



Citrix Hypervisor 8.1

Contents

Citrix Hypervisor 8.1 最新リリース	3
新機能	4
解決された問題	11
既知の問題	13
廃止と削除	17
システム要件	19
構成の制限	24
ゲストオペレーティングシステムのサポート	28
クイックスタート	32
製品の技術概要	55
技術面でのよくある質問	63
ライセンス	80
インストール	88
インストールと展開のシナリオ	97
既存バージョンからのアップグレード	103
ホストのアップデート	112
インストールのトラブルシューティング	125
SAN 環境からの起動	126
ネットワークブートによるインストール	129
ホストのパーティションレイアウト	134
小型デバイスへのインストール	136
ホストとリソースプール	137
クラスター化プール	150

ユーザーの管理	154
役割ベースのアクセス制御	162
RBAC 役割とアクセス権	163
CLI での RBAC の使用	174
ネットワーク	179
ネットワークの管理	195
ネットワークのトラブルシューティング	218
ストレージ	223
ストレージリポジトリの形式	227
シンプロビジョニングされた共有 GFS2 ブロックストレージ	245
ストレージリポジトリ (SR) の管理	252
ストレージのマルチパス	265
IntelliCache	267
ストレージ読み取りキャッシュ	271
PVS アクセラレータ	274
グラフィックスの概要	282
グラフィック処理のためのホストの準備	286
仮想 GPU が有効な仮想マシンの作成	296
メモリ使用率	302
環境の監視と管理	304
仮想マシンの管理	326
Windows 仮想マシン	331
Linux 仮想マシン	352
仮想マシンのメモリ	359

仮想マシンの移行	365
仮想マシンのインポートとエクスポート	369
Bromium Secure Platform	385
コンテナ管理	387
vApp	395
Demo Linux Virtual Appliance	398
仮想マシンに関する注意事項	400
Linux 仮想マシンの VNC 設定	410
仮想マシンの問題のトラブルシューティング	422
高可用性	429
障害回復とバックアップ	436
障害回復を有効にする	439
vApp	444
ホストと仮想マシンのバックアップと復元	445
仮想マシンスナップショット	450
マシン障害への対処	456
トラブルシューティング	460
メジャーブートのサブリメンタルパック	464
ワークロードバランス	467
ワークロードバランスの利用を開始する	469
ワークロードバランス仮想アプライアンスの管理	479
ワークロードバランスの証明書	542
VMware ワークロードの変換	550
vSwitch と Controller	566

vSwitch の管理	571
仮想ネットワークの可視性と制御	576
vSwitch Controller の管理と保守	594
コマンド	598
vSwitch Controller の問題のトラブルシューティング	602
コマンドラインインターフェイス	606
SDK および API	733
データガバナンス	733

Citrix Hypervisor 8.1 最新リリース

April 20, 2020

仮想アプリケーションとデスクトップのワークロード用に最適化された高性能のハイパーバイザーで、Xen Project ハイパーバイザーをベースとした、XenServer のこの信頼できるテクノロジーは、Citrix Hypervisor に名称が変更になりました。

最新リリース

Citrix Hypervisor 8.1 は、現時点での Citrix Hypervisor の最新リリースであり、このドキュメントにはその機能と構成が記載されています。

Citrix Hypervisor 8.1 の新機能については、「[新機能](#)」を参照してください。

以前のリリース

以前のサポートされるリリースのドキュメントについては、以下を参照してください：

- [Citrix Hypervisor 8.0 CR](#)
- [XenServer 7.1 LTSR](#)
- [XenServer 7.0](#)

サポートされなくなった Citrix Hypervisor および XenServer リリースでは、ドキュメントは[古いドキュメント](#)のページにアーカイブされています。

最新リリースおよび長期サービスリリースに対する Citrix Hypervisor 製品のライフサイクル戦略については、「[Citrix Hypervisor のライフサイクルマイルストーン](#)」で説明されています。

Citrix Hypervisor について

Citrix Hypervisor は、Citrix が提供する包括的なサーバー仮想化プラットフォームです。Citrix Hypervisor のパッケージには、ネイティブに近いパフォーマンスを提供するオープンソース準仮想化ハイパーバイザーの、Xen 上で動作する、仮想 x86 コンピューターの環境の作成と管理に必要なすべてのリソースが含まれています。Citrix Hypervisor は、Windows および Linux の仮想サーバーの両方向けに最適化されています。

Citrix Hypervisor は何らかのオペレーティングシステム上で動作するのではなく、サーバーのハードウェア上で直接動作します。このため、システムリソースが効率的に使用され、高いスケーラビリティが提供されます。Citrix Hypervisor は、物理マシンの各要素（ハードドライブ、リソース、ポートなど）を抽象化して、そのマシン上で動作する仮想マシンにそれらの要素を割り当てることで機能します。

仮想マシン (VM: Virtual Machine) は、すべての要素がソフトウェアで構成されたコンピュータを指し、物理コンピュータと同様にオペレーティングシステムやアプリケーションを実行できます。各仮想マシンは仮想的な (ソフトウェアベースの) CPU、RAM、ハードディスク、およびネットワークインターフェイスカードを持ち、物理コンピュータと同じように動作します。

Citrix Hypervisor では、仮想マシンの作成、ディスクスナップショットの作成、および仮想マシンワークロードの管理を行えます。Citrix Hypervisor の主な機能をまとめた一覧については、<https://www.citrix.com/products/citrix-hypervisor/>を参照してください。

XenCenter

XenCenter は、Windows GUI クライアントです。複数の Citrix Hypervisor サーバーとリソースプール、およびそれらに関連付けられた仮想インフラストラクチャを管理する場合に優れたユーザーエクスペリエンスを提供します。詳しくは、[XenCenter ドキュメント](#)

新機能

March 12, 2020

このリリースについて

XenServer のこの信頼できるテクノロジーは、仮想アプリケーションとデスクトップのワークロード用に最適化された高性能のハイパーバイザーで、Xen Project ハイパーバイザーをベースとしていますが、現在の名前は Citrix Hypervisor です。

Citrix Hypervisor 8.1 は最新リリース (CR) です。最新リリースモデルでは、お客様が新しい機能をいち早く利用できます。長期サービスリリース (XenServer 7.1 LTSR) と異なり、最新リリースでは、機能セットの安定性が保証されています。

Citrix Hypervisor 8.1 には、次のエディションがあります：

- Premium Edition (以前の Enterprise Edition)
- Standard Edition
- Express Edition (以前の Free Edition)

各エディションで使用できる機能については、[Citrix Hypervisor の機能マトリックス](#)を参照してください。

Citrix Hypervisor 8.1 で追加および強化された機能

Citrix Hypervisor 8.1 では、アプリケーション、デスクトップ、サーバー仮想化に使用できる機能が強化されました。Citrix Hypervisor 8.1 のすべての機能は、ライセンスを取得したすべての Citrix Virtual Apps and Desktops

(以前の XenApp および XenDesktop) のお客様が利用できます。

ゲスト UEFI ブートとセキュアブート

Citrix Hypervisor は仮想マシンが Windows 10 (64 ビット)、Windows Server 2016 (64 ビット) または Windows Server 2019 (64 ビット) を実行して UEFI モードで起動できるようにします。UEFI ブートにより、ゲストオペレーティングシステムがハードウェアとやり取りするための、充実したインターフェイスが提供されるため、Windows 仮想マシンの起動時間を大幅に短縮できます。

これらの Windows オペレーティングシステムの場合、Citrix Hypervisor は Windows セキュアブートもサポートしています。セキュアブートは、未署名のバイナリ、正しく署名されていないバイナリ、または変更されたバイナリが起動中に実行されるのを防ぎます。また、セキュアブートは、ゲスト内のマルウェアがブートファイルを操作したり、ブートプロセス中に実行されたりするリスクも減らします。

詳しくは、「[Windows 仮想マシン](#)」を参照してください。

注:

ゲスト UEFI ブートは試験段階の機能として Citrix Hypervisor 8.0 で提供されました。Citrix Hypervisor 8.0 で UEFI ブート仮想マシンを作成した場合、Citrix Hypervisor 8.1 に移行できません。Citrix Hypervisor 8.1 に更新する前に、これらの UEFI ブート仮想マシンをシャットダウンする必要があります。

複数 vGPU

複数 vGPU をサポートする NVIDIA GPU とドライバーの場合、複数の仮想 GPU を同時に使用するように単一の仮想マシンを構成できます。これらの追加の vGPU を使用して、計算処理を実行できます。特定の vGPU プロファイルのみを使用でき、単一の仮想マシンに接続されているすべての vGPU が同じタイプである必要があります。

詳しくは、「[グラフィックスの概要](#)」を参照してください。

パフォーマンスの向上

XVA 形式を使用する仮想マシンのインポートおよびエクスポートのパフォーマンス向上

Citrix Hypervisor 8.1 の XVA ファイルで使用されるチェックサムの変更により、この新しいチェックサムアルゴリズムを使用して仮想マシンをインポートまたはエクスポートする際のパフォーマンスが大幅に向上します。

仮想マシンのインポートまたはエクスポートにかかる時間がどのくらい短縮されるかは、マシンの特定のハードウェアによって異なります。仮想マシンが大きいほど、パフォーマンスの向上も大きくなります。

XenCenter 8.1 を使用し、新しいチェックサムアルゴリズムで XVA ファイルを使用するエクスポートされた仮想マシンを管理します。

XVA ファイルに含まれるチェックサムの形式に依存するカスタムアプリケーションがある場合は、新しい形式を使用するようにアプリケーションを更新します。チェックサムは、xxHash アルゴリズムを使用するように変更されました。チェックサムファイル名は、拡張子 `.xxhash` で終わるようになりました。

ストレージパフォーマンスの向上

Citrix Hypervisor 8.1 には、ストレージの次のパフォーマンス向上が含まれます：

- NFS SR において 64 KiB を超えるブロックサイズで I/O が実行されると、ストレージのパフォーマンスが大幅に向上します。
- ストレージのパフォーマンスを向上させるため、非 GFS2 ストレージリポジトリでマルチページサポートが提供されるようになりました。Windows 仮想マシンに Citrix VM Tools がインストールされている場合、仮想マシンでマルチページサポートが自動的に使用されます。Linux 仮想マシンでマルチページサポートを有効にするには、次の手順を実行します：
 1. 仮想マシンで、次のコマンドを実行します：`echo 'options xen_blkfront max_ring_page_order=3'>/etc/modprobe.d/xen_blkfront.conf`
 2. Linux ディストリビューションに応じて、次のコマンドのいずれかを実行します：
 - RHEL、CentOS、または Oracle Enterprise Linux の場合：`dracut -f -v`
 - Debian ベースディストリビューションの場合：`update-initramfs -u -k all`
 3. 仮想マシンを再起動します。

パフォーマンスが向上した新しい **Windows I/O** ドライバー

メジャーバージョン 9 (9.xxx) の更新された Windows I/O ドライバーは、Citrix Hypervisor のこのリリースで次のオペレーティングシステムに提供されます：Windows 8.1、Windows 10、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server Core 2016、Windows Server 2019、Windows Server Core 2019。これらの Windows I/O ドライバーには、多くのパフォーマンスの改善が含まれています。

Premium Edition ユーザーは、これらのドライバーを Windows Update から入手できます。

メジャーバージョン 8 (8.xxx) の Windows I/O ドライバーは、サポートされている古い Windows オペレーティングシステム用に引き続き提供されます。これらのドライバーには、パフォーマンスの改善は含まれていません。

ゲストオペレーティングシステムのサポートの変更点

Citrix Hypervisor がサポートするゲストオペレーティングシステム一覧がアップデートされました。詳しくは、「[ゲストオペレーティングシステムのサポート](#)」を参照してください。

追加

Citrix Hypervisor は、次の新しいゲストオペレーティングシステムをサポートします：

- SUSE Linux Enterprise Server 12 SP4 (64 ビット)
- SUSE Linux Enterprise Desktop 12 SP4 (64 ビット)
- SUSE Linux Enterprise Server 15 SP1 (64 ビット)
- SUSE Linux Enterprise Desktop 15 SP1 (64 ビット)
- Red Hat Enterprise Linux 8 (64 ビット)
- Oracle Enterprise Linux 8 (64 ビット)
- CentOS 8 (64 ビット)
- Debian Buster 10 (64 ビット)

更新

Citrix Hypervisor 8.1 で、次のゲストオペレーティングシステムの要件が変更されました：

- Windows 10

Citrix Hypervisor の以前のリリースでは、Windows 10 でサポートされる最小ディスク容量は 24GB でした。新しい Windows 10 仮想マシンでは 32GB がサポートされるようになりました。詳しくは、「[Windows 10 Version 1903 の新機能](#)」を参照してください。

削除

準仮想化 (PV) 仮想マシンのサポートは、Citrix Hypervisor のこのリリースで削除されました。更新またはアップグレード時に、PV ゲストがサポートされていないことが XenCenter で警告されます。

これらのオペレーティングシステムを使用する既存の仮想マシンは、Citrix Hypervisor 8.1 インストールにインポートできます。ただし、Citrix はこれらのオペレーティングシステムを使用する仮想マシンをサポートしません。できるだけ早く、サポートされている最新バージョンのオペレーティングシステムに仮想マシンをアップグレードしてください。詳しくは、「[PV から HVM ゲストへのアップグレード](#)」を参照してください。

次のゲストオペレーティングシステムのサポートは削除されました：

- Ubuntu 14.04
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- CentOS 5
- CentOS 6
- Oracle Enterprise Linux 5
- Oracle Enterprise Linux 6
- Scientific Linux 6
- NeoKylin Linux Advanced Server 6.2
- Debian Wheezy 7

- SUSE Linux Enterprise Server 11 SP3
- SUSE Linux Enterprise Server 11 SP4
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Server 12 SP2
- SUSE Linux Enterprise Desktop 11 SP3
- SUSE Linux Enterprise Desktop 12
- SUSE Linux Enterprise Desktop 12 SP1
- SUSE Linux Enterprise Desktop 12 SP2

プロセッサのサポートの変更

Citrix Hypervisor 8.1 では次のプロセッサがサポートされるようになりました：

- AMD EPYC 7xx2 (P)

詳しくは、[ハードウェア互換性リスト \(英語\)](#) を参照してください。

Citrix Hypervisor Conversion Manager コンソールの機能が **XenCenter** に含まれるように

Citrix Hypervisor 8.0 以前は、別の Conversion Manager コンソールが提供されていました。この機能は Citrix Hypervisor 8.1 から XenCenter に統合されています。従来の Citrix Hypervisor Conversion Manager コンソールは廃止されました。

以前に Citrix Hypervisor サーバーのインストールに含まれていた変換プラグインも、Citrix Hypervisor 8.1 から削除されました。このプラグインが削除されたため、変換機能を含む最新バージョンの XenCenter を Citrix Hypervisor 8.1 とともに使用する必要があります。(古いバージョンの Conversion Manager コンソールは Citrix Hypervisor 8.1 とともに使用できません)

ただし、VMware 仮想マシンを Citrix Hypervisor 仮想マシンに変換するには、Conversion Manager 仮想アプリケーションが引き続き必要です。このコンポーネントは[Citrix Hypervisor の製品ダウンロードページ](#)で提供されています。

詳しくは、「[VMware ワークロードの変換](#)」を参照してください。

XenCenter による製品終了またはサポート終了の通知

XenCenter は、管理対象の Citrix Hypervisor サーバーのバージョンが製品終了に近づいているか、製品終了したことを通知するようになりました。詳しくは、「[XenCenter のアラート](#)」を参照してください。

XenCenter はまた、最新リリースまたは累積更新プログラムが近づいている場合、またはそのリリースに対してこれ以上修正プログラムが発行されない日付を過ぎた場合にも通知します。将来の機能およびセキュリティ関連の問題

に対処するための更新を確実に適用できるように、この通知情報に基づいて行動し、環境を最新のサポート対象リリースに更新してください。

インストールオプション

Citrix Hypervisor 8.1 は、[Citrix Hypervisor の製品ダウンロードページ](#)から次のパッケージで入手できます：

- Citrix Hypervisor 8.1 アップデート ISO。このファイルを使用し、Citrix Hypervisor 8.0 への更新として Citrix Hypervisor 8.1 を適用します。
- Citrix Hypervisor 8.1 基本インストール ISO。このファイルを使用して、Citrix Hypervisor 8.1 の新規インストールを作成するか、XenServer 7.6、7.1 Cumulative Update 2、または 7.0 からアップグレードします。

注：

- ホストのアップグレードに XenCenter を使用する場合、アップデート前に、XenCenter を Citrix Hypervisor 8.1 ダウンロードページにある最新バージョンにアップデートしてください。
- プール内の他のホストをアップグレードする前に、必ずプールマスターをアップグレードしてください。
- XenServer 7.1 を累積更新プログラム 2 にアップデートしてから、Citrix Hypervisor 8.1 にアップグレードしてください。

はじめに

インストールを開始する前、または古いバージョンから移行する前に、次の記事を確認してください：

- [システム要件](#)
- [既知の問題](#)
- [廃止と削除](#)

インストール、アップグレード、または更新プロセスの詳細については、「[インストール](#)」を参照してください。

長期サービスリリース (LTSR) から最新リリース (CR) への変更

XenServer LTSR を実行していて、新機能を利用したい場合、Citrix Hypervisor 最新リリース (CR) ストリームに変更することもできます。CR ストリームから Citrix Hypervisor のバージョンを使用する場合、継続してサポートを利用するには、定期的に新しい CR を選択する必要があります。

XenServer 7.1 Cumulative Update 2 LTSR からアップグレードして、この最新リリースに移行してください。

最新リリース (CR) から長期サービスリリース (LTSR) への変更

Citrix Hypervisor CR を実行しているユーザーが、保証済みの固定機能セットが搭載された Citrix Hypervisor のバージョンに移行する場合、XenServer LTSR に変更できません。最新の XenServer LTSR は、Citrix Hypervisor の製品ダウンロードページから入手できます。

XenServer 7.1 Cumulative Update 2 LTSR の新規インストールを作成して最新の LTSR に移行してください。

LTSR および CR について詳しくは、「[Citrix Virtual Apps, Citrix Virtual Desktops, and Citrix Hypervisor Servicing Options](#)」を参照してください。

ライセンス

Citrix Hypervisor 8.1 のライセンスが必要な機能を使用するには、お客様が Citrix ライセンスサーバーをバージョン 11.14 以上にアップグレードする必要があります。

Citrix Hypervisor 8.1 ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

ハードウェアの互換性

ハードウェアの互換性についての最新情報を確認するには、「[Citrix Hypervisor ハードウェア互換性リスト \(英語\)](#)」を参照してください。

仮想 GPU が接続された仮想マシンがある場合は、Citrix Hypervisor の最新リリースにアップグレードする前に、サポートされているドライバーが使用できることを確認してください。詳しくは、「[ハードウェア互換性リスト \(英語\)](#)」および GPU ベンダーのドキュメントを参照してください。

シトリックス製品との互換性

Citrix Hypervisor 8.1 は、Citrix Virtual Apps and Desktops 7 1912 と相互運用可能です。

Citrix Hypervisor 8.1 は、Citrix Provisioning 1912 と相互運用可能です。

Citrix Hypervisor 8.1 は、Citrix Cloud と相互運用可能です。

Citrix 製品の名称は、製品ラインの統一のため改定されています。詳しくは、「<https://www.citrix.com/about/citrix-product-guide/>」を参照してください。

ローカライズのサポート

このリリースでは、XenCenter の日本語および簡体字中国語バージョンも使用できます。

製品ドキュメント

Citrix Hypervisor 8.1 の製品ドキュメントは、[Citrix Hypervisor 8.1 製品ドキュメント](#)を参照してください。

製品に付属のドキュメントは、必要に応じて改訂される場合があります。[ドキュメント履歴](#)の RSS フィードを購読して、最新のドキュメントを定期的にチェックすることをお勧めします。

解決された問題

January 20, 2020

この記事では、このリリースで解決された以前の問題について説明します。

セキュリティ

- Citrix Hypervisor 8.1 には CVE-2018-12207 の緩和策が含まれています効果を得るにはこれらの緩和策を有効にする必要があります。詳しくは、「<https://support.citrix.com/article/CTX263718>」を参照してください。(CA-330154)

一般

- ライブマイグレーション、ストレージライブマイグレーション、および VDI マイグレーションは、VIF が接続されていない仮想マシンで失敗する場合があります。この障害の後、仮想マシンはシャットダウンモードで停止します。(CA-327906)
- プール内ストレージのライブマイグレーションの完了時に、この情報が記録されません。その結果、操作が進行中としてリストに表示されます。これらの「進行中」の操作があると、ホストのアップグレードや更新など、ホストの退避が必要なアクションの実行がホストでブロックされる可能性があります。(CA-326621)
- ツールスタックの再起動中に、xcp-rrdd は CPU を 100%、長時間使用する可能性があります。(CA-322045)
- 多数のストレージリポジトリを追加すると、XAPI でファイル記述子が不足する可能性があります。(CA-322044)
- 高可用性デーモンが起動時に以前に失敗した場合、高可用性は起動できない可能性があります。次のエラーメッセージが表示されます:「ライブセットを形成できないため、プールの高可用性を有効にできませんでした。ストレージおよびネットワークハートビートのパスを確認してください。」(CA-315962)
- dom0 の vCPU カウントが、ホスト上の CPU の数に誤って設定されていました。(CA-312644)
- ストレージガベージコレクション処理が継続的に実行され、スナップショットの取得、結合、削除をほぼ永続的に繰り返す場合があります。これにより、ほとんどメリットのない高い IOPS 負荷が発生します。(CA-328536)
- 読み取りキャッシュを有効にすると、リーフからよりも親スナップショットからの読み取りが大幅に遅くなります。これは、順次読み取りで改善されました。(CA-327558)
- 最初に Citrix Hypervisor サーバーが XenServer 6.5 以前でインストールされ、その後 XenServer 7.6 にアップグレードされた場合 (中間リリースのアップグレードパスを使用)、ロギング機能が機能しないことがあります。(CA-319463)
- xenstore ユーティリティで使用可能な機能が拡張されました。(CA-327088)

グラフィック

- AMD MxGPU が接続されている仮想マシンを強制的にシャットダウンした場合、またはゲスト OS が異常なシャットダウンをした場合、Citrix Hypervisor サーバーのメモリが破損する可能性があります。協調的なシャットダウンを実行して、シャットダウンの処理中にハードウェアが正しくクリーンアップされるようにします。(CA-297891)
- まれに、複数の NVIDIA vGPU が接続された仮想マシンが起動時に黄色のアイコンで停止することがあります。これは、vGPU の1つで「`compatibility-metadata`」が間違っていて設定されていることが原因の可能性があります。メタデータを削除するには、その仮想マシンを一時停止して再開します。(CA-312226)

ゲスト

- PVS アクセラレータを有効にした後、複数の仮想マシンを同時に起動すると、ターゲットデバイス仮想マシンが PVS サーバーのログインで「ログイン要求のタイムアウト」エラーで停止することがあります。(CA-314317)
- `viridian` フラグを有効にして Windows 仮想マシンを実行すると、仮想マシンがクラッシュする場合があります。(CA-321550)

インストール

- ユーザー名またはパスワードに URL エンコードされた文字が含まれている場合、正しく解析されません。この問題により、Citrix Hypervisor のインストールが失敗します。(CA-329747)

ストレージ

- GFS2 ストレージリポジトリは、クラスター化されたストレージの非同期プラグが原因で、「サーバー起動時のストレージ接続に失敗しました」という誤ったアラートを生成することがあります。XenCenter のストレージリポジトリステータスを確認して、アラートが誤検知であったかどうかを確認します。(CA-311625)
- ストレージマネージャーのガベージコレクター処理により、ゾンビプロセスが生成されます。このエラーにより、Citrix Hypervisor の速度が低下し、プロセス ID が使用できなくなるためプロセスが失敗します。(CA-327382)

XenCenter

- XenCenter 8.1.0 の [アラート] 表示で、製品終了アラートを閉じるか製品終了アラートが含まれる一覧を並べ替えるようになると、XenCenter がクラッシュすることがあります。XenCenter 8.1.1 は 2020 年 1 月 6 日にリリースされ、この問題の修正が含まれています。XenCenter 8.1.1 は [Citrix Hypervisor ダウンロードページ](#) から入手できます。

- XenCenter のストレージライブマイグレーションまたは OVF/OVA のインポートウィザードの [次へ] ボタンが無効のまま処理を続行できないことがあります。この問題が発生した場合は、XenCenter を再起動してもう一度やり直してください。(CA-314346)
- XenCenter 7.6 以前で、XenCenter はサポートされている最大サイズを超える VDI の作成ができる状態になっていました。(XSI-465)

既知の問題

March 12, 2020

この記事では、Citrix Hypervisor 8.1 のリリースの既知の問題とその対応策、およびその他の考慮事項について説明します。

一般

- Citrix Hypervisor サーバーが Intel Sandy Bridge ファミリー CPU を含むハードウェアで実行されている場合、Citrix Hypervisor 8.1 への更新またはアップグレードの一環として、仮想マシンをシャットダウンして再起動することが必要な場合があります。詳しくは、「<https://support.citrix.com/article/CTX231947>」を参照してください。(CP-32460)
- プールの CPU 機能セットは、仮想マシンの実行中に変更される可能性があります (たとえば、新しいホストが既存のプールに追加された場合や、仮想マシンが別のプールのホストに移行された場合)。プールの CPU 機能セットが変更された場合、仮想マシンは起動時に適用された機能セットを使用し続けます。プールの新しい機能セットを使用するように仮想マシンをアップデートするには、仮想マシンの電源をオフにしてから起動する必要があります。XenCenter で [再起動] のクリックなどによって仮想マシンを再起動しても、仮想マシンの機能セットはアップデートされません。(CA-188042)
- Citrix Hypervisor 8.0 で dom0 に割り当てられるメモリ量が増加すると、VM の実行中に使用できるメモリがわずかに少なくなることがあります。一部のハードウェアでは、XenServer 7.6 以前のバージョンと同じハードウェア上で、Citrix Hypervisor 8.1 と同じ数の仮想マシンを実行できない場合があります。(CP-29627)
- シリアルコンソールを使用して Citrix Hypervisor サーバーに接続しようとする、シリアルコンソールがキーボード入力の受け付けを拒否することがあります。コンソールが 2 回更新されるまで待つと、キーボード入力を受け付けるようになります。(CA-311613)
- 読み取りキャッシュを有効にすると、リーフからよりも親スナップショットからの読み取りが大幅に遅くなります。これは順次読み取りでは改善されていますが、他のタイプの読み取りでは改善されていません。(CA-329760)

- 以前に Citrix ライセンスサーバー仮想アプライアンスバージョン 11.14 以前を Citrix Hypervisor サーバーでホストしていた場合、Citrix Hypervisor 8.1 へのアップグレードまたは更新時に、この仮想アプライアンスがサポートされていない PV 仮想マシンであることが警告されます。
- Citrix Hypervisor 8.0 から更新された Citrix Hypervisor 8.1 システムの場合、XAPI の再起動後に次のサービスでエラーが表示されることがあります：
 - usb-scan.service
 - storage-init.service
 - xapi-domains.service
 - mpathcount.service
 - create-guest-templates.service

これらのサービスのエラーはさまざまな問題を引き起こす可能性があります。たとえば、自動的に起動するよう構成された仮想マシンが起動しないことがあります。

これは、xapi-wait-init-complete.service が有効になっていないために発生します。この問題を回避するには、dom0 のコマンドラインで次のコマンドを実行して、必要なサービスを有効にすることができます：

```
1 systemctl preset-all --preset-mode=enable-only
```

(CA-333953)

グラフィック

- AMD MxGPU デバイスが接続された多数の仮想マシンを並列に起動すると、一部の仮想マシンが「VIDEO_TDR_FAILURE」で失敗することがあります。これは、ハードウェアの制限が原因である可能性があります。(CA-305555)
- AMD MxGPU が有効な仮想マシンは、UEFI セキュアブートではサポートされていません。(CP-32288)

ゲスト

- まれに、未処理の xenstore トランザクションがある Linux VM を中断または移行すると、仮想マシンの Linux カーネルの問題が原因で停止することがあります。仮想マシンでこの問題が発生した場合は、VM を強制的にシャットダウンして再起動してください。(CP-30551)
- PXE ネットワークブートを使用して Debian 10 (Buster) をインストールする場合、`console=tty0` をブートパラメーターに追加しないでください。このパラメーターは、インストールプロセスで問題を引き起こす可能性があります。ブートパラメーターでは `console=hvc0` のみを使用してください。(CA-329015)
- Ubuntu 18.04 の一部のマイナーバージョン (18.04.2 および 18.04.3 など) は、グラフィカルコンソールの実行時に問題が発生する可能性のある HWE カーネルをデフォルトで使用します。そうした問題を回避するには、これらの Ubuntu 18.04 のマイナーバージョンを GA カーネルで実行するか、グラフィック設定の一部

を変更するという選択肢があります。詳しくは、「[CTX265663 - Ubuntu 18.04.2 VMs can fail to boot on Citrix Hypervisor](#)」を参照してください。(XSI-527)

- Citrix Hypervisor 8.0 以前のバージョンで作成された、スケジュール済みの VSS スナップショットに仮想マシンを戻そうとすると、仮想マシンは起動しません。次のエラーが出て起動が失敗します:「指定した仮想ディスクが見つからないため、この処理を実行できません。」これは、VSS スナップショットの機能が Citrix Hypervisor 8.1 から削除されたためです。(CA-329435)
- FireEye エージェントがインストールされたドメイン参加 Windows 10 仮想マシン (1903 以降) では、RDP 接続が繰り返し成功すると、`ntoskrnl.exe` で CPU 使用率が 100% になり、仮想マシンがフリーズする可能性があります。この状態から回復するには、仮想マシンでハード再起動を実行する必要があります。(CA-323760)
- Citrix Hypervisor 8.0 で提供されたゲスト UEFI ブート機能は、実験的な機能でした。Citrix Hypervisor 8.1 は、Citrix Hypervisor 8.0 で作成された UEFI ブート仮想マシンの Citrix Hypervisor 8.1 への移行をサポートしていません。Citrix Hypervisor 8.1 にアップグレードする前に、UEFI ブート仮想マシンをシャットダウンする必要があります。(CA-330871)
- UEFI ブートまたは UEFI セキュアブート仮想マシンで、Citrix VM Tools がインストールされていない場合でも、I/O が最適化されているとレポートされることがあります。(CA-328093)
- UEFI ブート仮想マシンの起動時に、Tianocore のロゴが表示されます。(CP-30146)
- Citrix Hypervisor 8.1 で提供される Citrix VM Tools のインストールが成功する前に、仮想マシンの再起動が必要になる場合があります。(CA-331215)
- Citrix VM Tools を `guest-tools.iso` から Windows 仮想マシンにインストールする際に、「サービス「Citrix XenServer Windows 管理エージェント」(XenSvc) をインストールできませんでした。システムサービスをインストールするための十分な特権があるか確認してください。」というエラーメッセージが表示され、インストールが失敗する場合があります。この問題を回避するには、Citrix VM Tools をアンインストールし、仮想マシンを再起動してから新しいツールをインストールします。(CA-330751)
- まれに、Windows 10 仮想マシンに Citrix VM Tools の最新バージョンをインストールすると、インストール中に仮想マシンが停止し、画面が黒くなることがあります。この状態から抜け出すには、仮想マシンを強制的に再起動します。`xennet 9.0.0.7 Windows I/O ドライバー` を再インストールすることで、この問題を回避できます。(CA-325026)

インストール

- サーバーの「ローカルストレージ」ストレージリポジトリを使用して、仮想マシンで Citrix Hypervisor 8.0 を XenServer 6.5 以前からアップグレードしたことがある場合、またはディスクにベンダーのユーティリティパーティションがある場合、レガシーディスクレイアウトを使用していることになります。レガシーディスクレイアウトを使用しているということは、コントロールドメインの空き領域が現在のレイアウトより大幅に少ない (4GB 対 18GB) ことを意味します。

Citrix Hypervisor 8.1 のアップデートを Citrix Hypervisor 8.0 のインストールに適用すると、次のエラーメッセージが表示されます。「必要な空き領域がサーバーにありません。」これは、Citrix Hypervisor 8.1 のアップデートではディスクがフルになるのを避けるために十分な空き領域が必要であり、レガシーレイアウトはこれに対応していないためです。

このエラーが表示された場合、Citrix Hypervisor 8.1 にアップデートできないため、新規インストールを実行する必要があります。(CA-268846)

- Citrix Hypervisor 8.0 から 8.1 に更新すると、次のエラーが表示されることがあります：「Internal error: xenopsd internal error: Xenops_migrate.Remote_failed(“unmarshalling error message from remote”)」このエラーは、修正プログラムの適用時に存在する Windows 仮想マシンの viridian フラグが変更された場合に表示されます **XS80E003**。ただし、仮想マシンはシャットダウンされず、再起動されません。

この問題を回避するには、Citrix Hypervisor 8.1 に更新する前に、XS80E003 が適用された Citrix Hypervisor 8.0 サーバーでホストされているすべての Windows 仮想マシンに関する修正プログラム記事で、「この修正プログラムのインストール後」セクションのすべての手順を完了してください。(XSI-571)

国際化

- ホストコンソールでは、日本語などの非 ASCII 文字を使用することはできません。(CA-40845)
- Citrix VM Tools をインストールした Windows 仮想マシンでは、XenCenter でデフォルトのデスクトップコンソールを使用すると、2 バイト文字のコピーおよび貼り付けが失敗することがあります。貼り付けられた文字は疑問符 (?) で表示されます。

この問題を回避するには、代わりにリモートデスクトップコンソールを使用します。(CA-281807)

ストレージ

- GFS2 ストレージリポジトリを使用している場合にクラスター化されたプール内に 2 つのサーバーがあると、アップグレード中にクラスターのクォーラムやフェンスが失われる可能性があります。このような状況を回避するには、クラスターからサーバーを削除するか追加して、アップグレードプロセス中は 1 つまたは 3 つのサーバーがプールに存在するようにします。(CA-313222)
- GFS2 ストレージリポジトリを使用している場合、最大限の回復性を得るためにストレージのマルチパスを有効にします。ストレージのマルチパスが有効になっていないと、ファイルシステムブロックの書き込みが時間内に完了しない場合があります。(CA-312678)
- Citrix Hypervisor 8.0 マルチパスにアップグレードする際、ストレージリポジトリに HPE 3PAR ハードウェアを使用しており、XenServer が以前のリリースの場合、ホストペルソナに ALUA1 を使用していると、機能しなくなります。この問題を回避するには、ホストペルソナを ALUA2 に移行します。詳しくは、「https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02663749&docLocale=en_US」を参照してください。

- 2 TB を超える空き領域があるシンプロビジョニングされた LUN で領域の解放を実行すると、`ioctl not supported`エラーによって操作が失敗します。(CA-332782)

vSwitch Controller

- vSwitch Controller が stunnel サービスでメモリリークを経験することがあります。vSwitch Controller syslog で次のメッセージが表示される可能性があります: 「Possible memory leak at...」(XSI-592)

XenCenter

- XenCenter を実行するコンピューター上でフォントサイズや画面解像度を変更すると、ユーザーインターフェイスの表示が乱れる場合があります。デフォルトのフォントサイズは 96 DPI です (Windows 8 と Windows 10 では [100%] に相当します)。(CA-45514) (CAR-1940)
- XenCenter が Windows Server 2008 SP2 にインストールされている場合、Citrix Hypervisor ホストに接続できません。次のエラーメッセージが表示されます。「SSL/TLS の保護されたチャネルを作成できませんでした」。この問題を解決するには、Windows Server 2008 SP2 システムに KB4056564 または KB4019276 のいずれかの Windows Update がインストールされていることを確認します。詳しくは、「<http://support.microsoft.com/kb/4019276>」を参照してください。(CA-298456)
- Windows 10 (1903 以降) 仮想マシンで、Citrix VM Tools をインストールしてから XenCenter の仮想マシンで [リモートデスクトップに切り替える] オプションを使用できるようになるまでに、数分かかる場合があります。ツールスタックを再起動して、このオプションをすぐに表示できます。(CA-322672)

廃止と削除

March 12, 2020

この記事の告知は、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止されるプラットフォーム、シトリックス製品、機能について前もってお知らせするためのものです。シトリックスではお客様の使用状況とフィードバックをチェックして、各プラットフォーム、シトリックス製品、機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。製品ライフサイクルサポートについては、「[製品ライフサイクルサポートポリシー](#)」を参照してください。

廃止

以下に挙げられたハードウェア、プラットフォーム、Citrix 製品、機能は Citrix Hypervisor 8.1 で廃止されます。廃止されたアイテムはすぐには削除されません。このリリースでは Citrix が引き続きサポートしていますが、詳細のリリースでは削除される予定です。

- vSwitch Controller
- 動的メモリ制御
- 以下の従来のパーティションレイアウト：
 - DOS パーティションレイアウト
 - 古い GPT パーティションレイアウト

これらのパーティションレイアウトが削除されると、Citrix Hypervisor はプライマリディスクスペースが 46 GB 未満のサーバーをサポートできなくなります。

- 以下の従来のドライバー：
 - qla4xxx
 - qla3xxx
 - netxen_nic
 - qlge
 - qlcnic

以前のリリースでサポートされていた一部のハードウェアは、これらのドライバーが廃止されたため、現在は機能しない可能性があります。「[ハードウェア互換性リスト \(英語\)](#)」をチェックしてから Citrix Hypervisor 8.1 にアップグレードしてください。

削除

以下に挙げられたハードウェア、プラットフォーム、Citrix 製品、機能は Citrix Hypervisor 8.1 で削除されます。削除されたアイテムは Citrix Hypervisor で削除されたか、サポートされなくなりました。

- Nutanix と XenServer 7.1 CU2 または XenServer 7.6 との統合を使用している場合、この統合は Citrix Hypervisor 8.0 以降で削除されたことに注意してください。
- VSS および休止スナップショット
- 以下のゲストテンプレートのサポート（ベンダーがサポートを停止したオペレーティングシステムが使用されているため）：
 - Ubuntu 14.04
- すべての準仮想化 (PV) 仮想マシンのサポート。そのため、次のゲストテンプレートは削除されました：
 - Red Hat Enterprise Linux 5
 - Red Hat Enterprise Linux 6
 - CentOS 5
 - CentOS 6
 - Oracle Enterprise Linux 5
 - Oracle Enterprise Linux 6
 - Scientific Linux 6

- NeoKylin Linux Advanced Server 6.2
- Debian Wheezy 7
- SUSE Linux Enterprise Server 11 SP3
- SUSE Linux Enterprise Server 11 SP4
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 12 SP1
- SUSE Linux Enterprise Server 12 SP2
- SUSE Linux Enterprise Desktop 11 SP3
- SUSE Linux Enterprise Desktop 12
- SUSE Linux Enterprise Desktop 12 SP1
- SUSE Linux Enterprise Desktop 12 SP2

システム要件

March 12, 2020

Citrix Hypervisor を使用するには、物理コンピューターが少なくとも 2 台必要です: 1 台は Citrix Hypervisor サーバーとして動かし、もう 1 台で XenCenter アプリケーションまたは Citrix Hypervisor コマンドラインインターフェイス (CLI) を実行します。Citrix Hypervisor サーバーコンピューターは、Citrix Hypervisor の実行つまり仮想マシンのホストのみを行い、ほかのアプリケーションを実行することはできません。

警告:

Citrix Hypervisor のコントロールドメイン内にサードパーティ製インストールソフトウェアを直接インストールすることはサポートされていません。ただし、サブリメンタルパックとして提供され、シトリックスによって明示的に推奨されているソフトウェアは例外です。

XenCenter を実行するには、ハードウェア要件を満たす汎用の Windows システムを使用します。この Windows システムは、ほかのアプリケーションの実行に使用できます。

このシステムで XenCenter をインストールすると、Citrix Hypervisor CLI もインストールされます。スタンドアロンのリモート Citrix Hypervisor CLI は、RPM ベースのすべての Linux ディストリビューションにインストールできます。詳しくは、「[コマンドラインインターフェイス](#)」を参照してください。

Citrix Hypervisor サーバーのシステム要件

Citrix Hypervisor は一般的にサーバークラスのハードウェア上にインストールされますが、Citrix Hypervisor は多くのモデルのワークステーションやノートブックにもインストールできます。詳しくは、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) を参照してください。

このセクションでは、推奨される Citrix Hypervisor ハードウェア仕様について説明します。

Citrix Hypervisor サーバーは、仮想マシンをホストする 64 ビット x86 サーバークラスのマシンである必要があります。Citrix Hypervisor は、Xen 対応カーネルを使用する最適化され強化された Linux パーティションを作成します。このカーネルは、仮想マシンが認識する仮想化デバイスと物理ハードウェアの間の相互作用を制御します。

