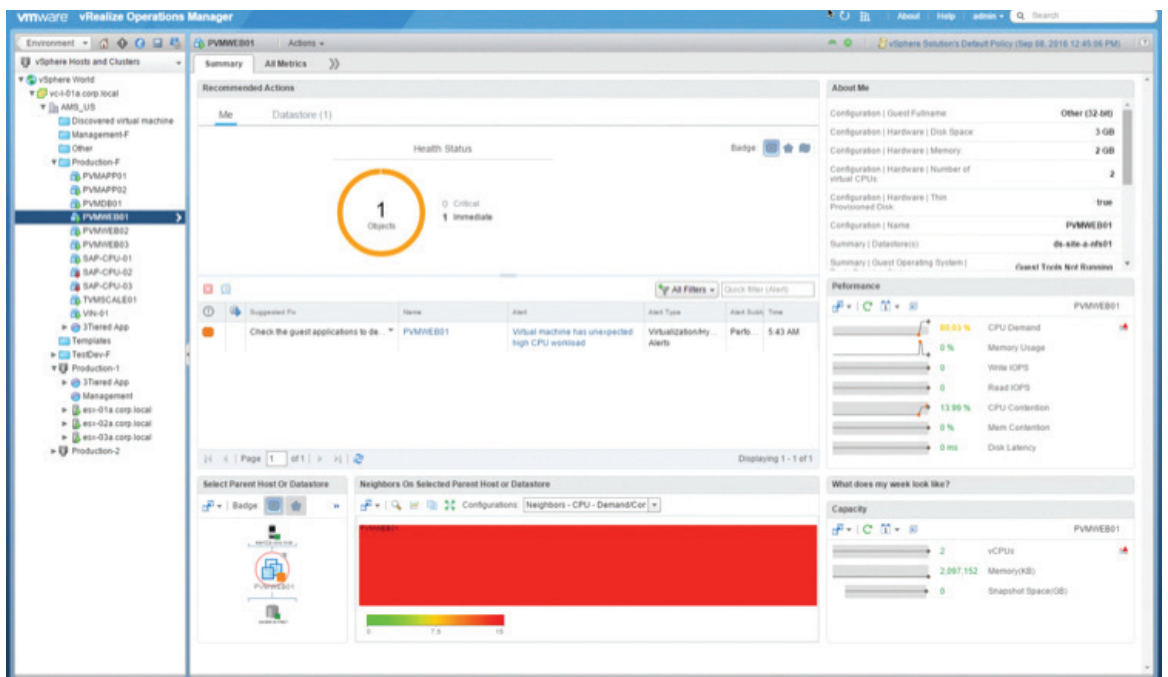


図 14: 新しいオブジェクト ベースのビューとデータへの効率的なアクセス

vRealize Operations Manager 6.4 には、ほかにも重要な機能強化があります。たとえば、[vSphere Hosts and Clusters Environment] ビューで vSphere の仮想マシン フォルダーを表示する機能や、優先度と対象範囲に応じてアラートをグループ化する機能があります。アラートをグループ化することにより、複数のアラートを一括で消去することもできます。KPI メトリックのグループ化機能もデフォルトで使用でき、ワンクリックで簡単にプロパティをグラフにしたり、相互に関連付けたりできます。

ログの監視

VMware vRealize Log Insight™ for vCenter™ も、管理者が問題の根本原因を迅速かつ効率的に判断するうえで重要です。vRealize Log Insight もバージョン 4.0 にアップデートされています。新しいバージョンには、新しい Clarity UI に準拠する UI、インストール プロセスに関連する API 機能の強化、エージェントへの自動アップデートを実行する機能、その他の全般的な UI の改善が含まれます。

開発者向けインターフェイスと自動化インターフェイス

vSphere 6.5 では、開発者と自動化の担当者の操作をさらに簡素化するために、開発者向けと自動化向けの機能が強化されています。アプリケーション プログラミング インターフェイス (API) とコマンド ライン インターフェイス (CLI) の両方でこれらの機能は強化されているため、お客様は言語バインディングや自動化ツールの利用方法を選択できます。

アプリケーション プログラミング インターフェイス (API)

vCenter Server では、REST ベースの API が新たに機能強化されています。vSphere 6.0 ではコンテンツ ライブラリとタグを管理する機能がこの API セットにありましたが、vSphere 6.5 では vCenter Server Appliance の管理と設定を行う機能と、基本的な仮想マシン管理機能が加わりました。

vCenter Server Appliance API

vCenter Server Appliance には、シンプルな新しい REST ベースの API が用意されており、次の機能を一貫して処理できます。

- アプライアンスの利用
- ユーザー アカウントの管理
- アプライアンスやそのサービスの健全性の確認
- ファイアウォール ルールやプロキシ設定などのネットワーク設定の管理
- アプライアンスのファイル ベースでのバックアップとリストア
- NTP などのシステム設定の管理
- 連続稼動時間やバージョンの確認

仮想マシンの API

仮想マシンを管理するための機能が追加されました。ユーザーは新しい REST ベースのインターフェイスを使用して、情報の読み取り、仮想マシンの作成 / 更新 / 削除、電源状態の設定、ハードウェアの操作を行うことができます。ハードウェアのタスクには、CD-ROM の接続、RAM 割り当ての更新、ネットワーク アダプターの追加、ハード ディスクの削除などが含まれます。

これらの機能はすべて開発者向けツールと自動化ツールから使用できるだけでなく、見つけやすいように簡素化されています。また、デフォルト設定が強化され、必要な情報を指定するだけで済みます。たとえば、仮想マシンを作成するために必要なのは、12 行の JSON を作成し、API を 1 回コールだけです。

API を検出する新しい API Explorer

vCenter Server の API Explorer は、使用できる API を検出するための新しい方法です。API Explorer では、API のモデルを理解できるようにするために、現在のエンドポイントで使用できる数々の API に関する情報が表示されます。また、ユーザーは各 API コールの拡張、必須項目の確認、リクエスト本文の理解、使用可能なフィルター情報や応答メッセージの一覧の確認を行うことができます。ユーザーは、API Explorer から直接 [Try It Out] ボタンを使用することもできます。このボタンを使用すると、API コールが実行され、ローカル システムから実行できる簡単な cURL コマンドが表示されます。