Citrix Hypervisor では次を使用できます：

- 最大 5TB の RAM
- 最大 16 枚の物理 NIC
- ホストあたり最大 288 基の論理プロセッサ

注：

サポートされる論理プロセッサの最大数は、CPU によって異なります。詳しくは、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) を参照してください。

Citrix Hypervisor サーバーのシステム要件は、以下のとおりです：

CPU

64 ビット x86 CPU、最低 1.5GHz、2GHz 以上の速度のマルチコア CPU を推奨。

Windows またはより新しいバージョンの Linux を実行する仮想マシンを使用するには、Intel VT または AMD-V をサポートする、64 ビット x86 ベースの CPU が必要です。

注：

Windows またはより新しいバージョンの Linux を実行している仮想マシンを使用するには、Citrix Hypervisor サーバーで仮想化のハードウェアサポートを有効にします。仮想化のサポートは、BIOS のオプションです。BIOS の設定で仮想化のサポートが無効になっている場合があります。詳しくは、BIOS のドキュメントを参照してください。

準仮想化 Linux 仮想マシンを実行するには、標準的な 64 ビット x86 ベースの CPU が必要です。

RAM

最小 2GB、4GB 以上を推奨

ディスク領域

- 最小 46GB の空きディスク領域を持つ (70GB を推奨)、ローカル接続されたストレージ (PATA、SATA、SCSI)
- SAN からマルチパスブートを使用してインストールする場合は、HBA 経由の SAN (ソフトウェア経由ではない)。

互換性のあるストレージソリューションの詳細なリストについては、「[ハードウェア互換性リスト \(HCL\) \(英語\)](#)」を参照してください。

ネットワーク

100Mbit/秒以上の速度の NIC。P2V、エクスポート/インポートデータ転送、および仮想マシンのライブマイグレーションを高速に実行するには、1つまたは複数のギガビット NIC、または 10 ギガビット NIC の使用が推奨されます。

冗長性のために複数の NIC を使用することをお勧めします。NIC の設定方法は、使用するストレージの種類により異なります。詳しくは、ベンダーのドキュメントを参照してください。

Citrix Hypervisor には、管理トラフィックおよびストレージトラフィック用の IPv4 ネットワークが必要です。

注:

- サーバーの BIOS の時間設定が UTC の現在時刻に設定されていることを確認してください。
- デバッグ時に、ホストのシリアルコンソールへのアクセスが必要になることがあります。Citrix Hypervisor のセットアップ時には、シリアルコンソールにアクセスできるように設定しておくことをお勧めします。物理シリアルポートを搭載していないホストや、適切な物理インフラストラクチャを使用できない環境では、埋め込み管理デバイスを設定できるかどうかを確認してください。たとえば、Dell DRAC または HP iLO です。シリアルコンソールアクセスの設定について詳しくは、「[CTX228930 - How to Configure Serial Console Access on XenServer and later](#)」を参照してください。

XenCenter システム要件

XenCenter には次のシステム要件があります:

- オペレーティングシステム:
 - Windows 10
 - Windows 8.1
 - Windows 7 SP1
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2 SP1
 - Windows Server 2008 SP2 (注を参照)
 - Windows Server 2016
 - Windows Server 2019
- **.NET Framework:** バージョン 4.6
- **CPU 速度:** 最低 750MHz、1GHz 以上を推奨
- **RAM:** 最小 1GB、2GB 以上を推奨
- **ディスク容量:** 最小 100MB
- **ネットワーク:** 100Mbit/秒以上の速度の NIC
- **画面の解像度:** 1024x768 ピクセル以上

XenCenter は、サポートされているすべてのバージョンの Citrix Hypervisor と互換性があります。

注:

XenCenter が Windows Server 2008 SP2 システムにインストールされている場合は、KB4056564 または KB4019276 のいずれかの Windows Update が Windows Server 2008 SP2 システムにインストールされていることを確認してください。詳しくは、「<http://support.microsoft.com/kb/4019276>」を参照してください。

サポートされるゲストオペレーティングシステム

サポートされている仮想マシンオペレーティングシステムの一覧については、「[ゲストオペレーティングシステムのサポート](#)」を参照してください。

リソースプールの要件

リソースプールは、同種または異種混在型のサーバーの集合で、最大サーバー数は 64 です。新しいリソースプールを作成したり、既存のリソースプールにサーバーを追加したりする前に、プール内のすべてのサーバーが以下の要件を満たしていることを確認してください。

ハードウェア要件

Citrix Hypervisor のリソースプール内のすべてのサーバーが、以下の互換性のある CPU を搭載している必要があります:

- CPU ベンダー (Intel または AMD) が、すべてのサーバーのすべての CPU で同じである。
- HVM 仮想マシンを実行する場合は、すべての CPU で仮想化が有効になっている。

その他の要件

上記のハードウェア要件に加えて、リソースプールに追加するサーバーは以下の要件を満たしている必要があります:

- 一貫した IP アドレス (サーバー上の静的 IP アドレスまたは静的 DHCP リース) を保持している。この要件は、共有 NFS または iSCSI ストレージを提供するサーバーにも当てはまります。
- システムの時計がプールマスタの時計と同期している (Network Time Protocol を使用している場合など)。
- 既存のほかのリソースプールに属していない。
- プールに追加するサーバー上に実行中または一時停止状態の仮想マシンがない。また、仮想マシンのシャットダウンやエクスポートなど、処理中の操作がない。プールに追加する前に、サーバー上のすべての仮想マシンをシャットダウンしてください。
- 共有ストレージが構成されていない。

- 管理インターフェイスのボンディングが設定されていない。プールに追加するには、サーバーの管理インターフェイスを再設定して物理 NIC 上に戻す必要があります。サーバーをプールに追加した後に、管理インターフェイスを再設定できます。
- 実行する Citrix Hypervisor のバージョンおよびパッチレベルが、プールの既存のサーバーと同じである。
- プール内の既存のサーバーと同じサブメンタルパックがインストールされている。サブメンタルパックは、Citrix Hypervisor のコントロールドメイン (dom0) にアドオンソフトウェアをインストールするときに使用されます。プールでのユーザーエクスペリエンスを一貫させるため、プール内のすべてのサーバーに同じサブメンタルパックの同じリビジョンをインストールする必要があります。
- プール内の既存のサーバーと同じ Citrix Hypervisor ライセンスがある必要があります。プールに追加した任意のサーバーのライセンスを変更することができます。ただし、そのプールで一番低いレベルのライセンスにより、すべてのプールメンバーで使用できる機能が決定されます。

Citrix Hypervisor サーバーに搭載されている物理ネットワークインターフェイスの数やローカルストレージリポジトリのサイズは、リソースプール内で異なっても構いません。また、完全に同一の CPU を搭載した複数のサーバーを入手することは難しい場合が多いため、軽微なばらつきは許容されます。CPU が異なるホストを同じリソースプールに追加したい場合は、CLI を使用してホストを強制的に追加することもできます。強制的な追加操作については、「[ホストとリソースプール](#)」を参照してください。

注:

リソースプールで共有される NFS または iSCSI ストレージを提供するサーバーは、静的な IP アドレスが設定されているか、DNS で正しく名前解決される必要があります。

同種型プール

同種型リソースプールは同一 CPU のサーバーの集合です。同種型リソースプールに追加するサーバー上の CPU は、ベンダー、モデル、および機能が、プール内の既存のサーバー上の CPU と同じである必要があります。

異種混在型プール

異種混在型リソースプールを作成するには、マスキングまたはレベリングと呼ばれる技術をサポートする Intel 社 (FlexMigration) または AMD 社 (Extended Migration) の CPU が必要です。これらの機能では、CPU を実際とは異なる製造元、モデル、および機能セットのものとして見せかけることができます。これらの機能により、異なる種類の CPU を搭載したホストでプールを構成しても、ライブマイグレーションがサポートされます。

異種混在型プールの作成については、「[ホストとリソースプール](#)」を参照してください。

構成の制限

January 20, 2020

Citrix Hypervisor の仮想環境および物理環境を選択して構成する場合、次の構成の制限をガイドラインとして使用することをお勧めします。Citrix Hypervisor では次に示すテスト済みの推奨される上限を完全にサポートしていません。

- 仮想マシンの制限値
- Citrix Hypervisor サーバーの制限
- リソースプールの制限値

ハードウェアや環境などの要因が、以下の制限値に影響する場合があります。サポートされるハードウェアについては詳しくは、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。ハードウェアの製造元が提供する制限事項のドキュメントを参照して、お客様の環境で構成の制限を超えていないかご確認ください。

仮想マシン (VM) の制限値

項目	上限
コンピューティング	
VM あたりの仮想 CPU 数 (Linux)	32 (注 1 参照)
VM あたりの仮想 CPU 数 (Windows)	32
メモリ	
VM あたりの RAM	1.5TiB (注 2 参照)
ストレージ	
VM あたりの仮想ディスクイメージ (VDI) 数 (CD-ROM を含む)	255 (注 3 参照)
VM あたりの仮想 CD-ROM ドライブ数	1
仮想ディスクのサイズ (NFS)	2TiB から 4GiB を引いた値
仮想ディスクのサイズ (LVM)	2TiB から 4GiB を引いた値
仮想ディスクのサイズ (GFS2)	16TiB

項目	上限
ネットワーク	
VM あたりの仮想 NIC 数	7 (注 4 参照)
グラフィックス機能	
仮想マシンごとの vGPU 数	8
デバイス	
パススルー USB デバイス	6

注:

1. ゲスト OS のドキュメントを参照して、サポートされている制限値を超えていないかご確認ください。
2. 使用可能な物理メモリの最大量は、お使いのオペレーティングシステムによって異なります。オペレーティングシステムがサポートするメモリ量の上限を超えると、その仮想マシンでパフォーマンスの問題が発生する場合があります。一部の 32 ビット版 Windows では、物理アドレス拡張 (PAE: Physical Address Extension) モードを使用することで 4GiB を超える RAM がサポートされます。詳しくは、ゲストオペレーティングシステムのドキュメントおよび「[ゲストオペレーティングシステムのサポート](#)」を参照してください。
3. サポートされる VDI の最大数は、ゲストオペレーティングシステムによって異なります。ゲストオペレーティングシステムのドキュメントを参照して、サポートされている制限値を超えていないかご確認ください。
4. 一部のゲストオペレーティングシステムには下限があります。この制限値を実現するために Citrix VM Tools のインストールが必要なゲストオペレーティングシステムもあります。

Citrix Hypervisor サーバーの制限

項目	上限
コンピューティング	
ホストあたりの論理プロセッサ数	288 (注 1 参照)
ホストあたりの同時実行 VM 数	1000 (注 2 参照)
ホストあたりの同時保護 VM 数 (高可用性が有効な場合)	500

項目	上限
ホストあたりの仮想 GPU を持つ VM 数	128 (注 3 参照)
メモリ	
ホストあたりの RAM	5TB (注 4 参照)
ストレージ	
ホストあたりの同時アクティブ仮想ディスク数	2048
ホストごとのストレージリポジトリ数	400
ネットワーク	
ホストあたりの物理 NIC 数	16
ネットワークボンディングあたりの物理 NIC 数	4
ホストあたりの仮想 NIC 数	512
ホストあたりの VLAN 数	800
ホストあたりのネットワークボンディング数	4
グラフィックス機能	
ホストあたりの GPU 数	12 (注 5 参照)

注:

1. サポートされる論理プロセッサおよび物理プロセッサの最大数は、CPU によって異なります。詳しくは、[ハードウェア互換性リスト \(英語\)](#) を参照してください。
2. サポートされる VM およびホストの最大数は、VM ワークロード、システム負荷、ネットワーク構成、特定の環境要因によって異なります。シトリックスは、システムが機能する上限値に影響を与える環境要因を特定する権利を留保します。500 を超える VM を実行するシステムの場合、コントロールドメイン (Dom0) に 8GB の RAM を割り当てることをお勧めします。Dom0 のメモリ量の設定について詳しくは、「[CTX134951 - How to Configure dom0 Memory in XenServer 6.2 and Later](#)」を参照してください。
3. NVIDIA vGPU の場合、4xM60 カード (4x32=128 VM) または 2xM10 カード (2x64=128 VM) で、vGPU で加速化された VM 数はホストあたり 128 です。Intel GVT-g の場合、ホストあたりの VM 数は

7. アパーチャサイズは 1,024MB です。アパーチャサイズを小さくすると、サポートされるホストあたりの GVT-g VM 数がさらに制限されます。この数字は変更される場合があります。現在サポートされている制限値については、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。
4. ホストに 32 ビット版の準仮想化ゲスト (Linux VM) が 1 つ以上ある場合、このホスト上で最大 128GB のメモリ容量がサポートされます。
5. この数字は変更される場合があります。現在サポートされている制限値については、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。

リソースプールの制限値

項目	上限
コンピューティング	
リソースプールあたりの VM 数	4096
リソースプールあたりのホスト数	64 (注 1 参照)
ネットワーク	
リソースプールあたりの VLAN 数	800
サーバー間のプライベートネットワークあたりのアクティブホスト数	64
リソースプールあたりのサーバー間のプライベートネットワーク数	16
サーバー間のプライベートネットワークあたりの仮想 NIC 数	16
サーバー間のプライベートネットワークにおける、リソースプールあたりの仮想 NIC 数	256
vSwitch Controller あたりのホスト数	64
vSwitch Controller あたりの仮想 NIC 数	1024
vSwitch Controller あたりの VM 数	1024
障害回復	
サイト回復機能で使用する、リソースプールあたりの統合されたストレージリポジトリ数	8

項目	上限
ストレージ	
LUN へのパス数	8
ホストあたりのマルチパス LUN 数	256 (注 2 参照)
ホストあたりのマルチパス LUN 数 (ストレージリポジトリで使用)	256 (注 2 参照)
SR あたりの VDI 数 (NFS、SMB、EXT、GFS2)	20000
SR あたりの VDI 数 (LVM)	1000
ストレージリポジトリごとに接続された VDI 数 (すべての種類)	600
プールごとのストレージリポジトリ数	400
ストレージライブマイグレーション	
VM あたりの VDI 数 (CD-ROM を除く)	6
VM あたりのスナップショット数	1
同時転送数	3
XenCenter	
プールあたりの同時操作数	25

注:

1. GFS2 ストレージを使用するクラスタ化されたプールでは、リソースプール内で最大 16 のホストがサポートされます。
2. 高可用性が有効になっている場合、1 つのホスト上にマルチパスの LUN が 31 以上存在する場合に、デフォルトのタイムアウト時間を 120 秒以上に増やすことをお勧めします。HA タイムアウトの増加については、「[CTX139166 - How to Change High Availability Timeout Settings](#)」を参照してください。

ゲストオペレーティングシステムのサポート

March 12, 2020

仮想マシンを作成する場合、実行するオペレーティングシステムや関連アプリケーションのメモリおよびディスク容

量に関するガイドラインに従って、メモリやディスクスペースなどのリソースを割り当てます。

オペレーティングシステム	最小 RAM	最大 RAM	最小ディスク容量
Windows 7 SP1、 Windows 8.1、 Windows 10 (32 ビット)	1GB	4GB	24GB (40GB 以上を推奨)
Windows 7 SP1 (64 ビット)	2GB	192GB	24GB (40GB 以上を推奨)
Windows 8.1 (64 ビット)	2GB	512GB	24GB (40GB 以上を推奨)
Windows 10 (64 ビット) [テスト済みの最新バージョンは 1909]	2GB	1.5TB	32GB (40GB 以上を推奨)
Windows Server 2008 SP2 (32 ビット)	512MB	64GB	24GB (40GB 以上を推奨)
Windows Server 2008 SP2 (64 ビット)	512MB	1TB	24GB (40GB 以上を推奨)
Windows Server 2008 R2 SP1	512MB	1.5TB	24GB (40GB 以上を推奨)
Windows Server 2012、 Windows Server 2012 R2 (64 ビット)	1GB	1.5TB	32GB (40GB 以上を推奨)
Windows Server 2016、 Windows Server Core 2016 (64 ビット)	1GB	1.5TB	32GB (40GB 以上を推奨)
Windows Server 2019、 Windows Server Core 2019 (64 ビット)	1GB	1.5TB	32GB (40GB 以上を推奨)
CentOS 7.x (64 ビット) [テスト済みの最新バージョンは 7.7]	2GB	1.5TB	10GB
CentOS 8.x (64 ビット) [テスト済みの最新バージョンは 8.0]	2GB	1.5TB	10GB

オペレーティングシステム	最小 RAM	最大 RAM	最小ディスク容量
Red Hat Enterprise Linux 7.x (64 ビット) [テスト済みの最新バージョンは 7.6]	2GB	1.5TB	10GB
Red Hat Enterprise Linux 8.x (64 ビット) [テスト済みの最新バージョンは 8.0]	2GB	1.5TB	10GB
SUSE Linux Enterprise Server 12 SP3、12 SP4 (64 ビット)	1GB	1.5TB	8GB
SUSE Linux Enterprise Server 15、15 SP1 (64 ビット)	1GB	1.5TB	8GB
SUSE Linux Enterprise Desktop 12 SP3、12 SP4 (64 ビット)	1GB	1.5TB	8GB
SUSE Linux Enterprise Desktop 15、15 SP1 (64 ビット)	1GB	1.5TB	8GB
Oracle Linux 7.x (64 ビット) [テスト済みの最新バージョンは 7.6]	2GB	1.5TB	10GB
Oracle Linux 8.x (64 ビット) [テスト済みの最新バージョンは 8.0]	2GB	1.5TB	10GB
Scientific Linux 7.x (64 ビット)	2GB	1.5TB	10GB
Debian Jessie 8 (32 ビット)	128MB	64GB	8GB
Debian Jessie 8 (64 ビット)	128MB	1.5TB	8GB

オペレーティングシステム	最小 RAM	最大 RAM	最小ディスク容量
Debian Stretch 9 (32 ビット)	256MB	64GB	10GB
Debian Stretch 9 (64 ビット)	256MB	1.5TB	10GB
Debian Buster 10 (64 ビット)	1GB	1.5TB	10GB
Ubuntu 16.04 (32 ビット)	512MB	64GB	10GB
Ubuntu 16.04 (64 ビット)	512MB	1.5TB	10GB
Ubuntu 18.04 (64 ビット)	512MB	1.5TB	10GB
CoreOS Stable (64 ビット) [テスト済みの最新バージョンは 2191.5.0]	2GB	512GB	8GB
NeoKylin Linux Advanced Server 7.2 (64 ビット)	1GB	1.5TB	10GB

- サポートされているすべてのオペレーティングシステムは、HVM モードで実行されます。

準仮想化 (PV) 仮想マシンのサポートは、Citrix Hypervisor 8.1 で終了します。これらのオペレーティングシステムを使用する既存の仮想マシンは、Citrix Hypervisor 8.1 以降のインストールにインポートできます。ただし、Citrix はこれらのオペレーティングシステムを使用する仮想マシンをサポートしません。できるだけ早く、サポートされている最新バージョンのオペレーティングシステムに仮想マシンをアップグレードしてください。

- オペレーティングシステムの個々のバージョンでは、ライセンス上の理由などから、サポートされるメモリの量に独自の最大制限を設けることもできます。
- 仮想マシンには、そのオペレーティングシステムで使用可能な物理メモリの上限を超えるメモリを割り当てないでください。オペレーティングシステムがサポートするメモリ量の上限を超えると、その仮想マシンの動作が不安定になる場合があります。
- 前述の表に一覧表示されている RHEL リリースより新しいマイナーバージョンの仮想マシンを作成する場合は、次の方法を使用します：
 - メジャーバージョン用にサポートされている最新のメディアから仮想マシンをインストール
 - `yum update` を使用して、仮想マシンを新しいマイナーバージョンにアップデート

この作業は、CentOS や Oracle Linux などの RHEL ベースのオペレーティングシステムにも適用されます。

- 一部の 32 ビット版 Windows では、物理アドレス拡張 (PAE: Physical Address Extension) モードを使用することで 4GB を超える RAM がサポートされます。ただし、仮想マシンに 4GB を超えるメモリを割り当てるには、XenCenter ではなく xe CLI を使用する必要があります (CLI の `memory-static-max` に 4GB を超えるバイト数を指定できるため)。

Long-Term Guest Support

Citrix Hypervisor には、Linux 仮想マシン向けの Long-Term Guest Support (LTS) ポリシーが含まれています。LTS ポリシーを使用すると、次のいずれかの方法でマイナーバージョンの更新プログラムを利用できるようになります:

- 新しいゲストメディアからインストールする
- 既存のサポートされているゲストからのアップグレード

クイックスタート

March 12, 2020

この記事では、Citrix Hypervisor と、その Windows ベースのグラフィックユーザーインターフェイスである XenCenter のインストールおよび設定の手順について説明します。まず、これらのソフトウェアをインストールし、Windows 仮想マシン (VM) を作成して、同様の仮想マシンを複数作成する時に便利な仮想マシンテンプレートを作成します。最後に、複数のホストによるリソースプールを作成し、仮想マシンを実行したまま他のホスト上に移行する方法 (ライブマイグレーション機能) について説明します。

この記事では、セットアップを簡潔にするために、最も基本的なシナリオを例にして説明します。

この記事では、Citrix Hypervisor および XenCenter を初めて使用するユーザーを対象にしており、Citrix Hypervisor 環境の管理に XenCenter を使用する場合を想定しています。Citrix Hypervisor コマンドラインインターフェイス (CLI) 上で Linux ベースの xe コマンドを実行して Citrix Hypervisor を管理する方法については、「[コマンドラインインターフェイス](#)」を参照してください。

用語および略語

- **ホスト**: Citrix Hypervisor を実行する物理コンピューターを指します。
- **仮想マシン (VM: Virtual Machine)**: すべての要素がソフトウェアで構成されたコンピューターを指し、物理コンピューターと同様にオペレーティングシステムやアプリケーションを実行できます。各仮想マシンは仮想的

な（ソフトウェアベースの）CPU、RAM、ハードディスク、およびネットワークインターフェイスカードを持ち、物理コンピュータと同じように動作します。

- リソースプール（プール）：複数の Citrix Hypervisor サーバーで構成され、仮想マシンをホストする単一の管理対象としてグループ化したものを指します。
- ストレージリポジトリ（SR: *Storage Repository*）：仮想ディスクを格納するストレージを指します。

主要コンポーネント

Citrix Hypervisor

Citrix Hypervisor は総合的なサーバー仮想化プラットフォームで、仮想インフラストラクチャの構築および管理に必要なすべての機能が用意されています。Citrix Hypervisor は Windows および Linux ベースの仮想サーバー用に最適化されています。

Citrix Hypervisor は、オペレーティングシステムなしで直接サーバーハードウェアで実行するため、効率的で拡張性の高いシステムを実現します。Citrix Hypervisor は物理マシンから要素（ハードドライブ、リソース、ポートなど）を抽象化し、物理マシン上の仮想マシン（VM）に割り当てます。

Citrix Hypervisor では、仮想マシンの作成、ディスクスナップショットの作成、および仮想マシンワークロードの管理を行えます。

XenCenter

XenCenter は、Windows ベースのグラフィックユーザーインターフェイスです。XenCenter では、Citrix Hypervisor サーバー、プール、および共有ストレージを視覚的に管理できます。Windows デスクトップマシン上で XenCenter を実行して、仮想マシンを展開、管理、および監視できます。

XenCenter の使用方法については、XenCenter のオンラインヘルプを参照してください。F1 キーを押すといつでも、状況依存のヘルプを参照することができます。

Citrix Hypervisor および XenCenter のインストール

この章では、Citrix Hypervisor の最小インストールをセットアップします。

この章の内容

以下の手順について説明します。

- 単一の物理ホスト上に Citrix Hypervisor をインストールする
- Windows コンピューター上に XenCenter をインストールする

- XenCenter と Citrix Hypervisor を接続してインフラストラクチャを構築することで、仮想マシン (VM) を作成して実行できます。

要件

開始するには、以下が必要です。

- Citrix Hypervisor サーバーとなる物理コンピューター
- XenCenter アプリケーションを実行する Windows コンピューター
- Citrix Hypervisor および XenCenter のインストールファイル

Citrix Hypervisor サーバーコンピューターは、Citrix Hypervisor の実行つまり仮想マシンのホストのみを行い、ほかのアプリケーションを実行することはできません。XenCenter は、ハードウェア要件を満たす汎用の Windows コンピューター上で実行でき、このコンピューター上で他のアプリケーションを実行することもできます。詳しくは、「[システム要件](#)」を参照してください。

[Citrix Hypervisor ダウンロード](#)からインストールファイルをダウンロードできます。

Citrix Hypervisor サーバーのインストール

すべてのホストには、少なくとも 1 つの IP アドレスが関連付けられています。ホストに静的な IP アドレスを割り当てる場合 (DHCP を使用しない場合) は、その IP アドレスを手元に用意しておいてください。

ヒント:

F12 キーを押すと次のインストーラー画面にすばやく進めます。ヘルプを表示するには **F1** キーを押します。

Citrix Hypervisor サーバーをインストールするには、次の手順に従います:

1. Citrix Hypervisor のインストールファイルを CD に書き込むか、起動可能な USB を作成します。

注:

インストールパッケージのソースとして HTTP、FTP、または NFS を使用する場合は、手順については、「[インストール Citrix Hypervisor](#)」を参照してください。

2. 保存したいデータをバックアップします。Citrix Hypervisor をインストールすると、インストール時に指定したすべてのハードディスク上のデータが上書きされます。
3. ホストコンピューターにインストールメディアを挿入します。
4. ホストコンピューターを再起動します。
5. コンピューターをローカルインストールメディアから起動します (起動順序の変更が必要な場合は、コンピューターに付属のドキュメントを参照してください)。
6. 起動メッセージおよび [**Welcome to Citrix Hypervisor**] 画面が表示されます。ここで、インストールに使用するキーボードレイアウトを選択します。

7. **[Welcome to Citrix Hypervisor Setup]** 画面が表示されたら、**[OK]** を選択します。
8. Citrix Hypervisor のライセンス契約書 (EULA) の内容を確認して、**[Accept EULA]** を選択します。

注:

[System Hardware] 警告画面が表示された場合は、インストール先コンピューターの CPU がハードウェア仮想化をサポートしているかどうかを確認してください。また、ハードウェアの製造元で BIOS のアップデートが提供されていないかどうかを確認してください。
9. ここでは新規インストール (Clean Installation) を行うので、**[OK]** を選択します。
10. 複数のローカルハードディスクがある場合は、インストール用のプライマリディスクを選択し、**[OK]** を選択します。

仮想マシストレージ用のディスクを選択します。**[OK]** を選択します。
11. インストールパッケージのソースとして、**[Local media]** を選択します。
12. インストールメディアの整合性を検証するかどうかを選択する画面で **[Skip verification]** を選択し、**[OK]** を選択します。

注:

インストール中に問題が発生した場合は、インストールメディアの整合性を検証してください。
13. ルートパスワードを設定します。確認のため、同じパスワードを 2 回入力する必要があります。ここで設定したルートパスワードは、後で XenCenter を使ってこの Citrix Hypervisor サーバーに接続する時に使用します。
14. 管理インターフェイスを設定します。このインターフェイスは、XenCenter への接続で使用されます。

コンピューターに複数のネットワークインターフェイスカード (NIC) がある場合は、管理トラフィックで使用する NIC (通常は最初の NIC) を選択します。
15. 管理インターフェイスとして使用する NIC の IP アドレスとして、特定の (静的な) アドレスを使用するか DHCP を使用するかを選択します。
16. ホスト名を設定して、DNS 設定を手作業で行うか DHCP を使って自動的に行うかを指定します。

DNS 設定を手作業で行う場合は、プライマリ (必須)、セカンダリ (オプション)、およびターシャリ (オプション) の DNS サーバーの IP アドレスを入力します。
17. タイムゾーンを選択します。
18. XenServer ホストのローカルの日時として、NTP による自動設定または手動設定を選択します。**[OK]** を選択します。
 - **[Using NTP]** を選択した場合は、タイムサーバーを指定する画面が表示されます。DHCP による自動設定を指定するか、1 つ以上の NTP サーバーの名前または IP アドレスを入力します。
 - 日時設定として **[Manual time entry]** を選択した場合、インストール中に日時を入力するための画面が表示されます。

19. **[Install] Citrix Hypervisor** を選択します。

インストールプロセスが開始されます。これには数分かかる場合があります。

20. 次の画面では、サプリメンタルパックをインストールするかどうかを選択する画面が表示されます。 **[No]** をクリックして続行します。

21. **[Installation Complete]** 画面が表示されたら、インストールメディアを取り出し、** [OK] ** を選択してサーバーを再起動します。

サーバーが再起動すると、Citrix Hypervisor のシステム設定コンソールである **xsconsole** が表示されます。

注:

表示された IP アドレスを控えておきます。この IP アドレスは、XenCenter をホストに接続する時に使
用します。



インストール XenCenter

XenCenter は、通常ローカルシステムにインストールします。XenCenter インストーラーは[シトリックスのダウンロードサイト](#)からダウンロードできます。

XenCenter をインストールするには、次の手順に従います:

1. XenCenter を実行するコンピューターに XenCenter インストーラーをダウンロードまたは転送します。
2. インストーラー (.msi ファイル) をダブルクリックしてインストールを開始します。
3. インストールウィザードの指示に従って、XenCenter をインストールします (必要な場合はインストール先を変更します)。

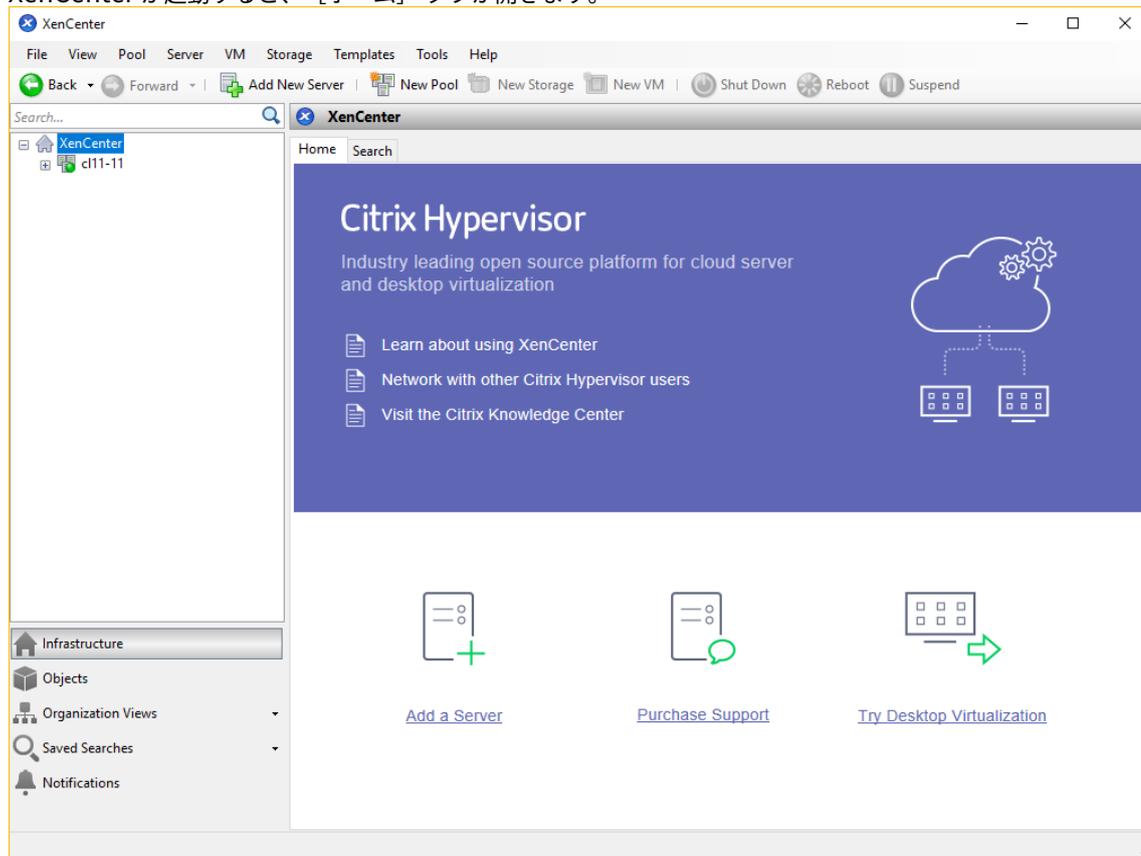
XenCenter による Citrix Hypervisor サーバーへの接続

XenCenter でホストに接続するには、以下の手順でホストを XenCenter に追加します。

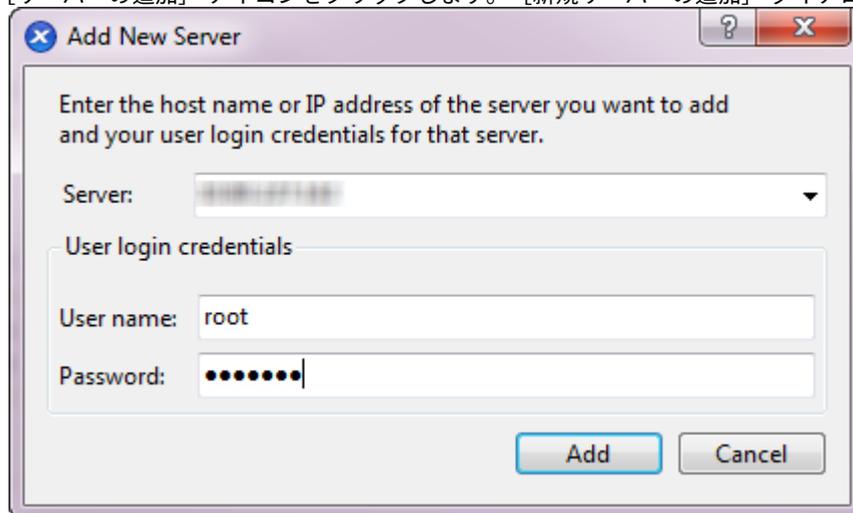
XenCenter を使って Citrix Hypervisor サーバーに接続するには、次の手順に従います:

1. XenCenter を起動します。

XenCenter が起動すると、[ホーム] タブが開きます。



2. [サーバーの追加] アイコンをクリックします。[新規サーバーの追加] ダイアログボックスが開きます。



3. [サーバー] ボックスに、接続先ホストの IP アドレスを入力します。Citrix Hypervisor のインストール時に設定したルートユーザー名とパスワードを入力します。[追加] をクリックします。

注:

ホストを初めて XenCenter に追加すると、[接続状態の保存と復元] ダイアログボックスが開きます。このダ

イアログボックスでは、ホストの接続情報を保持して、サーバー接続が自動的に復元されるように設定できます。

ライセンス Citrix Hypervisor

Citrix Hypervisor はライセンスなしで使用できます (Free Edition) が、このエディションで提供される機能セットでは、使用が制限されます。

Citrix Hypervisor のライセンスをお持ちの場合は、今すぐ適用してください。

詳しくは、「[ライセンス](#)」を参照してください。

Citrix Hypervisor サーバーのプールの作成

リソースプールは、複数の Citrix Hypervisor サーバーを単一の管理対象としてグループ化したものです。

リソースプール (プール) を作成すると、複数のホストとそれらの共有ストレージを単一リソースとして管理できます。リソースプールでは、リソース要求や業務上の優先度に応じて、仮想マシン環境を柔軟に展開できます。1つのプールには、互換性のあるハードウェアを持ち、同じバージョンの Citrix Hypervisor ソフトウェア (適用されたパッチも含む) を実行するホストを最大で 64 台まで追加できます。

リソースプールでは、1 台のホストがプールマスターとして動作します。プールマスターは、プール全体の単一接続ポイントになり、通信を必要に応じて個々のメンバーホストに転送します。リソースプールの各メンバーには、必要に応じてプールマスターの役割を引き継ぐための情報がすべて格納されています。プールマスターとして動作するホストは、XenCenter のリソースペインでそのプールの最上位に表示されます。また、プールマスターの IP アドレスは、プールマスターとして動作するホストの [検索] タブに表示されます。

共有ストレージが接続されたリソースプールでは、十分なメモリを備えた任意のプールメンバー上で仮想マシンを起動できるほか、別のホスト上に動的に移行することもできます。この場合、実行中の仮想マシンを、最小限のダウンタイムで移行できます。Citrix Hypervisor サーバーでハードウェア障害が生じた場合、管理者は、そのホスト上の仮想マシンを、同じリソースプール内の別のホスト上で再起動させることができます。

高可用性 (HA) 機能が有効な場合は、障害が生じたホスト上の仮想マシンを自動的に他のホスト上に移行させることができます。高可用性が有効なプールでは、プールマスターがシャットダウンされると新しいプールマスターが自動的に選出されます。

注:

異種混在型プールについて詳しくは、[ホストとリソースプール](#)を参照してください。

この章の内容

以下の手順について説明します。

- リソースプールを作成する

- プールのネットワークをセットアップする
- NIC をボンディングする
- プールの共有ストレージをセットアップする

Citrix Hypervisor ではさまざまな種類の共有ストレージソリューションを使用できますが、ここでは代表的な 2 種類 (NFS と iSCSI) のストレージについて説明します。

要件

共有ストレージでリソースプールを作成するには、以下が必要です。

- 類似したプロセッサ構成の 2 台目の Citrix Hypervisor サーバー。
このホストを XenCenter アプリケーションに接続します。
- IP ベースのストレージ用リポジトリ

ここでは、説明を簡潔にするために同種型プールを作成します。同種型プールのすべてのホストは、プロセッサに互換性があり、同じバージョンの Citrix Hypervisor を同じ種類の Citrix Hypervisor 製品ライセンスで実行している必要があります。同種型プールの要件について詳しくは、[システム要件](#)を参照してください。

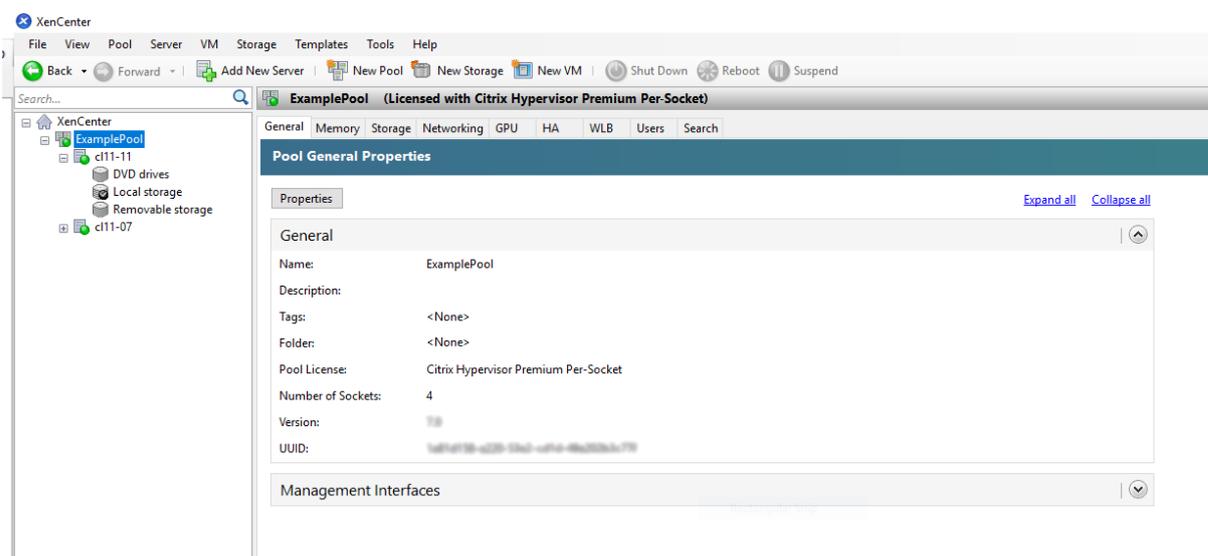
リソースプールの作成

リソースプールを作成するには

1. XenCenter のツールバーで [新規プール] をクリックします。



2. 新しいリソースプールの名前と、必要に応じて説明を入力します。
3. [マスター] ボックスの一覧で、プールマスタとして動作するホストを選択します。
4. [そのほかの追加メンバー] ボックスの一覧で、リソースプールに追加する 2 台目のホストを選択します。
5. [プールの作成] をクリックします。
リソースプールが作成され、リソースペインに追加されます。



プールのネットワークのセットアップ

Citrix Hypervisor をインストールすると、IP アドレスを指定した NIC（通常はプールの最初の NIC）上にネットワーク接続が作成されます（Citrix Hypervisor のインストール時）。

ただし、必要に応じてプールを VLAN や他の物理ネットワークに接続することができます。これを行うには、これらのネットワークをプールに追加します。Citrix Hypervisor を構成して各 NIC を 1 つの物理ネットワークに接続したり、複数の VLAN に接続したりできます。

ネットワークを作成する前に、実際のケーブル接続がプールの各ホストと一致していることを確認してください。つまり、各ホスト上の NIC が、他のプールメンバー上の対応する NIC と同じ物理ネットワークに接続されている必要があります。

注:

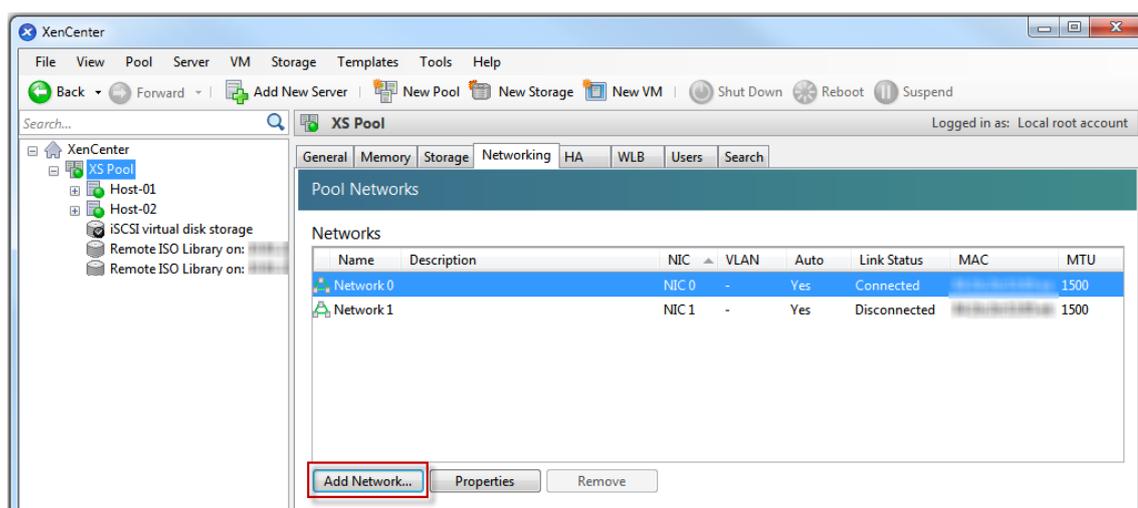
Citrix Hypervisor のインストール後に、ホスト上の NIC にその NIC が接続されていない場合:

- NIC を接続します。
- XenCenter で、[<your host> NICs] タブを選択します。
- [再スキャン] をクリックすると、新しい NIC が検出されます。

Citrix Hypervisor ネットワークの設定について詳しくは、「[ネットワーク](#)」および「[Citrix Hypervisor のネットワークについて](#)」を参照してください。

Citrix Hypervisor にネットワークを追加するには:

1. XenCenter のリソースペインで、リソースプールを選択します。
2. [ネットワーク] タブをクリックします。
3. [ネットワークの追加] をクリックします。



4. [種類の選択] ページで、[外部ネットワーク] を選択して [次へ] をクリックします。
5. [名前] ページで、わかりやすい名前と説明を入力します。
6. [ネットワーク設定] ページで、以下を行います：
 - **NIC**: Citrix Hypervisor でネットワークのデータを送受信する NIC を選択します。
 - **VLAN**: ネットワークが VLAN である場合は、その VLAN の ID (または「タグ」) を入力します。
 - **MTU**: ネットワークでジャンボフレームが使用されている場合は、MTU (Maximum Transmission Unit) を 1500 ~ 9216 で入力します。ジャンボフレームが使用されていない場合は、デフォルトの 1500 を使用します。

多くの仮想マシンで使用されるネットワークでは、[このネットワークを新規 VM に自動的に追加する] チェックボックスをオンにします。これにより、このネットワークがデフォルトで追加されます。
7. [完了] をクリックします。

NIC のボンディング

NIC をボンディングして複数の物理 NIC を単一の高性能チャネルのように使用することで、サーバーの耐障害性を向上させることができます。ここでは、NIC のボンディング (またはチーミング) の概要についてのみ説明します。実稼働環境でボンディングを作成する前に、詳細なボンディング情報を理解しておくことをお勧めします。詳しくは、「[ネットワーク](#)」を参照してください。

Citrix Hypervisor では、アクティブ/アクティブ、アクティブ/パッシブ (アクティブ/バックアップ)、および LACP のボンディングモードがサポートされています。アクティブ/アクティブモードでは、仮想マシントラフィックに対する負荷分散および冗長性が提供されます。ただし、他の種類のトラフィック (管理トラフィックおよびストレージトラフィック) は負荷分散されません。ストレージトラフィックでは、LACP ボンディングまたはマルチパスの方が適しています。マルチパスについて詳しくは、「[ストレージ](#)」を参照してください。ボンディングについて詳しくは、「[ネットワーク](#)」を参照してください。

ネットワークスタックとして vSwitch が使用されていない環境では、LACP モードのオプションは表示されません。また、IEEE 802.3ad 標準をサポートするスイッチを使用する必要があります。このスイッチには、ホスト上の LACP ボンディングごとに個別の LAG (リンクアグリゲーショングループ) が設定されている必要があります。LAG グループの作成について詳しくは、「[ネットワーク](#)」を参照してください。

NIC をボンディングするには

1. バインドする NIC (ボンドスレーブ) が使用されていないことを確認します。ボンドを作成する前に、ボンドスレーブを使用して仮想ネットワークインターフェイスを持つ VM をシャットダウンする必要があります。その後で仮想マシンの仮想ネットワークインターフェイスを適切なネットワークに再接続する必要があります。
2. リソースペインでサーバーを選択して、**[NIC]** タブの **[ボンディングの作成]** をクリックします。
3. ボンディングする NIC を選択します。一覧で、ボンディングに追加する NIC のチェックボックスをオンにします。最大で 4 つの NIC を選択できます。チェックボックスをオフにして、NIC の選択を解除します。柔軟で安全性の高いネットワークを維持するために、ネットワークスタックとして vSwitch を使用する場合は、最大で 4 つの NIC を使用してボンディングを作成できます。Linux ブリッジがネットワークスタックの場合、ボンディングを構成できる NIC は 2 つまでです。
4. **[ボンディングモード]** で、ボンディングの種類を指定します：
 - アクティブ/アクティブモードを指定するには、**[アクティブ/アクティブ]** を選択します。これにより、ボンディングされた NIC 間でトラフィックが分散されます。ボンディング内の一方の NIC に障害が発生した場合、ホストサーバーのネットワークトラフィックは自動的に他方の NIC 経由で転送されます。
 - アクティブ/パッシブモードを指定するには、**[アクティブ/パッシブ]** を選択します。この場合、トラフィックは一方の NIC のみで転送されます。このモードでは、ボンディングされた NIC のうち一方のみがアクティブになり、その NIC がネットワークから切断されるなど、障害が発生した場合のみ 2 つ目の NIC が使用されます。
 - **[LACP - 送信元の MAC アドレスによる負荷分散]** を選択して LACP ボンディングを作成します。このボンディングでは、送信元の仮想マシンの MAC アドレスに基づいてトラフィックの送信 NIC が選択されます。同一ホスト上でいくつかの仮想マシンが動作する環境では、このオプションによるトラフィック分散を使用します。仮想インターフェイス (VIF) の数が NIC よりも少ない場合、このハッシュアルゴリズムは適していません。トラフィックを複数の NIC に分散できないため、適切な負荷分散は提供されません。
 - **[LACP - 送信元/送信先のポートと IP による負荷分散]** を選択して LACP ボンディングを作成します。このボンディングでは、送信元の IP アドレスとポート番号、および送信先の IP アドレスとポート番号に基づいてトラフィックが NIC 間で分散されます。このオプションは、VIF の数が NIC よりも少ない環境で仮想マシンからのトラフィック負荷を分散させる場合に適しています。

注:

LACP ボンディングは、vSwitch でのみ使用できます。アクティブ/アクティブモードおよびアクティブ/パッシブモードのボンディングは、vSwitch および Linux ブリッジの両方で使用できま

す。ネットワークスタックについて詳しくは、「[ネットワーク](#)」を参照してください。

5. ジャンボフレームを使用する場合は、最大転送単位 (Maximum Transmission Unit: MTU) の値を 1500 から 9216 の範囲で指定します。
6. [新規 VM] ウィザードで新しい仮想マシンを作成するときに、ボンディングした新しいネットワークが自動的に追加されるようにするには、このチェックボックスをオンにします。
7. [作成] をクリックします。NIC ボンディングが作成され、ダイアログボックスが閉じます。

XenCenter で新しいボンディングが作成されると、管理インターフェイスおよびセカンダリインターフェイスがボンドスレーブからボンドマスターに移動します。ボンディング上に管理インターフェイスを持つサーバーはリソースプールに追加できません。プールに追加するには、サーバーの管理インターフェイスを再設定して物理 NIC 上に戻す必要があります。

プールの共有ストレージをセットアップする

プール内のホストをリモートのストレージアレイに接続するには、Citrix Hypervisor のストレージリポジトリを作成します。このストレージリポジトリは、仮想マシンの仮想ディスクを格納するストレージコンテナです。ストレージリポジトリは、Citrix Hypervisor ホストに依存しない永続的なオンディスクオブジェクトです。ストレージリポジトリは、内蔵および外付けのさまざまな種類の物理ストレージデバイス上に作成できます。これらの種類には、ローカルディスクデバイスや共有ネットワークストレージが含まれます。

Citrix Hypervisor では、以下の種類のストレージを使用して、ストレージリポジトリを作成できます：

- NFS
- ソフトウェア iSCSI
- ハードウェア HBA
- SMB
- ファイバチャネル
- ソフトウェア FCoE

ここでは、リソースプールのストレージリポジトリとして、NFS と iSCSI という 2 種類のストレージを使用します。これらの NFS または iSCSI ストレージアレイは、ストレージリポジトリを作成する前に設定しておく必要があります。設定方法は、使用するストレージソリューションによって異なります。詳しくは、ベンダーのドキュメントを参照してください。通常、ストレージソリューションの次の設定を完了しておく必要があります：

- **iSCSI** ストレージリポジトリ：ストレージアレイ上にボリュームおよび LUN を作成しておく。
- **NFS** ストレージリポジトリ：ストレージアレイ上にボリュームを作成しておく。
- ハードウェア **HBA**：LUN を提供するために必要な構成を行ってから [新規ストレージリポジトリ] ウィザードを実行する必要があります。

- ソフトウェア **FCoE SR**: LUN をホストに公開するために必要な設定を手動で完了している必要があります。この設定には、FCoE ファブリックの設定と、SAN のパブリックワールドワイドネーム (PWWN) への LUN の割り当てが含まれます。

IP ベースのストレージ (iSCSI または NFS) を作成する場合は、ストレージネットワークとして管理トラフィック用の NIC を使用したり、ストレージトラフィック用の NIC を作成してそれを使用したりできます。他の NIC をストレージトラフィック用に使用する場合は、その NIC に IP アドレスを割り当てる必要があります。これを行うには、管理インターフェイスを作成します。

管理インターフェイスを作成する場合、次の基準を満たす IP アドレスを割り当てる必要があります:

- 使用するストレージコントローラーと同じサブネットに属します
- Citrix Hypervisor インストール時に指定した IP アドレスとは異なるサブネットに属します
- ほかの管理インターフェイスとは異なるサブネットに属します。

NIC に IP アドレスを割り当てるには

1. NIC が別のサブネット上にあること、またはネットワークトポロジに適したルーティングが設定されていることを確認します。この設定では、選択した NIC 経由で目的のトラフィックが転送されます。
2. XenCenter の [リソース] ペインで、プール (またはスタンドアロンサーバー) を選択します。[ネットワーク] タブの [設定] をクリックします。
3. [IP アドレスの設定] ダイアログボックス左側の [IP アドレスの追加] をクリックします。
4. 新しいインターフェイスにわかりやすい名前 (「ストレージアレイネットワーク」など) を指定して、[ネットワーク] ボックスでストレージトラフィック用のネットワークを選択します。
5. [以下の設定を使用する] をクリックします。NIC に割り当てる静的 IP アドレス、サブネットマスク、およびゲートウェイを入力して、[OK] をクリックします。この IP アドレスは、接続先のストレージコントローラーと同じサブネットに属している必要があります。

注:

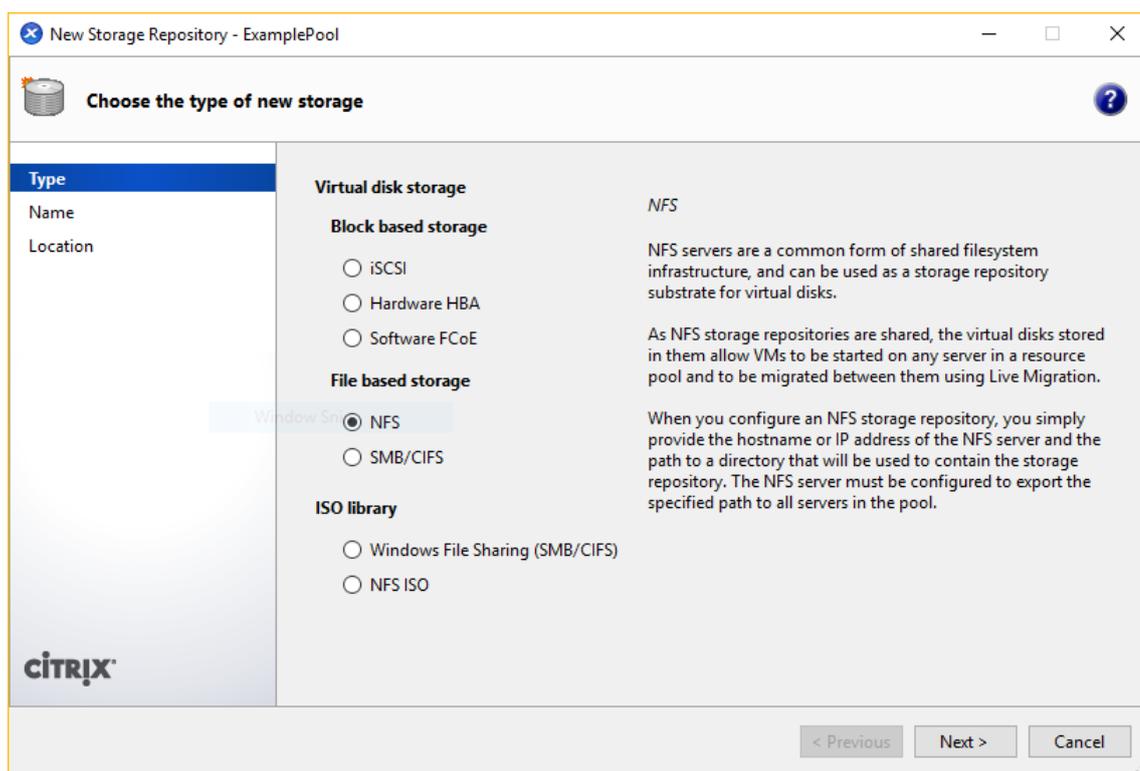
NIC に IP アドレスを割り当てるときは、そのプール内のほかの NIC に割り当てられている IP アドレスとは異なるサブネットに属している必要があります。これには、プライマリ管理インターフェイスが含まれます。

NFS または iSCSI の共有ストレージリポジトリを作成するには

1. リソースペインでリソースプールを選択します。XenCenter のツールバーで [新規ストレージ] をクリックします。



[新規ストレージリポジトリ] ウィザードが開きます。



2. [仮想ディスクストレージ] で、ストレージの種類として [NFS] または [iSCSI] を選択します。[次へ] をクリックして続行します。

3. NFS を選択した場合:

- a) 新しいストレージリポジトリの名前と、それを格納する共有の名前を入力します。指定した場所に既存の NFS ストレージリポジトリがあるかどうかを確認するには、[スキャン] をクリックします。

注:

指定したパスがプール内のすべての Citrix Hypervisor サーバーにエクスポートされるように NFS サーバーを設定しておく必要があります。

- b) [完了] をクリックします。

新しいストレージリポジトリが作成され、リソースペインのリソースプールの下に追加されます。

4. iSCSI を選択した場合:

- a) 新しいストレージリポジトリの名前と、iSCSI ターゲットの IP アドレスまたは DNS 名を入力します。

注:

プール内のすべての Citrix Hypervisor サーバーが LUN にアクセスできるように iSCSI ストレージターゲットを設定しておく必要があります。

- b) iSCSI ターゲットが CHAP 認証を使用するように設定されている場合は、ユーザー名とパスワードを入力します。

- c) [ターゲットホストのスキャン] をクリックして、[ターゲット IQN] ボックスの一覧から iSCSI ターゲットの IQN を選択します。

警告:

iSCSI ターゲットおよびプール内のすべてのホストで、固有の IQN が設定されている必要があります。

- d) [ターゲット LUN] をクリックして、[ターゲット LUN] ボックスの一覧から LUN を選択します。この LUN にストレージリポジトリが作成されます。

警告:

各 iSCSI ストレージリポジトリは全体が単一の LUN に含まれる必要があります、複数の LUN にまたがることはできません。また、選択した LUN 上の既存のデータはすべて破棄されます。

- e) [完了] をクリックします。

新しいストレージリポジトリが作成され、リソースペインのリソースプールの下に追加されます。

このストレージリポジトリは、リソースプールのデフォルトのストレージリポジトリになります。

仮想マシンの作成

XenCenter では、いくつかの方法で仮想マシンを作成でき、目的に応じて適した方法を選択できます。XenCenter では、簡単な操作で特定の構成を持つ個別の仮想マシンを作成したり、同じ構成の仮想マシンのグループを用意したりできます。

Citrix Hypervisor では、VMware の仮想マシンを XenServer 用に簡単に一括変換するためのツールが用意されています。詳しくは、「[Conversion Manager](#)」を参照してください。

このセクションでは、Windows 仮想マシンの作成方法について説明します。ここでは、説明を簡潔にするために最もシンプルな Citrix Hypervisor 環境を使用します。つまり、ローカルストレージを持つ単一の Citrix Hypervisor サーバーで仮想マシンを作成します (XenCenter でこの Citrix Hypervisor サーバーに接続すると、ストレージが対象ホストのローカルディスク上に自動的に設定されます)。

また、リソースプール内のホスト間で仮想マシンを動的に移行するライブマイグレーションの使用についても説明します。

以下の手順では、仮想マシンを作成してカスタマイズした後で、その仮想マシンをテンプレートに変換します。仮想マシンテンプレートには仮想マシンに加えられたカスタマイズ内容が保持され、そのテンプレートから同じ (または類似した) 構成の仮想マシンを簡単に作成できます。複数の仮想マシンを作成するのに要する時間も短くなります。

仮想マシンテンプレートは、既存の仮想マシンのスナップショットから作成することもできます。スナップショットは、実行中の仮想マシンのある時点での状態を記録したもので、元の仮想マシンの構成、ストレージ、およびネットワーク情報が保持されます。このため、仮想マシンをバックアップする目的でスナップショットを作成できます。スナップショットは、仮想マシンテンプレートを作成する簡単な方法です。このセクションでは、既存の仮想マシンか

らスナップショットを作成して、それを仮想マシンテンプレートに変換します。また、このセクションの最後に、仮想マシンテンプレートから新しい仮想マシンを作成する方法についても説明します。

この章の内容

以下の手順について説明します。

- Windows 8.1 仮想マシンを作成する
- インストール Citrix VM Tools
- 実行中の仮想マシンをプール内の他のホストに移行する
- 仮想マシンテンプレートを作成する
- テンプレートから仮想マシンを作成する

要件

共有ストレージでリソースプールを作成するには、以下が必要です。

- セットアップした Citrix Hypervisor プール
- XenCenter
- Windows 8.1 のインストールファイル

Windows 8.1 (32 ビット) 仮想マシンを作成する

注:

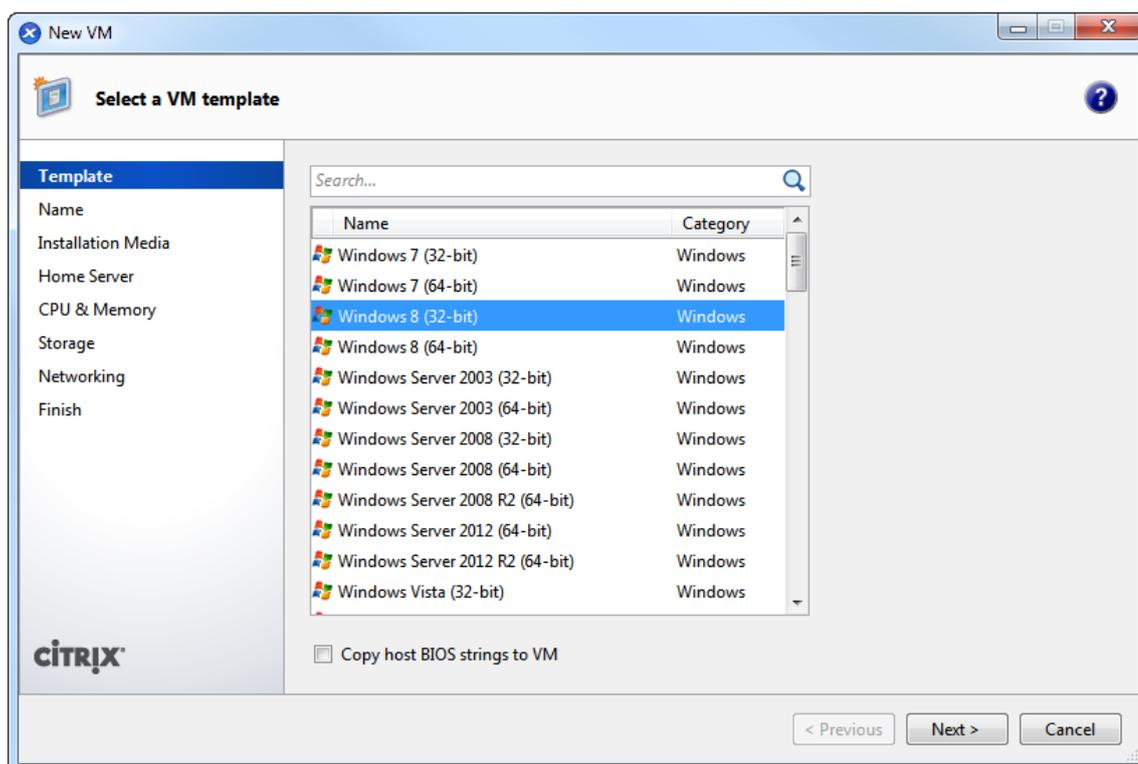
以下の手順では、Windows 8.1 (32 ビット、英語版) の仮想マシンを作成します。仮想マシンにインストールするオペレーティングシステムによっては、デフォルトの値が異なる場合があります。

Windows 仮想マシンを作成するには:

1. ツールバーで [新規 VM] をクリックします。[新規 VM] ウィザードが開きます。



[新規 VM] ウィザードでは、CPU、ストレージ、ネットワークなどの設定パラメータを選択しながら、目的に応じた仮想マシンを作成できます。



2. VM テンプレートを選択して [次へ] をクリックします。

各テンプレートには、仮想マシンを特定のゲストオペレーティングシステムおよび適切なストレージ設定で作成するために必要な情報が含まれています。このテンプレート一覧には、現在 Citrix Hypervisor でサポートされているゲストオペレーティングシステムのテンプレートが表示されます。

注:

新しい仮想マシンにインストールするオペレーティングシステムが特定のハードウェアでのみ動作する場合は、[ホストの **BIOS** 文字列を **VM** にコピーする] チェックボックスをオンにします。このオプションは、特定のコンピューターに同梱されていたインストール CD のオペレーティングシステムなどに使用します。

3. 新しい仮想マシンの名前と、必要に応じて説明を入力します。
4. 新しい仮想マシンにインストールするオペレーティングシステムのインストールメディアを選択します。

CD/DVD からのインストールが最も簡単な方法です。デフォルトのインストール元のオプション (Citrix Hypervisor サーバーの DVD ドライブ) を選択し、CD/DVD をホストの DVD ドライブに挿入して [次へ] をクリックします。

Citrix Hypervisor の既存の ISO ライブラリからインストールすることもできます。

既存の ISO ライブラリを接続するには、[新規 **ISO** ライブラリ] をクリックして ISO ライブラリの場所と種類を指定します。ISO ライブラリを指定すると、そのライブラリの ISO ファイルをリストで選択できるようになります。

5. 新しい仮想マシンのホームサーバーとして、現在のホストが指定されます。[次へ] を選択して続行します。
6. 新しい仮想マシンに割り当てる仮想 CPU とメモリを指定します。

Windows 8.1 の仮想マシンテンプレートでは、デフォルトで1つの仮想 CPU (1 ソケット、1 コア/ソケット) および 2GB の RAM が割り当てられます。必要に応じて、これらの設定を変更し、[次へ] をクリックして続行します。

注:

仮想マシンテンプレートには、各オペレーティングシステムで必要とされる構成情報が定義されています。

7. グラフィック処理装置 (GPU) を割り当てる。

新規 **VM** ウィザードにより、専用 GPU または仮想 GPU を仮想マシンに割り当てます。これにより、GPU の処理能力を仮想マシンで利用できるため、CAD、GIS、および医療用画像処理アプリケーションなどの高度な 3D グラフィックアプリケーションのサポートが向上します。

注:

GPU 仮想化は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。

8. 新しい仮想マシンのストレージを構成します。

デフォルトの割り当てサイズおよび設定のまま [次へ] をクリックします:

- a) 仮想ディスクの名前、説明、またはサイズを変更する場合は、[プロパティ] をクリックします。
- b) 新しい仮想ディスクを追加する場合は、[追加] をクリックします。

注:

リソースプールを作成すると、Citrix Hypervisor サーバーで仮想マシンを作成するときに共有ストレージを設定できます。

9. 新しい仮想マシンのネットワークを設定します。

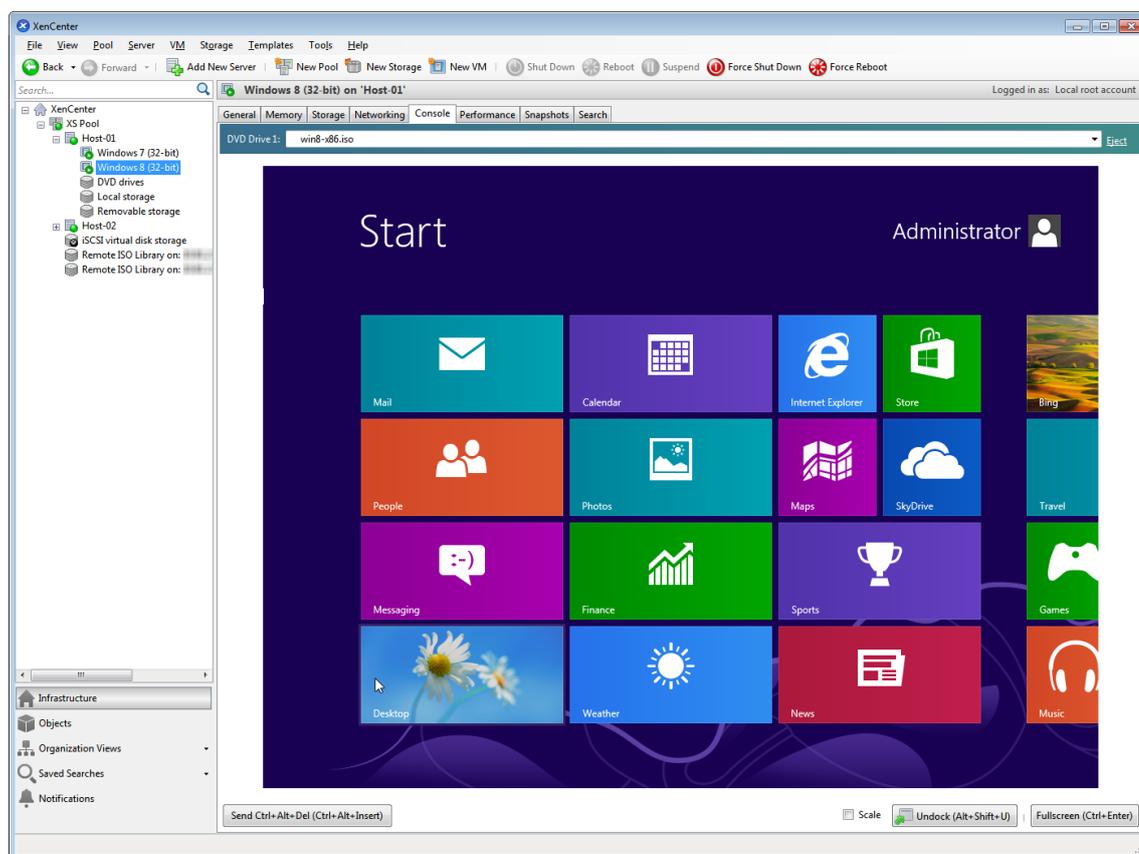
デフォルトの NIC および自動生成される MAC アドレスを使用する場合は、[次へ] をクリックします。または、以下の設定を変更します:

- a) 物理ネットワーク、MAC アドレス、および仮想ディスクの QoS (Quality of Service: サービス品質) 制限を変更するには、[プロパティ] をクリックします。
- b) 新しい仮想ネットワークインターフェイスを追加する場合は、[追加] をクリックします。

Citrix Hypervisor は、仮想ネットワークインターフェイスを使用してホスト上の物理ネットワークに接続します。その仮想マシンで使用するネットワークを選択してください。物理ネットワークの追加方法については、プールのネットワークのセットアップを参照してください。

10. 設定内容を確認し、[作成] をクリックして新しい仮想マシンを作成し、[検索] タブに戻ります。

新しい仮想マシンのアイコンが、[リソース] ペインのホストの下に表示されます。



リソースペインで仮想マシンを選択して、[コンソール] タブをクリックします。仮想マシンのコンソール画面が表示されます。

11. オペレーティングシステムのインストール画面の指示に従って、インストールを完了します。
12. オペレーティングシステムがインストールされ、仮想マシンが再起動したら、Citrix VM Tools をインストールします。

インストール **Citrix VM Tools**

Citrix VM Tools には従来型デバイスエミュレーションのようなオーバーヘッドがなく、高パフォーマンスの I/O サービスが提供されます。Citrix VM Tools は、I/O ドライバー（準仮想化ドライバーまたは PV ドライバーともいいます）と管理エージェントで構成されています。Citrix VM Tools でサポートされるすべての機能を使用するには、各仮想マシンにインストールする必要があります。仮想マシンはこれらがなくても機能しますが、パフォーマンスが低下します。また、仮想マシンを正しくシャットダウン/再起動/一時停止する機能やライブマイグレーションなど、Citrix VM Tools をインストールしないと有効にならない機能もあります。

警告:

Citrix VM Tools は、Windows 仮想マシンごとにインストールする必要があります。Citrix VM Tools をイン

ストールせずに Windows 仮想マシンを実行することはサポート対象外です。

Citrix VM Tools をインストールするには、次の手順に従います：

1. [リソース] ペインで仮想マシンを右クリックし、ショートカットメニューの [インストール] **Citrix VM Tools** をクリックします。または、[VM] メニューの [インストール] **Citrix VM Tools** を選択します。

または

仮想マシンの [全般] タブで、[I/O ドライバーおよび管理エージェントをインストール] をクリックします。

注：

仮想マシンに Citrix VM Tools をインストールすると、I/O ドライバー (PV ドライバー) と管理エージェントの両方がインストールされます。

2. 仮想マシンの CD/DVD ドライブで自動実行が有効になっている場合は、しばらくすると自動的にインストールが開始されます。I/O ドライバーと管理エージェントがインストールされ、必要に応じて仮想マシンが再起動されます。
3. 自動実行が無効になっている場合は、Citrix VM Tools インストーラーによってインストールオプションが表示されます。[インストール] **Citrix VM Tools** をクリックして、インストールを続行します。これにより、仮想マシンの CD/DVD ドライブに Citrix VM Tools ISO (`guest-tools.iso`) がマウントされます。
4. [setup.exe の実行] をクリックして Citrix VM Tools のインストールを開始し、確認メッセージが表示されたら仮想マシンを再起動してインストール処理を完了します。

注：

Windows Update からアップデートを受け取ることができる Windows 仮想マシンには、I/O ドライバーが自動的にインストールされます。ただし、Citrix VM Tools パッケージをインストールして管理エージェントをインストールし、サポートされている構成を保持することをお勧めします。次の機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます：

- Windows Update から I/O ドライバーを受信する機能
- 管理エージェントの自動更新

Citrix VM Tools をインストールしたら、必要に応じて仮想マシンにアプリケーションをインストールしたり設定を変更したりできます。同じ構成の仮想マシンを複数作成する必要がある場合は、既存の仮想マシンからテンプレートを作成し、そのテンプレートから仮想マシンを作成できます。詳しくは、「VM テンプレートの作成」を参照してください。

実行中の仮想マシンをプール内の他のホストに移行する

ライブマイグレーション機能を使用すると、実質的にサービスを中断することなく、ホスト上で実行されている仮想マシンを、同じリソースプール内の他のホストに移行 (移動) することができます。仮想マシンの移行先は、仮想マシンやリソースプールの構成に応じて選択できます。

実行中の仮想マシンを移行するには

1. リソースペインで、移行する仮想マシンを選択します。

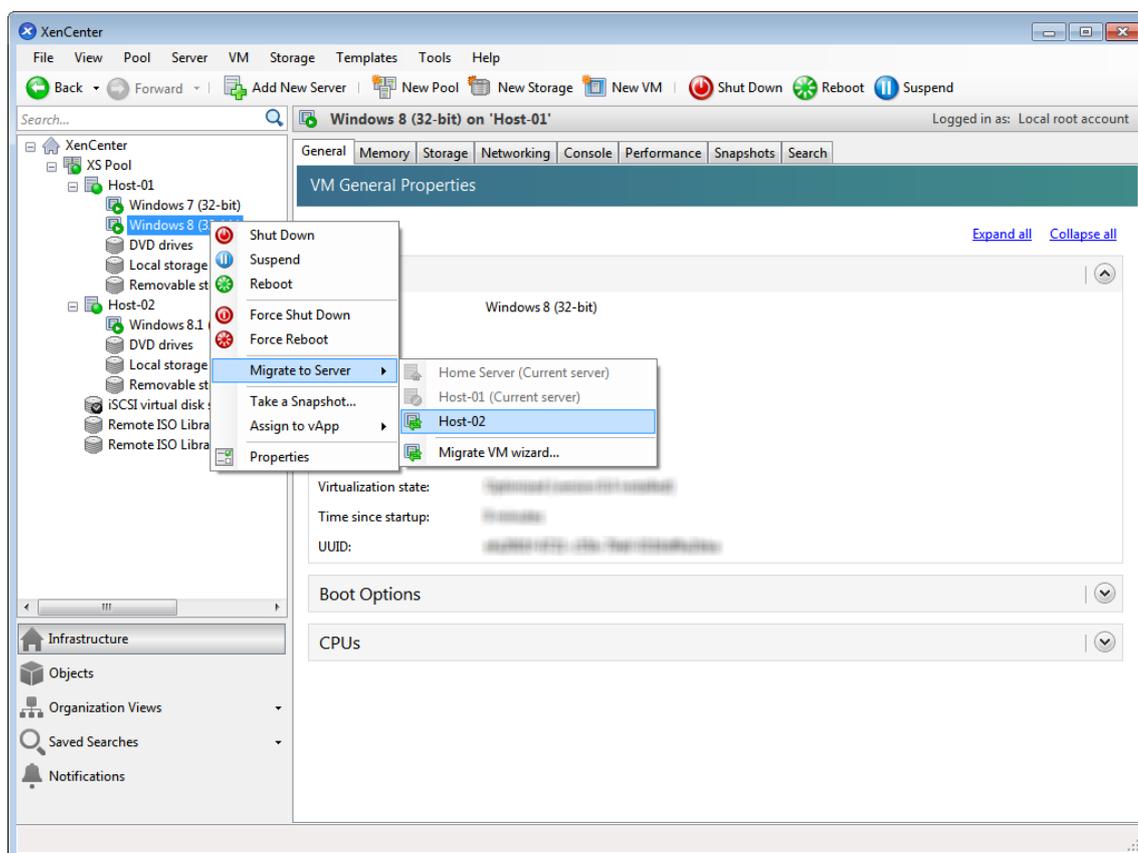
注:

その仮想マシンにローカルストレージが接続されていないことを確認してください。

2. 仮想マシンのアイコンを右クリックし、[移行先サーバー]、移行先のホスト名の順に選択します。

ヒント:

仮想マシンのアイコンを移行先ホストのアイコン上にドラッグすることもできます。



3. 移行処理が完了すると、リソースペインの移行先ホストにその仮想マシンが追加されます。

仮想マシンテンプレートの作成

既存の Windows 仮想マシンからテンプレートを作成するにはいくつかの方法があり、状況に応じて適した方法を選択できます。ここでは、既存の仮想マシンをテンプレートに変換する方法と、仮想マシンのスナップショットからテンプレートを作成する方法について説明します。これらの方法で作成するテンプレートには、元の仮想マシンやスナップショットでカスタマイズされた構成が保持されます。このテンプレートを使用して、同様の仮想マシンを簡単に作成することができます。ここでは、作成したテンプレートから新しい仮想マシンを作成する方法についても説明します。

既存の仮想マシンや仮想マシンスナップショットからテンプレートを作成する前に、元の仮想マシン上で Windows のユーティリティである **Sysprep** を実行しておくことをお勧めします。通常、ディスクイメージの複製（クローン）や復元の準備として **Sysprep** を実行します。Windows オペレーティングシステムには、インストール先に固有な情報（セキュリティ識別子やコンピューター名など）が多く含まれています。これらの情報は、複製した仮想マシンでも固有である必要があります。仮想マシン間でこれらの情報が重複すると、予期せぬ問題が発生することがあります。 **Sysprep** を実行すると、新しい仮想マシン上でこれらの情報が新しく生成されるため、この問題を避けることができます。

注:

小規模な環境やテスト環境では、 **Sysprep** の実行が不要である場合もあります。

Sysprep について詳しくは、Windows のドキュメントを参照してください。インストールされている Windows のバージョンによって、このユーティリティの使用方法が異なることがあります。

既存の仮想マシンから仮想マシンテンプレートを作成する

既存の仮想マシンから仮想マシンテンプレートを作成するには:

警告:

既存の仮想マシンからテンプレートを作成する場合、その仮想マシンはテンプレートに変換され、仮想マシンではなくなります。

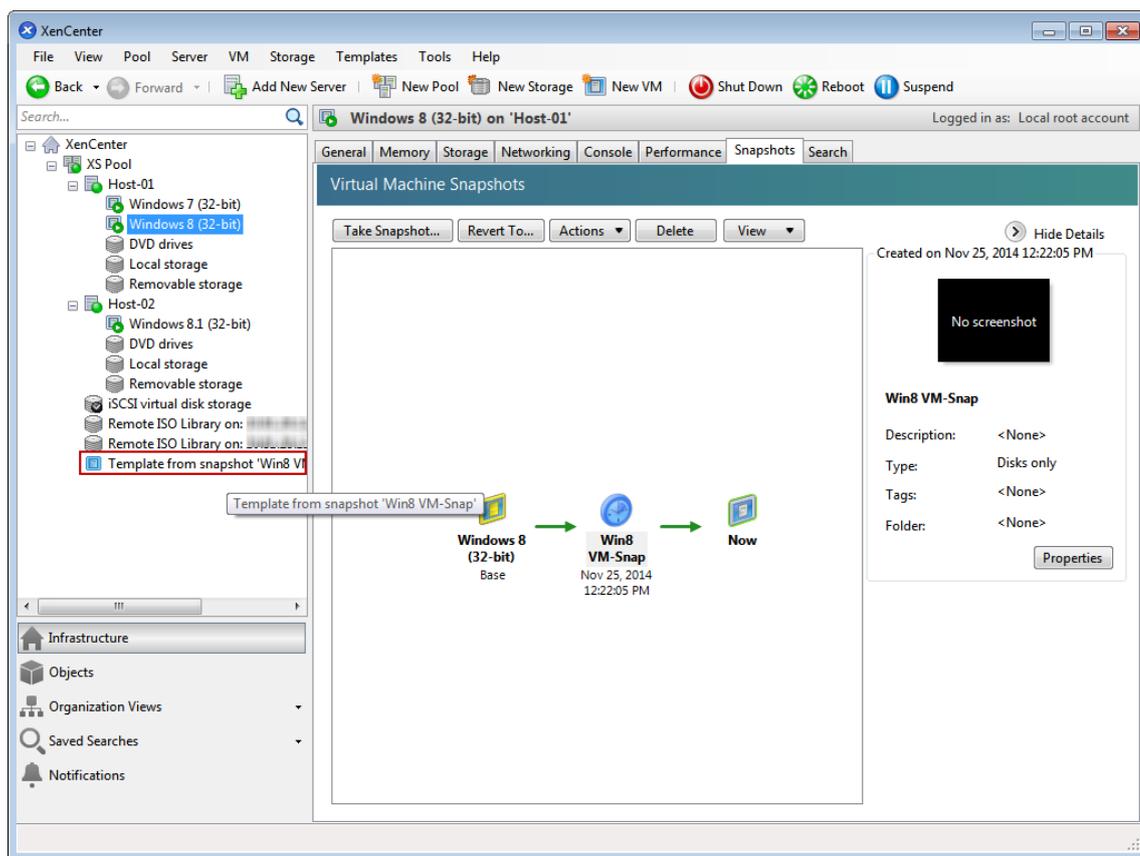
1. 変換する仮想マシンをシャットダウンします。
2. リソースペインで仮想マシンを右クリックして、[テンプレートへの変換] を選択します。
3. [変換] をクリックして確定します。