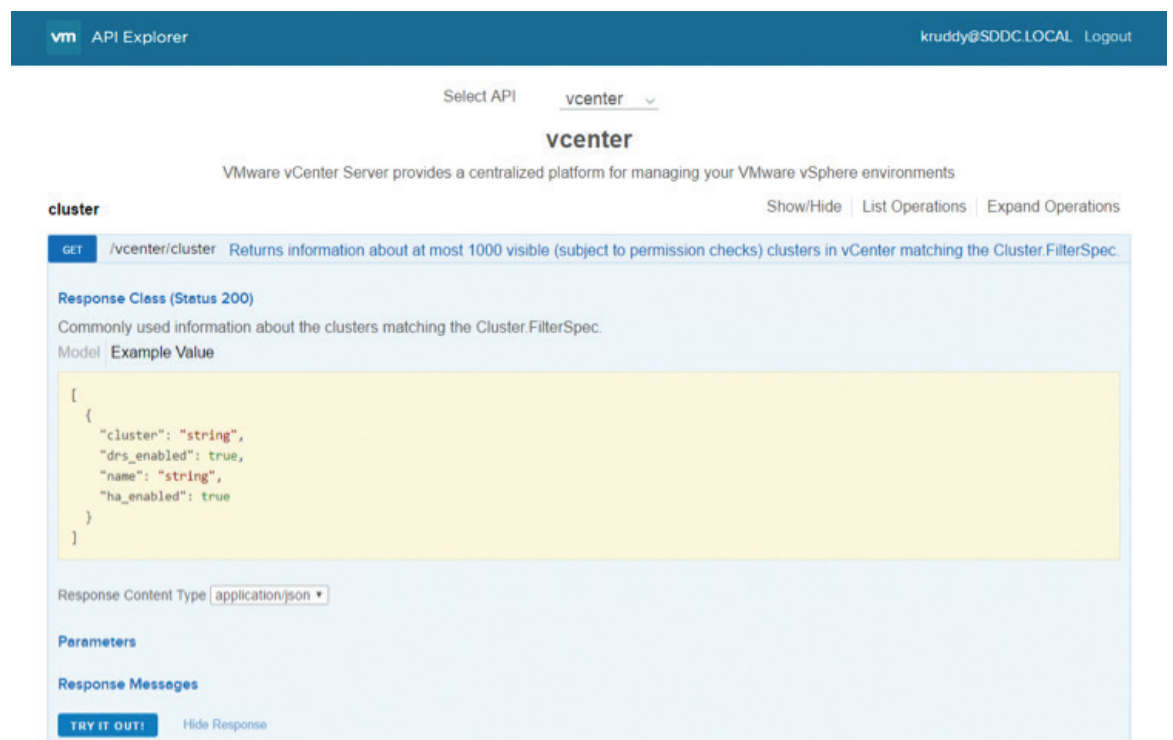


図 15：使用可能な API コールに関する情報を明確に表示する API Explorer

プロセスの改良

vSphere 6.5 では、これらの API の定義方法に関して、多くのプロセスが改良されています。また、開発者向けツールと自動化ツールの連携機能がデフォルトで提供します。ソフトウェア開発キット（SDK）は、Java、.NET、Python、Ruby、Perl などの複数の言語で自動的に生成されるようになりました。関連するドキュメントやサンプルは自動的に生成され、すべての機能が記載されているため、簡単に読んで理解できるようになっています。

The screenshot displays the VMware vCenter API documentation. On the left, a navigation pane lists various API categories under 'Operations', with 'vcenter' selected. The main content area is divided into two sections: 'cluster' and 'datacenter'. Each section provides a brief description of the service and a table of available API operations.

cluster

The cluster service provides operations to manage clusters in the vCenter Server.

Operation	HTTP request	Description
get	GET https://{server}/rest/vcenter/cluster/{cluster}	Retrieves information about the cluster corresponding to cluster.
list	GET https://{server}/rest/vcenter/cluster	Returns information about at most 1000 visible (subject to permission checks) clusters in vCenter matching the vcenter.cluster.filter_spec.

datacenter

The datacenter service provides operations to manage datacenters in the vCenter Server.

Operation	HTTP request	Description
create	POST https://{server}/rest/vcenter/datacenter	Create a new datacenter in the vCenter inventory
delete	DELETE https://{server}/rest/vcenter/datacenter/{datacenter}	Delete an empty datacenter from the vCenter Server
get	GET https://{server}/rest/vcenter/datacenter/{datacenter}	Retrieves information about the datacenter corresponding to datacenter.
list	GET https://{server}/rest/vcenter/datacenter	Returns information about at most 1000 visible (subject to permission checks) datacenters in vCenter matching the vcenter.datacenter.filter_spec.

図 16：最新の API ドキュメントの入手による API の理解と利用の効率化

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）は、環境内の効率と効果を最大限に高めたい vSphere の管理者と開発者の双方に最適です。CLI には、vSphere CLI と VMware PowerCLI の 2 つがあります。管理者は vSphere CLI を使用して、リモート マシンから ESXi や vCenter Server システムに対して一般的なコマンドを実行できます。このとき、ESXCLI とデータセンター CLI（DCLI）のコマンド セットが使用されます。VMware PowerCLI は Microsoft PowerShell を拡張したもので、VMware の多数の製品を操作できるコマンドレットが含まれます。

vSphere CLI では、ESXCLI と DCLI の両方のコマンドが更新されています。ESXCLI には、VMware vSAN™ のコアダンプ手順の処理、vSAN iSCSI 機能の利用、NVMe デバイスの管理を行う新しいストレージ ベースのコマンドと、その他の主要なストレージ コマンドが含まれるようになりました。また、ネットワーク側でも、キューイング、統合、基本的な FCoE タスクなどのネットワーク アダプター ベースのコマンドを処理するための機能が追加されました。DCLI では、前のセクションに記載した新しい vSphere REST API をすべて利用できるようになりました。

VMware vSphere PowerCLI

今回リリースで期待されていた VMware PowerCLI のアップデートの 1 つは、完全なモジュール式である点です。VMware は、VMware PowerCLI として他社に先駆けて PowerShell を採用しました。PowerShell v1.0 では、シェルを拡張して機能を追加する唯一の方法がスナップインでした。VMware PowerCLI のリリースのたびに、スナップインからモジュールへの進展があり、VMware PowerCLI 6.5 はその集大成です。

vSphere のコア モジュール

vSphere のコア モジュールもいくつかの点でアップデートされています。Move-VM コマンドレットが Cross vCenter vMotion に対応するようになりました。仮想マシンのコア数を指定する機能が New-VM と Set-VM の各コマンドレットに追加されました。Open-VMConsoleWindow コマンドレットでは、VMware Remote Client の最新バージョンが使用されるようになりました。

```
PowerCLI C:\> $sourceUC = "mgmt01vc01.sddc.local"
PowerCLI C:\> $destUC = "comp01vc01.sddc.local"
PowerCLI C:\> $sourceUCConn = Connect-UIServer -Server $sourceUC -Credential $creds
PowerCLI C:\> $destUCConn = Connect-UIServer -Server $destUC -Credential $creds
PowerCLI C:\> $vm = Get-VM -Name "MigrateVM01" -Server $sourceUCConn
PowerCLI C:\> $destination = Get-UMHost -Server $destUCConn ! Select-Object -First 1
PowerCLI C:\> $networkAdapter = Get-NetworkAdapter -VM $vm -Server $destUCConn
PowerCLI C:\> $destinationPortGroup = Get-UDSwitch -Name "vDS-Comp" -Server $destUCConn ! Get-UDPortgroup -Name "vDS-Comp-Management" -server $destUCConn
PowerCLI C:\> $destinationDatastore = Get-Datastore -Name "vsanDatastore" -Server $destUCConn
PowerCLI C:\> Move-VM -VM $vm -Destination $destination -NetworkAdapter $networkAdapter -PortGroup $destinationPortGroup -Datastore $destinationDatastore
```

Name	PowerState	Num CPUs	MemoryGB
MigrateVM01	PoweredOn	1	4.000

```
PowerCLI C:\>
```

図 17 : vSphere vMotion で Move-VM を使用して vCenter Server インスタンス間で仮想マシンを移行する例

ストレージ モジュール

ストレージ モジュールも複数の点で大きくアップデートされています。今回のリリースで多数の新しい vSAN コマンドレットが採用されました。vSAN クラスタ構成の取得と設定、vSAN のフォルト ドメインの管理、HCL データベースのアップデート、さまざまな vSAN テストの実行などの新しい機能があります。VMware vSphere Virtual Volumes™ レプリケーションを操作するコマンドレットもストレージ モジュールに追加されました。レプリケーション グループの取得と同期、レプリケーション フェイルオーバー準備の取得と開始、レプリケーション フェイルオーバーの開始といった機能がすべてコマンドレットとして追加されています。

VMware Horizon モジュール

VMware Horizon® モジュールは、完全に書き換える形で大幅にアップデートされています。このモジュールは、VMware Horizon Connection Server だけでなく、どこからでも実行できるようになりました。また、VMware PowerCLI インストーラーの一環としてインストールされるようになりました。コマンドレットは 2 つのみで、ユーザーは Horizon の Connection Server に接続するか、Connection Server から切断するかのいずれかです。ただし、接続すると、サーバーの ExtensionData プロパティを使用して Horizon パブリック API に完全にアクセスできます。リリース後は、VMware PowerCLI のサンプル スクリプトの GitHub リポジトリから、モジュールとともに使用できる高度な機能を手に入れます。

セキュリティ

vSphere 6.5 では、仮想マシンの暗号化、vMotion の暗号化、仮想マシンのセキュア ブートのサポート、ESXi のセキュア ブートとハイパーバイザーの暗号保証などの新機能によって、汎用的であると同時にスケーラビリティに優れたセキュリティと運用効率を実現しています。また、vSphere 6.5 では Syslog の機能が強化されており、監査目的での利用が可能な粒度でイベントが記録されます。