テンプレートが作成されると、リソースペインにそのテンプレートが追加され、元の仮想マシンが置き換わります。

仮想マシンのスナップショットから仮想マシンテンプレートを作成する

仮想マシンのスナップショットから仮想マシンテンプレートを作成するには:

1. リソースペインで仮想マシンを選択します。[スナップショット] タブをクリックし、[スナップショットの作成] をクリックします。
2. 新しいスナップショットの名前と、必要に応じて説明を入力します。[スナップショットの作成] をクリックします。
3. スナップショットが作成されると、[スナップショット] タブにそのスナップショットが追加されます。そのスナップショットのアイコンを選択します。



4. [操作] 一覧から、[スナップショットから新規テンプレート] を選択します。
5. テンプレートの名前を入力して、[作成] をクリックします。

仮想マシンテンプレートから仮想マシンを作成する

カスタマイズした仮想マシンテンプレートから仮想マシンを作成するには:

1. XenCenter リソースペインでテンプレートを右クリックして、[新規 VM] ウィザードを選択します。

[新規 VM] ウィザードが開きます。

2. [新規 VM] ウィザードの手順に従って、テンプレートから仮想マシンを作成します。

注:

オペレーティングシステムのインストールメディアの場所を指定するページでは、デフォルトのまま次のページに進みます。

仮想マシンが作成されると、リソースペインにその仮想マシンが追加されます。

既存の仮想マシンから作成したテンプレートでは、右クリックして [高速作成] を選択することもできます。このオプションでは、[新規 VM] ウィザードを使用せずに、テンプレートに保持されている構成で高速に仮想マシンが作成されます。

製品の技術概要

December 30, 2019

Citrix Hypervisor は、デスクトップ、サーバー、およびクラウドの仮想化インフラストラクチャをコスト効率よく実現するためのオープンソースプラットフォームとして、業界で高い評価を得ています。Citrix Hypervisor を使用すると、組織の規模や種類を問わず、コンピューティングリソースを集約して仮想ワークロードに変換することで今日のデータセンターの要件に対応しつつ、シームレスな方法でワークロードをクラウドに移行することができます。

Citrix Hypervisor の主な機能は次のとおりです：

- 物理サーバー上に複数の仮想マシン (VM) を集約できます。
- 管理すべきディスクイメージの数を削減できます。
- 既存のネットワークおよびストレージインフラストラクチャを容易に統合できます。
- 実行中の仮想マシンを Citrix Hypervisor ホスト間でライブマイグレーションして、ダウンタイムのない保守作業を行えます。
- 高可用性機能を使用して、障害発生時に、そのサーバー上の仮想マシンをほかのサーバー上で再起動するためのポリシーを設定できます。
- 幅広い仮想インフラストラクチャに対応する、汎用性の高い仮想マシンイメージを作成できます。

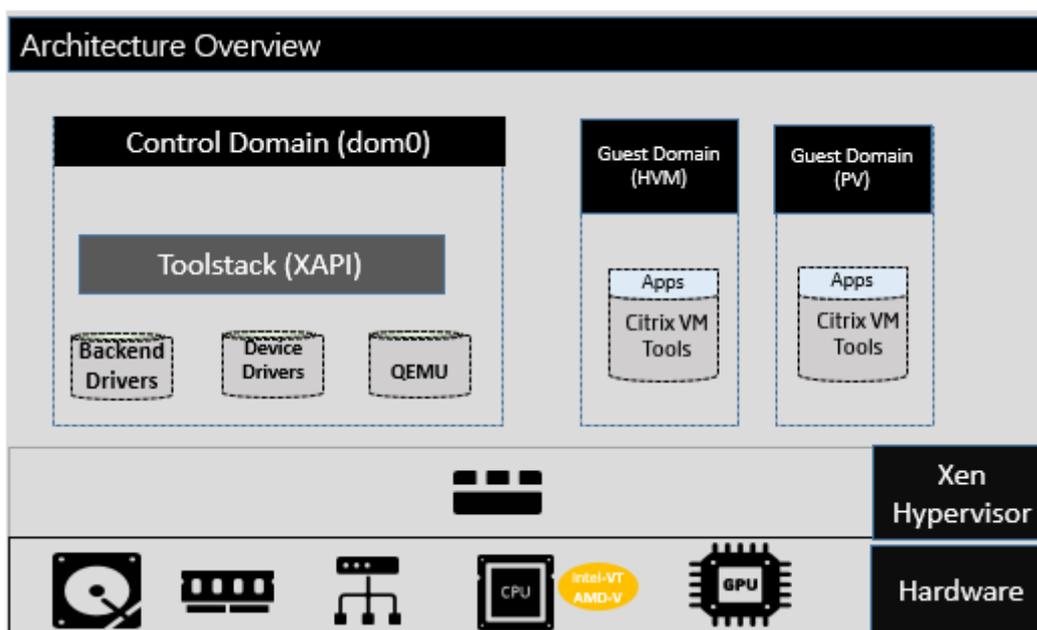
仮想化とハイパーバイザー

仮想化、つまりハードウェア仮想化は、単一の物理コンピュータ上で複数の仮想マシンを個別に実行する方法です。これらの仮想マシン上で実行されるソフトウェアは、基になるハードウェアリソースから分離されます。これによって最新の強力なサーバーで利用可能な物理リソースが最大限に活用されるため、サーバーの展開に必要な総所有コスト (TCO) を削減することができます。

ハイパーバイザーはソフトウェアの基本的な抽象化レイヤーで、CPU スケジューリングなどの下位レベルタスクや仮想マシンのメモリ分離などを行います。ハイパーバイザーは、ハードウェアの抽象化レイヤーを仮想マシンに提供し、ネットワーク、外部ストレージデバイス、ビデオなどの処理は行いません。

主要コンポーネント

ここでは、Citrix Hypervisor のしくみの概要を説明します。Citrix Hypervisor の以下の主要コンポーネントについては、次の図を参照してください：



ハードウェア

ハードウェアレイヤーには、CPU、メモリ、ネットワーク、およびディスクドライブなどの物理サーバーコンポーネントが含まれます。

サポートされているすべてのゲスト OS を実行するには、Intel VT または AMD-V をサポートする、64 ビット x86 ベースの CPU が 1 つまたは複数必要です。Citrix Hypervisor のホストシステム要件については、「システム要件」を参照してください。

Citrix Hypervisor の認定済みのハードウェアおよびシステムの完全な一覧については、「[ハードウェア互換性リスト \(英語\) \(HCL\)](#)」を参照してください。

Xen ハイパーバイザー

Xen Project ハイパーバイザーは、オープンソースのタイプ 1 またはベアメタルハイパーバイザーです。Xen ハイパーバイザーを使用すると、単一のオペレーティングシステムまたは異なるオペレーティングシステムの複数のインスタンスを、単一のコンピュータ (ホスト) 上で並行して実行できます。Xen ハイパーバイザーは、サーバー仮想化、IaaS (Infrastructure as a Service)、デスクトップ仮想化、セキュリティアプリケーション、埋め込み、およびハードウェアアプライアンスなど、さまざまな商用アプリケーションとオープンソースアプリケーションの基礎として使用されています。

Citrix Hypervisor は Xen Project ハイパーバイザーをベースに、Citrix が提供する機能やサポートが追加されています。Citrix Hypervisor 8.1 では、Xen ハイパーバイザーのバージョン 4.13 が使用されます。

コントロールドメイン

コントロールドメインは「Domain0」または「dom0」とも呼ばれ、Citrix Hypervisor の管理ツールスタック (「XAPI」 とも呼ばれます) を実行するセキュアな特権 Linux 仮想マシンです。この Linux 仮想マシンは、CentOS 7.5 ディストリビューションに基づいています。コントロールドメインは、Citrix Hypervisor 管理機能を提供するほか、ネットワークやストレージなどのための物理デバイスドライバーも実行します。コントロールドメインは、ハイパーバイザーと通信して、ゲスト仮想マシンを起動または停止するよう指示できます。

ツールスタック

ツールスタック (「XAPI」 とも呼ばれます) は、仮想マシンのライフサイクル操作、ホストおよび仮想マシンのネットワーク、仮想マシンストレージ、およびユーザー認証を制御するソフトウェアスタックです。また、Citrix Hypervisor リソースプールを管理することもできます。

XAPI により提供される管理 API についてはドキュメントが公開されており、このインターフェイスは仮想マシンやリソースプールを管理するためのすべてのツールで使用されます。詳しくは、「<https://developer-docs.citrix.com>」を参照してください。

ゲストドメイン (VM)

ゲストドメインは、dom0 のリソースを要求する、ユーザーが作成した仮想マシンです。Citrix Hypervisor のゲストドメインでは、完全な仮想化 (HVM) およびハードウェア仮想マシン上の準仮想化 (PV on HVM) がサポートされています。サポートされているディストリビューションの詳細な一覧については、「[サポートされるゲストオペレーティングシステム、仮想メモリ、および仮想ディスクのサイズ制限](#)」を参照してください。

完全な仮想化

完全な仮想化 (「ハードウェア支援による仮想化」 とも呼ばれます) では、ホスト CPU の仮想化拡張機能を使用してゲストを仮想化します。完全に仮想化されたゲストでは、カーネルのサポートが不要になります。このようなゲストはハードウェア仮想マシン (HVM) と呼ばれます。HVM では、メモリおよび権限のある操作のために Intel VT または AMD-V のハードウェア拡張機能が必要です。Citrix Hypervisor は Quick Emulator (QEMU) を使用して、BIOS、IDE ディスクコントローラ、VGA グラフィックアダプター、USB コントローラ、ネットワークアダプターなどの PC ハードウェアをエミュレートします。ディスクやネットワークへのアクセスなど、ハードウェアが重要となる操作のパフォーマンスを向上させるために、HVM ゲストには Citrix Hypervisor ツールがインストールされています。詳しくは、「ハードウェア仮想マシン上の準仮想化 (PV on HVM)」を参照してください。

通常、HVM は、カーネルを変更して仮想化が認識されるようにすることが不可能な、Microsoft Windows などのオペレーティングシステムを仮想化する場合に使用します。

ハードウェア仮想マシン上の準仮想化 (PV on HVM)

ハードウェア仮想マシン上の準仮想化 (PV on HVM) には、準仮想化と完全なハードウェア仮想化が混在しており、特に最適化された準仮想化ドライバーを使用して、HVM ゲストのパフォーマンスを向上させることを主な目的とします。このモードでは、最新プロセッサの x86 仮想コンテナ技術により良好なパフォーマンスが得られます。ただし、これらのゲストでのネットワークアクセスおよびストレージアクセスは、カーネルに組み込まれたドライバーにより PV モードで行われます。

Citrix Hypervisor の PV on HVM モードでは、Windows ディストリビューションおよび一部の Linux ディストリビューションを使用できます。PV on HVM を使用するサポート対象 Linux ディストリビューションの一覧については、「[HVM Linux ディストリビューション](#)」を参照してください。

Citrix VM Tools

Citrix VM Tools (ゲストツールともいいます) には従来型デバイスエミュレーションのようなオーバーヘッドがなく、高パフォーマンスの I/O サービスが提供されます。Citrix VM Tools は、I/O ドライバー (準仮想化ドライバーまたは PV ドライバーともいいます) と管理エージェントで構成されています。

I/O ドライバーにはフロントエンドストレージ、ネットワークドライバー、および低レベル管理インターフェイスが含まれています。準仮想化ドライバーは、エミュレートされたドライバーに置き換わり、仮想マシンと Citrix Hypervisor ソフトウェア間的高速トランスポートを提供します。

管理エージェント (ゲストエージェントともいいます) は、高レベルの仮想マシン管理機能を備えており、すべての機能を XenCenter (Windows 仮想マシンの場合) に提供します。

注:

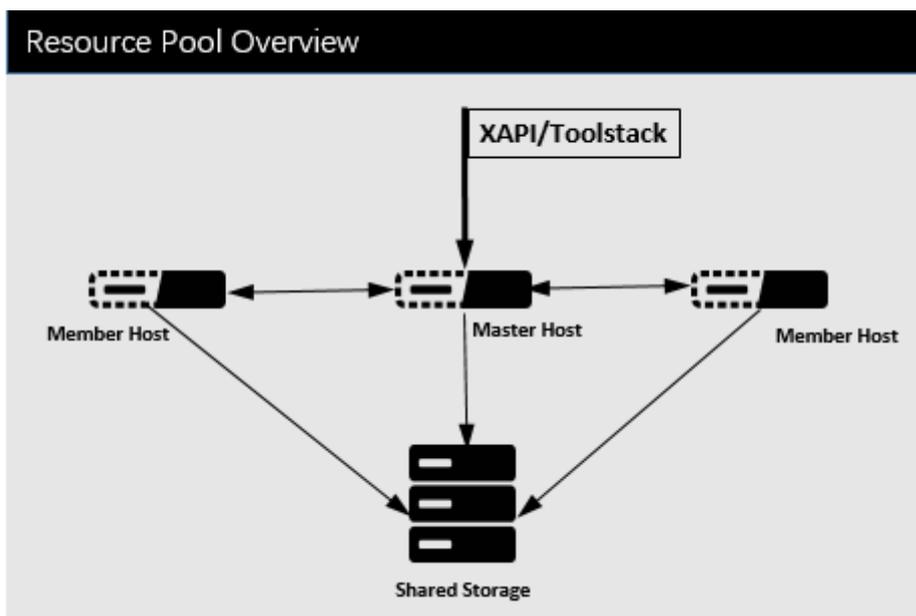
- 仮想マシンが完全にサポートされる構成にするには、各 Windows 仮想マシンに Citrix VM Tools をインストールする必要があります。仮想マシンは、Citrix VM Tools がなくても機能しますが、I/O ドライバー (PV ドライバー) がインストールされていないと、パフォーマンスが大幅に低下します。
- Windows 仮想マシンの場合、Citrix VM Tools は Windows ゲストツールと呼ばれ、Windows PV ドライバーと管理エージェントが含まれています。
- Linux 仮想マシンの場合、PV ドライバーは Xen カーネルに含まれています。

詳しくは、「[Citrix VM Tools](#)」を参照してください。

主な概念

リソースプール

Citrix Hypervisor リソースプールを使用すると、複数のサーバーとそれらの共有ストレージを単一のエンティティとして管理できます。リソースプールを使用すると、仮想マシンを別の Citrix Hypervisor ホストに移動して実行できるほか、すべてのサーバーがネットワークとストレージの共通フレームワークを共有できるようになります。1つのプールには、互換性のあるハードウェアを持ち、同じバージョンの Citrix Hypervisor ソフトウェア (適用されたパッチも含む) を実行するサーバーを最大で 64 台まで追加できます。詳しくは、「[ホストとリソースプール](#)」を参照してください。



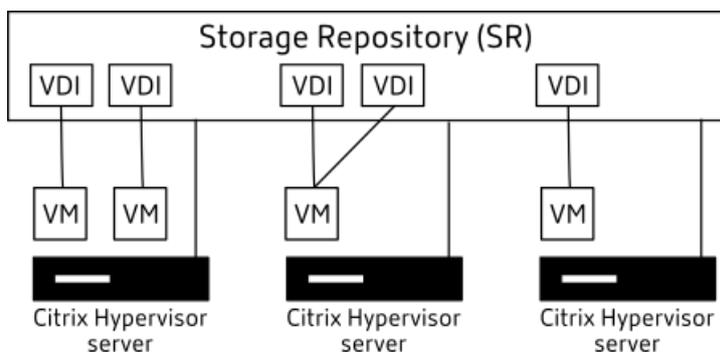
Citrix Hypervisor リソースプールには、XAPI によって実装されるマスタ/スレーブアーキテクチャが採用されています。プールマスタからプールメンバーに XAPI コールが転送され、プールメンバーはプールマスタに対して DB リモートプロシージャコール (RPC) を行います。プールマスタは、プール内のリソースの統合とロックを行い、すべての制御操作を処理します。メンバーホストは、HTTP と XMLRPC を通じてプールマスタと通信しますが、(同じチャネルを介して) 相互に通信し、次のことを実行できます：

- VM メモリイメージの転送 (VM の移行)
- ディスクのミラーリング (ストレージの移行)

ストレージリポジトリ

Citrix Hypervisor ストレージ対象は、ストレージリポジトリ (SR) と呼ばれます。ストレージリポジトリには、仮想ディスクの内容を含む仮想ディスクイメージ (VDI) が格納されます。

ローカル接続の IDE、SATA、SCSI、および SAS ドライブ、そしてリモート接続の iSCSI、NFS、SAS、およびファイバチャネルに対するサポートが組み込まれているため、目的に応じたさまざまなストレージリポジトリをホストで使用できます。ストレージリポジトリと VDI の抽象化によって、シンプロビジョニング、VDI スナップショット、高速複製などの高度なストレージ機能を、サポートされているストレージターゲット上で提供できるようになります。



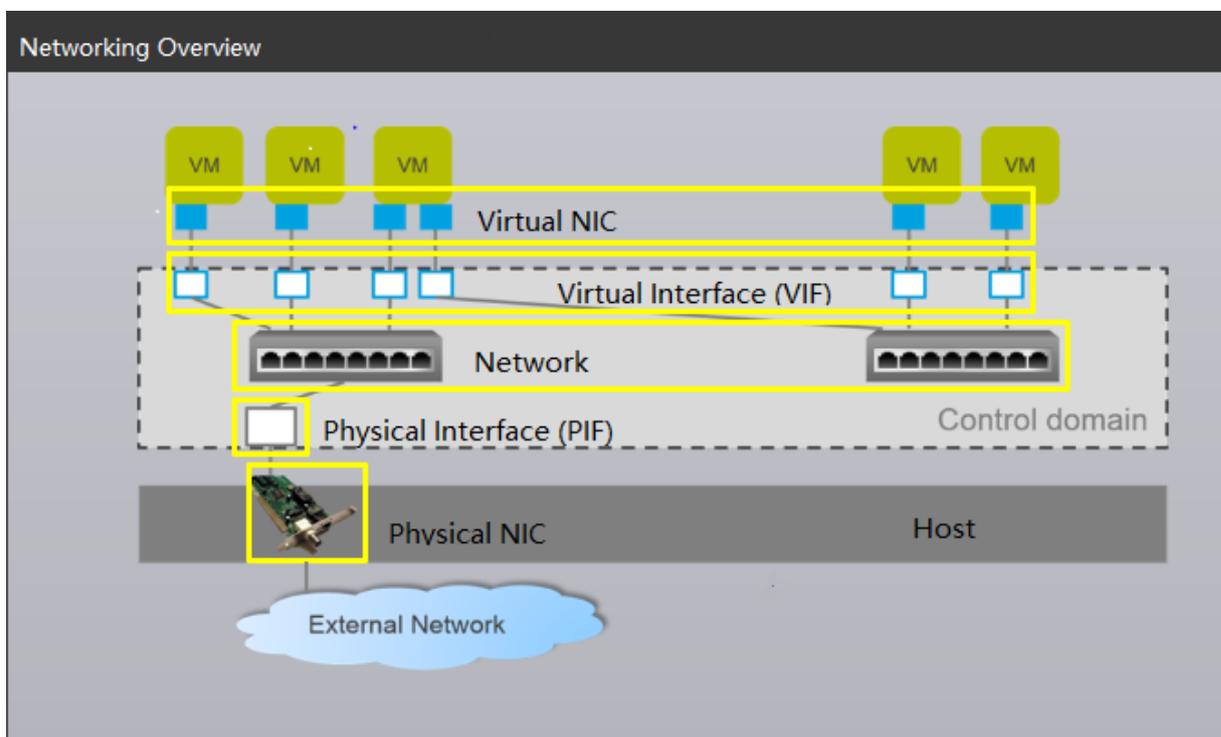
各 Citrix Hypervisor ホストでは、複数の異なる種類のストレージリポジトリを同時に使用することができます。これらのストレージリポジトリは、ホスト間で共有したり、特定のホスト専用にしてもできます。共有ストレージは、定義済みのリソースプール内の複数のホスト間でプール（共有）されます。共有されたストレージリポジトリは、プールの各ホストとネットワークで接続されている必要があります。リソースプールでは、すべてのホストが少なくとも1つの共有ストレージリポジトリを使用している必要があります。共有ストレージを複数のプール間で共有することはできません。

ストレージリポジトリの操作方法については、「[ストレージの構成](#)」を参照してください。

ネットワーク

アーキテクチャレベルでは、ネットワークエンティティを表す3つの種類のサーバー側ソフトウェアオブジェクトがあります。以下のオブジェクトを使用します。

- **PIF** (Physical Interface) は、dom0 内で使用されるソフトウェアオブジェクトであり、ホスト上の物理インターフェイスを表します。PIF オブジェクトは、名前と説明、UUID、対応する NIC のパラメータ、および接続先のネットワークとサーバーという属性を持ちます。
- **VIF** (Virtual Interface) は、dom0 内で使用されるソフトウェアオブジェクトであり、仮想マシン上の仮想インターフェイスを表します。VIF オブジェクトは、名前と説明、UUID、および接続先のネットワークと仮想マシンという属性を持ちます。
- ネットワークは、ネットワークホスト上のネットワークトラフィックをルーティングするために使用されるホストの仮想イーサネットスイッチです。ネットワークオブジェクトは、名前と説明、UUID、および接続先の VIF と PIF の集合という属性を持ちます。



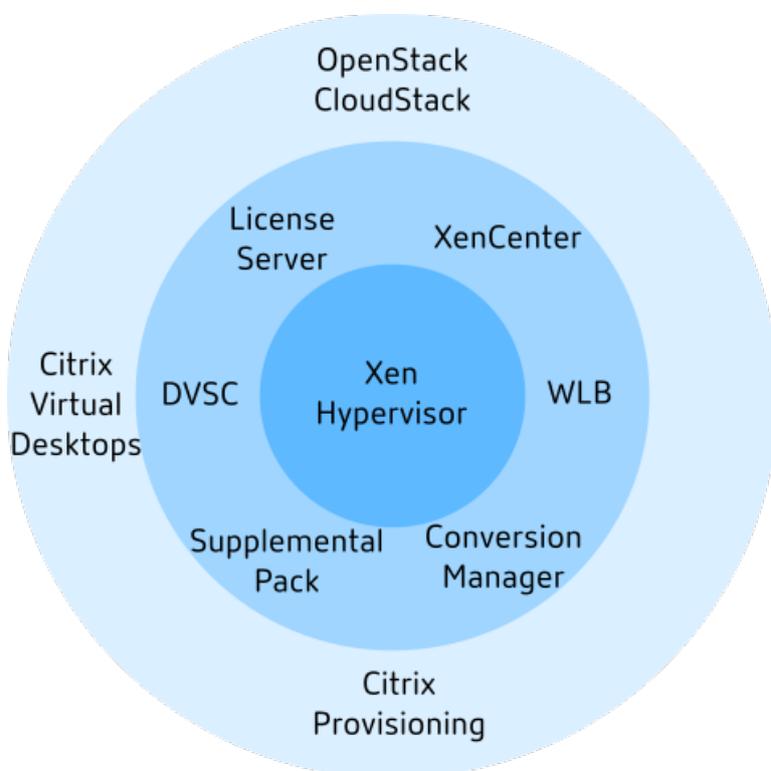
Citrix Hypervisor 管理 API では、以下の操作が可能になります：

- ネットワークオプションの設定
- 管理操作に使用する NIC の制御
- VLAN や NIC ボンディングなどの高度なネットワーク機能の作成

XenServer でネットワークを管理する方法については、「[ネットワーク](#)」を参照してください。

関連アドオンおよびアプリケーション

Xen ハイパーバイザーはコアレベルで動作しますが、Citrix Hypervisor ではアドオンに関連した、ハイパーバイザーに依存しないアプリケーションとサービスが提供されるため、仮想化エクスペリエンスを完成させることができます。



- **XenCenter**

仮想マシン管理用の Windows GUI クライアント。管理 API に基づいて実装されます。XenCenter は、複数の Citrix Hypervisor ホスト、リソースプール、およびこれらに関連付けられた仮想インフラストラクチャ全体を管理するための、快適な操作性をユーザーに提供します。

- **ワークロードバランス (WLB)**

ワークロードバランスは、リソースプール内の最適なサーバーに仮想マシンを移行することでプールのワークロードを分散させるための機能で、ワークロードバランス仮想アプライアンスにより提供されます。詳しく

は、「ワークロードバランス」(</ja-jp/citrix-hypervisor/vswitch-controller.html>) を参照してください。

- **分散仮想スイッチコントローラー (DVSC)**

XAPI に対応した OpenFlow 規則を作成するために使用する Debian ベースのアプライアンス。この実装は以下によって構成されます:

- 各 Citrix Hypervisor および vSwitch Controller 上で動作する、仮想化に対応したスイッチ (vSwitch)。
- 単一の vSwitch の外観を実現するために、個々の vSwitch の動作を管理および調整する集中管理型サーバー。

詳しくは、「[vSwitch と Controller](#)」を参照してください。

- **Citrix ライセンスサーバー**

特定のサーバーのライセンスを要求するために XenCenter が接続する Linux ベースのアプライアンス。

- **Citrix Hypervisor Conversion Manager (XCM)**

既存の VMware 仮想マシンを同等のネットワークおよびストレージ接続を備えた Citrix Hypervisor 仮想マシンに変換できるコンソール付きの仮想アプライアンス。詳しくは、「[Conversion Manager](#)」を参照してください。

- **メジャーブートのサプリメンタルパック**

ブート時に Citrix Hypervisor ホストの主要コンポーネントを測定し、リモート構成証明ソリューションを通じてこれらの測定値を安全に収集することを可能にする API を提供します。詳しくは、「[メジャーブートのサプリメンタルパック](#)」を参照してください。

- **Citrix Provisioning**

共通イメージからの PXE ブートをサポートするプロビジョニングサービス。Citrix Virtual Desktops および Citrix Virtual Apps で広く使用されています。詳しくは、「[プロビジョニング](#)」を参照してください。

- **Citrix Virtual Desktops**

Windows デスクトップに特化した仮想デスクトップインフラストラクチャ (VDI) 製品。Citrix Virtual Desktops では、XAPI を使用して、プール内に複数のホストが含まれる構成の Citrix Hypervisor を管理します。詳しくは、「[Citrix Virtual Apps and Desktops](#)」を参照してください。

- **OpenStack/CloudStack**

パブリック/プライベートクラウドを構築するためのオープンソースソフトウェア。管理 API を使用して XenServer を制御します。詳しくは、<https://www.openstack.org/> および <https://cloudstack.apache.org/> を参照してください。

技術面でのよくある質問

March 12, 2020

ハードウェア

Citrix Hypervisor を実行するための最小システム要件は何ですか？

このリリースの最小システム要件については、「[システム要件](#)」を参照してください。

Citrix Hypervisor の実行には、64 ビット x86 プロセッサを搭載したシステムが必要ですか？

はい。すべての[サポートされるゲストオペレーティングシステム](#)を実行するには、1 つまたは複数の CPU が搭載された、Intel VT または AMD-V のいずれかの 64 ビット x86 ベースのシステムが必要です。

ホストシステム要件について詳しくは、「[システム要件](#)」を参照してください。

ハードウェア仮想化をサポートするシステムは必要ですか？

Windows オペレーティングシステムまたは HVM Linux ゲストを実行するには、プロセッサと BIOS で、Intel VT または AMD-V のいずれかのハードウェア仮想化技術をサポートする 64 ビット x86 プロセッサベースのシステムが必要です。

HVM Linux ゲストについて詳しくは、「[Linux 仮想マシン](#)」を参照してください。

Citrix Hypervisor 実行の認定を受けているシステムは何ですか？

Citrix Hypervisor の認定済みシステムの全一覧については、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) を参照してください。

Citrix Hypervisor は、AMD Rapid Virtualization Indexing と Intel 拡張ページテーブルをサポートしていますか？

はい。Citrix Hypervisor は、AMD Rapid Virtualization Indexing と Intel 拡張ページテーブルをサポートしています。Rapid Virtualization Indexing では、ネストされたテーブルテクノロジーを実装することで、Xen ハイパーバイザーのパフォーマンスがさらに強化されます。拡張ページテーブルでは、ハードウェア支援のページングを実装することで、Xen ハイパーバイザーのパフォーマンスがさらに強化されます。

Citrix Hypervisor は、ノートブックまたはデスクトップクラスのシステムで実行できますか？

Citrix Hypervisor は、最小 CPU 要件に準拠しているノートブックまたはデスクトップクラスのシステムの多くで動作します。ただし、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) に記載されている、認定済みのシステムのみがサポートされます。デモやテストの目的でサポート対象外のシステム上で実行することもできますが、電源管理などの一部の機能は動作しません。

製品の制限

注:

Citrix Hypervisor でサポートされている制限の全一覧については、「[構成の制限](#)」を参照してください。

Citrix Hypervisor がホストシステムで使用できるメモリの最大サイズはどれくらいですか？

Citrix Hypervisor のホストシステムは、最大 5TB の物理メモリを使用できます。

Citrix Hypervisor で使用できるプロセッサの数はいくつですか？

Citrix Hypervisor では、ホストあたり最大 288 基の論理プロセッサがサポートされます。サポートされる論理プロセッサの最大数は、CPU によって異なります。

詳しくは、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) を参照してください。

Citrix Hypervisor では、何台の仮想マシンを同時に実行できますか？

Citrix Hypervisor のホストで実行できる仮想マシン (VM) の数は、最大で 1000 台です。500 台を超える VM を実行するシステムの場合、Dom0 に 8GB の RAM を割り当てることをお勧めします。Dom0 のメモリ量の設定について詳しくは、「[CTX134951 - How to Configure dom0 Memory in XenServer 6.2 and Later](#)」を参照してください。

特定のシステムでは、同時に、かつ許容できるパフォーマンスで実行できる仮想マシンの数は、利用可能なリソースと仮想マシンのワークロードによって異なります。Citrix Hypervisor では、利用可能な物理メモリに基づいて、コントロールドメイン (Dom0) に割り当てられたメモリ量を自動的にスケーリングします。

注:

ホストあたりの VM の数が 50 台を超えていて、かつホストの物理メモリが 48GB 未満の場合は、この設定を上書きすることをお勧めします。詳しくは、「[メモリ使用率](#)」を参照してください。

Citrix Hypervisor でサポートされる物理ネットワークインターフェイスの数はいくつですか？

Citrix Hypervisor では、最大 16 個の物理 NIC ポートがサポートされます。これらの NIC をボンディングして、最大 8 個の論理ネットワークボンドを作成できます。各ボンディングには、NIC を最大 4 つ含めることができます。

Citrix Hypervisor で、仮想マシンに割り当てることができる仮想プロセッサ (vCPU) の数はいくつですか？

Citrix Hypervisor では、仮想マシンあたり最大 32 基の vCPU がサポートされます。サポートできる vCPU の数は、ゲスト OS によって異なります。

注:

ゲスト OS のドキュメントを参照して、サポートされている制限値を超えていないかご確認ください。

Citrix Hypervisor で、仮想マシンに割り当てることができるメモリの量はいくつですか？

Citrix Hypervisor では、ゲストあたり最大 1.5TB がサポートされます。サポートできるメモリ容量は、ゲスト OS によって異なります。

注:

使用可能な物理メモリの最大量は、お使いのオペレーティングシステムによって異なります。オペレーティングシステムがサポートするメモリ量の上限を超えると、その仮想マシンでパフォーマンスの問題が発生する場合があります。一部の 32 ビット版 Windows では、物理アドレス拡張 (PAE: Physical Address Extension) モードを使用することで 4GB を超える RAM がサポートされます。詳しくは、ゲストオペレーティングシステムのドキュメントおよび「[サポートされるゲストオペレーティングシステム](#)」を参照してください。

Citrix Hypervisor で、仮想マシンに割り当てることができる仮想ディスクイメージ (VDI) の数はいくつですか？

Citrix Hypervisor では、仮想マシンあたり、仮想 DVD-ROM デバイス 1 台を含む、最大 255 個の VDI を割り当てることができます。

注:

サポートされる VDI の最大数は、ゲストオペレーティングシステムによって異なります。ゲスト OS のドキュメントを参照して、サポートされている制限値を超えていないかご確認ください。

Citrix Hypervisor で、仮想マシンに割り当てることができる仮想ネットワークインターフェイスの数はいくつですか？

Citrix Hypervisor では、仮想マシンあたり最大 7 個の仮想 NIC を割り当てることができます。サポートできる仮想 NIC の数は、ゲスト OS によって異なります。

リソースの共有

処理リソースは仮想マシン間でどのように分割されますか？

Citrix Hypervisor では、処理リソースは、公平分散アルゴリズムを使用して vCPU 間で分割されます。このアルゴリズムによって、すべての仮想マシンが、それぞれの分のシステムの処理リソースを取得することができます。

Citrix Hypervisor では、仮想マシンに割り当てる物理プロセッサはどのように選択されますか？

Citrix Hypervisor では、特定の仮想マシンに物理プロセッサが静的に割り当てられることはありません。代わりに、Citrix Hypervisor では、負荷に応じて、利用可能な論理プロセッサが動的に仮想マシンに割り当てられます。この動的な割り当てにより、空き容量があればどこでも仮想マシンを実行できるため、プロセッササイクルを効率的に使用することができます。

ディスク I/O リソースは仮想マシン間でどのように分割されますか？

Citrix Hypervisor では、仮想マシン間のディスク I/O リソースには、公平なリソース分割を使用します。また、ディスク I/O リソースへの優先度の高いアクセスまたは低いアクセスを、仮想マシンに提供することもできます。

ネットワーク I/O リソースは仮想マシン間でどのように分割されますか？

Citrix Hypervisor では、仮想マシン間のネットワーク I/O リソースには、公平なリソース分割を使用します。また、Open vSwitch を使用して、仮想マシンごとの帯域幅調整の制限を制御することもできます。

ゲストオペレーティングシステム

Citrix Hypervisor では、**32** ビットのオペレーティングシステムをゲストとして実行できますか？

はい。詳しくは、「[サポートされるゲストオペレーティングシステム](#)」を参照してください。

Citrix Hypervisor では、**64** ビットのオペレーティングシステムをゲストとして実行できますか？

はい。詳しくは、「[サポートされるゲストオペレーティングシステム](#)」を参照してください。

Citrix Hypervisor で、ゲストとして実行できる **Microsoft Windows** のバージョンはどれですか？

サポートされる Windows ゲストオペレーティングシステムの一覧については、「[サポートされるゲストオペレーティングシステム](#)」を参照してください。

Citrix Hypervisor で、ゲストとして実行できる Linux のバージョンはどれですか？

サポートされる Linux ゲストオペレーティングシステムの一覧については、「[サポートされるゲストオペレーティングシステム](#)」を参照してください。

サポートされているオペレーティングシステムの別のバージョンや、リストに記載されていないオペレーティングシステムは実行できますか？

シトリックスでは、OS のベンダーサポート対象のオペレーティングシステム (OS) のみがサポートされます。サポートされていないオペレーティングシステムでも引き続き動作する可能性はありますが、問題を調査するにあたって、サポート対象のオペレーションシステムサービスパックへのアップグレードをお願いする場合があります。

サポートされていないオペレーションシステムバージョンでは、使用できるドライバーがない場合があります。ドライバーがないと、これらのオペレーションシステムバージョンは最適化されたパフォーマンスで機能しません。

多くの場合、Linux のその他のディストリビューションをインストールすることもできます。しかし、「[サポートされるゲストオペレーティングシステム](#)」に記載されているオペレーティングシステムのみがサポートされます。問題を調査する前に、サポートされているオペレーティングシステムに切り替えるようお願いする場合があります。

Citrix Hypervisor では、ゲストオペレーティングシステムとして、**FreeBSD** や **NetBSD** などの **BSD** をサポートしていますか？

Citrix Hypervisor では、汎用の仮想化環境に、BSD ベースのゲストオペレーティングシステムはサポートしていません。ただし、Citrix Hypervisor 上で実行されている FreeBSD 仮想マシンは、特定のシトリックス製品での使用が認定されています。

Citrix VM Tools とは何ですか？

Citrix VM Tools は、Windows および Linux ベースのゲストオペレーティングシステム用のソフトウェアパッケージです。Windows オペレーティングシステムの場合、Citrix VM Tools には、高性能 I/O ドライバー (PV ドライバー) と管理エージェントが含まれます。Linux ベースのオペレーティングシステムの場合、Citrix VM Tools には、仮想マシンに関する追加情報を Citrix Hypervisor ホストに提供するゲストエージェントが含まれます。詳しくは、「[Citrix VM Tools](#)」を参照してください。

XenCenter

XenCenter は、**Windows** コンピューターで実行しなければならないのですか？

はい。XenCenter の管理コンソールは、Windows オペレーティングシステム上で実行されます。システム要件については、「[システム要件](#)」を参照してください。

Windows を実行しない場合は、xe CLI を使用するか、システム構成コンソールの xsconsole を使用して、Citrix Hypervisor のホストとプールを管理することができます。

Active Directory のユーザーアカウントを使用して、**XenCenter** にログオンできますか？

はい。Citrix Hypervisor のすべてのエディションで、Active Directory を使用するように XenCenter のログイン要求を設定できます。

特定のユーザーに対して、**XenCenter** の特定の機能へのアクセスを制限できますか？

はい。役割ベースのアクセス制御機能と Active Directory 認証を組み合わせることで、XenCenter でのユーザーのアクセスを制限できます。

1 つの **XenCenter** コンソールで複数の **Citrix Hypervisor** ホストに接続することはできますか？

はい。1 つの XenCenter コンソールで、複数の Citrix Hypervisor ホストシステムに接続することができます。

XenCenter を使用して、異なるバージョンの **Citrix Hypervisor** を実行する複数のホストに接続することはできますか？

はい。XenCenter は、現在サポートされている、異なるバージョンの Citrix Hypervisor を実行している複数のホストシステムと下位互換性があります。

XenCenter を使用して、複数のリソースプールに接続することはできますか？

はい。1 つの XenCenter コンソールから、複数のリソースプールに接続することができます。

どうすれば **Linux** ベースの仮想マシンのコンソールにアクセスできますか？

XenCenter の [コンソール] タブから、Linux ベースのオペレーティングシステムを実行する仮想マシンの、テキストベースのグラフィックコンソールにアクセスできます。Linux 仮想マシンのグラフィックコンソールに接続できるようにするには、VNC サーバーと X ディスプレイマネージャーを仮想マシンにインストールして、適切に設定しておく必要があります。

また、XenCenter では、仮想マシンの [コンソール] タブの [SSH コンソールを開く] オプションを使用して、SSH 経由で Linux 仮想マシンに接続することもできます。

どうすれば **Windows** ベースの仮想マシンのコンソールにアクセスできますか？

XenCenter では、Windows 仮想マシンのエミュレートされたグラフィックにアクセスすることができます。XenCenter が仮想マシンでリモートデスクトップ機能を検出すると、XenCenter がクイック接続ボタンを表示し、組み込みの RDP クライアントが起動します。このクライアントが仮想マシンに接続します。または、外部のリモートデスクトップソフトウェアを使用して、ゲストに直接接続することもできます。

コマンドラインインターフェイス (CLI)