仮想マシンの暗号化

仮想マシンの暗号化は、仮想マシンに依存しない暗号化手法で、スケーラビリティに優れ、実装と管理が容易です。

仮想マシンの暗号化には多数のメリットがあります。

1. 仮想マシンではなくハイパーバイザー レベルで暗号化されるので、ゲスト OS とデータストアのタイプに関係なく使用できます。
2. ポリシーで暗号化を管理します。ゲスト OS に関係なく、多数の仮想マシンにポリシーを適用できます。仮想マシンが暗号化されているかどうかは、ポリシーが適用されているかどうかで確認できます。使用されるポリシー フレームワークでは、vSphere のストレージ ポリシー ベースの管理 (SPBM) が利用されます。
3. 暗号化は仮想マシン内で管理されません。これは、重要な違いです。ゲスト内の設定や監視が必要となる暗号化の「特例」はありません。暗号化キーは仮想マシンのメモリー内に格納されず、またどのような方法でも仮想マシンからアクセスできません。
4. キー管理には業界標準の Key Management Interoperability Protocol (KMIP) を使用します (KMIP バージョン 1.1 に準拠)。vCenter Server は KMIP クライアントと見なされ、多数の KMIP 1.1 キー マネージャーに対応します。このため、お客様の選択肢が広がり、柔軟性が向上します。また、キーの使用とキーの管理を別々の担当者に割り当てることができます。たとえば、大規模企業では vCenter Server を使用して、セキュリティ部門がキーを管理し、IT 部門がキーを使用することができます。
5. 仮想マシンの暗号化では、CPU ハードウェアの最新テクノロジーが AES-NI 暗号化で利用されます。Advanced Encryption Standard New Instruction (AES-NI) セットは、x86 の命令セットの拡張であり、CPU のコアごとに暗号化と復号化を高速で行います。

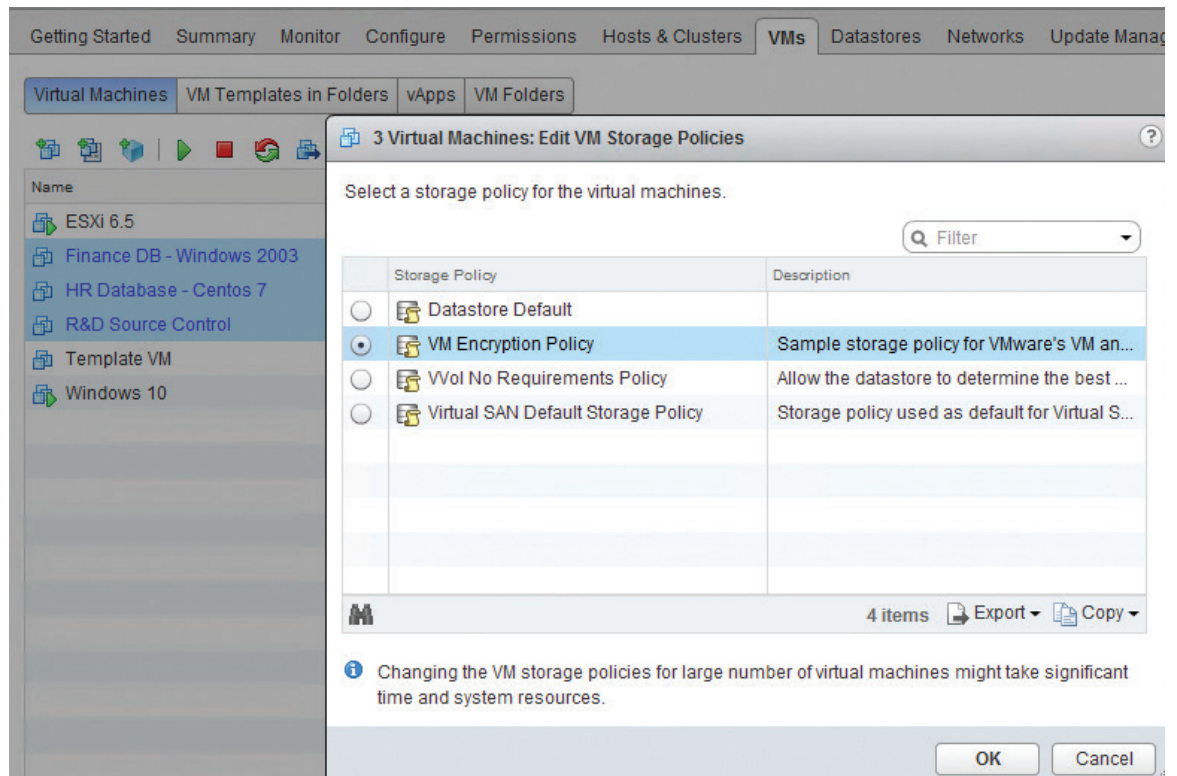


図 18：仮想マシンのストレージ暗号化ポリシー

vMotion の暗号化

vMotion の暗号化は、仮想マシン単位で設定します。ネットワーク自体が暗号化されるのではなく、ネットワーク上を送信されるデータが暗号化されます。このため、柔軟性に優れ、容易に実装できます。256 ビットのランダム キーと 64 ビットの nonce（ナンス）が生成され、これを 1 回だけ使用して VMware vSphere vMotion® で移行されます。nonce は、ネットワーク上を送信されるすべてのパケットに一意的カウンターを生成する際に使用されます。この方法でリプレイ攻撃を防止し、128 ビットのデータ ブロックを 264 個暗号化できます。

キーと nonce は、vSphere vMotion の移行の仕様にパッケージングされます。移行の仕様は、vCenter Server インスタンスと ESXi ホストの間の暗号化された既存の管理接続を通じて、クラスタ内の両システムに送信されます。

vSphere vMotion のトラフィックでは、はじめにホスト A でキーと nonce を使ってすべてのパケットが暗号化されます。独自に暗号化された各パケットは受け取り側のホスト B で復号化され、vSphere vMotion による移行が完了します。

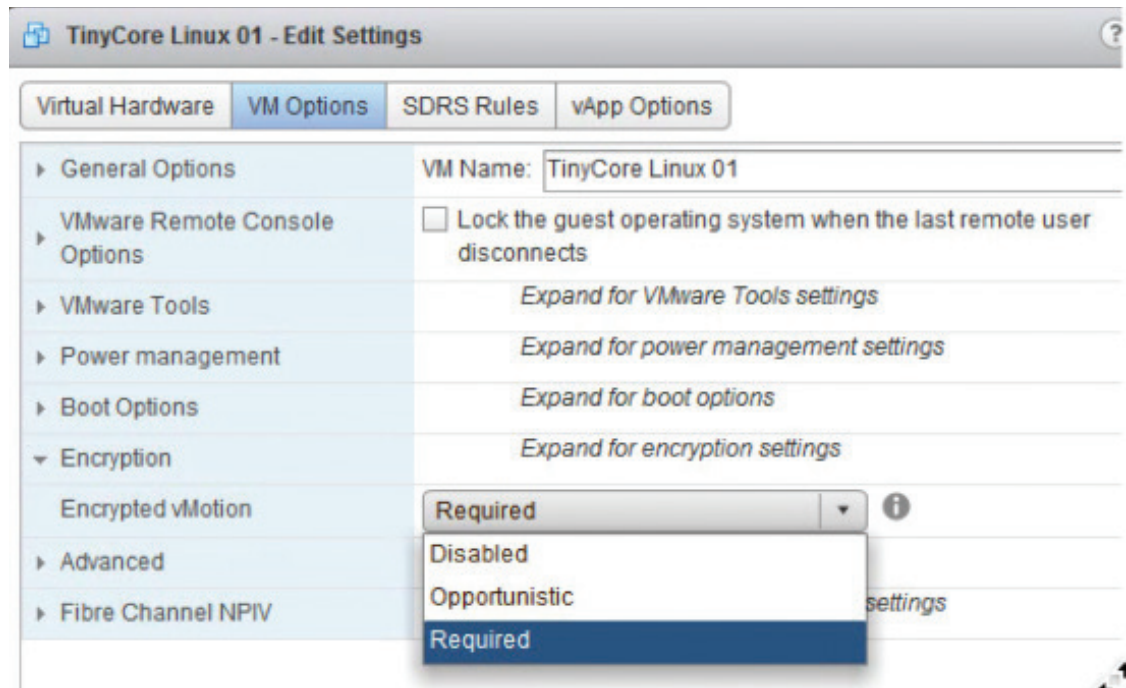


図 19 : vMotion の暗号化オプション

セキュア ブートのサポート

vSphere 6.5 では、仮想マシンと ESXi ハイパーバイザーのセキュア ブートをサポートするようになりました。UEFI セキュア ブートは、OS ハンドオフ前に信頼できるコードだけが EFI ファームウェアによって読み込まれるメカニズムです。信頼の可否は、ファームウェアで管理されるキーと証明書で判断されます。仮想マシンでこの機能を実装すると、仮想マシン内の EFI 対応 OS のセキュア ブートが可能です。

仮想マシンのセキュア ブート

セキュア ブートを有効にするには、仮想マシンを EFI ファームウェアから起動する必要があります。EFI ファームウェアは、Windows、Linux、ネストされた ESXi をサポートしています。セキュア ブートが機能するためには、ゲスト OS もセキュア ブートをサポートしている必要があります。たとえば、Windows 8 と Windows Server 2012 以降、VMware Photon™ OS、RHEL/Centos 7.0、Ubuntu 14.04、ESXi 6.5 などの OS がセキュア ブートをサポートしています。

仮想マシンに対してセキュア ブートを有効にするのは簡単で、UI で該当するチェック ボックスを選択するだけです。

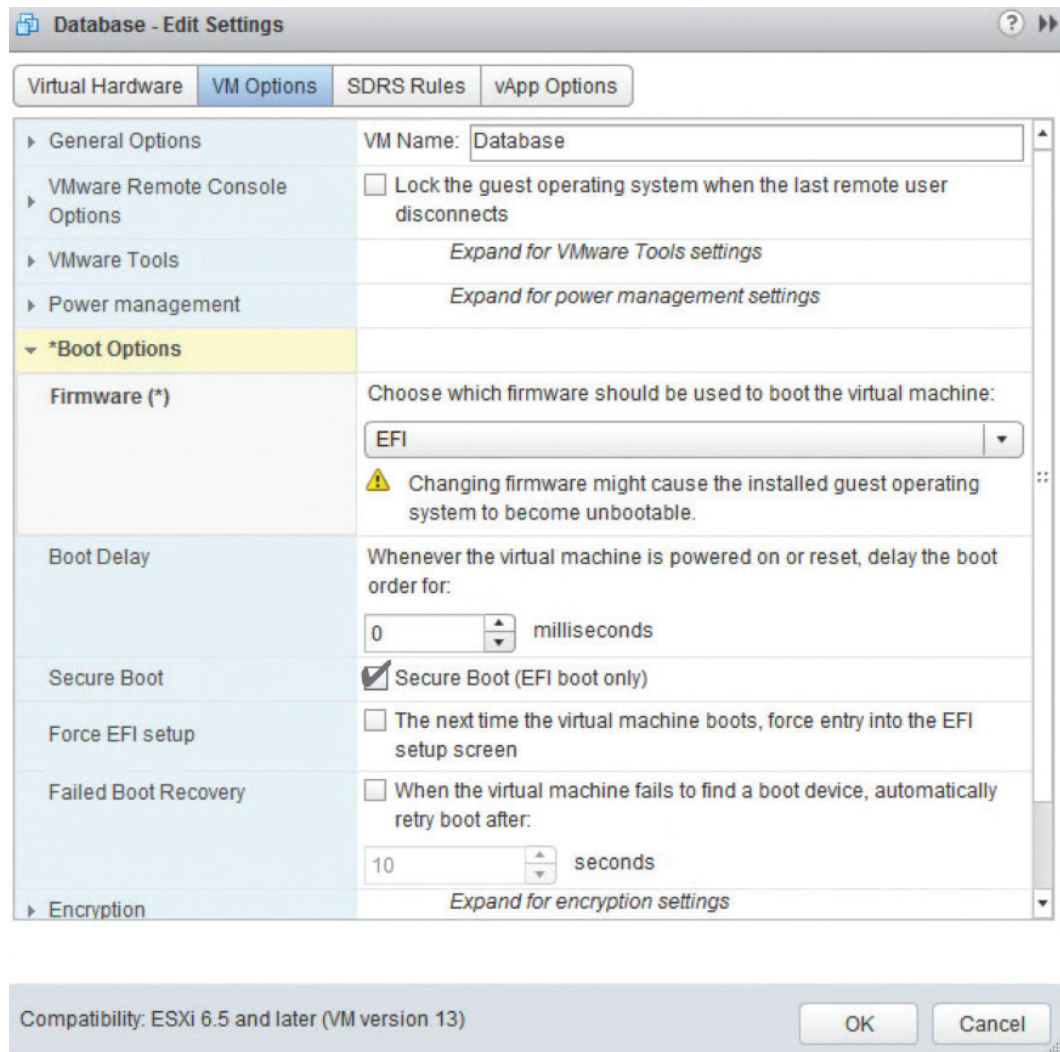


図 20：仮想マシンのセキュア ブートのオプション

ESXi ホストのセキュア ブート

セキュア ブートを有効にすると、UEFI ファームウェアは、UEFI ファームウェアに保存されているデジタル証明書に基づいて、デジタル署名付き OS カーネルを検証します。ESXi 6.5 では、さらに ESXi カーネルでもこの機能が利用され、ESXi コンポーネントの暗号保証が追加されています。

ESXi はすでに vSphere インストール バンドル (VIB) と呼ばれるデジタル署名付きパッケージで構成されており、安全にパッケージングされています。起動時に ESXi のファイルシステム (visorfs) がこのパッケージのコンテンツをマッピングし、その後にカーネルによってホスト UEFI ファームウェア内にある同じデジタル証明書を利用して VIB の正当性が検証されます。これにより、不正なコードを利用した起動を未然に防ぐことが可能となります。

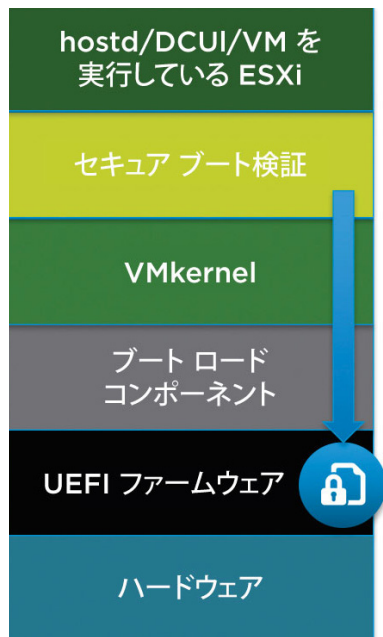


図 21: セキュア ブート検証

セキュア ブートが有効になっているときは、署名のないコードをロードして ESXi を起動することができません。ペータドライバなど署名のないコードを実行するには、セキュア ブートを無効にする必要があります。署名のない VIB がインストールされている場合にセキュア ブートを有効にすると、セキュア ブート検証機能が実行され、署名のない VIB が検出されてシステムがクラッシュします。これをパープル スクリーン (PSOD) イベントといいます。クラッシュ時には、削除する必要がある VIB が通知されます。修正するには、セキュア ブートを無効にして ESXi ホストを起動し、VIB を削除してから、セキュア ブートを有効にしてホストを再起動します。

ログ機能の強化

vSphere 6.5 では、監査に使用できるログ記録機能が実装されています。vSphere 6.5 より前のバージョンでは、ログの目的は IT の運用やセキュリティではなく、「トラブルシューティング」でした。たとえば、仮想マシンを再構成してあるネットワークから別のネットワークに移動した場合、ログの情報のほとんどは「仮想マシン <仮想マシン名> が再構成された」ことを示すもので、監査利用に対しては不十分でした。