Citrix Hypervisor に CLI は含まれていますか？

はい。Citrix Hypervisor のすべてのエディションに、**xe**と呼ばれる、コマンドラインインターフェイス (CLI) が含まれています。

Citrix Hypervisor CLI には、ホスト上で直接アクセスできますか？

はい。CLI にアクセスするには、ホストに直接接続された画面とキーボードを使用するか、ホストのシリアルポートに接続された端末エミュレーターを使用します。

リモートシステムから **Citrix Hypervisor CLI** にアクセスできますか？

はい。シトリックスには **xe CLI** が付属しています。この CLI を Windows および 64 ビットの Linux マシンにインストールすることで、Citrix Hypervisor をリモートで制御できます。XenCenter を使用して [コンソール] タブからホストのコンソールにアクセスすることもできます。

Active Directory のユーザーアカウントで **Citrix Hypervisor CLI** を使用することはできますか？

はい。Citrix Hypervisor のすべてのエディションで、Active Directory を使用してログインすることができます。

特定の **CLI** コマンドの使用権限を特定のユーザーに制限できますか？

はい。Citrix Hypervisor CLI で、ユーザーアクセスを制限することができます。

仮想マシン

VMware または **Hyper-V** で作成された仮想マシンは、**Citrix Hypervisor** 上で実行できますか？

はい。業界標準の OVF 形式を使用して、仮想マシンのエクスポートおよびインポートができます。

また、Citrix Hypervisor Conversion Manager 使用して仮想マシンをバッチで変換することもできます。サードパーティ製のツールも利用できます。詳しくは、「[Conversion Manager](#)」を参照してください。

ゲストオペレーティングシステムのインストールには、どのようなインストールメディアを使用できますか？

ゲストオペレーティングシステムは、次の方法でインストールできます：

- ホストの CD-ROM ドライブ内の CD
- iLO や DRAC などの技術を使用した仮想 CD-ROM ドライブ
- 共有ネットワークドライブへの ISO イメージの配置
- 特定のゲストがサポートするネットワークインストール。

詳しくは、「[仮想マシンの管理](#)」を参照してください。

既存の仮想マシンのクローンを作成することはできますか？

はい。Citrix Hypervisor で作成された仮想マシンはすべて、クローン、または VM テンプレートに変換できます。その後、VM テンプレートを使用して仮想マシンをさらに作成することができます。

仮想マシンは、あるバージョンの **Citrix Hypervisor** からエクスポートして、別のバージョンに移動できますか？

はい。古いバージョンの Citrix Hypervisor からエクスポートされた仮想マシンは、新しいバージョンにインポートできます。

オープンソース版の **Xen** から **Citrix Hypervisor** に仮想マシンを変換することはできますか？

いいえ。

Citrix Hypervisor には、仮想マシンのディスクスナップショット機能はありますか？

はい。Citrix Hypervisor では、すべてのエディションでスナップショットがサポートされています。詳しくは、「[仮想マシンスナップショット](#)」を参照してください。

ストレージ

Citrix Hypervisor では、どのようなローカルストレージが使用できますか？

Citrix Hypervisor では、SATA や SAS などのローカルストレージをサポートしています。

Citrix Hypervisor では、どのような **SAN/NAS** ストレージが使用できますか？

Citrix Hypervisor では、ファイバチャネル、FCoE、ハードウェアベースの iSCSI (HBA)、iSCSI、NFS、SMB のストレージリポジトリがサポートされます。詳しくは、「[ストレージ](#)」および「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。

Citrix Hypervisor では、ソフトウェアベースの **iSCSI** はサポートされますか？

はい。Citrix Hypervisor には、ソフトウェアベースの iSCSI イニシエーター (オープン iSCSI) が組み込まれています。

リモートストレージの使用に必要な **NFS** のバージョンを教えてください？

Citrix Hypervisor でリモートストレージを使用するには、NFSv3 over TCP または NFSv4 over TCP が必要です。現在、Citrix Hypervisor では、NFS over UDP (ユーザーデータグラムプロトコル) はサポートしていません。

リモート共有ストレージの汎用サーバーを実行するソフトウェアベースの **NFS** を使用することはできますか？

はい。ただし、許容可能なレベルの I/O パフォーマンスを達成するため、NFSv3 または NFSv4 を備えた専用 NAS デバイスを、高速の不揮発性キャッシングで使用することを推奨しています。

iSCSI、ファイバチャネル、または **FCoE** の **SAN** から、**Citrix Hypervisor** ホストシステムを起動できますか？

はい。Citrix Hypervisor は、ファイバチャネル、HBA、FCoE、HBA、および iSCSI HBA を使用した SAN からの起動をサポートしています。

UEFI を使用して **Citrix Hypervisor** ホストを起動できますか？

はい。Citrix Hypervisor は、BIOS および UEFI からの起動をサポートしています。

Citrix Hypervisor では、ストレージ接続にマルチパス **I/O (MPIO)** をサポートしていますか？

はい。シトリックスでは耐障害性のあるストレージ接続にマルチパスを使用することを推奨しています。

Citrix Hypervisor では、ソフトウェアベースの **RAID** 実装をサポートしていますか？

いいえ。Citrix Hypervisor では、ソフトウェア RAID はサポートしていません。

Citrix Hypervisor では、**HostRAID** または **FakeRAID** のソリューションはサポートしていますか？

いいえ。Citrix Hypervisor では、HostRAID や FakeRAID などの、独自の RAID のようなソリューションはサポートしていません。

Citrix Hypervisor では、既存の仮想マシンのシンクローニングはサポートされていますか？

はい。シンクローニングは、NFS および SMB ストレージリポジトリのほかに、EXT3 としてフォーマットされたローカルディスクでも使用できます。

Citrix Hypervisor では、**Distributed Replicated Block Device (DRBD)** ストレージはサポートされていますか？

いいえ。Citrix Hypervisor では、DRBD はサポートしていません。

Citrix Hypervisor では、**ATA over Ethernet** をサポートしていますか？

いいえ。Citrix Hypervisor では、ATA over Ethernet ベースのストレージはサポートしていません。

ネットワーク

仮想マシンのグループを分離するプライベートネットワークは作成できますか？

はい。1つのホスト上に、常駐している仮想マシン用のプライベートネットワークを作成できます。vSwitch Controller アプライアンスを使用すると、暗号化の有無にかかわらず、複数のホストにまたがるプライベートネットワークを作成することもできます。

Citrix Hypervisor では、複数の物理ネットワーク接続をサポートしていますか？

はい。物理ネットワーク上の異なるネットワークインターフェイスに接続している複数の物理ネットワークに接続したり、関連付けたりすることができます。

仮想マシンは複数のネットワークに接続できますか？

はい。仮想マシンは、ホストで使用可能なネットワークに接続できます。

Citrix Hypervisor では IPv6 はサポートされますか？

Citrix Hypervisor でホストされるゲスト仮想マシンは、IPv4 および IPv6 で構成されたアドレスのあらゆる組み合わせを使用できます。

ただし、Citrix Hypervisor のコントロールドメイン (Dom0) での IPv6 の使用は、サポートしていません。ホスト管理ネットワークおよびストレージネットワークには、IPv6 は使用できません。IPv4 が、Citrix Hypervisor ホストで使用可能である必要があります。

Citrix Hypervisor では、物理ネットワークインターフェイス上の VLAN をサポートしていますか？

はい。Citrix Hypervisor では、指定された VLAN への仮想マシンネットワークの割り当てをサポートしています。

Citrix Hypervisor の仮想ネットワークは、すべてのネットワークトラフィックをすべての仮想マシンに渡しますか？

いいえ。Citrix Hypervisor では、Open vSwitch (OVS) を使用します。OVS は、レイヤー 2 スイッチとして機能します。仮想マシンは、その仮想マシンのトラフィックのみを認識します。さらに、Citrix Hypervisor のマルチテナントのサポートにより、分離とセキュリティのレベルが向上します。

仮想ネットワークインターフェイスとネットワークは、無作為検出モードをサポートしていますか？

はい。仮想ネットワークインターフェイスは、無作為検出モードに設定できます。これにより、仮想スイッチ上のすべてのトラフィックを表示することができます。無作為検出モード構成について詳しくは、次のナレッジセンターの記事を参照してください：

- [CTX116493 - How to Enable Promiscuous Mode on a Physical Network Card](#)
- [CTX121729 - How to Configure a Promiscuous Virtual Machine in XenServer](#)

また、Open vSwitch を使用すると、RSPAN を構成してネットワークトラフィックをキャプチャできるようになります。

Citrix Hypervisor では、物理ネットワークインターフェイスのボンディングやチーミングはサポートされますか？

はい。Citrix Hypervisor では、フェールオーバーとリンクアグリゲーションに対して、物理ネットワークインターフェイスボンディングをサポートしています。オプションで、LACP もサポートしています。詳しくは、「[ネットワーク](#)」を参照してください。

メモリ

Citrix Hypervisor を実行するとメモリの消費量はどれくらいですか？

Citrix Hypervisor ホストでのメモリ占有量を計算する場合、考慮すべき3つのコンポーネントがあります。

1. Xen ハイパーバイザー
2. ホスト上のコントロールドメイン (dom0)
3. Citrix Hypervisor クラッシュカーネル

dom0 の実行に必要なメモリ容量は、自動的に調整されます。割り当てられるメモリの量は、次の表に示すように、ホスト上の物理メモリの量に基づきます：

ホストメモリ (GB)	割り当てられたコントロールドメインメモリ (MB)
24 未満	752
24 ~ 47	2048
48 ~ 63	3072
64 ~ 1024	4096

注：

コントロールドメインには、この表の値以上のメモリを割り当てることもできます。ただし、割り当てるメモリ量を増やす操作は、シトリックスサポートの指示の下でのみ行ってください。

XenCenter では、[メモリ] タブの [Xen] フィールドには、コントロールドメイン、Xen ハイパーバイザー、Citrix Hypervisor クラッシュカーネルにより使用されているメモリ量が表示されます。多くのメモリを搭載したホスト上では、ハイパーバイザーにより使用されるメモリ量も大きくなります。

詳しくは、「[メモリ使用率](#)」を参照してください。

Citrix Hypervisor では、仮想マシンのメモリ使用量は最適化されますか？

はい。Citrix Hypervisor では、動的メモリ制御 (DMC) を使用して、実行中の仮想マシンのメモリを自動的に調整します。この調整によって、各仮想マシンに割り当てられたメモリ量を特定の範囲内で増減して、パフォーマンスを維持しながら仮想マシン密度を向上させることができます。

詳しくは、「[仮想マシンのメモリ](#)」を参照してください。

リソースプール

リソースプールとは何ですか？

リソースプールとは、1つのユニットとして管理される、一連の Citrix Hypervisor ホストのコレクションです。通常、リソースプールは、ネットワーク接続されたストレージの一定の量を共有し、仮想マシンを、あるホストからプール内の別のホストに迅速に移行できるようにします。詳しくは、「[ホストとリソースプール](#)」を参照してください。

Citrix Hypervisor では、リソースプールの管理に専用のホストが必要ですか？

いいえ。プール内のホストを1つプールマスタとして指定する必要があります。プールマスタは、プールに必要な管理作業をすべて制御します。この設計は、外部の単一障害点がないことを意味します。プールマスタに障害が発生した場合、プール内のほかのホストは引き続き動作し、常駐する仮想マシンは通常どおりに動作し続けます。プールマスタがオンラインに復帰できない場合、Citrix Hypervisor によってプール内のほかのホストから1つをマスタに昇格させ、プールの制御を回復させます。

このプロセスは、高可用性機能によって自動で行われます。詳しくは、「[高可用性](#)」を参照してください。

リソースプールの構成データはどこに保存されますか？

構成データのコピーは、リソースプール内のすべてのホストに保存されます。現在のプールマスタに障害が発生した場合、このデータにより、リソースプール内の任意の1つホストが新しいプールマスタになります。

リソースプールレベルではどのような種類の構成を行うことができますか？

リソースプールレベルでは、リモート共有ストレージとネットワークの構成を行うことができます。構成がリソースプール上で共有されている場合、マスターシステムによって構成の変更がすべてのメンバーシステムに自動的に反映されます。

新しいホストシステムがリソースプールに追加されると、このホストシステムは共有設定で自動的に構成されますか？

はい。リソースプールに追加された新しいホストシステムには、共有ストレージ設定およびネットワーク設定と同じ構成が自動的に適用されます。

同じ Citrix Hypervisor リソースプールで、異なる種類の CPU を使用できますか？

はい。はい。シトックスでは、プール全体で同じ CPU タイプを使用することを推奨しています（同種型リソースプール）。ただし、CPU のベンダーが同じであれば、CPU タイプが異なるホストをプールに追加することもできます（異種混在型）。

詳しくは、「[ホストとリソースプール](#)」を参照してください。

特定の CPU タイプに対する機能マスクのサポートに関する最新情報は、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。

ライブマイグレーション (旧 XenMotion)

実行中の仮想マシンをあるホストから別のホストに移動することはできますか?

ライブマイグレーションでは、ホストが (プール内の) 同じストレージを共有している場合に、実行中の仮想マシンを移動することができます。

さらに、ストレージのライブマイグレーションでは、ストレージを共有しないホスト間での移行ができます。仮想マシンは、同一のプール内でも、異なるプール間でも移行できます。

高可用性

Citrix Hypervisor には高可用性機能がありますか?

はい。高可用性機能 (HA) が有効な場合、Citrix Hypervisor は、プール内のホストの健全性を継続的に監視します。ホストに障害があることを HA が検出すると、ホストは自動的にシャットダウンされます。この操作により、代替の正常なホストで仮想マシンを安全に再起動することができます。

Citrix Hypervisor の高可用性機能は、ローカルストレージをサポートしていますか?

いいえ。HA を使用する場合は、共有ストレージが必須です。この共有ストレージにより、ホストに障害が発生した場合に仮想マシンを再配置することができます。ただし、HA を使用すると、再起動後にホストが回復するときに、ローカルストレージに保存されている仮想マシンを自動的に再起動するようにマークできます。

HA を使用して、リカバリされた仮想マシンの再起動を自動的に順序付けすることはできますか?

はい。HA 構成では、仮想マシンを起動する順序を定義できます。この機能により、相互に依存する仮想マシンを自動的に順序付けすることができます。

パフォーマンスメトリック

Citrix Hypervisor 管理ツールでは、パフォーマンス情報は収集されますか?

はい。Citrix Hypervisor では、パフォーマンスメトリックの詳細な監視ができます。監視対象のメトリックは、CPU、メモリ、ディスク、ネットワーク、C-状態/P-状態情報、ストレージなどです。これらのメトリックは、必要に

応じてホスト単位または仮想マシン単位で監視できます。パフォーマンスメトリックは、直接アクセスして使用したり（ラウンドロビンデータベースとして公開）、XenCenter やその他のサードパーティ製アプリケーションで視覚的に表示したりできます。詳しくは、「[環境の監視と管理](#)」を参照してください。

Citrix Hypervisor パフォーマンスメトリックはどのように収集されますか？

Citrix Hypervisor パフォーマンスメトリックのデータは、さまざまなソースから収集されます。収集対象のソースには、Xen ハイパーバイザー、Dom0、標準 Linux インターフェイス、WMI などの標準 Windows インターフェイスなどがあります。

XenCenter では、パフォーマンスメトリックはリアルタイムで表示されますか？

はい。XenCenter では、[パフォーマンス] タブに、実行中の各仮想マシンと Citrix Hypervisor ホストのリアルタイムのパフォーマンスメトリックが表示されます。表示されるメトリックはカスタマイズできます。

XenCenter では、パフォーマンスメトリックの履歴の保存および表示はできますか？

はい。Citrix Hypervisor では、昨年からのパフォーマンスメトリックが保持されます（粒度は低下します）。XenCenter では、これらのメトリックがリアルタイムのグラフィック表示で視覚化されます。

インストール

Citrix Hypervisor は、既存のオペレーティングシステムを既に実行しているシステム上にインストールされますか？

いいえ。Citrix Hypervisor はベアメタルハードウェア上に直接インストールされるため、オペレーティングシステムの介在による複雑さ、オーバーヘッド、およびパフォーマンス上のボトルネックが生じません。

既存の **Citrix Hypervisor** または **XenServer** インストールを新しいバージョンにアップグレードできますか？

はい。サポートされているバージョンの Citrix Hypervisor または XenServer を既にインストールしている場合、新規のインストールではなく、Citrix Hypervisor の新しいバージョンに更新またはアップグレードすることができます。詳しくは、「[更新](#)」および「[アップグレード](#)」を参照してください。

サポートが終了しているバージョンの **Citrix Hypervisor** または **XenServer** インストールから、このバージョンにアップグレードできますか？

Citrix Hypervisor または XenServer の既存のバージョンのサポートが終了している場合、Citrix Hypervisor の最新バージョンに直接アップグレードまたは更新することはできません。

- XenServer と 6.5 Service Pack 1 については、まず XenServer 7.1 Cumulative Update 2 にアップグレードし、その後 XenServer 7.1 Cumulative Update 2 から Citrix Hypervisor 8.1 にアップグレードします。
- それ以外の 6.x バージョンの XenServer では、最新バージョンへのアップグレードはできません。Citrix Hypervisor 8.1 の新規インストールを作成する必要があります。
- サポートが終了している XenServer の 7.x 最新リリースの場合、最新バージョンへのアップグレードはできません。Citrix Hypervisor 8.1 の新規インストールを作成する必要があります。

これ以外の方法によるアップグレードは、サポートが終了しているバージョンではサポートされません。

Citrix Hypervisor を物理ホストシステムにインストールする場合に必要なローカルストレージの容量はどれくらいですか？

Citrix Hypervisor では、物理ホストシステム上に 46GB 以上のローカルストレージが必要です。

ホストシステムに **Citrix Hypervisor** のネットワークインストールを実行するときに、**PXE** を使用できますか？

はい。PXE を使用して、Citrix Hypervisor をホストシステムにインストールできます。事前構成された回答ファイルを作成することで、PXE を使用して Citrix Hypervisor を自動的にインストールすることもできます。

Xen ハイパーバイザーは **Linux** で実行できますか？

いいえ。Xen は、ホストハードウェア（「ベアメタル」）上で直接実行される、タイプ1のハイパーバイザーです。ハイパーバイザーが読み込まれると、特権を持つ管理ドメイン（コントロールドメイン）が起動します。このドメインには、最小限の Linux 環境が含まれています。

Citrix Hypervisor のデバイスドライバーサポートは、どこで入手できますか？

Citrix Hypervisor では、Linux カーネルで提供されるデバイスドライバーが使用されます。このため、幅広いハードウェアデバイスやストレージデバイス上で Citrix Hypervisor を実行できます。ただし、シトリックスでは認定デバイスドライバーを使用することをお勧めしています。

詳しくは、[ハードウェア互換性リスト（英語）](#) を参照してください。

ライセンス

Citrix Hypervisor のライセンス取得方法を教えてください？

Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

テクニカルサポート

シトリックスでは、**Citrix Hypervisor** の直接のテクニカルサポートを提供していますか？

はい。詳しくは、[シトリックスのサポートとサービス](#)を参照してください。

1つのサポート契約で、**Citrix Hypervisor** とそれ以外のシトリックス製品のテクニカルサポートを受けることはできますか？

はい。シトリックスのテクニカルサポート契約では、Citrix Hypervisor はもちろん、それ以外のシトリックス製品に対してもサポートインシデントを開くことができます。

詳しくは、[シトリックスのサポートとサービス](#)を参照してください。

シトリックスのテクニカルサポートは、**Citrix Hypervisor** を購入したときと同じタイミングで購入する必要がありますか？

いいえ。シトリックスのテクニカルサポート契約は、製品の購入時でも、それ以外の時でも購入できます。

Citrix Hypervisor のテクニカルサポートを受けるための代替チャンネルはありますか？

はい。Citrix Hypervisor のテクニカルサポートを受けるためのチャンネルには、何種類かあります。そのほかに、[Citrix Support Knowledge Center](#)やフォーラムをご利用いただくこともできます。また、テクニカルサポートサービスを提供している、Citrix Hypervisor の認定パートナーに問い合わせることもできます。

シトリックスでは、オープンソースの **Xen** プロジェクトに対するテクニカルサポートは提供していますか？

いいえ。オープンソースの Xen プロジェクトに対するテクニカルサポートは提供していません。詳しくは、<http://www.xen.org/>を参照してください。

技術以外の問題が発生した場合、シトリックスのテクニカルサポートインシデントを開くことはできますか？

いいえ。技術以外のことに関する Citrix Hypervisor の問題は、シトリックスカスタマーサービスを通じてご連絡ください。たとえば、ソフトウェアのメンテナンス、ライセンス、管理サポート、注文確認に関連する問題などです。

ライセンス

January 20, 2020

Citrix Hypervisor 8.1 には、次のエディションがあります：

- Premium Edition（以前の Enterprise Edition）
- Standard Edition
- Express Edition（以前の Free Edition）

Standard Edition はエントリーレベルの商品です。Premium Edition で提供される高度な機能は使用できませんが、強固で高性能な仮想化プラットフォームに必要なさまざまな機能を備えています。シトリックスの包括的なサポートおよび保守サービスも提供されます。

Premium Edition は最上位レベルの商品で、サーバー、デスクトップ、およびクラウドワークロード用に最適化されています。Standard Edition で利用可能な機能に加えて、Premium Edition には以下の機能があります：

- 自動 Windows VM Driver 更新
- 管理エージェントの自動更新
- SMB ストレージのサポート
- Direct Inspect API
- BitDefender ハイパーバイザーレベルの内観のサポート
- 動的ワークロードバランス機能
- NVIDIA GRID、AMD MxGPU、および Intel GVT-g による GPU 仮想化
- VMware vSphere から Citrix Hypervisor への変換ユーティリティ
- Intel セキュアメジャーブート (TXT)
- プールリソースデータのエクスポート
- インメモリ読み取りキャッシュ
- PVS アクセラレータ
- プールのローリングアップグレード
- XenCenter を使用した自動アップデート
- Citrix Hypervisor のライブパッチ
- Citrix Virtual Desktops タブレットモードの有効化
- 変更ブロック追跡
- IGMP スヌーピング
- USB パススルー
- SR-IOV ネットワークのサポート
- 共有ブロックストレージデバイスのシンプロビジョニング

Citrix Hypervisor の以前のリリースでは、Premium Edition は Enterprise Edition という名称でした。ほかのシトリックス製品とエディション名を統一するために名称を変更しましたが、提供される機能に変更はありません。

Citrix Virtual Apps または Citrix Virtual Desktops を既に購入されている場合は、Citrix Hypervisor を使用する

権限があります。つまり、Premium Edition のすべての機能を使用できます。

Express Edition で使用できる機能には制限があり、シトリックスサポートおよび保守サービスは提供されません。Express Edition の使用にはライセンスは必要ありません。Citrix Hypervisor の Express Edition を実行しているホストは、XenCenter で「ライセンス無効」と表示されます。

Citrix Hypervisor の以前のリリースでは、Express Edition は Free Edition という名称でした。ほかのシトリックス製品とエディション名を統一するために名称を変更しましたが、提供される機能に変更はありません。

詳しくは、[Citrix Hypervisor 機能マトリックス](#)を参照してください。

Citrix Hypervisor では、ほかのシトリックス製品と同じライセンス処理が行われます。このため、ライセンスサーバー上に有効なライセンスをインストールする必要があります。ライセンスサーバーは、[Citrix ライセンスサーバー](#)からダウンロードできます。Citrix Hypervisor は、(Citrix Virtual Apps and Desktops ライセンス以外に) ソケット単位のライセンスが適用されます。ライセンスの割り当ては、環境内のスタンドアロンの Citrix ライセンスサーバー（物理サーバーまたは仮想サーバー）により一元管理されます。ソケット単位のライセンスを適用すると、Citrix Hypervisor に *Citrix Hypervisor [Per-Socket Edition]* と表示されます。

注:

ライセンス済みのサーバーとそうでないサーバーを同一プール内で混在させた場合、ライセンスが適用されていない状態として動作します。

ライセンスがないホストには、いくつかの制限があります。詳しくは、「その他の質問」を参照してください。

ライセンス手順の概要

Citrix Hypervisor Premium Edition または Standard Edition のライセンスを取得するには、次のアイテムが必要です:

- Citrix Hypervisor のライセンス
- Citrix ライセンスサーバー
- Citrix Hypervisor サーバー
- XenCenter

次の手順は、プロセスの概要を示しています:

1. Citrix Hypervisor サーバーに、Citrix ライセンスサーバーをインストールするか、Citrix ライセンスサーバー - VPX をインポートします。
2. ライセンスファイルのダウンロード
3. ライセンスファイルの Citrix ライセンスサーバーへの追加
4. XenCenter を使用して、ライセンスサーバーの詳細を入力し、リソースプール内のホストに適用します。

Citrix ライセンスサーバーについて詳しくは、[Citrix ライセンスのドキュメント](#)を参照してください。

ライセンス Citrix Hypervisor

Q: Citrix Hypervisor のライセンスはどこで購入できますか?

A: <http://citrix.com/buy> のライセンスは Citrix Hypervisor でご購入いただけます。

Q: Citrix Hypervisor のライセンスを適用するにはどうすればよいですか?

A: Citrix Hypervisor では、ライセンスサーバーが必要です。Citrix Hypervisor のライセンス購入後に、.LIC ライセンスアクセスコードが送付されます。このライセンスアクセスコードを次のいずれかにインストールします:

- Citrix ライセンスサーバーソフトウェアが動作する Windows サーバー

Citrix Hypervisor サーバーにライセンスを割り当てると、Citrix Hypervisor が Citrix ライセンスサーバーと通信して、必要なライセンスを要求します。これに成功したらライセンスがチェックアウトされ、ホストがライセンス化されるライセンスについての情報がライセンスマネージャに表示されます。

Q: リソースプールにライセンスを適用するには、いくつのライセンスが必要ですか?

A: Citrix Hypervisor には、CPU ソケット単位のライセンスが適用されます。リソースプールにライセンスが適用されていると見なされるには、プール内のすべての Citrix Hypervisor サーバーにライセンスを割り当てる必要があります。Citrix Hypervisor では、使用される CPU ソケット数のみが考慮されます。

Citrix ライセンスサーバーを使用して、ライセンス管理コンソールのダッシュボードに利用可能なライセンスの数を表示できます。

Q: 使用されていないソケットにはソケット単位のライセンスが必要ですか?

A: いいえ。使用される CPU ソケットのみ、ライセンスが適用されるソケットの数にカウントされます。

Q: ライセンスの有効期限が切れると、仮想マシン (VM) は失われますか?

A: いいえ、仮想マシンやそのデータが失われることはありません。

Q: ライセンスプールを所有しており、ライセンスサーバーが利用できなくなった場合はどうなりますか?

A: ライセンスの有効期限は切れていないもののライセンスサーバーが使用できない場合は、以前に適用されたライセンスのレベルで 30 日間の猶予期間が与えられます。

Q: ソケット単位のライセンスで以前のバージョンの **Citrix Hypervisor** を **Citrix Hypervisor 8.1** にアップグレードしたいのですが、何か手続きは必要ですか？

A: いいえ。カスタマーサクセスサービスが少なくとも 2019 年 12 月 13 日まで有効な場合は、以前に購入したソケット単位のライセンスを使用してホストを Citrix Hypervisor 8.1 Premium Edition にアップグレードできます。

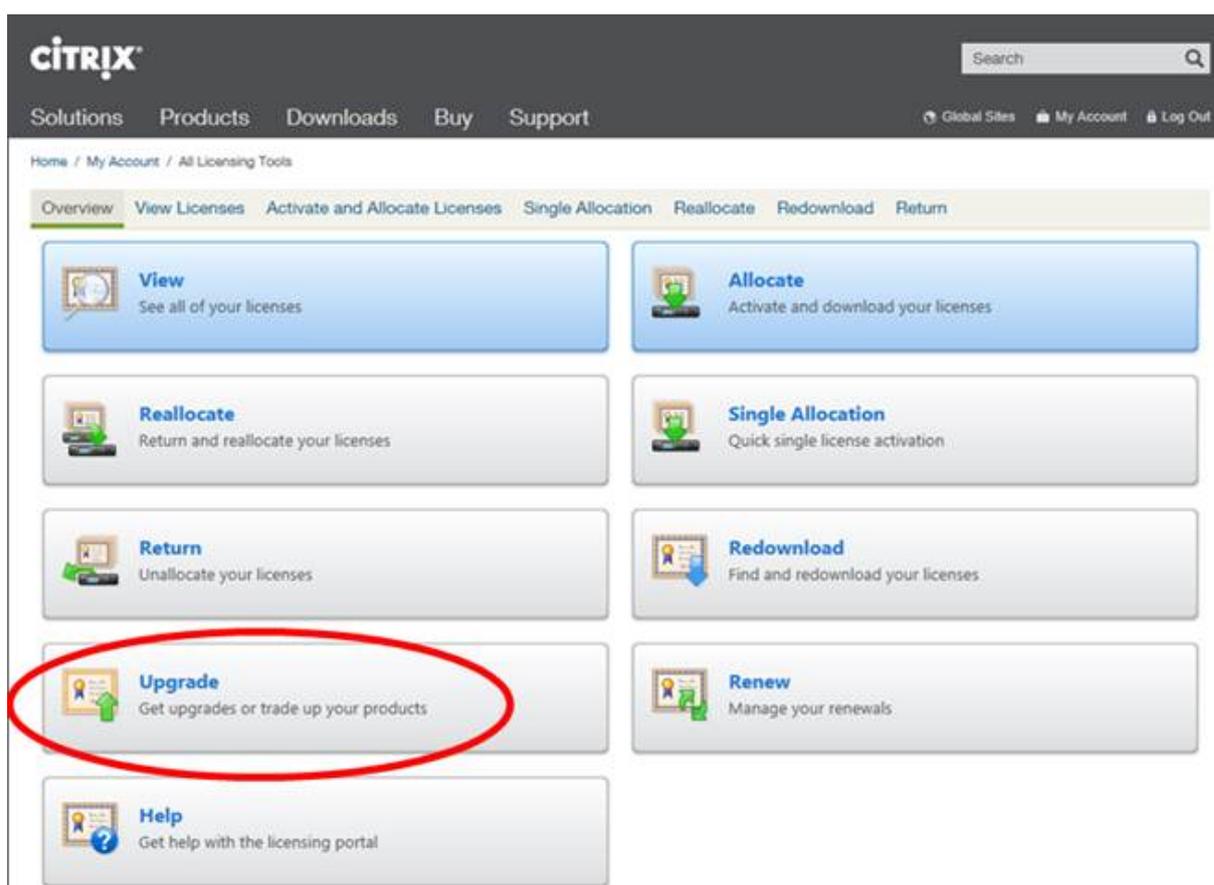
ただし、最初の購入後にカスタマーサクセスサービスを更新した場合は、ライセンスサーバー上のライセンスファイルを更新して、カスタマーサクセスサービスの資格が表示されるようにする必要がある場合があります。

Q: ライセンスが適用されていないエディションの **Citrix Hypervisor 8.0** から **Citrix Hypervisor 8.1** に移行したいのですが、何か手続きは必要ですか？

A: いいえ。ホストを Citrix Hypervisor 8.1 にアップグレードまたはアップデートできます。ただし、適切なライセンスが適用されるまでは、サポートサービスは提供されず、Premium 機能（プールのローリングアップグレードを含む）も使用できません。

Q: **Citrix Virtual Apps and Desktops** を使用しています。 **Citrix Hypervisor 8.0** から **Citrix Hypervisor 8.1** に移行したいのですが、何か手続きは必要ですか？

A: いいえ。Citrix Virtual Apps または Citrix Virtual Desktops をご利用のお客様は、Citrix Hypervisor 8.1 にシームレスにアップデートできます。インストールされた既存の Citrix Virtual Apps または Citrix Virtual Desktops のライセンスでは、変更は一切必要なく、Citrix Hypervisor の利用特典が付与されます。



Q: Citrix Virtual Apps and Desktops のライセンスを持つ、**Citrix Service Provider** です。**Citrix Hypervisor** のこのライセンスは、**Citrix Hypervisor 8.1** にアップグレードする時に使用できますか？

A: はい。Citrix Hypervisor 8.1 では、お持ちのライセンスがサポートされます。このライセンスでは、Citrix Hypervisor の Premium Edition で提供されるすべての Premium 機能を使用できます。このライセンスをプールに適用するには、プール内のすべてのホストをアップグレードまたはアップデートしてから Citrix Hypervisor 8.1 を実行してください。

Q: Citrix Virtual Apps and Desktops サービスのサブスクリプションを持つユーザーには、**Citrix Hypervisor 8.1** を使用する権限がありますか？

A: はい。オンプレミスでデスクトップおよびアプリを使用できる Citrix Virtual Apps and Desktops サービスのサブスクリプションをお持ちの場合、Citrix Hypervisor でこれらのデスクトップやアプリをホストする権限があります。

ライセンス管理ツールを使用してライセンスをダウンロードします。このライセンスをライセンスサーバーにインストールして、Citrix Virtual Apps and Desktops サービスサブスクリプションでオンプレミスの Citrix Hypervisor を使用します。

このライセンスでは、オンプレミスの Citrix Virtual Apps and Desktops の権限と同様にすべての Premium 機能を使用できます。このライセンスをプールに適用するには、プール内のすべてのホストをアップグレードしてから Citrix Hypervisor 8.1 を実行してください。

Q: Citrix Virtual Apps and Desktops の一環として提供される、**Citrix Hypervisor Premium Edition** の高度な仮想化管理機能の使用において、どのような制約がありますか？

A: Citrix Virtual Apps and Desktops ではすべてのエディションで、Citrix Hypervisor Premium Edition の高度な仮想化管理機能をご使用いただけます。Citrix Virtual Apps や Citrix Virtual Desktops のライセンスで有効なすべての機能の完全な一覧については、Citrix Hypervisor の機能マトリックスを参照してください。

Citrix Hypervisor の利用特典では、Citrix Virtual Apps または Citrix Virtual Desktops の機能コンポーネントを提供するために必要なインフラストラクチャの仮想化が可能になります。これらの機能の使用は、Citrix Virtual Apps または Citrix Virtual Desktops のライセンスが適用されたユーザーまたはデバイスに限定する必要があります。

このライセンスでカバーされる Citrix Virtual Apps または Citrix Virtual Desktops インフラストラクチャと同じ Citrix Hypervisor リソースプールに展開され、Citrix Virtual Apps または Citrix Virtual Desktops インフラストラクチャのみをサポートするために使用される場合、インフラストラクチャをサポートする追加のサーバー (Microsoft ドメインコントローラーや SQL Server など) もカバーされます。

Citrix Virtual Apps または Virtual Desktops ライセンスの Citrix Hypervisor 利用特典は、Citrix Virtual Apps または Citrix Virtual Desktops インフラストラクチャや Citrix Virtual Deliver Agent (VDA) をホストしていない Citrix Hypervisor プールには使用できません。また、上記の権限でカバーされていない仮想マシンのホストには、この権限を使用できません。これらの用途については、Citrix Hypervisor を別途ご購入いただく必要があります。

Citrix ライセンスサーバー

Q: Citrix Hypervisor ではどのライセンスサーバーを使用できますか？

A: バージョン 11.14 以降の Citrix ライセンスサーバー (Microsoft Windows を実行しているサーバーの場合) を使用できます。

Q: Citrix ライセンスサーバーにライセンスをインポートするにはどうすればよいですか？

A: ライセンスファイルのインポート方法については、[ライセンス管理のドキュメント](#)を参照してください。

- [Citrix Licensing Manager](#) を使用したライセンスのインストール
- [ライセンス管理コンソール](#)を使用したライセンスファイルのインポート
- [コマンドライン](#)を使用したライセンスファイルのインストール

Q: Citrix Hypervisor プール上でライセンスサーバーを実行できますか?

A: はい。Citrix ライセンスサーバーのソフトウェアを Windows 仮想マシンにインストールできます。

Citrix Hypervisor ライセンスサーバーが起動できるようになるまで「猶予」ライセンスで動作します。このため、プール内の Citrix Hypervisor サーバーにライセンスを適用し、Citrix ライセンスサーバーが稼働しているホストを再起動すると、ライセンスサーバーが再起動されるまでそのホストに猶予期間が適用されます。

Q: Citrix Hypervisor で **Windows** バージョンの **Citrix** ライセンスサーバーを使用できますか?

A: はい。

Q: Windows にインストールした **Citrix** ライセンスサーバーソフトウェアで、ほかのシトリックス製品のライセンスをインストールできますか?

A: はい、Windows にインストールした Citrix ライセンスサーバーソフトウェアを使用して、ほかのシトリックス製品のライセンスを取得できます。詳しくは、[シトリックス製品ドキュメント](#)の Web サイトの「[ライセンス](#)」を参照してください。

Citrix Hypervisor プールへのライセンス適用

Q: XenCenter を使用してすべてのホストにライセンスを適用するにはどうすればよいですか?

A: ライセンスを適用するには、以下の手順に従ってください:

1. [ツール] メニューの [ライセンスマネージャ] を選択します。
2. ライセンスを割り当てるプールまたはホストを選択し、[ライセンスの割り当て] をクリックします。
3. [ライセンスの適用] ダイアログボックスで、ホストに割り当てるエディションの種類を指定し、ライセンスサーバーのホスト名または IP アドレスを入力します。

Q: XenCenter を使用せずにライセンスを適用できますか?