現在は、Syslog を通じて vCenter Server から出力されるログが追加され、vCenter Server イベントの情報が記録されるようになりました。これらのログには設定の変更前と変更後が明確に表示されます。vSphere 環境内での変更点が具体的に示されるので、IT 部門やセキュリティ部門の管理者は、トラブルシューティングしやすくなります。図 22 では、仮想マシンを「PCI-vSwitch」というラベルのネットワークから「Non-PCI-vSwitch」に移動しています。「PCI-vSwitch」というラベルは、ネットワークが安全な PCI (Payment Card Industry) ネットワーク トラフィックの範囲内にあることを示しています。

d Table	Event Types	Event Trends	1 to 2 out of 2 events	View ▾
<pre> 2016-08-12T16:37:49.586202+00:00 mgt-vc-01 vpxd 3546 - - [46197] [1-1] [2016-08-12T16:37:49.585736Z] [vim.event.VmReconfiguredEvent] [info] [VSPHERE.LOCAL\Administrator] [Datacenter] [46196] [Reconfigured TinyCore esxi-vsan-2.lab1.local in Datacenter. </pre>				
Modified:				
<pre> config.changeVersion: "2016-08-12T16:37:42.7008Z" -> "2016-08-12T16:37:45.978741Z"; </pre>				
<pre> config.hardware.device(4001) deviceInfo.summary: "PCI-vSwitch" -> "Non-PCI-vSwitch"; </pre>				
<pre> config.hardware.device(4001) backing.deviceName: "PCI-vSwitch" -> "Non-PCI-vSwitch"; </pre>				

図 22 : vSphere 6.5 のイベント ログ

PCI の範囲内にある仮想マシンを PCI ネットワークから PCI 以外のネットワークに移動した場合、深刻なセキュリティの問題となります。vSphere 6.5 の強化されたログ機能では、Syslog を通じてログ ソリューションに直接通知が出力されます。ここで解析され、アラートが生成されて、影響を受ける担当者に深刻な状況が伝えられます。

vSphere 6.5 では、仮想マシンの変更だけでなく、vSphere のすべての変更についてログ機能が強化されています。vCenter Server のロールや権限の変更、仮想マシンのダウンロードなどのデータストアの参照、vCenter Server のクラスタやホストの作成や変更などの操作で、ログが詳細に出力されるようになりました。

vSphere 5.x や 6.0 のログ機能を使用していたときのように、このような変更のために、ログ レベルを「情報」から引き上げる必要はありません。また、vCenter Server インスタンスの負荷が大幅に増えたり、vCenter Server データベースのデータが増えたりすることはありません。これらの情報は既存の vCenter Server イベントの一部としてすでに記録されているためです。強化されたログ機能では、Syslog ストリームを通じてこれらの情報を表示しています。トラブルシューティングとサポートのログは影響を受けず、今後も必要に応じてサポートに使用されます。

仮想マシン サンドボックス

ESXi アーキテクチャが更新され、仮想マシンの安全性とセキュリティが強化されています。仮想マシンは「サンドボックス」内で実行され、使用できるハイパーバイザー機能が厳しく制御されます。仮想マシン サンドボックスを使用するために必要な設定はありません。

自動化

仮想マシンの暗号化、vMotion の暗号化、仮想マシンのセキュア ブートの有効化はすべて、VMware PowerCLI、VMware vRealize® Automation™ などの一般的な IT ツールを使用するか、vSphere API を直接使用して、完全に自動化できます。このため、運用への影響を最小限に抑えて、既存のワークフローにセキュリティを組み込むことができます。次にいくつかの例を示します。

1. 仮想マシンの暗号化と復号化
2. 仮想マシンのセキュア ブートの有効化
3. 仮想マシン単位で vMotion の暗号化を有効化

VMware PowerCLI を使用した仮想マシンの暗号化の例を次に示します。

```
# 仮想マシンの名前
$vmname = "Tiny"
# 仮想マシン名を使用してハード ディスク オブジェクトを取得
$harddisk = Get-VM -name $vmname |Get-HardDisk
# 暗号化ポリシーを取得
$Encryptionpolicy = Get-SpbmStoragePolicy -Name "Encryption Policy"
# ポリシーを仮想マシンとそのハード ディスクに適用してディスクを暗号化
Set-SpbmEntityConfiguration $vmname, $harddisk -StoragePolicy
$Encryptionpolicy -Confirm:$false
```

vSphere 6.5 の可用性の向上

Proactive HA

Proactive HA は、特定のハードウェア パートナーと連携して実現した機能です。問題が発生してサービスが中断される前に、性能が低下したコンポーネントを検出し、影響を受ける vSphere ホストから仮想マシンを退避します。

ハードウェア パートナーは、システム メモリー、ローカル ストレージ、電源装置、冷却ファン、ネットワーク アダプターの健全性の状態を知らせる vCenter Server プラグインを提供しています。ハードウェア コンポーネントの性能が低下してくると、Proactive HA は危険な状態にあるホストを判断し、「隔離モード」にします。隔離モードでは、アフィニティ ルールや非アフィニティ ルールの違反にならない範囲で仮想マシンが健全なホストに移行されるため、仮想マシンのパフォーマンスに影響することはありません。また、新しい仮想マシンをクラスタに追加するときに、問題のあるホスト以外に配置されます。

VMware vSphere High Availability による再起動のオーケストレーション

再起動のオーケストレーションによって、複数の仮想マシン間で実行されているアプリケーションの復元性が向上します。これは、仮想マシン間の再起動ルールを通じて、仮想マシン間に依存関係チェーンを作成することで実現されます。再起動ルールでは、依存関係チェーン内の各仮想マシンを再起動する順序を指定し、VMware vSphere High Availability (vSphere HA) で仮想マシンが再起動されるときに、影響を受けるアプリケーションが正常に復元される可能性を高めます。

vSphere HA の再起動ルールは、vCenter Server を使用して作成、管理します。ただし、vCenter Server を使用できない場合でも、vSphere HA は設定に沿ってリカバリを実行し、再起動ルールを適用します。

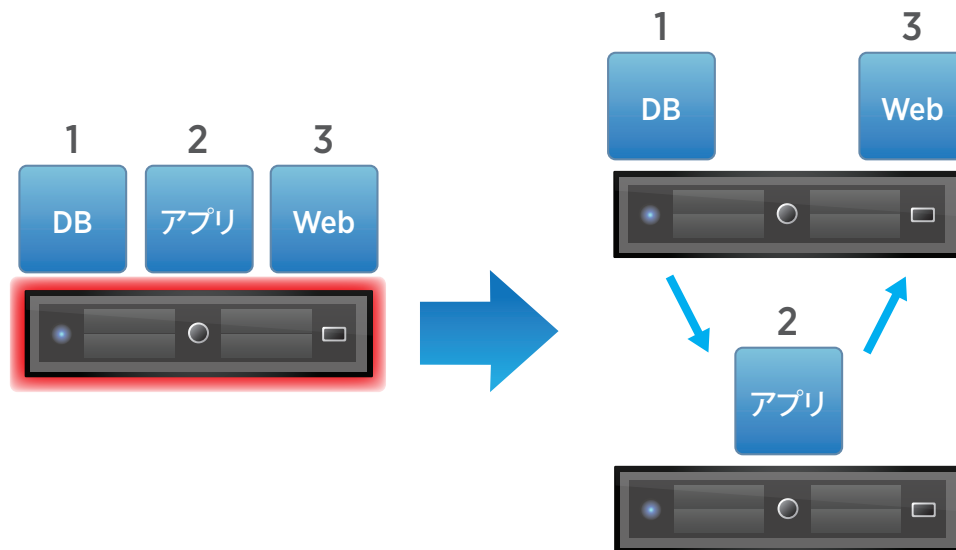


図 23：マルチティア仮想マシンのリカバリ

vSphere HA のアドミッション コントロールの強化

vSphere HA のアドミッション コントロールの設定を簡素化するために、いくつかの改良が加えられています。vSphere 6.5 以降、デフォルトのアドミッション コントロール ポリシーが [Cluster Resource Percentage] になりました。このポリシーでは、クラスター内で使用可能な CPU リソースとメモリー リソースの合計に対する割合 (%) を使用して、予約するフェイルオーバー キャパシティの量を計算します。ホストの許容する障害の数 (FTT) を定義すると、この割合が自動で計算されるようになりました。

Admission Control

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Increasing the value of host failures cluster tolerates will increase the availability constraints and capacity reserved.