A: はい、xe CLI を使用できます。host-apply-edition コマンドを実行します。たとえば、ホストにライセンスを適用するには、次のように入力します:

```
1     xe host-apply-edition edition=enterprise-per-socket|desktop-plus|
      desktop|standard-per-socket \
2
3     license-server-address=<licenseserveraddress> host-uuid=<
      uuidofhost> \
```

```
4
5     license-server-port=<licenseserverport>
```

プールにライセンスを適用するには、`pool-apply-edition` コマンドを使用します。次に例を示します：

```
1     xe pool-apply-edition edition=enterprise-per-socket|desktop-plus|
2         desktop|standard-per-socket \
3         license-server-address=<licenseserveraddress> pool-uuid=<
4         uuidofpool> \
5         license-server-port=<licenseserverport>
```

Q: ホストやプールのライセンスの状態を確認するにはどうすればよいですか？

A: サーバーやプールのライセンスの種類は、XenCenter に表示されます。

サーバーやプールのライセンスの種類を確認するには、ツリー表示から対象のサーバーまたはプールを選択します。XenCenter のタイトルバーに、選択したサーバーまたはプールの名前とライセンスの状態が表示されます。

ライセンス済みのサーバーとそうでないサーバーを同一プール内で混在させた場合、ライセンスが適用されていない状態として動作します。XenCenter のツリー表示には、ライセンス対象外のプールが三角形の警告アイコン付きで表示されます。

その他の質問

Q: Citrix Hypervisor を評価するためのライセンスはどうすれば取得できますか？

A: Citrix Hypervisor を評価する場合はライセンスは必要ありません。ライセンスが適用されていない状態で Citrix Hypervisor を使用できます。ただし、Premium 機能は使用できません。また、シトリックスサポートおよび保守サービスは提供されません。

Premium Edition の機能はトライアルライセンスで試用できます。詳しくは、「[導入](#)」を参照してください。

Q: Citrix Hypervisor をライセンスなしで使用できますか？

A: はい。ライセンスが適用されていない状態の Citrix Hypervisor (Express Edition) を使用すると、シトリックスサポートや保守を利用できなくなります。また、次の機能も制限され、ライセンスが必要になります：

- ホストが 3 台以上含まれるプール

注:

既存のプールに 3 台以上のホストがある場合、プールに新規ホストを追加しない限りこの制限の影響を受けません。

- 高可用性
- 動的メモリ制御
- ストレージモーション
- 役割ベースのアクセス制御
- GPU パススルー
- Site Recovery Manager
- Active Directory の統合
- プールのローリングアップグレード

Citrix Hypervisor Premium Edition はトライアルライセンスで試用できます。詳しくは、「[Citrix Hypervisor の導入](#)」を参照してください。

詳細情報の表示

- Citrix Hypervisor 8.1 リリースについて詳しくは、[Citrix Hypervisor 8.1 リリースノート](#)を参照してください。
- Citrix Hypervisor 8.1 の製品ドキュメントは、[Citrix Hypervisor 8.1 製品ドキュメント](#)を参照してください。
- Citrix Hypervisor の製品の概要については、「[製品の技術概要](#)」を参照してください。
- Citrix Hypervisor に関する非技術的な問題（カスタマーサクセスサービスプログラムのサポート、ライセンス管理、管理サポート、注文の確認など）については、[シトリックスカスタマーサービス](#)を通じて報告してください。

インストール

March 12, 2020

このセクションでは、Citrix Hypervisor のインストール、設定、および初期操作の説明に加え、インストール中に発生する可能性のある問題とそのトラブルシューティング情報、および追加情報の入手方法について説明します。

この情報は、物理サーバー上で Citrix Hypervisor サーバーを設定するシステム管理者を主な対象としています。

Citrix Hypervisor はベアメタルハードウェア上に直接インストールされるため、オペレーティングシステムの介在による複雑さ、オーバーヘッド、およびパフォーマンス上のボトルネックが生じません。デバイスドライバーは、Linux カーネルで提供されるものが使用されます。このため、幅広いハードウェアデバイスおよびストレージデバイス上で Citrix Hypervisor を実行できます。ただし、認定デバイスドライバーを使用するようにしてください。

詳しくは、[ハードウェア互換性リスト \(HCL\) \(英語\)](#) を参照してください。

重要:

Citrix Hypervisor サーバーは、専用の 64 ビット x86 サーバーにインストールする必要があります。Citrix Hypervisor サーバーとのデュアルブート構成としてほかのオペレーティングシステムをインストールしないでください。この構成はサポートされていません。

はじめに

Citrix Hypervisor 8.1 をインストールする場合、次の要因を考慮してください:

- どのリリースストリームの Citrix Hypervisor を使用するか
- どのインストール方法が最適か
- どのようなシステム要件があるか

Citrix Hypervisor リリースストリーム

Citrix Hypervisor リリースは、次のいずれかのリリースストリームに属します: 最新リリース (CR) または長期サービスリリース (LTSR)。Citrix Hypervisor 8.1 は最新リリースです。CR ストリームまたは LTSR ストリームのどちらから Citrix Hypervisor のバージョンをインストールするかを選択するときは、次の点を考慮してください:

- Citrix Hypervisor のバージョンアップデートする頻度
- 安定性のある機能セットまたは最新の機能セットを好むかどうか

最新リリース

Citrix Hypervisor の最新リリースでは、可能な限り早い時期に新しい機能を使用することができます。CR ストリームでは Citrix Hypervisor の新しいバージョンは、四半期ごとにリリースされます。CR ストリームを使用している場合、継続してサポートを利用するために、定期的に新しい CR を採用する必要があります。Citrix Hypervisor CR で検出されたほとんどの問題は、次の最新リリースで修正されます。セキュリティの問題は、CR に適用できる Hotfix で修正されています。

Citrix Hypervisor 8.0 または XenServer 7.6 がインストールされている場合、継続してサポートを利用するためには、Citrix Hypervisor 8.1 にアップデートする必要があります。

長期サービスリリース

Citrix Hypervisor (旧称 XenServer) の長期サービスリリースでは、Citrix Hypervisor の機能セットに関して、安定した動作が保証されています。LTSR ストリームでは Citrix Hypervisor の新しいバージョンは 2 年ごとにリリースされ、最大 10 年間サポートされます。Citrix Hypervisor LTSR のすべての問題は、Citrix Hypervisor LTSR に適用できる Hotfix または累積更新プログラム (CU) で修正されています。

現在 XenServer 7.1 Cumulative Update 2 LTSR がインストールされている場合、Citrix Hypervisor の最新リリース (CR) ストリームにアップグレードして新しい機能を利用することができます。

インストール方法

Citrix Hypervisor 8.1 は、次のいずれかの方法でインストールできます：

- 新規インストール
- Citrix Hypervisor 8.0 のアップデート
- サポート対象である旧バージョンの XenServer のアップグレード

既存のバージョンの Citrix

Hypervisor または XenServer	取得方法: Citrix Hypervisor 8.1	使用する ISO ファイル
なし	新規インストール	基本インストール ISO
8.0	更新	アップデート ISO
7.6、7.1 Cumulative Update 2、 7.0	アップグレード	基本インストール ISO

注:

アップグレードのサポート対象になるのは、LTSR の最新の累積更新プログラムから行う場合のみです。既存の XenServer のバージョンが 7.1 または 7.1 Cumulative Update 1 の場合は、7.1 Cumulative Update 2 を適用してから Citrix Hypervisor 8.1 にアップグレードします。

サポート対象外のバージョンの XenServer から直接 Citrix Hypervisor 8.1 にするアップグレードパスはサポートされていません。その場合は、新規にインストールする必要があります。

新規インストール

Citrix Hypervisor 8.1 を新規にインストールする場合：

- **Citrix Hypervisor 8.1** 基本インストール **ISO** ファイルを使用します。このファイルは[シトリックスのダウンロードサイト](#)からダウンロードできます。
- **システム要件**、**ライセンス Citrix Hypervisor**、Citrix Hypervisor と XenCenter のインストールの情報を確認してから、Citrix Hypervisor をインストールします。

更新

Citrix Hypervisor 8.0 から Citrix Hypervisor 8.1 にアップデートする場合:

- **Citrix Hypervisor 8.1** アップデート **ISO** ファイルを使用します。このファイルは[シトリックスのダウンロードサイト](#)からダウンロードできます。
- Citrix Hypervisor をアップデートする前に、[システム要件とのアップデート](#)の情報を確認してください。

アップグレード

XenServer 7.6、XenServer 7.1 Cumulative Update 2、または 7.0 を Citrix Hypervisor 8.1 にアップグレードする場合:

- **Citrix Hypervisor 8.1** 基本インストール **ISO** ファイルを使用します。このファイルは[シトリックスのダウンロードサイト](#)からダウンロードできます。
- [システム要件](#)および[既存バージョンからのアップグレード](#)の情報を確認してから、Citrix Hypervisor をアップグレードします。

インストール済みの Citrix Hypervisor が検出された場合は、アップグレードインストールを実行するためのオプションが表示されます。アップグレードでは、新規インストールと同様の画面が表示されますが、いくつかの手順が省略され、既存のネットワーク設定やシステムの日時設定などは保持されます。

サブメンタルパック

サブメンタルパックは、Citrix Hypervisor をインストールした後で、必要に応じてインストールできます。サブメンタルパック (filename.iso) をコンピューター上の把握しやすい場所にダウンロードして、アップデートと同じ方法でインストールします。

詳しくは、「[Supplemental Packs and the DDK Guide \(英語\)](#)」を参照してください。

Citrix Hypervisor サーバーのインストール

ヒント:

インストール中は、F12 キーを押すとすばやく次の画面に進みます。要素間を移動するには Tab キー、選択するには Space または Enter キーを押します。ヘルプを表示するには F1 キーを押します。

Citrix Hypervisor サーバーをインストールまたはアップグレードするには、次の手順に従います:

1. 保存したいデータをバックアップします。Citrix Hypervisor をインストールすると、インストール時に指定したすべてのハードディスク上のデータが上書きされます。
2. インストールメディアから、またはネットワークブートを使用してコンピューターを起動します:
 - 起動可能な USB から Citrix Hypervisor サーバーをインストールするには:

- a) rufus や diskpart などのツールを使用して、Citrix Hypervisor インストール ISO を使うことで起動可能な USB を作成します。ツールにより ISO ファイルの内容が変更されないようにしてください。
- b) 起動可能な USB ドライブをターゲットシステムに挿入します。
- c) システムを再起動します。
- d) BIOS で、USB からシステムを起動するように設定を変更します。

(起動順序の変更が必要な場合は、コンピューターに付属のドキュメントを参照してください)

- CD から Citrix Hypervisor サーバーをインストールするには:

- a) Citrix Hypervisor のインストール ISO ファイルを CD に書き込みます。
- b) 起動可能な CD をターゲットシステムの CD/DVD ドライブに挿入します。
- c) システムを再起動します。
- d) BIOS で、CD からシステムを起動するように設定を変更します。

(起動順序の変更が必要な場合は、コンピューターに付属のドキュメントを参照してください)

- ネットワーク上に TFTP サーバーを起動するようにセットアップするには:

ネットワークを使用してインストーラーを起動するための TFTP サーバーの設定方法について詳しくは、[ネットワークブートによるインストール](#)を参照してください。

- Citrix Hypervisor を SAN 上のリモートディスクにインストールして SAN ブート環境をセットアップするには:

詳しくは、「[SAN 環境からの起動](#)」を参照してください。

3. 起動メッセージおよび [ようこそ Citrix Hypervisor へ] 画面が表示されます。ここで、インストールに使用するキーマップ (キーボードレイアウト) を選択します。

注:

[システムハードウェア] 警告画面が表示され、インストール先コンピューターの CPU がハードウェア仮想化をサポートしている場合は、ハードウェアの製造元で BIOS のアップデートが提供されていないかどうかを確認してください。

4. [ようこそ Citrix Hypervisor セットアップへ] 画面が表示されます。

Citrix Hypervisor には、最近の多くのサーバーハードウェアをサポートするドライバーが付属しています。ただし、追加のドライバーが提供されている場合は、F9 キーを押します。これにより、追加ドライバーをインストールするための手順が表示されます。

警告:

インストールプロセスのこの段階では、ドライバーディスクが含まれたアップデートパッケージのみがインストールされます。ただし、後の段階でサプリメンタルパックを含むアップデートパッケージをイ

インストールするようメッセージが表示されます。

必要なすべてのドライバーのインストールが完了したら、**[OK]** を選択して続行します。

Citrix Hypervisor は、FCoE から Citrix Hypervisor インストールを起動するように構成できます。F10 キーを押し、画面に表示される指示に従って FCoE を設定します。

注:

FCoE から Citrix Hypervisor サーバーを起動できるようにする前に、LUN をホストに提供するために必要な設定を手動で行ってください。この設定には、ストレージファブリックの設定と、SAN のパブリックワールドワイドネーム (PWWN) への LUN の割り当てが含まれます。この設定を完了した後、使用可能な LUN が SCSI デバイスとしてホストの CNA にマウントされます。これにより、ローカルで接続されている SCSI デバイスのように、SCSI デバイスを使用して LUN にアクセスできるようになります。FCoE をサポートするための物理スイッチおよびアレイの構成については、ベンダーが提供するドキュメントを参照してください。

FCoE ファブリックの設定に VLAN 0 を使用しないでください。Citrix Hypervisor サーバーは VLAN 0 上のトラフィックを検出できません。

警告:

場合によっては、ソフトウェア FCoE スタックを使用して FCoE SAN から Citrix Hypervisor サーバーを起動すると、ホストが応答を停止することがあります。この問題は、ホスト初期化フェーズで一時的にリンクが切断されるために発生します。ホストが長時間応答に失敗する場合は、この問題を回避するためにホストを再起動できます。

5. Citrix Hypervisor のライセンス契約書が表示されます。Page Up キーと Page Down キーを使用してスクロールしながら、契約書を確認します。**[ライセンス契約書に同意する]** を選択して続行します。
6. 適切な操作を選択します。以下のオプションが表示されます:
 - クリーンインストールの実行
 - *Upgrade*: インストール済みの Citrix Hypervisor または XenServer が検出された場合は、アップグレードするためのオプションが表示されます。Citrix Hypervisor サーバーのアップグレードについては詳しくは、「[既存バージョンからのアップグレード](#)」を参照してください。
 - *Restore*: 作成済みのバックアップが検出された場合は、そのバックアップから Citrix Hypervisor を復元するためのオプションが表示されます。

選択したら、**[OK]** を選択して続行します。

7. 複数のローカルハードディスクがある場合は、インストール用のプライマリディスクを選択し、**[OK]** を選択します。
8. 仮想マシンストレージ用のディスクを選択します。ディスクに関する情報を表示するには、**F5** キーを押します。

ストレージを有効利用するためにシンプロビジョニングを使用する場合は、**[シンプロビジョニングを有効に**

する] を選択します。これにより、ホストのローカルストレージリポジトリが仮想マシン VDI のローカルキャッシュとして使用されるようになります。Citrix Virtual Desktops を使用する場合は、ローカルキャッシュが正しく機能するように、このオプションを選択することをお勧めします。詳しくは、「[ストレージ](#)」を参照してください。

[**OK**] を選択します。

9. インストールメディアのソースを選択します。

USB または CD からインストールするには、[**Local media**] を選択します。ネットワークを使用してインストールするには、[**HTTP**]、[**FTP**]、または [**NFS**] を選択します。[**OK**] を選択して続行します。

[**HTTP**]、[**FTP**]、または [**NFS**] を選択した場合は、Citrix Hypervisor インストールメディアファイルに接続できるようネットワークをセットアップします：

- a) コンピューターに複数の NIC (ネットワークインターフェイスカード) がある場合は、Citrix Hypervisor インストールメディアファイルへのアクセスに使用する NIC を 1 つ選択します。[**OK**] を選択して続行します。
- b) DHCP を使用して NIC を構成する場合は [**Automatic configuration (DHCP)**] を選択し、手動で NIC を構成する場合は [**Static configuration**] を選択します。[**Static configuration**] を選択した場合は、必要な NIC 設定を行います。
- c) 使用するインストールメディアが VLAN ネットワークにある場合は、VLAN ID を指定します。
- d) [**HTTP**] または [**FTP**] を選択した場合は、必要に応じて、HTTP または FTP リポジトリの URL、ユーザー名、およびパスワードを入力します。

[**NFS**] を選択した場合は、NFS 共有のサーバー名およびパスを入力します。

[**OK**] を選択して続行します。

10. インストールメディアの整合性を検証するかどうかを選択する画面が表示されます。[**Verify installation source**] を選択すると、パッケージの SHA256 のチェックサムが計算され、既知の値と比較されます。この処理には時間がかかる場合があります。選択したら、[**OK**] を選択して続行します。

11. ルートパスワードを設定します。確認のため、同じパスワードを 2 回入力する必要があります。ここで設定したルートパスワードは、後で XenCenter を使ってこの Citrix Hypervisor サーバーに接続する時に使用します。また、このパスワード (ユーザー名は「root」) は、システム設定コンソールである **xsconsole** にログオンするときにも使用します。

注：

Citrix Hypervisor ルートパスワードには ASCII 文字のみを含める必要があります。

12. プライマリの管理インターフェイスを設定します。このインターフェイスは、XenCenter とこの XenServer ホストとの接続で使用されます。

コンピューターに複数の NIC がある場合、管理インターフェイスとして使用する NIC を選択します。[**OK**] を選択して続行します。

13. 管理インターフェイスとして使用する NIC の IP アドレスとして、DHCP を使用するか（**[Automatic configuration (DHCP)]**）、特定のアドレスを使用するか（**[Static configuration]**）を選択します。VLAN ネットワーク上で管理インターフェイスを使用するには、VLAN ID を指定します。

注:

リソースプールを構成する Citrix Hypervisor サーバーでは、静的な IP アドレスを設定するか、DNS で正しく名前解決されるように設定しておく必要があります。DHCP を使用する場合は、静的 DHCP 予約ポリシーが設定されていることを確認してください。

14. ホスト名を設定して、DNS 設定を手作業で行うか DHCP を使って自動的に行うかを指定します。

[Hostname Configuration] セクションでは、ホスト名を指定します。**[Automatically set via DHCP]** を選択すると、IP アドレスだけでなくホスト名が DHCP サーバーから自動的に取得されます。特定のホスト名を指定する場合は、**[Manually specify]** を選択し、フィールドにサーバーのホスト名を入力します。

注:

特定のホスト名を手動で指定する場合は、完全修飾ドメイン名 (FQDN) ではなく、ホスト名のみを入力します。FQDN を入力すると、外部認証に失敗する場合や、Citrix Hypervisor サーバーが別の名前前で AD に追加される場合があります。

[DNS Configuration] セクションでは、**[Automatically set via DHCP]** を選択します。これにより、DHCP を使用してネームサービス設定が取得されます。**[Manually specify]** を選択した場合は、プライマリ (必須)、セカンダリ (オプション)、およびターシャリ (オプション) の DNS サーバーの IP アドレスを入力します。

[OK] を選択して続行します。

15. 地理的領域と都市名でタイムゾーンを選択します。この一覧では、対象ロケールの先頭の文字を入力すると、その文字で始まる最初のエントリにカーソルが移動します。**[OK]** を選択して続行します。

16. XenServer ホストのローカルの日時として、NTP による自動設定または手動設定を選択します。選択したら、**[OK]** を選択して続行します。

- NTP を使用する場合は、**[NTP is configured by my DHCP server]** を選択するか、下のフィールドに1つ以上の NTP サーバーの名前または IP アドレスを入力します。**[OK]** を選択して続行します。
- 日時設定として **[Manual time entry]** を選択した場合、インストール中に日時を入力するための画面が表示されます。**[OK]** を選択して続行します。

注:

Citrix Hypervisor は、サーバーの BIOS の時間設定が UTC の現在時刻であることを想定して動作します。

17. **[Install] Citrix Hypervisor** を選択します。

インストールプロセスが開始されます。これには数分かかる場合があります。

18. 次の画面では、サブメンタルパックをインストールするかどうかを選択する画面が表示されます。ハードウェアの供給元からサブメンタルパックが提供されている場合は、**[Yes]** を選択します。

サブメンタルパックのインストールを選択した場合、ディスクの挿入を求めるメッセージが表示されます。Citrix Hypervisor のインストールメディアを取り出して、適切なメディアを挿入します。**[OK]** を選択します。

[Use media] を選択して続行すると、Linux Pack またはサブメンタルパックのインストールが開始されます。

インストールするパックごとに繰り返します。

19. **[Installation Complete]** 画面が表示されたら、インストールメディアを取り出して（USB または CD からインストールしている場合）、**[OK]** を選択してサーバーを再起動します。

サーバーが再起動すると、Citrix Hypervisor のシステム設定コンソールである **xsconsole** が表示されます。**xsconsole** からローカルシェルにアクセスするには、**Alt+F3** キーを押します。シェルから **xsconsole** に戻るには、**Alt+F1** キーを押します。

注:

表示された IP アドレスを控えておきます。この IP アドレスは、XenCenter を Citrix Hypervisor サーバーに接続する時に使用します。

インストール XenCenter

XenCenter は、Citrix Hypervisor サーバーとネットワークで接続されている Windows マシン上にインストールします。このシステムに .NET Framework バージョン 4.6 以上がインストールされていることを確認してください。

XenCenter をインストールするには:

1. XenCenter の最新バージョンを [Citrix Hypervisor ダウンロードページ](#) からダウンロードしてインストールします。
2. インストーラーの `.msi` ファイルを起動します。
3. インストールウィザードの指示に従って、XenCenter をインストールします（必要な場合はインストール先を変更します）。

XenCenter の使用について詳しくは、[XenCenter ドキュメント](#) を参照してください。

XenCenter による Citrix Hypervisor サーバーへの接続

XenCenter を使って **Citrix Hypervisor** サーバーに接続するには、次の手順に従います:

1. XenCenter を起動します。XenCenter が起動すると、**[ホーム]** タブが開きます。
2. **[サーバーの追加]** アイコンをクリックします。

3. [サーバー] フィールドに、Citrix Hypervisor サーバーの IP アドレスを入力します。Citrix Hypervisor のインストール時に設定したルートユーザー名とパスワードを入力します。[追加] をクリックします。
4. ホストを初めて XenCenter に追加すると、[接続状態の保存と復元] ダイアログボックスが開きます。このダイアログボックスでは、ホストの接続情報を保持して、ホスト接続が自動的に復元されるように設定できます。この設定は、XenCenter または Windows のレジストリエディターを使用して変更できます。
XenCenter では、[ツール] メニューの [オプション] を選択し、[オプション] ダイアログボックスの [保存と復元] ページで適切な変更を行います。[OK] をクリックして変更を保存します。
Windows のレジストリエディターを使用してこれを行うには、キー `HKEY_LOCAL_MACHINE\Software\Citrix\XenCenter` に移動し、文字列値 `true` または `false` で `AllowCredentialSave` という名前のキーを追加します。

インストールと展開のシナリオ

December 30, 2019

ここでは、以下の一般的なインストールおよび展開のシナリオについて説明します：

- ローカルストレージを備えた 1 つまたは複数の Citrix Hypervisor サーバー
- 共有ストレージを持つ Citrix Hypervisor サーバーのリソースプール：
 - 共有 NFS ストレージを備えた 2 つ以上の Citrix Hypervisor サーバー
 - 共有 iSCSI ストレージを備えた 2 つ以上の Citrix Hypervisor サーバー

ローカルストレージを備えた **Citrix Hypervisor** サーバー

Citrix Hypervisor の最もシンプルな展開シナリオは、ローカルストレージを備えた 1 つまたは複数の Citrix Hypervisor サーバー上で仮想マシンを実行する方法です。

注：

Citrix Hypervisor サーバー間での仮想マシンのライブマイグレーションは、共有ストレージがある場合にのみ使用できます。ただし、ストレージライブマイグレーションは引き続き利用できます。

基本的なハードウェア要件

- ローカルストレージを備えた 1 つまたは複数の 64 ビット x86 サーバー
- Citrix Hypervisor サーバーと同じネットワーク上にある 1 つまたは複数の Windows システム

基本手順

1. Citrix Hypervisor サーバーソフトウェアを各サーバーにインストールする。
2. XenCenter を Windows システムにインストールする。
3. XenCenter で Citrix Hypervisor サーバーに接続する。

XenCenter で Citrix Hypervisor サーバーに接続すると、そのホストのローカルディスク上にストレージが自動的に設定されます。

共有ストレージを持つ **Citrix Hypervisor** サーバーのリソースプール

リソースプールとは、複数の Citrix Hypervisor サーバーを単一の管理対象としてグループ化したものです。リソースプールに共有ストレージを接続すると、十分なメモリを備えた任意の Citrix Hypervisor サーバー上で仮想マシンを起動できるようになります。さらに、最小限のダウンタイムで、実行中の仮想マシンを別のホスト上に動的に移行することもできます（「ライブマイグレーション」とも呼ばれます）。Citrix Hypervisor サーバーでハードウェア障害が生じた場合、管理者は、そのホスト上の仮想マシンを、同じリソースプール内の別のホスト上で再起動させることができます。

高可用性（HA）機能が有効な場合は、障害が生じたホスト上の仮想マシンを自動的に他のホスト上に移行させることができます。

プールのホスト間で共有ストレージをセットアップするには、ストレージリポジトリを作成する必要があります。Citrix Hypervisor ストレージリポジトリ（SR）は仮想ディスクが格納されるストレージコンテナです。仮想ディスクと同様に、ストレージリポジトリは Citrix Hypervisor ホストに依存しない永続的なオンディスクオブジェクトです。ストレージリポジトリは、ローカルディスクデバイスや共有ネットワークストレージを含む、内蔵および外付けのさまざまな種類の物理ストレージデバイス上に作成できます。以下の種類のストレージを使用して、ストレージリポジトリを作成できます：

- NFS VHD ストレージ
- ソフトウェア iSCSI ストレージ
- ハードウェア HBA ストレージ
- GFS2 ストレージ

ここでは、Citrix Hypervisor サーバーのリソースプールのストレージリポジトリとして、NFS と iSCSI という 2 種類の共有ストレージを使用します。これらの NFS または iSCSI ストレージは、ストレージリポジトリを作成する前に設定しておく必要があります。設定方法は、使用するストレージソリューションによって異なります。詳しくは、ベンダーのドキュメントを参照してください。使用するストレージの種類に限らず、共有ストレージを提供するサーバーに静的な IP アドレスを設定するか、DNS で正しく名前解決されるように設定しておく必要があります。共有ストレージのセットアップについて詳しくは、「[ストレージ](#)」を参照してください。

共有ストレージを追加する前に、リソースプールを作成しておくことをお勧めします。プールの要件とセットアップ手順については、XenCenter のドキュメントの「[リソースプールの要件](#)」または「[ホストとリソースプール](#)」を参照してください。

共有 **NFS** ストレージを備えた **Citrix Hypervisor** サーバー

基本的なハードウェア要件

- ローカルストレージを備えた 2 つ以上の 64 ビット x86 サーバー
- Citrix Hypervisor サーバーと同じネットワーク上にある 1 つまたは複数の Windows システム
- NFS で共有ディレクトリをエクスポートするサーバー

基本手順

1. Citrix Hypervisor サーバーソフトウェアを各サーバーにインストールする。
2. XenCenter を Windows システムにインストールする。
3. XenCenter で Citrix Hypervisor サーバーに接続する。
4. Citrix Hypervisor サーバーのプールを作成する。
5. NFS サーバーを設定する。
6. プールレベルで NFS 共有上にストレージリポジトリを作成する。

NFS ストレージの設定

ストレージリポジトリを作成する前に、NFS ストレージを設定する必要があります。プールで使用される NFS 共有には、静的な IP アドレスを設定するか、DNS での名前解決を正しく設定する必要があります。また、NFS サーバーには、NFS クライアント（プールの Citrix Hypervisor サーバーなど）でマウント可能な 1 つまたは複数のターゲットが存在している必要があります。設定方法は、使用するストレージソリューションによって異なります。詳しくは、ベンダーのドキュメントを参照してください。

XenCenter を使用してプールレベルで **NFS** 共有上にストレージリポジトリを作成するには:

1. リソースペインでリソースプールを選択します。XenCenter のツールバーで [新規ストレージ] をクリックします。[新規ストレージリポジトリ] ウィザードが開きます。
2. [仮想ディスクストレージ] で、ストレージの種類として [NFS VHD] を選択します。[次へ] をクリックして続行します。
3. 新しいストレージリポジトリの名前と、それを格納する共有の名前を入力します。指定した場所に既存の NFS ストレージリポジトリがあるかどうかを確認するには、[スキャン] をクリックします。

注:

指定したパスがプール内のすべての Citrix Hypervisor サーバーにエクスポートされるように NFS サーバーを設定しておく必要があります。

4. [完了] をクリックします。

新しいストレージリポジトリが作成され、リソースペインのリソースプールの下に追加されます。

xe CLI を使用してプールレベルで **NFS** 共有上にストレージリポジトリを作成する

1. プール内の任意の Citrix Hypervisor サーバーで、コンソールを開きます。
2. 次のコマンドを実行して、`server:/path` にストレージリポジトリを作成します:

```
1 xe sr-create content-type=user type=nfs name-label=sr_name= \  
2   shared=true device-config:server=server \  
3   device-config:serverpath=path
```

ここで、`device-config-server` に NFS サーバーの名前を指定し、`device-config-serverpath` にそのサーバー上のパスを指定します。`shared` に `true` を指定しているため、プール内のすべてのホストにこの共有ストレージが自動的に接続されます。また、このプールに後で追加するすべてのホストにもこの共有ストレージが自動的に接続されます。作成されたストレージリポジトリの UUID がコンソールに出力されま

3. `pool-list` コマンドを実行して、プールの UUID を確認します。
4. 次のコマンドを実行して、このストレージリポジトリをプール全体のデフォルトとして設定します:

```
1 xe pool-param-set uuid=pool_uuid \  
2   default-SR=storage_repository_uuid
```

共有ストレージがプールのデフォルトとして設定されたため、今後作成するすべての仮想マシンのディスクがデフォルトでこのストレージリポジトリに作成されます。

共有 iSCSI ストレージを備えた Citrix Hypervisor サーバー

基本的なハードウェア要件

- ローカルストレージを備えた 2 つ以上の 64 ビット x86 サーバー
- Citrix Hypervisor サーバーと同じネットワーク上にある 1 つまたは複数の Windows システム
- iSCSI で共有ディレクトリを提供するサーバー

基本手順

1. Citrix Hypervisor サーバーソフトウェアを各サーバーにインストールする。
2. XenCenter を Windows システムにインストールする。

3. XenCenter で Citrix Hypervisor サーバーに接続する。
4. Citrix Hypervisor サーバーのプールを作成する。
5. iSCSI ストレージを設定する。
6. 必要に応じて、iSCSI デバイスの複数のイニシエータを有効にする。
7. 必要に応じて、各 Citrix Hypervisor サーバーに iSCSI Qualified Name (IQN) を設定する。
8. プールレベルで iSCSI 共有上にストレージリポジトリを作成する。

iSCSI ストレージの設定

ストレージリポジトリを作成する前に、iSCSI ストレージを設定する必要があります。プールで使用される iSCSI ストレージには、静的な IP アドレスを設定するか、DNS での名前解決を正しく設定する必要があります。また、仮想マシンストレージ用として SAN 上の iSCSI ターゲットを提供し、それを認識して接続できるように Citrix Hypervisor サーバーを設定する必要があります。これを行うには、各 Citrix Hypervisor サーバー上の各 iSCSI イニシエータと iSCSI ターゲットに固有の IQN を指定します。詳しくは、ベンダーのドキュメントを参照してください。

各 Citrix Hypervisor サーバーの iSCSI IQN の設定

Citrix Hypervisor をインストールすると、そのホストに固有の IQN が自動的に関連付けられます。この IQN を変更する必要がある場合は、そのホストのコンソールで次のコマンドを実行します：

```
1 xe-set-iscsi-iqn iscsi_iqn
```

または、xe CLI を使用して次のコマンドを実行することもできます：

```
1 xe host-param-set uuid=host_uuid other-config-iscsi_iqn=iscsi_iqn
```

XenCenter を使用してプールレベルで **iSCSI** 共有上にストレージリポジトリを作成するには：

警告：

iSCSI および NetApp ストレージで Citrix Hypervisor ストレージリポジトリを作成すると、そのボリューム上のすべてのデータが破棄されます。

1. リソースペインでリソースプールを選択します。XenCenter のツールバーで [新規ストレージ] をクリックします。[新規ストレージリポジトリ] ウィザードが開きます。
2. [仮想ディスクストレージ] で、ストレージの種類として [ソフトウェア iSCSI] を選択します。[次へ] をクリックして続行します。
3. 新しいストレージリポジトリの名前と、iSCSI ターゲットの IP アドレスまたは DNS 名を入力します。

注:

プール内のすべての Citrix Hypervisor サーバーが LUN にアクセスできるように iSCSI ストレージターゲットを設定しておく必要があります。

4. iSCSI ターゲットが CHAP 認証を使用するように設定されている場合は、[CHAP を使用する] チェックボックスをオンにして詳細を入力します。
5. [IQN の検出] をクリックして、[ターゲット IQN] ボックスの一覧から iSCSI ターゲットの IQN を選択します。

警告:

iSCSI ターゲットおよびプール内のすべてのホストで、固有の IQN が設定されている必要があります。

6. [LUN の検出] をクリックして、[ターゲット LUN] ボックスの一覧から LUN を選択します。この LUN にストレージリポジトリが作成されます。

警告:

各 iSCSI ストレージリポジトリは全体が単一の LUN に含まれる必要があり、複数の LUN にまたがることはできません。また、選択した LUN 上の既存のデータはすべて破棄されます。

7. [完了] をクリックします。

新しいストレージリポジトリが作成され、リソースペインのリソースプールの下に追加されます。

xe CLI を使用してプールレベルで **iSCSI** 共有上にストレージリポジトリを作成するには:

警告:

iSCSI および NetApp ストレージで Citrix Hypervisor ストレージリポジトリを作成すると、そのボリューム上のすべてのデータが破棄されます。

1. プール内の任意のサーバーのコンソールで、次のコマンドを実行します:

```
1 xe sr-create name=label=name_for_sr \  
2     host-uuid=host_uuid device-config:target=  
3     device-config:targetIQN=iscsi_target_iqn device-config:SCSIid=  
4     scsi_id \  
5     content-type=user type=lvmoiscsi shared=true
```

`device-config:target` 引数では、iSCSI サーバーの名前または IP アドレスを指定します。`shared` に `true` を指定しているため、プール内のすべてのホストにこの共有ストレージが自動的に接続されます。また、このプールに後で追加するすべてのホストにもこの共有ストレージが自動的に接続されます。

このコマンドにより、作成されたストレージリポジトリの UUID が返されます。

2. `pool-list` コマンドを実行して、プールの UUID を確認します。
3. 次のコマンドを実行して、このストレージリポジトリをプール全体のデフォルトとして設定します:

```
1 xe pool-param-set uuid=pool_uuid default-SR=iscsi_shared_sr_uuid
```

共有ストレージがプールのデフォルトとして設定されたため、今後作成するすべての仮想マシンのディスクがデフォルトでこのストレージリポジトリに作成されます。

既存バージョンからのアップグレード

December 30, 2019

ここでは、XenCenter または xe CLI を使用して Citrix Hypervisor にアップグレードする方法について説明します。リソースプールやスタンドアロンの Citrix Hypervisor サーバーを自動的（XenCenter の「プールのローリングアップグレードウィザード」を使用）にアップグレードしたり、手作業でアップグレードしたりする手順について説明します。

シトリックスでは以前のバージョンの Citrix Hypervisor から Citrix Hypervisor 8.1 への移行に使用できるアップグレードおよびアップデート機能を提供します。アップグレードまたはアップデート機能を使用すると、フルインストールプロセスを完了する必要なく、Citrix Hypervisor 8.1 を適用することができます。Citrix Hypervisor 8.1 にアップグレードまたはアップデートすると、既存の仮想マシン、ストレージリポジトリ、構成が保持されます。

- 基本インストール **ISO** で XenServer 7.6、7.1 Cumulative Update 2 (LTSR) 、または 7.0 を Citrix Hypervisor 8.1 にアップグレードできます。0 ここでは、Citrix Hypervisor 8.1 にアップグレードする方法について説明します。

注:

XenServer 7.1 または 7.1 Cumulative Update 1 から Citrix Hypervisor 8.1 へのアップグレードはサポートされていません。アップグレードする前に、累積更新プログラムが Citrix Hypervisor 7.1 に適用されていることを確認してください。

- インストール **ISO** のアップデートを使用して、Citrix Hypervisor 8.1 を Citrix Hypervisor 8.0 へのアップデートとして適用できます。詳しくは、「[ホストのアップデート](#)」を参照してください。
- XenServer の他のすべてのバージョンでは、直接 Citrix Hypervisor 8.1 にアップグレードすることはできません。この場合、最初に Citrix Hypervisor をより新しいバージョンにアップグレードしてそのバージョンを 8.1 にアップグレードするか、基本インストール **ISO** を使用してクリーンインストールを実行します。詳しくは、「[インストール](#)」を参照してください。

注:

以前の Citrix Hypervisor または XenServer のインストールから仮想マシンを保持するには、仮想マシンをエクスポートし、それを Citrix Hypervisor 8.1 のクリーンインストールにインポートします。Citrix Hypervisor または XenServer のサポートされているバージョンからエクスポートされた仮想マシンは、Citrix Hypervisor 8.1 にインポートできます。詳しくは、「[仮想マシンのインポートとエクスポート](#)」を参照

してください。

はじめに

アップグレードを開始する前に、次の情報を確認してください。アップグレードプロセスを確実に成功させるために必要な手順を実行します。

- Citrix Hypervisor サーバー特に Citrix Hypervisor サーバーのプールのアップグレードは、慎重に計画し、実行する必要があります。既存のデータが失われないように、次のいずれかを行います：
 - アップグレードパスを慎重に決定します。
 - XenCenter の「プールのローリングアップグレードウィザード」を使用します。また、インストーラの画面で必ずアップグレードオプションを選択してください。
- ホストのアップグレードに XenCenter を使用している場合は、XenCenter の最新のバージョンをダウンロードしてインストールします。たとえば、Citrix Hypervisor 8.1 にアップグレードする場合は、Citrix Hypervisor 8.1 と動作する XenCenter を使用する必要があります。以前のバージョンの XenCenter を使用した新しいバージョンの Citrix Hypervisor へのアップグレードはサポートされていません。
- 手動によるアップグレード処理では、SAN ブート設定が保持されません。ISO または PXE を使用してアップグレードする場合は、`multipathd` が正しく設定されるように、後述のインストール手順に従う必要があります。詳しくは、「[SAN 環境からの起動](#)」を参照してください。
- 休止スナップショットはサポートされなくなりました。休止スナップショットを作成する既存のスナップショットスケジュールがある場合、これらのスナップショットスケジュールはアップグレード後に失敗します。スナップショットの作成を継続するには、アップグレードを実行する前に既存のスケジュールを削除し、非休止スナップショットを作成する新しいスケジュールを作成します。

プールのローリングアップグレード

Citrix Hypervisor では、プールのローリングアップグレードを実行できます。プールのローリングアップグレードでは、プールのサービスやリソースの提供を中断することなく、そのプール内のすべてのホストをアップグレードできます。このアップグレード方法では、同時に複数の Citrix Hypervisor サーバーがオフラインになることはありません。この間、アップグレード対象のホスト上で実行中の仮想マシンは自動的にほかのホスト上に移行されます。

注:

プールのローリングアップグレード中も仮想マシンの実行を続けるには、プールに共有ストレージが必要です。プールに共有ストレージがない場合、仮想マシンはライブマイグレーションができないため、アップグレード前に仮想マシンを停止する必要があります。

ストレージライブマイグレーションは、プールのローリングアップグレードではサポートされていません。

プールのローリングアップグレードは、XenCenter または xe CLI を使用して実行できます。XenCenter を使用している場合は、プールのローリングアップグレード (RPU) ウィザードの使用をお勧めします。このウィザードでは、

アップグレードパスが自動的に構成され、アップグレード手順が順番に表示されます。xe CLI では、まずアップグレードパスを決定して、実行中の仮想マシンを Citrix Hypervisor サーバー間でライブマイグレーションしながらプールのローリングアップグレードを手動で実行する必要があります。

プールのローリングアップグレードウィザードは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスできるユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

重要:

SAN ブート環境では、プールのローリングアップグレードを実行しないでください。SAN ブート環境でのアップグレードについては、「[SAN 環境からの起動](#)」を参照してください。

XenCenter のプールのローリングアップグレードウィザードを使用して **Citrix Hypervisor** サーバーをアップグレードする

プールのローリングアップグレード (RPU) ウィザードでは、Citrix Hypervisor サーバー、プールまたはスタンドアロンのホストを Citrix Hypervisor の最新バージョンにアップグレードできます。

[プールのローリングアップグレード] ウィザードでは、アップグレードパスが自動的に構成され、アップグレード手順が順番に表示されます。リソースプールでは、プールマスタが最初にアップグレードされ、ほかのホストが順番にアップグレードされます。アップグレードの前に、ウィザードによりいくつかの事前チェックが実行されます。これにより、高可用性などのプールレベルの機能が一時的に無効になっており、個々のホストでアップグレードの準備が完了しているかどうかを確認されます。ローリングアップグレードでは、プール内のホストが1台ずつオフラインになり、アップグレードがインストールされます。そのホスト上で実行中の仮想マシンは、自動的にほかのホスト上に移行されます。

プールのローリングアップグレードウィザードでは、新しいバージョンの Citrix Hypervisor にアップグレードするときに、利用可能な Hotfix を自動的に適用することもできます。これにより、スタンドアロンのホストまたはプールを、最小限の再起動回数で最新の状態にすることができます。この機能を使用するには、アップグレードプロセス中にインターネットに接続する必要があります。

Citrix Hypervisor 8.1 と共に発行された XenCenter を使用して、サポート対象バージョンの Citrix Hypervisor または XenServer からアップグレードする場合は、Hotfix 自動適用機能を利用できます。

注:

XenCenter を使用したプールのローリングアップグレードは、Citrix Hypervisor Premium Edition のユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスできるユーザーが使用できます。

このウィザードでは、アップグレードモードとして [手動モード] または [自動モード] を選択できます。

- 手動モードでは、各ホスト上で Citrix Hypervisor インストーラーを順次手作業で実行して、ホストのシリアルコンソールに表示されるメッセージに従ってアップグレードします。アップグレードが開始されると、アッ

ブグレード対象の各ホストについて、XenCenter インストールメディアの挿入またはネットワークブートサーバーの指定を確認するメッセージが XenCenter に表示されます。

- 自動モードでは、HTTP、NFS、または FTP サーバー上のインストールファイルにより、プール内のすべてのホストが自動的にアップグレードされます。このモードでは、インストールメディアを挿入したり、ホストを再起動したり、各ホストのシリアルコンソールに表示されるメッセージに従って操作したりする必要はありません。この方法では、インストールメディアの内容を HTTP、NFS、または FTP サーバー上にコピーしておく必要があります。

アップグレードの前に

アップグレードを行う前に、以下の準備を行います：

- Citrix Hypervisor 8.1 と動作する XenCenter を、[Citrix Hypervisor 製品ダウンロードページ](#)からダウンロードしてインストールします。以前のバージョンの XenCenter を使用した新しいバージョンの Citrix Hypervisor へのアップグレードはサポートされていません。
- `pool-dump-database xe` CLI コマンドを使用して、アップグレード前のプールをバックアップしておくことを強くお勧めします。詳しくは、「[コマンドラインインターフェイス](#)」を参照してください。これにより、仮想マシンデータを失うことなく、ローリングアップグレードを中断して元の状態に戻すことも可能になります。
- 各サーバーで、アップグレードに必要なメモリが使用可能であることを確認してください。