Host failures cluster tolerates	1 <input type="button" value="▲"/> <input type="button" value="▼"/>	Maximum is one less than number of hosts in cluster.
Define host failover capacity by	Cluster resource percentage <input type="button" value="▼"/>	
	<input type="checkbox"/> Override calculated failover capacity.	
	CPU 33 <input type="button" value="▲"/> <input type="button" value="▼"/> %	Memory 34 <input type="button" value="▲"/> <input type="button" value="▼"/> %
Performance degradation VMs tolerate	100 <input type="button" value="▲"/> <input type="button" value="▼"/> %	Percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure.
	0% - Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart. 100% - Warning is disabled.	

図 24：アドミッション コントロールの設定

計算された割合は、クラスタ内でホストの追加や削除があった場合、FTT 値を満たすように動的に変化します。この簡素化された設定は、ホストの構成が同じクラスタと構成が異なるクラスタの両方に適用されます。予約に適したフェイルオーバー キャパシティは、最悪のシナリオに基づき、もっともリソースが多いホストで障害が発生する場合を想定して計算されます。

このため、スロット ベースと割合ベースのアドミッション コントロール ポリシーの両方の長所が取り入れられています。このような機能強化によって、手動での計算が不要になり、ユーザーのミスが発生する可能性が低くなります。

もう 1 つの機能強化として、[Performance Degradation VMs Tolerate] があります。この設定は、障害発生後にどの程度のパフォーマンス低下を許容するかをコントロールします。vSphere HA は、vSphere DRS から提供された仮想マシンのパフォーマンス データを使用して、フェイルオーバー後に同等のパフォーマンスを維持するための十分なキャパシティがあるかどうかを判断します。これは、仮想マシンの予約を使用せず、使用済みのキャパシティがフェイルオーバー キャパシティを超えたときに役立ちます。値が 0 % の場合は、パフォーマンスの低下を許容しないことを示します。値が 100 % の場合は、警告が無効になります。

vSphere HA による NVIDIA GRID vGPU が構成された仮想マシンのサポート

NVIDIA GRID vGPU 共有バス スルー デバイスを備えた仮想マシンが、vSphere HA で保護されるようになりました。仮想マシンで障害が発生した場合、vSphere HA は、同じ NVIDIA GRID vGPU プロファイルを持つ別のホスト上でその仮想マシンを再起動しようとします。この条件を満たす正常なホストがなかった場合、仮想マシンをパワーオンできません。

注：vSphere HA のアドミッション コントロール ポリシーでは、NVIDIA GRID vGPU のリソースは考慮されません。

VMware vSphere Fault Tolerance

VMware vSphere Fault Tolerance (vSphere FT) 6.5 では、vSphere DRS との連携が強化され、配置先を的確に判断できるようになりました。使用可能なネットワーク帯域幅に基づいてホストに優先順位が設定され、セカンダリ VMDK ファイルの配置先となるデータストアが推奨されます。

プライマリ仮想マシンとセカンダリ仮想マシンの間のネットワーク遅延は大幅に低減されました。遅延の影響を受けやすい特定のタイプのアプリケーションに対するパフォーマンスの影響が小さくなったため、ダウンタイムを許容できないミッション クリティカルなアプリケーションをより幅広く使用できるようになりました。

複数のポート グループを使用して、vSphere FT のログ トラフィック用の帯域幅全体を拡張できるようになりました。これは、単一のネットワーク アダプターで提供される帯域幅よりも多くの帯域幅を必要とする環境で、通信チャンネルを追加提供するために vSphere vMotion で複数の NIC を構成することと似ています。

リソース管理の強化

Predictive DRS

Predictive DRS は、vRealize Operations Manager の予測分析機能と、vSphere DRS の強力なリソース スケジューラー アルゴリズムを利用する新しい機能です。この 2 つの製品を組み合わせることで、リソース使用率が急増する前に特定の仮想マシンのワークロードを分散できるようになり、以前発生していた可能性がある大量のリソース競合を防止できます。

vRealize Operations Manager は、データ収集対象の仮想マシンに対して動的しきい値アルゴリズムを夜間に実行し、これらの動的しきい値から、仮想マシンの今後の使用率に関するメトリックを予測します。その後 vSphere DRS がメトリックを受け取り、リソース使用率が急増する前に仮想マシンの最適な配置とバランスを判断します。ホスト上で実行されている仮想マシンの使用率パターンを予測可能な場合、Predictive DRS はそのホスト上のリソース競合防止に役立ちます。

vSphere DRS のロード バランシング アルゴリズムの改良

vSphere DRS では、ロード バランシングを実行するメトリックとして、目標標準偏差を使用します。vSphere DRS はクラスタ内の現在の負荷を監視し、標準偏差を最小限に抑えるための推奨事項を生成します。標準偏差が目標標準偏差以下のとき、クラスタはバランスがとれていると見なされます。

標準偏差モデルは、ほとんどの場合に適切に機能することが実証されています。ただし、クラスタが大規模になると、分布が正規化され、外れ値が発生します。外れ値とは、使用率がクラスタの平均使用率を超えているが、標準偏差に大きな影響を及ぼさないホストのことです。

このような外れ値を検出できるように vSphere DRS のアルゴリズムが改良されました。vSphere DRS では、標準偏差に加えて、使用率がもっとも高いホストともっとも低いホストの間の差が計算され、この差を縮めるための移行の推奨が補助的に表示されます。ペアワイズ計算として知られるこの方法は外れ値に対処し、クラスタ リソースと各仮想マシンのパフォーマンスのバランスが、全体的に良くなります。

vSphere DRS の追加オプション

VMware vSphere Web Client にあるチェック ボックスを使用して、vSphere DRS クラスタでもっとも一般的に使用されている次の 3 つの詳細オプションを容易に設定できるようになりました。

- 仮想マシンの分散：vSphere DRS がホスト間で仮想マシンを均等に分散し、単一ホストの障害の影響を最小限に抑えることができます。配置を推奨する際の実行優先事項は仮想マシンのパフォーマンスであり、vSphere DRS は要求が満たされていることを継続的に確認します。リソースの競合が深刻な状況では、均等な分散よりもパフォーマンスが優先されるため、このオプションが完全に守られない場合もあります。
- ロード バランシングのメモリー メトリック：vSphere DRS は、ホスト上のメモリーの負荷を計算するときに、アクティブ メモリー + 25 % を主なメトリックとして使用します。このオプションを選択すると、メモリーの負荷を計算する際のメトリックが変わり、アクティブ メモリーではなく使用済みのメモリー容量が使用されます。このオプションは、メモリーのオーバーコミットがないクラスタ、つまり仮想マシンの割り当てメモリーが物理ホストのメモリーを超えないクラスタでのみ使用できます。
- CPU のオーバーコミットメント：クラスタ レベルで物理 CPU に対する仮想 CPU の最大比率を適用します。クラスタがこの定義した値に到達したあとは、仮想マシンを追加でパワーオンすることはできません。このため、仮想デスクトップ環境のように多数の仮想マシンでワークロードが同時に急増する環境で CPU の競合を防止できます。