一般的に、プール内のホストの数を N とすると、プール内で実行されているすべての仮想マシンに十分な量のメモリが $(N - 1)$ 台のホストで提供されなければなりません。このため、不要な仮想マシンをすべてサスペンド状態にしておくことをお勧めします。

- プールに実行されている vGPU 対応仮想マシンがある場合、仮想マシンの実行中にプールを移行するための次の手順を完了してください：
 - 使用している GPU がアップグレード先のバージョンでサポートされていることを確認してください。
 - 現在のバージョンの Citrix Hypervisor およびアップグレード先のバージョンの Citrix Hypervisor の両方で使用できる NVidia GRID ドライバーを見つけます。可能であれば、入手可能な最新のドライバーを選択してください。
 - 使用中の Citrix Hypervisor サーバーに新しい GRID ドライバーをインストールして、vGPU 対応仮想マシンに一致するゲストドライバーをインストールします。
 - アップグレード先の Citrix Hypervisor のバージョンに一致するバージョンの GRID ドライバーがあることも確認してください。プールのローリングアップグレードプロセスで、これらのドライバーをサブリメンタルパックとしてインストールするように求められます。

プールのローリングアップグレードウィザードでは、以下の項目がチェックされます。アップグレード前に、以下の項目を確認してください：

- プール内の各仮想マシンの CD/DVD ドライブを空にします。

- 高可用性を無効にします。

アップグレードプロセス

XenCenter プールのローリングアップグレードウィザードを使用して **Citrix Hypervisor** ホストをアップグレードするには:

1. プールのローリングアップグレードウィザードを開きます。これを行うには、[ツール] メニューの [プールのローリングアップグレード] を選択します。
2. [はじめに] ページの注意事項を確認して、[次へ] をクリックします。
3. アップグレードするリソースプールまたは個々のホストを選択して、[次へ] をクリックします。
4. 次のいずれかのモードを選択します:
 - 既存の HTTP、NFS、または FTP サーバー上のインストールファイルを使った自動アップグレードを行う場合は [自動モード]
 - USB/CD/DVD ドライブのインストールメディアまたはネットワークブートサーバーを使った手動アップグレードを行う場合は [手動モード]

注:

[手動モード] を選択した場合、各ホスト上で Citrix Hypervisor インストーラを順次実行して、ホストのシリアルコンソールに表示されるメッセージに従ってアップグレードする必要があります。アップグレードが開始されると、アップグレード対象の各ホストについて、Citrix Hypervisor インストールメディアの挿入またはネットワークブートサーバーの指定を確認するメッセージが XenCenter に表示されます。

5. 新しいバージョンにアップグレードした後に、XenCenter で自動的に最小限のアップデート (Hotfix) をダウンロードしてインストールするかを選択します。アップデートを適用するオプションは、デフォルトで選択されています。ただし、アップデートをダウンロードしてインストールするには、インターネット接続が必要です。
6. アップグレードモードを選択したら、[事前チェックの実行] をクリックします。
7. 事前チェックにより問題が見つかった場合は、適切な解決処置を行います。[すべて解決] をクリックすると、XenCenter により問題の解決が試行されます。

すべての問題を解決したら、[次へ] をクリックします。
8. Citrix Hypervisor インストールメディアを用意します。

[自動モード] を選択した場合は、ネットワーク上のインストールメディアに接続するための情報を入力します。ネットワークインストールファイルの場所として [HTTP]、[NFS] または [FTP] を選択して、URL、ユーザー名、およびパスワードを入力します。

注:

- 1 - [FTP] を選択する場合は、URLのファイルパスセクションにある先頭のスラッシュをエスケープしてください。
- 2
- 3 - HTTPまたはFTPサーバーにアクセスするための資格情報が必要な場合は、HTTPまたはFTPサーバーに関連付けられているユーザー名およびパスワードを入力します。Citrix Hypervisorプールに関連付けられているユーザー名とパスワードは入力しないでください。
- 4
- 5 - Citrix Hypervisor パッシブモードのみでFTPをサポートします。

[手動モード] を選択した場合は、表示されるアップグレードプランおよび手順を確認します。

[アップグレードの開始] をクリックします。

9. アップグレードを開始すると、各ホストのアップグレードに必要な手順がウィザードに表示されます。この手順に従って、プールのすべてのホストをアップグレードおよびアップデートします。

vGPU 対応仮想マシンがある場合、サプリメンタルパックを指定するオプションを選択する段階で、vGPU 対応仮想マシンの一致する GRID ドライバーをアップロードします。アップグレード先の Citrix Hypervisor バージョンに対応したバージョンのドライバーをアップロードしてください。

注:

何らかの理由でアップグレードまたはアップデートプロセスが失敗した場合、プールのローリングアップグレードウィザードはプロセスを停止します。これによって、[再試行] ボタンをクリックして問題を修正し、アップグレードまたはアップデートプロセスを再開できます。

10. アップグレードが完了すると、[プールのローリングアップグレード] ウィザードにその結果が表示されます。[完了] をクリックしてウィザードを終了します。

xe CLI を使用して Citrix Hypervisor サーバーをアップグレードする

xe CLI を使用してプールをローリングアップグレードする場合は、慎重に計画する必要があります。以下の説明をよく読んでからアップグレードを始めてください。

アップグレードパスを計画する

以下の点に注意してください:

- 仮想マシンは、Citrix Hypervisor の以前のバージョンを実行している Citrix Hypervisor サーバーから同じバージョン以上を実行しているホストにのみ移行できます (たとえば、バージョン 7.0 からバージョン 7.1 Cumulative Update 2 またはバージョン 7.1 Cumulative Update 2 からバージョン 8.1)。

アップグレード済みのホストから、アップグレード前の Citrix Hypervisor を実行しているホストに仮想マシンを移行することはできません（バージョン 8.1 からバージョン 7.1 Cumulative Update 2 への移行など）。仮想マシンを移行するための容量が Citrix Hypervisor サーバーにあることを確認してください。

- 混在モード（Citrix Hypervisor の複数のバージョンが共存する状態）のプールを必要以上に継続運用することは極力避けるよう、強くお勧めします。ローリングアップグレード中のプールは、パフォーマンスが低下します。
- アップグレードの間、一部の制御機能は使用できなくなります。制御操作はしないでください。仮想マシンは通常どおり動作を続けますが、移行を除く主な仮想マシン操作（シャットダウン、コピー、エクスポートなど）を実行することは避けてください。特に、仮想ディスクの追加、削除、またはサイズ変更などのストレージ関連の操作を行うと、予期せぬ問題が発生することがあります。
- 常にプールマスタを最初にアップグレードしてください。また、アップグレード時に、XenCenter でプールマスタを保守モードに切り替えないでください。プールマスタが保守モードになると、新しいプールマスタが選出されてしまいます。
- ホストをアップグレードしたら、アップグレードバージョンの Citrix Hypervisor 用にリリースされている Hotfix を適用してから仮想マシンを移行します。
- `pool-dump-database xe` CLI コマンドを使用して、アップグレード前のプールをバックアップしておくことを強くお勧めします。詳しくは、「[コマンドラインインターフェイス](#)」を参照してください。これにより、仮想マシンデータを失うことなく、ローリングアップグレードを中断して元の状態に戻すことも可能になります。何らかの理由でローリングアップグレードを元に戻す必要が生じた場合、仮想マシンのシャットダウンが必要になることがあります。アップグレード済みの Citrix Hypervisor サーバーからアップグレード前の Citrix Hypervisor ホストに仮想マシンを移行することはできないため、この操作が必要です。

プールをローリングアップグレードする前に

- XenCenter を使用する場合は、XenCenter を最新バージョンにアップグレードする。最新バージョンの XenCenter を使用して、古いバージョンが動作する Citrix Hypervisor サーバーを管理することもできます。
- プール内の各仮想マシンの CD/DVD ドライブを空にする。方法については、「[単一 Citrix Hypervisor サーバーをアップグレードする前に](#)」を参照してください。
- 高可用性を無効にします。

xe CLI を使用してプールのローリングアップグレードを実行する

1. プールマスタを最初にアップグレードします。`host-disable` コマンドを使用して、プールマスタを無効にします。これにより、このホスト上で新しい仮想マシンが起動することを防ぎます。
2. プールマスタ上で仮想マシンが実行されていないことを確認します。実行されている場合は、シャットダウンまたはサスペンド状態にするか、プール内のほかのホストに移行します。

仮想マシンを特定のホストに移行するには、`vm-migrate`コマンドを使用します。`vm-migrate`コマンドでは、移行対象の仮想マシンおよび移行先ホストを指定できます。

すべての仮想マシンをプール内のほかのホストにライブマイグレーションするには、`host-evacuate`コマンドを使用します。`host-evacuate`コマンドでは、Citrix Hypervisor により移行先ホストが決定されま

3. プールマスタをシャットダウンします。

重要:

プールマスタのアップグレードが完了するまで、このホストに接続できなくなります。プールマスターをシャットダウンすると、プール内の他のホストが緊急モードに入ります。プールマスタへの接続が切断され、何回かの接続試行後も再接続できない場合に、そのプールのホストが緊急モードに切り替わります。仮想マシンはホストで引き続き緊急モードで実行されますが、制御操作はできません。

4. Citrix Hypervisor インストールメディア (USB またはネットワーク上のインストールファイル) からプールマスターを起動します。Citrix Hypervisor のインストール手順に従って操作し、アップグレードの画面まで進めます。[**Upgrade**] を選択します。詳しくは、「[インストール](#)」を参照してください。

警告:

- 1 - 既存のデータが失われないように、必ずアップグレードオプションを選択してください。
- 2
- 3 - プールマスタのアップグレードが中断された場合、または何らかの理由でアップグレードに失敗した場合は、アップグレードを続行しないでください。プールマスタを再起動して、正常なバージョンに復元してください。

プールマスタが再起動するとほかのホストの緊急モードが終了し、しばらくして通常のサービスが復元されます。

5. 新しいバージョンの Citrix Hypervisor 用にリリースされた Hotfix をプールマスタに適用します。
6. プールマスタ上でシャットダウン状態またはサスペンド状態にしておいた仮想マシンを起動または再開します。また、ほかのホストに移行しておいた仮想マシンを必要に応じてプールマスタに戻します。
7. 計画したアップグレードパスで次のアップグレード対象になっている Citrix Hypervisor サーバーを選択し、そのホストを無効にします。
8. そのホスト上で仮想マシンが実行されていないことを確認します。実行されている場合は、シャットダウンまたはサスペンド状態にするか、プール内のほかのホストに移行します。
9. ホストをシャットダウンします。
10. 上記の手順 4. のプールマスタと同様の手順で、ホストをアップグレードします。

注:

プールマスター以外のホストのアップグレードが中断された場合、またはアップグレードに失敗した場合は、ホストを復元する必要はありません。この場合、`host-forget` コマンドを実行してそのホストの接続を消去し、Citrix Hypervisor を再インストールしてください。その後で、`pool-join` コマンドを使用してそのホストをプールに追加します。

11. 新しいバージョンの Citrix Hypervisor 用にリリースされた Hotfix をホストに適用します。
12. ホスト上でシャットダウン状態またはサスペンド状態にしておいた仮想マシンを起動または再開します。また、ほかのホストに移行しておいた仮想マシンを必要に応じて元のホストに戻します。
13. プール内の残りのホストについて、手順 6～10 を繰り返します。

xe CLI を使用して単一の Citrix Hypervisor サーバーをアップグレードする

単一の Citrix Hypervisor サーバーをアップグレードする前に

スタンドアロンの Citrix Hypervisor サーバーをアップグレードする前に、そのホスト上で実行されている仮想マシンをシャットダウンまたはサスペンドする必要があります。仮想マシンをサスペンドする場合は、その仮想マシンの CD/DVD ドライブを空にしておく必要があります。CD/DVD ドライブにディスクが挿入されたまま仮想マシンを一時停止した場合、ホストのアップグレード後にその仮想マシンを再開できなくなることがあります。

仮想マシンの CD/DVD ドライブを空にするとは、ISO イメージや Citrix Hypervisor サーバーの物理 CD/DVD が仮想マシンにマウントされていない状態にすることです。また、Citrix Hypervisor サーバーの物理 CD/DVD ドライブに仮想マシンが接続されていないことを確認する必要があります。

xe CLI を使用して仮想マシンの **CD/DVD** ドライブを空にするには:

1. CD/DVD ドライブが空になっていない仮想マシンを特定します。これを行うには、次のコマンドを実行します:

```
1 xe vbd-list type=CD empty=false
```

これにより、以下のように、CD/DVD ドライブが空でない仮想マシンの一覧が表示されます:

```
1  uuid ( RO ) : abae3997-39af-2764-04a1-ffc501d132d9
2  vm-uuid ( RO ): 340a8b49-866e-b27c-99d1-fb41457344d9
3  vm-name-label ( RO ): VM02_DemoLinux
4  vdi-uuid ( RO ): a14b0345-b20a-4027-a233-7cbd1e005ede
5  empty ( RO ): false
6  device ( RO ): xvdd
7
8  uuid ( RO ) : ec174a21-452f-7fd8-c02b-86370fa0f654
9  vm-uuid ( RO ): db80f319-016d-0e5f-d8db-3a6565256c71
10 vm-name-label ( RO ): VM01_DemoLinux
11 vdi-uuid ( RO ): a14b0345-b20a-4027-a233-7cbd1e005ede
```

```
12     empty ( RO): false
13     device ( RO): xvdd
```

この一覧から、仮想マシンの `uuid` (最初の項目) を控えておきます。

2. 次のコマンドを実行して、仮想マシンの CD/DVD ドライブを空にします:

```
1 xe vbd-eject uuid=uuid
```

xe CLI を使用して単一の **Citrix Hypervisor** サーバーをアップグレードする

xe CLI を使用して単一の **Citrix Hypervisor** サーバーをアップグレードするには:

1. 次のコマンドを実行して、アップグレードする Citrix Hypervisor サーバーを無効にします:

```
1 xe host-disable host-selector=host_selector_value
```

無効にした Citrix Hypervisor サーバー上では、仮想マシンの作成や起動ができなくなります。また、そのホスト上に仮想マシンを移行することもできません。

2. `xe vm-shutdown` または `xe vm-suspend` コマンドを実行して、アップグレードするホスト上で実行されている仮想マシンをシャットダウンまたは一時停止します。
3. `xe host-shutdown` コマンドを実行して、ホストをシャットダウンします。
4. Citrix Hypervisor のインストール手順に従って操作し、アップグレードの画面まで進めます。 **[Upgrade]** を選択します。詳しくは、「[インストール](#)」を参照してください。

警告:

既存のデータが失われないように、必ずアップグレードオプションを選択してください。

アップグレードインストールの場合、設定内容を再入力する必要はありません。アップグレードでは、新規インストールと同様の画面が表示されますが、いくつかの手順が省略され、既存のネットワーク設定やシステムの日時設定などは保持されます。

ホストが再起動してしばらくすると、通常のサービスが再開されます。

5. 新しいバージョンの Citrix Hypervisor 用にリリースされた Hotfix を適用します。
6. シャットダウンまたはサスペンドした仮想マシンを起動または再開します。

ホストのアップデート

December 30, 2019

通常、アップデートは、サービスの中断を最小限に抑えながら適用できます。XenCenter を使用して、すべてのアップデートを適用することをお勧めします。Citrix Hypervisor プールでは、XenCenter のアップデートのインストールウィザードを使用して、仮想マシンのダウンタイムなしにアップデートできます。アップデートのインストールウィザードを使用して、実行中の仮想マシンを自動的にほかのホストに移行しながら、ホストを 1 台ずつアップデートできます。

XenCenter は、Citrix Hypervisor と XenCenter のアップデートや新しいバージョンが使用できるかどうかを定期的に確認するように設定できます。この場合、すべてのアラートが通知ペインに表示されます。

アップデートの種類

Citrix Hypervisor では次の種類の更新プログラムを利用できます：

- **Current Release (CR)** は、最新リリース (CR) ストリームにおける Citrix Hypervisor のフルバージョンです。CR ストリームのサポート対象バージョンの Citrix Hypervisor にも、一部の CR をアップデートとして適用できます。
- **Hotfix** は通常、1 つまたは複数の特定の問題を解決するための修正プログラムを提供します。サポートされる Citrix Hypervisor または XenServer リリースのために Hotfix が提供されます。
- 累積更新プログラム。以前にリリースされた Hotfix を含み、新しいゲストやハードウェアのサポートに対応していることもあります。CU は、長期サービスリリース (LSTR) の Citrix Hypervisor リリースに適用されます。

パートナーから提供されたサプリメンタルパックも、Citrix Hypervisor へのアップデートとして適用できます。

最新リリース

Citrix Hypervisor 8.1 は Citrix Hypervisor の最新リリースです。次の表は、Citrix Hypervisor 8.1 をアップデートとして適用できる Citrix Hypervisor または XenServer の以前のバージョンです：

バージョン	Citrix Hypervisor 8.1 をアップデートとして適用可能？
Citrix Hypervisor 8.0	はい
XenServer 7.6	いいえ
XenServer 7.1 Cumulative Update 2	いいえ
XenServer 7.0	いいえ

Citrix Hypervisor 8.1 をアップデートとして適用できないバージョンの XenServer の場合は、基本インストール ISO を使用し、既存のインストールをアップグレードします。詳しくは、「[既存バージョンからのアップグレード](#)」を

参照してください。

注:

- ホストのアップデートに XenCenter を使用する場合、最初にインストールされている XenCenter を最新バージョンにアップデートする必要があります。
- 必ずプールマスターを先にアップデートしてから、その他のホストをアップデートします。
- 従来のディスクパーティションレイアウトを使用する既存の Citrix Hypervisor のインストールに、Citrix Hypervisor 8.1 をアップデートとして適用すると、領域不足でアップデートが失敗することがあります。この場合は、Citrix Hypervisor 8.1 を新規にインストールします。

Hotfix

Citrix Hypervisor 8.1 の特定の問題に対する Hotfix を提供することがあります。

Citrix Hypervisor 8.1 の Hotfix は、[Citrix Knowledge Center](#)から入手できます。こまめに Knowledge Center をチェックして、新しいアップデートが公開されていないかを確認することをお勧めします。または、<http://www.citrix.com/support/>でアカウントを登録することにより、Citrix Hypervisor へのアップデートのアラートメールをサブスクライブできます。

最新の CR の Hotfix は、すべての Citrix Hypervisor ユーザーに提供されます。ただし、サポート対象となっている以前の CR の Hotfix は、有効な Citrix カスタマーサクセスサービス (CSS) アカウントのユーザーのみが利用できます。

LTSR ストリームの Hotfix は、有効な CSS アカウントのユーザーが利用できます。詳しくは、「[ライセンス](#)」を参照してください。

累積更新プログラム (CU)

累積更新プログラムは、Citrix Hypervisor の LTSR で提供されます。累積更新プログラムは問題に対する Hotfix を提供し、新しいゲストやハードウェアのサポートが含まれることもあります。

累積更新プログラムは、有効な CSS アカウントのユーザーのみが利用できます。

アップデート用にプールを準備する

Citrix Hypervisor のアップデートは、Hotfix、累積更新プログラム (Cumulative Update)、または最新リリース (Current Release) として提供されます。これらのアップデートに付属するリリースノートの内容を慎重に確認してください。アップデートによっては、準備やアップデート後の操作など、インストール手順が異なる場合があります。以下のセクションでは、Citrix Hypervisor システムにアップデートを適用する場合の、一般的な注意点および手順について説明します。

Citrix Hypervisor プールにアップデートを適用する前に、以下の内容を慎重に確認してください:

- **Citrix Hypervisor 8.1 Hotfix** のみに該当: Hotfix を適用する前に、プール内のすべてのホストで Citrix Hypervisor 8.1 が実行されている必要があります。
- バックアップを作成してから、アップデートを適用してください。バックアップ手順については、「[障害回復とバックアップ](#)」を参照してください。
- プール内のすべてのサーバーを短期間でアップデートしてください。アップデート済みのサーバーとそうでないサーバーを同一プール内で混在運用することはサポートされません。このため、アップデート済みのサーバーとそうでないサーバーが同時に動作する時間が最小になるようにアップデートのスケジュールを決定する必要があります。
- 必ずプールマスタを最初にアップデートし、残りのサーバーを順次アップデートします。XenCenter のアップデートのインストールウィザードでは、このプロセスが自動的に管理されます。
- プール内のすべての Citrix Hypervisor サーバーにアップデートを適用したら、必要なドライバーディスクをアップデートしてからサーバーを再起動してください。
- 累積更新プログラムまたは最新リリースをホストに適用したら、関連する Hotfix をすべて適用してから仮想マシンを移行します。

アップデートする前に

- 完全な管理権限を持つアカウント（プール管理者やローカルのルートアカウントなど）でログインします。
- サスペンドする仮想マシンの CD/DVD ドライブを空にします。方法については、[単一の Citrix Hypervisor サーバーをアップグレードする前に](#)を参照してください。
- 高可用性が有効な場合は、無効にします。

プールにアップデートを適用する

XenCenter のアップデートインストールメカニズムでは、サポート Web サイトからアップデートをダウンロードして抽出し、アップデートのインストールウィザードを使用して複数のホストおよびプールに同時にアップデートを適用することができます。この処理の間に、アップデートのインストールウィザードでは、各サーバーに対して次の手順を実行します：

- サーバーから仮想マシンを移行します。
- サーバーを保守モードに切り替えます。
- サーバーにアップデートを適用します。
- 必要に応じてホストを再起動します。
- 元の仮想マシンをそのホスト上に戻します。

アップデートの事前チェック時に実行された問題解決処理（高可用性の無効化など）も、すべて復元されます。

アップデートのインストールウィザードでは、事前チェックと呼ばれる一連の処理を実行してから、アップデートプロセスを開始します。このチェックでは、プールの設定が有効であることが確認されます。また、ウィザードでは、

アップデートパスと仮想マシンの移行が自動的に管理されます。アップデートパスの決定および仮想マシンの移行を手作業で行うには、各ホストを個別にアップデートします。

アップデートを自動適用する

XenCenter では、サーバーを最新状態にするために必要な自動アップデートを適用できます。これらのアップデートを、1つまたは複数のプールに適用できます。自動アップデートを使用する場合、XenCenter は選択したプールまたはスタンドアロンサーバーを最新状態にするために必要な最小限のアップデートセットを適用します。XenCenter は、このプールまたはスタンドアロンサーバープールを最新状態にするために必要な再起動回数を最小限にします。可能な場合、XenCenter は最後に1回再起動を行うだけにします。詳しくは、「自動アップデートを適用する」を参照してください。

利用可能なアップデートを表示する

[通知] ビューの [アップデート] セクションでは、すべての接続されたサーバーおよびプールで利用できるアップデートが一覧表示されます。

注:

- XenCenter はデフォルトで、Citrix Hypervisor および XenCenter のアップデートを定期的にチェックします。アップデートを必要に応じてチェックするには、[更新] をクリックします。
- アップデートの自動チェックを無効にしている場合、[アップデート] タブにメッセージが表示されます。アップデートを手動で確認するには、[アップデートのチェック] をクリックします。

[表示] リストから、アップデートの一覧を [アップデートごと] で表示するか、[サーバーごと] で表示するかを選択できます。

[アップデートごと] を選択すると、XenCenter にアップデート一覧が表示されます。サーバー/プールまたは日付の順に並べ替えることができます。

- 累積更新プログラム (CU) と新しいリリースは、この一覧の一番上に表示されます。すべての新しいリリースがアップデートとして適用できるわけではありません。
- この情報を.csv ファイルとしてエクスポートするには、[すべてをエクスポート] をクリックします。.csv ファイルには、次の情報が含まれています：
 - アップデートの名称
 - アップデートの説明
 - このアップデートが適用されるサーバー
 - アップデートの日付
 - アップデートをダウンロードできる Web ページへのリンク
- アップデートをサーバーに適用するには、対象アップデートの [操作] リストで [ダウンロードしてインストール] を選択します。これにより、アップデートファイルが抽出され、アップデートのインストールウィザ

ードの [サーバーの選択] ページが開いて対象のサーバーが表示されます。詳しくは、「プールにアップデートを適用する」を参照してください。

- アップデートのリリースノートを開くには、[操作] リストで **[Web ページを開く]** を選択します。

アップデート一覧をサーバーごとで表示すると、XenCenter は XenCenter に接続されたサーバーの一覧を表示します。このリストには、サーバーに適用できるアップデートと、サーバーにインストールされているアップデートの両方が表示されます。

- この情報を.csv ファイルとしてエクスポートするには、[すべてをエクスポート] をクリックします。.csv ファイルには、次の情報が含まれています：
 - サーバーが属するプール
 - サーバー名
 - Citrix Hypervisor インストール済みの状態
 - サーバーの更新状態
 - このサーバーに必要なアップデート
 - このサーバーにインストールされたアップデート。
- このアップデートを適用するには、[アップデートのインストール] をクリックします。アップデートのインストールウィザードの [アップデートの選択] ページに利用可能なアップデートが一覧表示されます。詳しくは、「プールにアップデートを適用する」を参照してください。

プールにアップデートを適用する

XenCenter を使用してプールにアップデートを適用するには：

1. XenCenter で、[ツール] メニューの [アップデートのインストール] を選択します。
2. [はじめに] ページの注意事項を確認して、[次へ] を選択します。
3. アップデートのインストールウィザードの [アップデートの選択] ページに利用可能なアップデートが一覧表示されます。一覧から必要なアップデートを選択し、[次へ] をクリックします。
4. [サーバーの選択] ページでアップデートするプールとサーバーを選択します。

累積更新プログラム (CU) または最新リリース (CR) を適用する場合、最小限の Hotfix を適用するかどうかを選択できます。

[次へ] をクリックします。

5. アップデートのインストールウィザードにより、いくつかの事前チェックが実行され、プールの設定が有効であることが確認されます。

ウィザードは、次の条件もチェックします：

- アップデート後にホストの再起動が必要かどうかもチェックされ、結果が表示されます。

- Hotfix のライブパッチが使用できるか、ライブパッチがホストに適用できたかもチェックされます。ライブパッチについて詳しくは、ライブパッチを参照してください。
6. アップデート事前チェックにより問題が見つかった場合は、画面上に表示される解決処置に従ってください。[すべて解決] をクリックすると、XenCenter により問題の解決が試行されます。事前チェックの問題を解決したら、[次へ] をクリックします。
 7. CU または CR をインストールする場合、XenCenter はアップデートをダウンロードしてから、プールのデフォルトのストレージリポジトリにアップロードして、アップデートをインストールします。[アップロードしてインストール] ページに進行状況が表示されます。

注:

- 1 - プールのデフォルトのストレージリポジトリが共有されていない、または十分な領域がない場合は、XenCenter により別の共有ストレージリポジトリにアップデートがアップロードされます。十分な領域があるストレージリポジトリがない場合は、プールマスターのローカルストレージにアップデートがアップロードされます。 - 何らかの理由でプールのアップデートプロセスが完了できない場合、XenCenter がプロセスを停止します。この操作によって、** [再試行] ** ボタンをクリックして問題を修正し、アップデートプロセスを再開できます。

インストールプロセスを完了するには、手順 10 を参照します。

8. Hotfix をインストールする場合は、アップデートモードを選択します。画面の説明を参照して、適切なモードを選択してください。ホストに正常に適用できるライブパッチが Hotfix に含まれている場合、[実行するタスク] 画面に **No action required** と表示されます。

注:

この段階で [キャンセル] をクリックすると、変更内容が元に戻り、アップデートファイルがサーバーから削除されます。

9. [アップデートのインストール] をクリックすると、インストールが開始されます。[アップデートのインストール] ウィザードにはアップデートの進行状況が表示され、プール内の各サーバーをアップデートする間に XenCenter が実行する主な操作が表示されます。
10. アップデートが適用されたら、[完了] をクリックしてウィザードを終了します。手動モードを選択した場合は、アップデート後に必要なタスクをここで行います。

xe CLI を使用した Citrix Hypervisor サーバーのプールのアップデート

xe CLI を使用して Citrix Hypervisor ホストのプールをアップデートするには:

1. xe CLI を実行するコンピューター上の新規のフォルダーにアップデートをダウンロードします。ファイルのパスを控えておきます。

2. 次のコマンドを実行して、アップデートファイルをプールにアップロードします。

```
1 xe -s server -u username -pw password update-upload file-name=  
filename [sr-uuid=storage_repository_uuid]
```

ここで `-s` はプールマスタの名前です。このコマンドを実行すると、Citrix Hypervisor によりアップデートファイルに割り当てられた UUID が表示されます。UUID は控えておきます。

ヒント:

アップデートを Citrix Hypervisor サーバーにアップロードしたら、`update-list` および `update-param-list` コマンドを使用して、このファイルの情報を確認できます。

3. アップデートの障害となる問題が Citrix Hypervisor で検出されると、アラートが表示されます。これらの問題を解決してからアップデートを適用してください。

必要な場合は、`vm-shutdown` または `vm-suspend` コマンドを実行して、アップデートするホスト上で実行されている仮想マシンをシャットダウンまたは一時停止します。

仮想マシンを特定のホストに移行するには、`vm-migrate` コマンドを使用します。`vm-migrate` コマンドでは、移行対象の仮想マシンおよび移行先ホストを指定できます。

すべての仮想マシンをプール内のほかのホストにライブマイグレーションするには、`host-evacuate` コマンドを使用します。`host-evacuate` コマンドでは、Citrix Hypervisor により移行先ホストが決定されます。

4. 次のコマンドを実行して、ホストにアップデートを適用します。ここで、`uuid=` にアップデートファイルの UUID を指定します:

```
1 xe update-pool-apply uuid=UUID_of_file
```

このコマンドでは、プール内のすべてのホストにアップデートや Hotfix が適用されます（プールマスタから始まる）。

または、次のコマンドを実行して個々のホストにアップデートを適用し、ローリング方式でホストを更新および再起動することができます:

```
1 xe update-apply host=host uuid=UUID_of_file
```

ほかのプールメンバーをアップデートする前に、必ずプールマスタをアップデートしてください。

5. `update-list` コマンドを実行して、アップデートが適用されていることを確認します。アップデートが正しく適用されると、そのアップデートの `hosts` フィールドにホストの UUID が表示されます。
6. 必要に応じて、アップデート後に必要なタスクを行います（XAPI ツールスタックの再開、各ホストの再起動など）。これらの操作は、最初にプールマスタで実行してください。

xe CLI を使用して個別ホストをアップデートする

xe CLI を使用して個別ホストをアップデートするには:

1. xe CLI を実行するコンピューター上の新規のフォルダーにアップデートをダウンロードします。ファイルのパスを控えておきます。
2. `vm-shutdown` または `vm-suspend` コマンドを実行して、アップデートするホスト上で実行されている仮想マシンをシャットダウンまたは一時停止します。
3. 次のコマンドを実行して、アップデートファイルをホストにアップロードします。

```
1 xe -s server -u username -pw password update-upload file-name=  
filename [sr-uuid=storage_repository_uuid]
```

ここで `-s` はホスト名です。このコマンドを実行すると、Citrix Hypervisor によりアップデートファイルに割り当てられた UUID が表示されます。UUID は控えておきます。

ヒント:

アップデートを Citrix Hypervisor サーバーにアップロードしたら、`update-list` および `update-param-list` コマンドを使用して、アップデートについての情報を確認できます。

4. アップデートの障害となる問題が Citrix Hypervisor で検出されると、アラートが表示されます。これらの問題を解決してからアップデートを適用してください。
5. 次のコマンドを実行して、ホストにアップデートを適用します（ここで、`host-uuid=` にホストの UUID を指定し、`uuid=` にアップデートファイルの UUID を指定します）:

```
1 xe update-apply host-uuid=UUID_of_host uuid=UUID_of_file
```

ホストがプールのメンバーである場合は、ほかのプールメンバーをアップデートする前に、必ずプールマスタをアップデートしてください。

6. `update-list` コマンドを実行して、アップデートが正しく適用されていることを確認します。アップデートが正しく適用されると、そのアップデートの `hosts` フィールドにホストの UUID が表示されます。
7. 必要に応じて、アップデート後に必要なタスクを行います（XAPI ツールスタックの再開、各ホストの再起動など）。

自動アップデートを適用する

[自動アップデート] モードは、ホストで使用できるすべての Hotfix および累積更新プログラム (CU) を適用します。このモードは、プールまたはスタンドアロンサーバープールを最新の状態にするのに必要な再起動の回数を最低限にします。可能な場合、[自動アップデート] モードは最後に 1 回再起動を行うだけにします。

新しい最新リリース（CR）のバージョンがアップデートとして使用できる場合、[自動アップデート] モードはこのアップデートを適用しません。新しい CR にアップデートするには、手動で選択する必要があります。

XenCenter には必要なアップデートをフェッチするためにインターネットアクセスが必要です。

必要な更新のリストを表示するには、次の手順を実行します：

1. XenCenter の [リソース] ペインでホストを選択します。
2. [全般] タブをクリックします。
3. [アップデート] を展開します。

以下が表示されます：

- [適用済み] - 既に適用されているアップデートが一覧表示されます。
- [必要なアップデート] - サーバーを最新の状態にするのに必要な一連のアップデートが一覧表示されます。

注：

必要なアップデートがない場合、[必要なアップデート] は表示されません。

- [インストールされたサブメンタルパック] - サーバーにインストールされているサブメンタルパックが一覧表示されます（存在する場合）。

注：

サーバーではなくプールを選択した場合、[アップデート] には、既に適用されているアップデートが [すべて適用済み] として一覧表示されます。

特定のアップデートを選択してインストールする場合は、プールにアップデートを適用するを参照してください。

注：

自動アップデート機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[シトリックス Web サイト](#)を参照してください。詳しくは、「[ライセンス](#)」を参照してください。

自動アップデート機能は、Citrix Hypervisor Premium Edition ユーザーが使用できます。

アップデートのインストールウィザードを使用して自動アップデートを適用する

次のトピックでは、プールまたはスタンドアロンホストを最新状態にするために必要な一連のアップデートを自動的に適用する手順について説明します。

1. XenCenter で、[ツール] メニューの [アップデートのインストール] を選択します。
2. [はじめに] ページの注意事項を確認して、[次へ] を選択します。

3. [アップデートの選択] ページで、アップデートをインストールする方法を選択します。以下のオプションを表示できます：

- [自動アップデート] - (デフォルト) このオプションは、少なくとも1つのライセンスを持つプールまたはライセンスを持つスタンドアロンサーバーに XenCenter が接続されている場合にのみ表示されます。このオプションは、プールまたはスタンドアロンサーバーを最新の状態にするために、すべての最新のアップデートを自動でダウンロードおよびインストールする場合に選択します。
- [Citrix からのアップデートをダウンロード] - [アップデートのインストール] ウィザードに、サポートサイトからの利用可能なアップデートが一覧表示されます。アップデートを適用するには、「プールにアップデートを適用する」を参照してください。
- [ディスクからアップデートまたはサブリメンタルパックを選択] - 既にダウンロードしたアップデートをインストールする方法については、プールにアップデートを適用するを参照してください。サブリメンタルパックのアップデートをインストールするには、XenCenter ドキュメントの「[サブリメンタルパックのインストール](#)」を参照してください。

4. Hofix の自動適用を続行するには、[自動アップデート] を選択して、[次へ] をクリックしてください。

5. アップデートするプールまたはスタンドアロンサーバーを1つまたは複数選択し、[次へ] をクリックします。アップデートを適用できないプールまたはサーバーは選択できません。

6. アップデートのインストールウィザードにより、いくつかのアップデート事前チェックが実行され、プールの設定が有効であることが確認されます。

アップデート事前チェックにより問題が見つかった場合は、画面上に表示される解決処置に従ってください。[すべて解決] をクリックすると、XenCenter により問題の解決が試行されます。事前チェックの問題を解決したら、[次へ] をクリックします。

7. アップデートのインストールウィザードは、推奨されるアップデートを自動的にダウンロードしてインストールします。このウィザードにはアップデートの全体的な進行状況が表示され、プール内の各サーバーをアップデートする間に XenCenter が実行する主な操作が表示されます。

注：

- 1 - アップデートは、プールのデフォルトのストレージリポジトリにアップロードされます。デフォルトのストレージレポジトリが共有されていない、または十分な領域がない場合は、XenCenter により十分な領域がある別の共有ストレージリポジトリにアップデートがアップロードされます。十分な領域があるSRがない場合は、各ホストのローカルストレージにアップデートがアップロードされます。
- 2
- 3 - 何らかの理由でプールのアップデートプロセスが完了できない場合、XenCenter がプロセスを停止します。これによって、** [再試行] ** ボタンをクリックして問題を修正し、アップデートプロセスを再開できます。

8. すべてのアップデートが適用されたら、[完了] をクリックしてウィザードを終了します。

Citrix Hypervisor のライブパッチ

ライブパッチ適用機能は、Hotfix のみに適用されます。最新リリース (CR) および累積更新プログラム (CU) をライブパッチとして適用することはできません。

Citrix Hypervisor サーバーを展開している Citrix Hypervisor ユーザーは、Hotfix を適用した後にサーバーの再起動が必要なことが頻繁にあります。この再起動により、ホストでダウンタイムが発生し、ユーザーはシステムが再起動されるまで待機しなければなりません。これによって業務に影響を及ぼします。ライブパッチを使用して、ユーザーはホストを再起動することなく、いくつかの Linux カーネルおよび Xen ハイパーバイザーの Hotfix をインストールできます。Hotfix にはホストのメモリに適用されるライブパッチ、およびディスクのファイルをアップデートする Hotfix が含まれています。ライブパッチを使用すると、メンテナンスのコストを削減し、ダウンタイムを短縮できます。

XenCenter でアップデートを適用すると、[アップデートのインストール] ウィザードによって、アップデート後にサーバーの再起動が必要かどうかチェックされ、結果が XenCenter の事前チェックページに表示されます。これにより、ユーザーはアップデート後タスクを事前に把握することができ、Hotfix の適用を適宜スケジュールできます。

注:

Citrix Hypervisor ライブパッチは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[シトリックス Web サイト](#)を参照してください。ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

ライブパッチのシナリオ

Hotfix にはプール全体で、ホストで、またはスタンドアロンサーバー上でライブパッチを適用できます。一部のアップデートでは再起動が必要となります。また、アップデート後のタスクがない Hotfix もあります。アップデートにライブパッチが利用可能なシナリオ、および利用可能ではないシナリオを以下に示します。

- ライブパッチを使用する **Hotfix** - Linux カーネルおよび Xen ハイパーバイザーをアップデートする Hotfix では、Hotfix 適用後の再起動は必要ありません。ただし、まれにライブパッチを適用できない場合は、再起動が必要になることがあります。
- ライブパッチを使用しないアップデート - 動作に変更はありません。通常通りに機能します。

注:

ホストを再起動する必要がない、または Hotfix にライブパッチが含まれている場合、XenCenter は [アップデートモード] ページに「[No action required](#)」と表示します。

自動アップデートとライブパッチを適用する

XenCenter の [自動アップデート] モードでは、プールやスタンドアロンホストを最新状態に保つために必要な Hotfix の最低限のセットを自動的にダウンロードし、適用できます。[自動アップデート] モードは、ホストで使用できるすべての累積更新プログラム (CU) を適用します。ただし、新しい最新リリース (CR) のバージョンがアップデートとして使用できる場合、[自動アップデート] モードはこのアップデートを適用しません。新しい CR にアップデートするには、手動で選択する必要があります。

XenCenter の [自動アップデート] モードで Hotfix を適用する場合、ライブパッチ機能を活用できます。ライブパッチが使用可能で、[自動アップデート] モードを使用してアップデートされたホストに正常に適用できる場合、ホストを再起動する必要がなくなります。[自動アップデート] モードについて詳しくは、「自動アップデートを適用する」を参照してください。

XenCenter および xe CLI を使用してライブパッチを有効にする

ライブパッチ機能は、デフォルトで有効になっています。XenCenter または xe CLI コマンドで、ライブパッチを有効または無効にできます。

XenCenter での手順

1. [リソース] ペインでプールまたはスタンドアロンホストを選択します。
2. [プール] メニュー (スタンドアロンホストの場合 [サーバー] メニュー) で [プロパティ] を選択して、[ライブパッチ] をクリックします。
3. [ライブパッチ] ページで:
 - [可能であればライブパッチを使用する] を選択してライブパッチを有効にします。
 - [ライブパッチを使用しない] を選択してライブパッチを無効にします。

xe CLI の使用

- ライブパッチを有効にするには、次のコマンドを実行します:

```
1 xe pool-param-set live-patching-disabled=false uuid="pool_uuid"
```