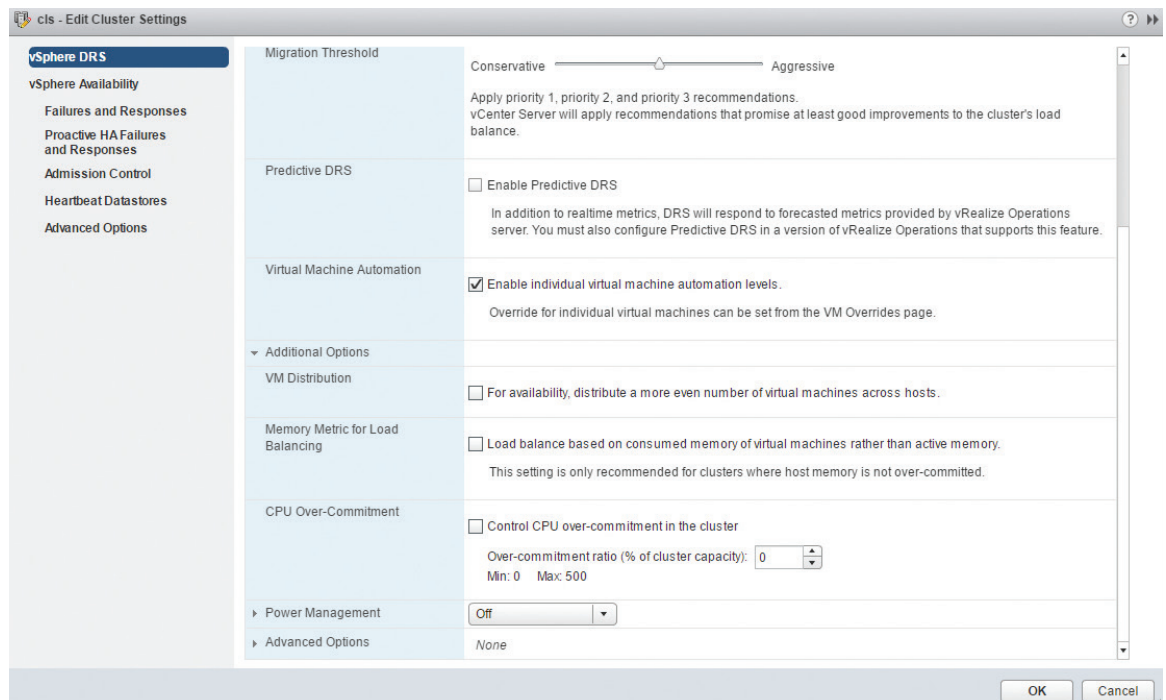


図 25 : vSphere DRS の追加オプション

ネットワークの使用率を認識する vSphere DRS (Network-aware DRS)

vSphere DRS は、移行を推奨する際に使用している既存の 25 種類以上のメトリックに加え、ネットワークの使用率も考慮します。接続されている物理アップリンクの送信速度と受信速度を監視し、ネットワークが輻輳状態にあると考えられるホストに仮想マシンを配置しないようにします。ネットワークの使用率が 80 % を超えると輻輳状態と見なされます。ネットワーク使用率のみに基づいてホストへの分散配置を行うことはありません。ネットワーク使用率は、仮想マシンの配置先としてホストが適切な状態にあるかどうかを判断する際の付属的な情報として使用されます。vSphere DRS はネットワーク使用率を考慮して配置先を適切に判断し、仮想マシンのパフォーマンスを最適化します。

VMware vSphere Storage I/O Control におけるストレージ ポリシー ベースの管理 (SPBM) の使用

SPBM を使用して VMware vSphere Storage I/O Control (SIOC) の設定をするようになりました。IOPS の制限は、VMware vSphere Storage APIs – I/O Filtering (VAIO) を使用して適用されます。SPBM フレームワークは、仮想マシンに適用するストレージ ポリシーを統合管理するため、ストレージのサービス レベルが複数ティアある場合に管理負担が軽減され、ポリシーのコンプライアンスの監査と検証が容易になります。

vSphere Storage APIs – I/O Filtering は、ストレージ ポリシーで定義されている IOPS の制限のみを適用します。IOPS の予約やシェアは、mClock スケジューラーを使用して適用されます。

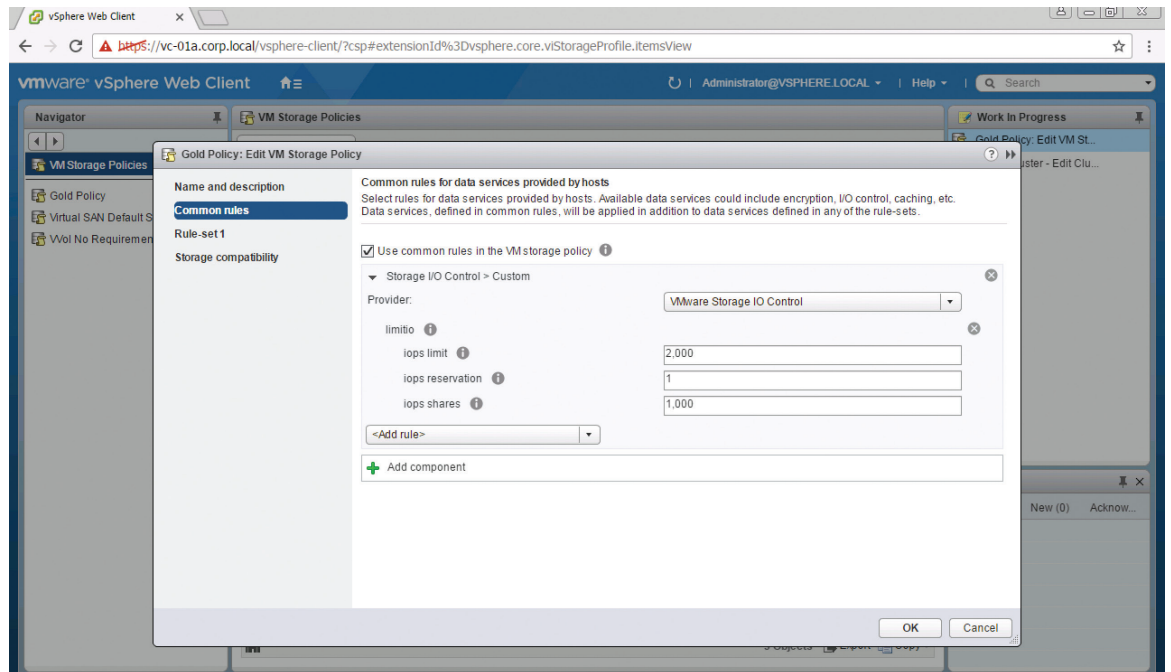


図 26 : vSphere Storage I/O Control の設定

vSphere Integrated Containers

vSphere は、従来のアプリケーションと次世代のアプリケーションの両方をサポートするユニバーサル アプリケーション プラットフォームです。この 2 つの環境は大きく異なりますが、主要なビジネス目標を満たすためには、いずれもスケラビリティ、パフォーマンス、可用性を備えたインフラストラクチャが必要です。

次世代のアプリケーションではコンテナなどの新しいテクノロジー要素が取り入れられていますが、vSphere 6.5 では、あらゆるアプリケーションを実行するために、このような次世代のアプリケーションのスケール アップとスケールアウトに重点を置いて対応可能なワークロードのモデルを拡張しています。今回のリリースでは、VMware vSphere Integrated Containers™ を採用しています。vSphere のユーザーはこれを使用して既存の vSphere 環境に簡単にコンテナを導入することができます。

vSphere Integrated Containers は、開発チームと vSphere 運用チームの双方に適したエンタープライズ コンテナ インフラストラクチャです。仮想マシンと同じように、コンテナを簡単に有効にして管理することができます。プロセスやツールを変更する必要はありません。

vSphere Integrated Containers によって、お客様は既存のインフラストラクチャを再構築することなく、コンテナを取り入れてビジネスを変革できます。vSphere Integrated Containers は、次の 3 つのコンポーネントで構成されます。

- Engine：中核的コンテナのランタイム環境を提供するエンジン
- Harbor：コンテナ イメージのエンタープライズ レジストリ
- Admiral：開発チームがコンテナを管理するためのポータル

vSphere Integrated Containers によって、IT 運用チームは、既存の vSphere インフラストラクチャで動作する Docker 互換のインターフェイスをアプリケーション チームに提供できます。vSphere Integrated Containers は、VMware NSX と緊密に連携して、最高クラスのネットワークの自動化やスケールアウトをサポートします。また、vSAN と連携して、高パフォーマンスのパーシステント ストレージをサポートします。

vSphere 6.5 のストレージの機能強化

アドバンスド フォーマット ドライブと 512e モード

ディスクの標準セクター サイズはこれまで 10 年以上、512 バイトのままでした。ストレージ業界は、大容量のドライブを提供するために、アドバンスド フォーマット (AF) ドライブに向けた取り組みを進めています。AF ドライブの物理セクター サイズは、4,096 バイトです。ディスク ドライブのベンダーは、この新しい 4 KB の AF フォーマットで信頼性に優れた大容量 HDD を開発し、大容量ストレージへのニーズに対応できます。AF ドライブは、ギガバイトあたりのコストが低く、費用対効果に優れています。

AF ドライブには 2 種類があり、vSphere 6.5 は VMware vSphere VMFS データストアと RDM で 512 エミュレーション (512e) モードをサポートします。このモードでは、従来の OS やアプリケーションで大容量ドライブを使用できます。512e モードでは大きな変更があり、VMFS のメタデータも合わせて 4K に変更されたため、vSphere 6.5 で入手可能な VMFS 6 のバージョンが必要です。vSphere は 512e LUN をサポートするストレージと連携します。

UNMAP の自動化

UNMAP は、VMware vSphere Storage APIs – Array Integration の基本機能であり、シン プロビジョニングされた VMFS ボリューム上の使用済み領域または割り当て済み領域の再利用を可能にします。vSphere 6.0 では、簡単な ESXCLI コマンドを実行して、ストレージから削除されたブロックを解放できましたが、vSphere 6.5 では、VMFS が削除されたブロックを追跡し、削除された領域をバックグラウンドでバックエンド アレイから再利用する UNMAP のプロセスが自動化されています。バックグラウンドで処理することで、UNMAP 処理に起因するストレージ I/O への影響が最小限に抑えられます。UNMAP は、Windows と Linux の新しいバージョンがインストールされたゲスト OS レベルで動作します。

LUN のスケーラビリティ

お客様の環境は継続的に拡大しており、ストレージ パスや LUN でスケーラビリティの向上が求められています。vSphere 6.0 では現在、LUN の最大数が 256 個、パスの最大数が 1,024 に制限されています。この制限は、次のような場合に問題になります。

- インフラストラクチャに LUN へのパスが 8 通りある場合、1 つのクラスタあたりの LUN の最大数は 128 個になります。
- 多くのお客様は、重要なデータを分離し、バックアップとリストアを簡単に行うために、LUN のサイズを小さくしています。この方法では、現在の LUN とパスの制限に達する可能性があります。
- アクティブ / アクティブ クラスタにおける LUN の最大数は 128 個であり、これは現在サポートされている制限の半分になります。LUN の制限数が大きいと、クラスタの規模を拡大し、管理負担を軽減できます。

vSphere 6.5 は、512 個の LUN と 2,000 通りのパスをサポートするため、ストレージ インフラストラクチャのスケーラビリティが大幅に向上します。

NFS 4.1 のサポート

NFS 4.1 は vSphere 6.0 ですでにサポートされていましたが、Microsoft Active Directory を使用した Kerberos 認証で暗号化アルゴリズムが強化されています。vSphere 6.5 では、Kerberos 認証に加えて Kerberos 整合性チェック (SEC_KRB5i) が採用されました。また、Kerberos では IPV6 がサポートされ、vSphere 6.5 のホスト プロファイルには NFS 4.1 のサポートが含まれます。このような機能強化により、セキュリティが強化されています。

ソフトウェア iSCSI のスタティック ルーティングのサポート

これまでは、ソフトウェア iSCSI を使用するとき、iSCSI のイニシエーターとターゲットが同じサブネットに配置されている必要がありました。vSphere 6.5 では、ソフトウェア iSCSI のイニシエーターとターゲットのサブネットが異なってもかまいません。イニシエーターのサブネットとターゲットのサブネットの間でスタティック ルートを設定できます。vSphere 6.5 では、イニシエーターとターゲットが同じネットワーク上になくてもマルチパスを容易に設定できます。

vSphere 6.5 のネットワークの機能強化

VMkernel ネットワーク アダプター専用のゲートウェイ

vSphere 6.5 より前のバージョンでは、vSphere DRS、vSphere vMotion、iSCSI、プロビジョニングで単一のゲートウェイを使用していました。すべてのホストにスタティック ルートを追加する必要があったため、妨げとなっていました。これらのルートの管理は煩雑で、スケーラビリティも限られていました。

vSphere 6.5 では、サービスごとに異なるデフォルト ゲートウェイを使用できるようになりました。エンド ユーザーはスタティック ルートを追加せずにこれらの機能を使用できます。VMkernel ベースのすべてのサービスに対してスタティック ルートを用意する必要がないので、効率性とスケーラビリティに優れています。

SR-IOV のプロビジョニング

vSphere 6.5 より前のバージョンでは、SR-IOV デバイスの仮想マシン プロビジョニング ワークフローで、ユーザーが SR-IOV ネットワーク アダプターを手動で割り当てる必要がありました。このため、仮想マシンを柔軟にプロビジョニングできず、大規模環境での自動化に適していませんでした。vSphere 6.5 では、SR-IOV デバイスをほかのデバイスと同様に仮想マシンに追加できるため、管理と自動化が容易になりました。

ERSPAN のサポート

ERSPAN は、1 つまたは複数の「ソース」ポートのトラフィックをミラーリングし、このミラーリングしたトラフィックを別のスイッチにある 1 つまたは複数の「ターゲット」ポートに配信します。vSphere 6.5 では、ERSPAN プロトコルをサポートしています。

データパスの機能強化

vSphere 6.5 では、次のようにデータパスが機能強化されています。

- VMkernel 機能で 2 MB のページをサポート
- VMKAPI ロックの機能強化により、VMware vSphere Distributed Switch™ のスケーラビリティを向上
- 健全性チェックのスケーラビリティを向上

まとめ

VMware vSphere 6.5 は、アプリケーション、クラウド、ビジネスに最適な、投資対効果に優れたプラットフォームです。vSphere 6.5 は Software-Defined Data Center (SDDC) の主要コンポーネントの 1 つであり、VMware のクラウド戦略に不可欠な要素です。vSphere 6.5 を使用することで、利用するクラウドやデバイスのタイプを問わずに、共通の運用環境でアプリケーションを実行、管理、接続、保護することが可能です。

執筆者について

Adam Eckerle は VMware vCenter Server と、vSphere Web Client、HTML5 ベースの vSphere Client を含む VMware vSphere Client を担当するシニア テクニカル マーケティング アーキテクトです。Twitter アカアカウントは [@eck79](#) です。

Mike Foley は、VMware vSphere プラットフォームのセキュリティを担当するシニア テクニカル マーケティング アーキテクトです。仮想化ベースのインフラストラクチャ セキュリティの権威として名高く、この分野で特許 (8,601,544) を保有しています。Twitter アカアカウントは [@MikeFoley](#) です。

Eric Gray は、クラウド プラットフォーム事業部門に所属するチーフ テクニカル マーケティング アーキテクトです。2005 年に VMware に入社し、現在は VMware vSphere ホストのライフサイクル管理を担当しています。Twitter アカアカウントは [@eric_gray](#) です。

Matthew Meyer は、Software-Defined Data Center テクノロジーに取り組んでいるシニア テクニカル マーケティング アーキテクトです。VMware vSphere の可用性とリソース管理を専門としています。VMware Certified Design Expert (VCDX#69) や CompTIA A+ など、多数の業界認定資格を保有しています。

Kyle Ruddy は、VMware vSphere with Operations Management™ および vSphere の自動化インターフェイスと開発者向けインターフェイスを担当するシニア テクニカル マーケティング エンジニアです。Twitter アカアカウントは [@kmruddy](#) です。

Emad Younis は、クラウド プラットフォーム事業部門に所属するシニア テクニカル マーケティング エンジニアです。現在は VMware vCenter Server Appliance と vCenter Server の移行を担当しています。Twitter アカアカウントは [@emad_younis](#) です。

本資料は原題「What's New in VMware vSphere® 6.5」の翻訳版です。



ヴェムウェア株式会社 〒105-0013 東京都港区浜松町1-30-5 浜松町スクエア 13F www.vmware.com/jp

Copyright © 2017 VMware, Inc. All rights reserved. 本製品は米国および国際著作権法・知的財産権法により保護されています。VMware 製品は、<http://www.vmware.com/download/patents.html> のリストに表示されている 1 件または複数の特許対象です。VMware は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。アイテム No. : VMW-TWP-vSPHR-6.5-A4-102 Docsource : OIC-FP-1819