- ライブパッチを無効にするには、次のコマンドを実行します:

```
1 xe pool-param-set live-patching-disabled=true uuid="pool_uuid"
```

インストールのトラブルシューティング

December 30, 2019

シトリックスでは、次の 2 種類のサポートを提供しています: www.citrix.com/supportで無料セルフヘルプサポートを利用するか、このサイトからサポートサービスを購入できます。シトリックスのテクニカルサポートを受けるには、オンラインでサポートケースを登録したり、サポート担当者に電話したりできます。

シトリックスのサポートサイト (www.citrix.com/support) では、さまざまな情報が提供されています。これらの情報はインストール時に想定外の動作、クラッシュ、およびその他の問題が発生した場合に役立ちます。リソースには次が含まれます: フォーラム、ナレッジベースの記事、ソフトウェアの更新、セキュリティ情報、ツール、および製品のドキュメント。

XenServer のインストール中、ホストマシンに直接接続されたキーボード（シリアルポート経由で接続されたものではなく）を使用して、以下の 3 つの仮想ターミナルにアクセスできます。

- **Alt+F1** キーを押して、メインの Citrix Hypervisor インストーラーにアクセスします。
- **Alt+F2** キーを押して、ローカルシェルにアクセスします。
- **Alt+F3** キーを押して、イベントログにアクセスします。

製品のインストール時に不明なエラーが発生した場合、そのホストのログファイルを取得してテクニカルサポートに提供してください。ログファイルを収集するには、次の手順を実行します。

ログファイルを収集して保存するには:

1. **Alt+F2** キーを押して、ローカルシェルにアクセスします。
2. 以下のコマンドを実行します。

```
1 /opt/xensource/installer/report.py
```

3. これにより、ログファイルの保存場所を選択するためのメッセージが表示されます: ログファイルの保存場所として、**[NFS]**、**[FTP]**、または **[Local media]** を選択できます。

ネットワーク上のほかのマシン上に保存するには、**[NFS]** または **[FTP]** を選択します。この場合、保存先のマシンにネットワークで接続でき、書き込みアクセスが許可されている必要があります。

ローカルマシンの USB フラッシュドライブなどのリムーバブルストレージに保存するには、**[Local media]** を選択します。

保存場所を選択すると、ログファイルがそこに書き込まれます。ファイル名は `support.tar.bz2` です。

収集したログファイルをサポートチームに送信して、調査を依頼します。

SAN 環境からの起動

December 30, 2019

XenServer を SAN 環境から起動する SAN ブート環境を構成すると、パフォーマンスや冗長性の向上、ストレージの効率利用などのメリットが提供されます。このような環境では、ブートディスクがローカルホスト上ではなく、リモートの SAN 上に配置されます。ホストは、ホストバスアダプタ (HBA) を使って SAN と通信します。HBA の BIOS に含まれている情報に基づいてブートディスクからホストが起動します。

SAN ブート環境では、ハードウェアファイバチャネルまたは HBA iSCSI アダプタサポートの SAN ベースディスクアレイが必要です。SAN ブート環境の冗長性を確保するには、I/O アクセスをマルチパス構成にします。このためには、ルートデバイスのマルチパスサポートを有効にする必要があります。使用する SAN 環境でマルチパスを使用できるかどうかについては、ストレージベンダまたは管理者に問い合わせてください。マルチパスを使用できる環境では、Citrix Hypervisor のインストール時にマルチパス機能を有効にできます。

警告:

アップグレード処理では、SAN ブート設定が保持されません。ISO またはネットワークブートを使用してアップグレードする場合は、`multipath` が正しく設定されるように、後述のインストール手順に従う必要があります。

マルチパスを有効にして **SAN** 上に **Citrix Hypervisor** をインストールするには:

1. 「Welcome to Citrix Hypervisor」画面で、**F2** キーを押します。
2. ブートプロンプトが開いたら、次のように入力します。 `multipath`

Citrix Hypervisor のインストールプロセスでは、マルチパス構成のリモート SAN からブートされる Citrix Hypervisor サーバーを設定します。

PXE または UEFI インストールでファイルシステムマルチパスを有効にするには、設定ファイルに `device_mapper_multipath=yes` を追加する必要があります。以下は設定例です:

```
1 default xenserver
2 label xenserver
3   kernel mboot.c32
4   append /tftpboot/xenserver/xen.gz dom0_max_vcpus=1-2 \
5   dom0_mem=1024M,max:1024M com1=115200,8n1 \
6   console=com1,vga --- /tftpboot/xenserver/vmlinuz \
7   xencons=hvc console=hvc0 console=tty0 \
8   device_mapper_multipath=yes \
9   install --- /tftpboot/xenserver/install.img
```

Citrix Hypervisor 環境のストレージマルチパス構成について詳しくは、「[ストレージ](#)」を参照してください。

Cisco UCS の Software-boot-from-iSCSI

Software-boot-from-iSCSI 機能により、iSCSI を使用して SAN から Citrix Hypervisor をインストールしたり起動したりできます。この機能を使用して、Citrix Hypervisor を iSCSI ターゲットが提供する LUN にインストールすることや、この LUN から起動および実行することができます。iSCSI ターゲットは、iSCSI ブートファームウェアテーブルで指定されています。この機能により、ルートディスクを iSCSI 経由で接続できます。

Citrix Hypervisor は Software-boot-from-iSCSI の以下の機能をサポートします。

- PXE ブート経由のホストのインストール
- Cisco UCS vNIC
Software-boot-from-iSCSI は、従来の BIOS および UEFI ブートモードで、Cisco UCS vNICs および Power Vault、NetApp および EqualLogic アレイを使用してテストされています。そのほかの構成も正常に動作する可能性があります。検証されていません。
- Cisco UCS マネージャーで構成されたジャンボフレーム (MTU=9000)
- Cisco UCS のラインレート制限
- 非タグ付き VLANs
- vSwitch バックエンドを使用するネットワーク
- 同一または異なる SAN/NAS 上の LVHDoiSCSI SR および NFS SR
- iSCSI ルートディスクのマルチパス化
- 一般的な Citrix Hypervisor (ネットワーク、メンテナンス) の操作との互換性

要件

- プライマリ管理インターフェイス (IP アドレスの割り当てが可能) および VM トラフィック用ネットワークは、別のインターフェイスを使用する必要があります。
- ストレージ (iSCSI ターゲット) は、ホスト上の IP アドレスを持つほかのすべてのネットワークインターフェイスへの別のレイヤー 3 (IP) ネットワークに属している必要があります。
- ストレージは、Citrix Hypervisor サーバーのストレージインターフェイスと同じサブネットに属している必要があります。

CD メディアを使用して **Citrix Hypervisor** をインストールする

CD を使用して Citrix Hypervisor をインストールするには、以下の手順に従います。

1. 起動メニューにアクセスします。boot: プロンプトで、menu.c32 と入力します。
2. カーソルキーを使用して、以下のインストールオプションを選択します：

- 単一パスの LUN の場合は、**install** を選択します。
- マルチパスの LUN の場合は、**multipath** を選択します。

3. Tab キーを押します。

以下で終わる行を編集します：

```
1 --- /install.img
```

4. カーソルキーを使用して、この行を次のように変更します：

```
1 use_ibft --- /install.img
```

5. **Enter** キーを押します。

Citrix Hypervisor サーバーのインストールが通常どおりに処理されます。

PXE を使用して Citrix Hypervisor をインストールする

PXE を使用して Citrix Hypervisor をインストールするには、以下の手順に従います。

注：

カーネルパラメーターに、キーワード **use_ibft** を追加したことを確認する必要があります。マルチパス化が必要な場合は、**device_mapper_multipath=enabled** を追加する必要があります。

以下の例では、単一の LUN の PXE 構成を示しています：

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc
   console=tty0
5 console=hvc0 use_ibft --- XS/install.img
```

以下の例では、マルチパスの LUN の PXE 構成を示しています：

```
1 label xenserver
2 kernel mboot.c32
3 append XS/xen.gz dom0_max_vcpus=2 dom0_mem=1024M,max:1024M
4 com1=115200,8n1 console=com1,vga --- XS/vmlinuz xencons=hvc
   console=tty0
5 console=hvc0 use_ibft device_mapper_multipath=enabled --- XS/
   install.img
```

ネットワークブートによるインストール

January 20, 2020

Citrix Hypervisor では、UEFI モードを使用したホストの起動がサポートされています。UEFI モードでは、ブートローダーとオペレーティングシステム向けの標準化された機能が豊富に用意されています。これにより、UEFI がデフォルトの起動モードであるホストに、Citrix Hypervisor をより簡単にインストールできます。

以下のセクションでは、TFTP サーバーと NFS、FTP、または HTTP サーバーをセットアップして、Citrix Hypervisor サーバーをインストールするための PXE および UEFI ブートを有効にする方法について説明します。また、無人インストールを実行するための XML 回答ファイルの作成方法についても説明します。

Citrix Hypervisor のインストールのために PXE および UEFI 環境を構成する

Citrix Hypervisor インストールメディアをセットアップする前に、TFTP サーバーおよび DHCP サーバーをセットアップする必要があります。以下のセクションでは、TFTP サーバーを PXE および UEFI ブート用に構成する方法について説明します。一般的なセットアップ手順については、ベンダーのドキュメントを参照してください。

注:

Citrix Hypervisor 6.0 以降、MBR によるディスクパーティションから GUID パーティションテーブル (GPT) に変更されています。一部の PXE システムでは、ホストにイメージを展開する前に、そのホストのハードディスク上にあるパーティションテーブルの読み込みが試行されます。

PXE システムに GPT パーティションスキームとの互換性がなく、さらにそのホストのハードディスクで GPT を使用する Citrix Hypervisor のバージョンが以前使用されていた場合、PXE システムは失敗することがあります。この問題を回避するには、ディスク上のパーティションテーブルを削除してください。

TFTP サーバーと DHCP サーバーに加えて、Citrix Hypervisor のインストールファイルをホストするための NFS、FTP、または HTTP サーバーが必要です。これらのサーバーは、同一マシン上に設定したり、ネットワーク上の複数のマシンに分散させたりできます。

また、PXE ブートで Citrix Hypervisor サーバーをインストールする各ホストで、PXE ブート対応のイーサネットカードが必要です。

次の手順は、使用する Linux サーバーが RPM をサポートしていることを前提としています。

PXE ブート用に TFTP サーバーを構成する

1. `/tftpboot`ディレクトリに、ディレクトリ `xenserver` を作成します。
2. `mboot.c32`ディレクトリの `pxelinux.0`と `/usr/lib/syslinux`を、`/tftpboot`ディレクトリにコピーします。

注:

同じソース (同じ Citrix Hypervisor ISO など) の `mboot.c32` と `pxelinux.0` を使用することを強くお勧めします。

3. Citrix Hypervisor インストールメディアのルートディレクトリにある `install.img` と、`/boot` ディレクトリにある `vmlinux` および `xen.gz` を、TFTP サーバーに作成した `/tftpboot/xenserver` ディレクトリにコピーします。
4. `/tftpboot` ディレクトリに、ディレクトリ `pxelinux.cfg` を作成します。
5. `pxelinux.cfg` ディレクトリに、設定ファイル `default` を作成します。

このファイルの内容は、PXE ブート環境の構成方法によって異なります。ここでは、設定ファイルの例を 2 つ挙げます。1 つ目の例では、TFTP サーバーから起動するマシンでインストールを開始します。このインストールでは、手動の応答が必要です。2 つ目の例は、管理者の介在が不要な無人インストールです。

注:

以下の 2 つの例では、物理コンソール `tty0` 上でインストールが実行されます。ほかのコンソールを使用する場合は、そのコンソールを右端で指定してください。

```

1  default xenserver
2  label xenserver
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5          dom0_mem=1024M,max:1024M com1=115200,8n1 \
6          console=com1,vga --- /tftpboot/xenserver/vmlinux \
7          xencons=hvc console=hvc0 console=tty0 \
8          --- /tftpboot/xenserver/install.img

```

指定された URL の回答ファイルを使用して無人インストールを実行するサンプル構成:

注:

回答ファイルを取得するネットワークアダプタを指定するには、`answerfile_device=ethX` または `answerfile_device=MAC` パラメーターを追加して、イーサネットデバイス番号または MAC アドレスを指定します。

```

1  default xenserver-auto
2  label xenserver-auto
3      kernel mboot.c32
4      append /tftpboot/xenserver/xen.gz dom0_max_vcpus=2 \
5          dom0_mem=1024M,max:1024M com1=115200,8n1 \
6          console=com1,vga --- /tftpboot/xenserver/vmlinux \
7          xencons=hvc console=hvc0 console=tty0 \
8          answerfile=http://pxehost.example.com/answerfile \
9          install --- /tftpboot/xenserver/install.img

```

PXE 構成ファイルの内容について詳しくは、[SYSLINUX](#)の Web サイトを参照してください。

UEFI ブート用に TFTP サーバーを構成する

UEFI ブート用に TFTP サーバーを構成するには:

1. /tftpbootディレクトリに、ディレクトリEFI/xenserverを作成します。
2. DHCP サーバーを構成し、起動ファイルとして/EFI/xenserver/grubx64.efiを指定します。
3. grub.cfgファイルを作成します。次に例を示します:

- インストール時のプロンプトに手動の応答が必要な場合:

```
1  menuentry "Citrix Hypervisor Install (serial)" {
2
3      multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
        watchdog \
4      dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
5      module2 /EFI/xenserver/vmlinuz console=hvc0
6      module2 /EFI/xenserver/install.img
7  }
```

- 回答ファイルを使用した無人インストールの場合:

```
1  menuentry "Citrix Hypervisor Install (serial)" {
2
3      multiboot2 /EFI/xenserver/xen.gz dom0_mem=1024M,max:1024M
        watchdog \
4      dom0_max_vcpus=4 com1=115200,8n1 console=com1,vga
5      module2 /EFI/xenserver/vmlinuz console=hvc0 console=tty0
        answerfile_device=eth0 answerfile=ftp://ip_address/
        path_to_answerfile install
6      module2 /EFI/xenserver/install.img
7  }
```

回答ファイルの使用について詳しくは、「無人 PXE および UEFI インストールのための回答ファイルの作成」を参照してください。

4. grub.cfgファイルを TFTP サーバーの/tftpboot/EFI/xenserverディレクトリにコピーします。
5. Citrix Hypervisor インストールメディアのルートディレクトリにあるgrubx64.efiおよびinstall.imgと、/bootディレクトリにあるvmlinuzおよびxen.gzを、TFTP サーバーに作成した/tftpboot/EFI/xenserverディレクトリにコピーします。

特定のオペレーティングシステムについては、使用するオペレーティングシステムのマニュアルを参照してください。ここでは、Red Hat、Fedora、およびほかの RPM ベースのディストリビューションでの設定手順について説明しま

す。

HTTP、FTP、または NFS サーバー上に **Citrix Hypervisor** インストールメディアをセットアップするには:

1. HTTP、FTP、または NFS サーバー上に、Citrix Hypervisor インストールメディアをホストするためのディレクトリを作成します。
2. Citrix Hypervisor インストールメディアのすべての内容を、上記の手順で作成したディレクトリにコピーします。このディレクトリがインストールリポジトリになります。

注:

Citrix Hypervisor インストールメディアをコピーする場合は、新しく作成したディレクトリに `.treeinfo` ファイルをコピーしたことを確認する必要があります。

インストール先のシステムを準備するには:

1. システムを起動し、ブートメニューを表示します (多くの BIOS プログラムでは起動処理中に **F12** キーを押します)。
2. 起動順序を設定するメニューで、イーサネットカードから起動するように設定します。
3. これまでの手順で設定したインストールソースからシステムが PXE ブートし、インストールスクリプトが実行されます。回答ファイルを設定した場合は、そのまま無人インストールが実行されます。

Citrix Hypervisor のインストール中にサブリメンタルパックをインストールする

サブリメンタルパックは、コントロールドメイン (Dom0) 内にソフトウェアをインストールすることによって Citrix Hypervisor の機能を修正および拡張するために使用されます。たとえば、OEM パートナーが Citrix Hypervisor を SNMP エージェントのインストールが必要な管理ツールセットと共に出荷しようとする場合があります。ユーザーはサブリメンタルパックを最初の Citrix Hypervisor インストール時に、またはインストール後いつでも追加できます。

Citrix Hypervisor のインストール中にサブリメンタルパックをインストールする場合、各サブリメンタルパックも個別のディレクトリに解凍する必要があります。

また、サブリメンタルパックを Citrix Hypervisor のインストールリポジトリに追加して自動工場インストールを可能にする OEM パートナー用のファシリティも存在します。

無人 PXE および UEFI インストールのために回答ファイルを作成する

無人インストールを実行するには、XML 形式の回答ファイルを作成する必要があります。次に回答ファイルの例を示します。

```
1 <?xml version="1.0"?>
2   <installation srtype="ext">
3     <primary-disk>sda</primary-disk>
```

```

4      <guest-disk>sdb</guest-disk>
5      <guest-disk>sdc</guest-disk>
6      <keymap>us</keymap>
7      <root-password>mypassword</root-password>
8      <source type="url">http://pxehost.example.com/citrix-hypervisor
      /</source>
9      <post-install-script type="url">
10     http://pxehost.example.com/myscripts/post-install-script
11     </post-install-script>
12     <admin-interface name="eth0" proto="dhcp" />
13     <timezone>Europe/London</timezone>
14 </installation>

```

回答ファイルでは、*installation* という名前のルートノード内に、すべてのノードを記述します。

注:

シンプロビジョニングを有効にするには、`srtype`属性を`ext`として指定します。この属性を指定しない場合、デフォルトのローカルストレージの種類はLVMです。のシンプロビジョニングでは、ローカルストレージの種類がEXT3になり、Citrix Virtual Desktopsのローカルキャッシュが正しく機能するようになります。詳しくは、「[ストレージ](#)」を参照してください。

次の表は、各エレメントの説明です。特に明記しない限りノード内の値はすべてテキストであり、いくつかの必須エレメントがあります。

<primary-disk>

必須か: はい

説明: コントロールドメインのインストール先ストレージデバイスの名前。手動のインストールでは、[*Select Primary Disk*] 画面の設定に相当します。

属性: `guest-storage`属性には、値として`yes`または`no`を指定できます。

次に例を示します: `<primary-disk guest-storage="no">sda</primary-disk>`

デフォルト値は`yes`です。ストレージリポジトリを作成しない無人インストールを行う場合は、ここで`no`を指定し、`guest-disk` キーは指定しないでおきます。

<guest-disk>

必須か: いいえ

説明: ゲストを格納するストレージデバイスの名前。追加する各ディスクについて、このエレメントを記述します。

属性: なし

<keymap>

必須か: はい

説明: インストール中に使用するキーマップの名前。<keymap>us</keymap>値を指定しない場合、デフォルトでusが適用されます。

属性: なし

回答ファイルを適切に変更することにより、自動アップグレードを実行することもできます。この場合、<installation> エLEMENTの mode 属性で *upgrade* を指定し、*existing-installation* ELEMENTで既存のインストール先ディスクを指定します。*primary-disk* ELEMENTと *guest-disk* ELEMENTは指定しません。次に例を示します:

```
1 <?xml version="1.0"?>
2 <installation mode="upgrade">
3     <existing-installation>sda</existing-installation>
4     <source type="url">http://pxehost.example.com/citrix-hypervisor/</
   source>
5     <post-install-script type="url">
6         http://pxehost.example.com/myscripts/post-install-script
7     </post-install-script>
8 </installation>
```

ホストのパーティションレイアウト

December 30, 2019

XenServer 7.0 では、新しいホストディスクパーティションレイアウトが導入されています。ログファイルをより大きな別のパーティションに移動することで、XenServer ではより詳細なログをより長期間保存することができ、問題点の診断能力が向上しました。同時に、Dom0 のルートディスクの需要を軽減し、ログファイルがディスクスペースを消費することによる潜在的なスペースの問題を回避できます。デフォルトレイアウトには、以下のパーティションが含まれています:

- 18GB の Citrix Hypervisor サーバーコントロールドメイン (dom0) パーティション
- 18GB のバックアップパーティション
- 4GB のログパーティション
- 1GB のスワップパーティション
- 0.5GB の UEFI 起動パーティション

XenServer 6.5 以前のリリースでは、4GB のコントロールドメイン (dom0) パーティションが、スワップとログを含むすべての dom0 機能で使用されていました。リモート syslog を使用しない場合や、サードパーティの監視ツールやサプリメントパックを使用する場合、パーティションサイズが制限されていました。Citrix Hypervisor ではこの問題を解消し、dom0 専用に 18GB のパーティションが用意されています。また、dom0 専用の大きいパーティションにより、dom0 ルートディスクに対する需要が低下し、パフォーマンスの大幅な向上を実現できます。

4GB の専用ログパーティションが導入されたことにより、過剰なログで dom0 パーティションがいっぱいになり、ホストの動作に影響するシナリオがなくなります。また、詳細なログリストを長時間にわたって保持することができ、問題の診断能力を向上できます。

新しいパーティションレイアウトには、UEFI ブートに必要な 500MB の専用パーティションも含まれています。

注:

上記の新しいパーティションレイアウトで Citrix Hypervisor をインストールする場合、ディスクサイズが 46GB 以上あることを確認する必要があります。

これより小さいデバイスに Citrix Hypervisor をインストールする場合、従来の DOS パーティションレイアウトで Citrix Hypervisor のクリーンインストールを実行できます。小型デバイスとは、ディスクスペースが 12GB 以上 46GB 未満のデバイスのことです。詳しくは、「[小型デバイスへのインストール](#)」を参照してください。

重要:

46GB 以上のディスクスペースを割り当て、新しい GPT パーティションレイアウトで Citrix Hypervisor をインストールすることをお勧めします。

従来のパーティションレイアウト

注:

従来の DOS パーティションレイアウトは廃止され、将来のリリースで削除される予定です。

- XenServer 5.6 Service Pack 2 以前では、DOS パーティションテーブルを使用してルートファイルシステムおよびバックアップのパーティションをローカルストレージから隔離していました。
- XenServer 6.0 では、GUID パーティションテーブルが導入され、ルートファイルシステム、バックアップ、およびローカルストレージが隔離されました。
- また、Citrix Hypervisor 8.1 をインストールする場合でも、最初の必須のパーティションが予約されているサーバーでは、DOS パーティションテーブルが使用されます。

以下の表は、インストールおよびアップグレードのシナリオと、これらの操作後に適用されるパーティションレイアウトの一覧です:

操作	アップグレード前のパーティション数	インストール/アップグレード後のパーティション数	パーティションテーブルの種類
プライマリディスクスペースが 46GB 以上のクリーンインストール	-	6	新しい GPT
プライマリディスクスペースが 12GB 以上の <code>disable-gpt</code> によるクリーンインストール	-	3 (ユーティリティパーティションがある場合は 4)	DOS
ユーティリティパーティションのあるマシンへのクリーンインストール	-	3 (ユーティリティパーティションがある場合は 4)	DOS

小型デバイスへのインストール

December 30, 2019

Citrix Hypervisor では、小型デバイスを使用する場合に、従来の DOS パーティションレイアウトで Citrix Hypervisor 8.1 をインストールできます。小型デバイスとは、ディスクスペースが 12GB 以上 46GB 未満のデバイスのことです。従来の DOS パーティションレイアウトには以下が含まれます。

- 4GB の起動パーティション
- 4GB のバックアップパーティション
- SR パーティション (ローカルディスク上にある場合)

小型デバイスに Citrix Hypervisor をインストールする場合は、`dom0` パラメーターに `disable-gpt` を追加する必要があります。 `menu.c32` を使用して、`dom0` にパラメーターを追加できます。

注:

インストール処理前からホストに存在するユーティリティパーティションは保持されます。

重要:

46GB 以上のディスクスペースを割り当て、新しい GPT パーティションレイアウトで Citrix Hypervisor をインストールすることをお勧めします。詳しくは、「[ホストのパーティションレイアウト](#)」を参照してください。

ホストとリソースプール

December 30, 2019

ここでは、xe コマンドラインインターフェイス (CLI) の使用例を基に、リソースプールの作成方法について説明します。シンプルな NFS ベースの共有ストレージ構成を使用した例を挙げて、仮想マシンの管理について説明します。また、物理ノードの障害に対処する手順についても説明します。

Citrix Hypervisor サーバーとリソースプールの概要

「リソースプール」(または単に「プール」)は、複数の Citrix Hypervisor サーバーで構成され、仮想マシンをホストする単一の管理対象としてグループ化したものです。リソースプールに共有ストレージを接続すると、十分なメモリを備えた任意の Citrix Hypervisor サーバー上で仮想マシンを起動できるようになります。さらに、最小限のダウンタイムで、実行中の仮想マシンを Citrix Hypervisor 別のサーバー上に動的に移行することもできます(「ライブマイグレーション」とも呼ばれます)。Citrix Hypervisor サーバーでハードウェア障害が生じた場合、管理者は、そのホスト上の仮想マシンを、同じリソースプール内の別の Citrix Hypervisor サーバー上で再起動させることができます。リソースプールの高可用性機能を有効にすると、ホストに障害が発生した場合に、そのホスト上の仮想マシンが自動的に移行されるようになります。リソースプールでは、最大で 64 台のホストがサポートされます。ただし、この制限は強制的なものではありません。

リソースプールには、プールマスタと呼ばれる 1 つの物理ノードが常に存在します。プールマスタだけが、XenCenter および Citrix Hypervisor コマンドラインインターフェイス (xe CLI) に管理インターフェイスを提供します。管理者が実行する管理コマンドは、プールマスタにより、必要に応じて個々のメンバホストに転送されます。

注:

高可用性機能が有効なリソースプールでは、プールマスタに障害が発生すると、別のホストがマスタとして選出されます。

リソースプール作成の要件

リソースプールは、同種(または制限付きの異種混在型)の Citrix Hypervisor サーバーの集合で、最大ホスト数は 64 です。ここで「同種の XenServer ホスト」とは、以下の条件を満たすものを指します。

- プールに追加するサーバー上の CPU は、ベンダー、モデル、および機能が、プール内の既存のサーバー上の CPU と同じである。
- インストールされている Citrix Hypervisor ソフトウェアが同じバージョンである。

以上のほか、リソースプールに追加するサーバーに適用される制限として、Citrix Hypervisor は特に以下の条件を満たしていることを確認します:

- ほかのリソースプールのメンバーではない。

- 共有ストレージが設定されていない。
- 実行中または一時停止している仮想マシンをホストしていない。
- 仮想マシンのシャットダウンなど、サーバー上で処理をアクティブに実行している仮想マシンがない。
- システムの時計が、プールマスタと同期している (NTP を使用している場合など)。
- サーバーの管理インターフェイスがボンディングされていない (リソースプールに追加した後はボンディング可能)。
- 管理 IP が静的である (そのサーバー上または DHCP サーバー上で固定アドレスが指定されている)。

Citrix Hypervisor サーバーに搭載されている物理ネットワークインターフェイスの数やローカルストレージリポジトリのサイズは、リソースプール内で異なっても構いません。また、完全に同一の CPU を搭載した複数のサーバーを入手することは難しい場合が多いため、軽微なばらつきは許容されます。CPU が異なるホストをリソースプールに追加しても問題がないと判断できる場合は、`--force`パラメータを指定してホストを強制的に追加することもできます。

プール内のすべてのホストは同じサイトに存在し、低遅延のネットワークで接続されている必要があります。

注:

リソースプールで共有される NFS または iSCSI ストレージを提供するサーバーは、静的な IP アドレスが設定されている必要があります。

プールには、仮想マシンを実行する Citrix Hypervisor サーバーを動的に選択したり、Citrix Hypervisor サーバー間で仮想マシンを動的に移行したりするための共有ストレージリポジトリが含まれている必要があります。可能な場合は、共有ストレージを設定してからリソースプールを作成してください。共有ストレージを追加したら、ローカルストレージ上にディスクを持つ既存の仮想マシンを共有ストレージ上に移動しておくことをお勧めします。仮想マシンを移動するには、`xe vm-copy`コマンドまたは XenCenter を使用します。

リソースプールを作成する

リソースプールは、XenCenter または CLI を使用して作成できます。新しいホストをリソースプールに追加すると、そのホスト上のローカルデータベースがプールのデータベースと同期され、プールに適用されているいくつかの設定がそのホストに継承されます:

- 仮想マシン、ローカル、およびリモートのストレージ設定は、プールのデータベースに追加されます。プールへの追加処理が完了し、管理者がリソースを明示的に共有するまで、この設定はプールに追加するホストに適用されません。
- リソースプールに追加したホストには、プールに設定されている既存の共有ストレージリポジトリが継承され、その共有ストレージへのアクセスが自動的に可能になるように適切な物理ブロックデバイス (PBD) レコードが作成されます。
- 一部のネットワーク設定も、新しいホストに継承されます。つまり、ネットワークインターフェイスカード (NIC) の構造的な詳細、仮想 LAN (VLAN)、およびボンディングされたインターフェイスはすべて継承され

ますが、ポリシー情報は継承されません。追加したホスト上で再設定する必要があるポリシーには、以下のものが含まれます:

- 管理インターフェイスの IP アドレス (プールに追加する前に設定済みのアドレスが保持されます)。
- 管理インターフェイスの場所 (プールに追加する前の設定が保持されます)。たとえば、プール内のほかのホストの管理インターフェイスがボンディングされたインターフェイス上に設定されている場合は、新しいホストの管理インターフェイスをそのボンディングに移行する必要があります。
- ストレージ専用のネットワークインターフェイス。XenCenter または CLI を使って新しいホストに再割り当てし、トラフィックが正しく転送されるように物理ブロックデバイスを接続し直す必要があります。これは、プールに追加するときに IP アドレスが割り当てられないため、このように正しく設定しないとストレージ用のネットワークインターフェイスを使用できません。CLI を使用したストレージ専用 NIC の設定について詳しくは、「[ネットワークの管理](#)」を参照してください。

注:

ホストの管理インターフェイスがリソースプールと同じタグが付けられた VLAN にある場合にのみ、新しいホストをリソースプールに追加することができます。

CLI を使用して **Citrix Hypervisor** サーバー **< host1 >** および **< host2 >** をリソースプールに追加するには

1. Citrix Hypervisor サーバー **< host2 >** をコンソールで開きます。
2. 次のコマンドを実行して、Citrix Hypervisor サーバー **< host2 >** を、Citrix Hypervisor サーバー **< host1 >** のプールに追加します:

```
1 xe pool-join master-address=host1 master-username=
  administrators_username master-password=password
```

ここで、**master-address**には Citrix Hypervisor サーバー **< host1 >** の完全修飾ドメイン名を指定し、**password**には Citrix Hypervisor サーバー **< host1 >** のインストール時に設定した管理者パスワードを指定します。

前の手順で使用した 2 つの Citrix Hypervisor サーバーは、デフォルトで名前のないリソースプールに属しています。リソースプールを作成するには、次のコマンドを実行して、名前のないリソースプールに名前を設定します。Tab キーを押して **pool_uuid**を取得することもできます:

```
1 xe pool-param-set name-label="New Pool" uuid=pool_uuid
```

異種混在型リソースプールを作成する

Citrix Hypervisor では、種類の異なるハードウェアを使って異種混在型のリソースプールを作成できるため、新しいハードウェアによる環境の拡張が簡単に行えます。異種混在型のリソースプールを作成するには、マスキングまた

はレベリングと呼ばれる技術をサポートする Intel 社 (FlexMigration) または AMD 社 (Extended Migration) の CPU が必要です。これらの機能では、CPU を実際とは異なる製造元、モデル、および機能のものとして見せかけることができます。これにより、異なる種類の CPU を搭載したホストでプールを構成しても、ライブマイグレーションがサポートされます。

注:

異種混在型プールに追加する Citrix Hypervisor サーバーの CPU が、プール内のホストと同一ベンダー (AMD または Intel) のものである必要があります。ただし、ファミリー、モデル、およびステッピング数などは異なっても構いません。

Citrix Hypervisor では、異種混在型プールのサポートが簡素化されました。ホストは、(CPU が同じベンダーファミリーからのものである限り) 基になる CPU の種類に関係なく既存のリソースプールに追加できるようになりました。プールの機能セットは、以下が行われるたびに動的に計算されます:

- 新しいホストをプールに追加した場合
- プールメンバーをプールから除外した場合
- プールメンバーが再起動の後に再接続した場合

プールの機能セットにおける変更は、プールで実行中の仮想マシンには影響しません。実行中の仮想マシンは、開始時に適用された機能セットを引き続き使用します。この機能セットは起動時に固定され、移行、サスペンド、および再開操作中も継続されます。機能の劣るホストがプールに追加されてプールのレベルが低下する場合、実行中の仮想マシンはプール内の新しく追加されたホストを除く任意のホストに移行できます。仮想マシンをプール内またはプール間で別のホストに移動または移行しようとする、Citrix Hypervisor によって、移行先ホストの機能セットに対して仮想マシンの機能セットが比較されます。機能セットに互換性があることが分かった場合は、仮想マシンの移行が許可されます。これによって、仮想マシンで使用している CPU 機能に関係なく、仮想マシンをプール間で自由に移動できるようになります。ワークロードバランスを使用して、仮想マシンを移行するのに最適な移行先ホストを選択すると、互換性のない機能セットが使用されているホストは、移行先ホストとして推奨されません。

共有ストレージを追加する

サポートされている共有ストレージの種類の一覧については、「[ストレージリポジトリの形式](#)」を参照してください。ここでは、共有ストレージ (ストレージリポジトリと呼びます) を既存の NFS サーバー上に作成する方法について説明します。

CLI を使用して **NFS** 共有ストレージをリソースプールに追加するには

1. プール内の任意の Citrix Hypervisor サーバーで、コンソールを開きます。
2. 次のコマンドを実行して、server:/path にストレージリポジトリを作成します。

```
1 xe sr-create content-type=user type=nfs name=example SR  
   shared=true \
```

```
2 device-config:server=server \  
3 device-config:serverpath=path
```

ここで、`device-config:server`は NFS サーバーのホスト名であり、`device-config:serverpath`は NFS サーバー上のパスです。`shared`に `true` を指定しているため、プール内のすべての Citrix Hypervisor サーバーに共有ストレージが自動的に接続されます。また、このプールに後で追加するすべての Citrix Hypervisor サーバーにもこの共有ストレージが自動的に接続されます。ストレージリポジトリの汎用一意識別子 (Universally Unique Identifier: UUID) が、画面上に出力されます。

3. 次のコマンドを実行して、プールの UUID を確認します:

```
1 xe pool-list
```

4. 次のコマンドを実行して、共有ストレージをプール全体のデフォルトとして設定します。

```
1 xe pool-param-set uuid=pool_uuid default-SR=sr_uuid
```

共有ストレージがプールのデフォルトとして設定されたため、今後作成するすべての仮想マシンのディスクがデフォルトで共有ストレージに作成されます。ほかの種類共有ストレージを作成する方法については、「[ストレージリポジトリの形式](#)」を参照してください。

リソースプールから **Citrix Hypervisor** サーバーを削除する

注:

Citrix Hypervisor サーバーをプールから削除する前に、そのホスト上のすべての仮想マシンがシャットダウン状態であることを確認してください。シャットダウンされていない仮想マシンが検出されると、警告メッセージが表示され、ホストを削除できません。

リソースプールからホストを削除 (イジェクト) すると、サーバーが再起動して再初期化され、新規インストールと同じ状態になります。ただし、ローカルディスク上に重要なデータがある場合は、プールから Citrix Hypervisor サーバーを削除しないでください。

CLI を使用してホストをリソースプールから削除するには

1. プール内の任意のホストで、コンソールを開きます。
2. 次のコマンドを実行して、目的のホストの UUID を確認します。

```
1 xe host-list
```

3. 次のコマンドを実行して、そのホストをプールから削除します:

```
1 xe pool-eject host-uuid=host_uuid
```

Citrix Hypervisor サーバーがリソースプールから削除され、新規インストールの状態になります。

警告:

ローカルディスクに重要なデータが格納されている場合は、そのホストをリソースプールから削除しないでください。ホストをプールから削除すると、すべてのデータが消去されます。ローカルディスク上のデータを保持するには、XenCenter または `xe vm-copy` CLI コマンドを使用して、仮想マシンをプールの共有ストレージにコピーしておきます。

ローカルディスク上に仮想マシンがある Citrix Hypervisor サーバーをプールから削除すると、これらの仮想マシンはプールのデータベースに残り、ほかの Citrix Hypervisor サーバーからもプール内に存在しているように見えます。このような仮想マシンを起動可能にするためには、その仮想マシンに関連付けられている仮想ディスクを、プール内のほかの Citrix Hypervisor サーバーからアクセスできる共有ストレージ上のものに変更するか、仮想ディスクを削除する必要があります。このため、プールにホストを追加する場合には、ローカルストレージの内容を共有ストレージ上に移動することをお勧めします。これにより、プールから Citrix Hypervisor サーバーを削除したりホストに物理的な障害が発生したりしたときのデータの損失を回避することができます。

注:

ホストがタグ付き VLAN ネットワーク上で管理インターフェイスがあるプールから削除されると再起動され、このマシンの管理インターフェイスが同じネットワーク上で利用できるようになります。

Citrix Hypervisor サーバーのプールを保守するための準備

リソースプール内のホストの保守を行う場合は、そのホストを無効にして、仮想マシンが起動しなくなるようにしてから、仮想マシンをプール内の別の Citrix Hypervisor サーバーに移行しておく必要があります。これを行うには、XenCenter を使用して、Citrix Hypervisor サーバーを保守モードに切り替えます。詳しくは、XenCenter ドキュメントの「[保守モードでの実行](#)」を参照してください。

予備の同期処理は 24 時間ごとに機能します。プールマスタを保守モードにすると、オフラインになった仮想マシンに対するラウンドロビンデータベースが最大で 24 時間分失われます。

警告:

アップグレードをインストールする前に、すべての Citrix Hypervisor サーバーを再起動して、設定を確認することを強くお勧めします。これにより、Citrix Hypervisor が再起動するまで適用されない変更内容が原因でアップデートに失敗することを回避できます。

CLI を使用してプール内のホストを保守するための準備を行うには

1. 次のコマンドを実行します。

```
1 xe host-disable uuid=Citrix Hypervisor_host_uuid
2 xe host-evacuate uuid=Citrix Hypervisor_host_uuid
```

これにより、Citrix Hypervisor サーバーが無効になり、実行中の仮想マシンがプール内の別の Citrix Hypervisor サーバーに移行されます。

2. 保守作業を行います。
3. 保守作業が終了したら、次のコマンドを実行して、Citrix Hypervisor サーバーを有効にします：

```
1 xe host-enable
```

4. シャットダウンまたはサスペンドした仮想マシンを起動または再開します。

リソースプールデータのエクスポート

[リソースデータのエクスポート] オプションを使用すると、リソースプールのリソースデータレポートを生成し、それを XLS ファイルや CSV ファイルとしてエクスポートできます。このレポートには、リソースプール内のサーバー、ネットワーク、ストレージ、仮想マシン、VDI、GPU など、さまざまなリソースについての詳細な情報が記述されます。これにより、管理者は CPU、ストレージ、およびネットワークなどのワークロードに基づいて、リソースの追跡、計画、および割り当てを行うことができます。

注：

[リソースプールデータのエクスポート] は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。

このレポートに記述されるリソースおよびリソースデータの一覧を以下に示します：

サーバー：

- 名前
- プールマスター
- UUID
- アドレス
- CPU 使用率
- ネットワーク（平均/最大 KB/秒）
- 使用メモリ
- ストレージ
- アップタイム
- 説明

ネットワーク：

- 名前
- 接続状態
- MAC
- MTU
- VLAN

- 種類
- 場所

VDI:

- 名前
- 種類
- UUID
- サイズ
- ストレージ
- 説明

ストレージ:

- 名前
- 種類
- UUID
- サイズ
- 場所
- 説明

仮想マシン:

- 名前
- 電源状態
- 実行サーバー
- アドレス
- MAC
- NIC
- オペレーティングシステム
- ストレージ
- 使用メモリ
- CPU 使用率
- UUID
- アップタイム
- テンプレート
- 説明

GPU:

- 名前
- サーバー
- PCI バスのパス
- UUID
- 使用電力

- 温度
- 使用メモリ
- コンピューター使用率

注:

GPU に関する情報は、GPU を搭載した Citrix Hypervisor サーバーでのみ出力されます。

リソースデータをエクスポートするには

1. XenCenter のナビゲーションペインで [インフラストラクチャ] をクリックし、リソースプールをクリックします。
2. [プール] メニューをクリックし、[リソースデータのエクスポート] を選択します。
3. レポートの保存先を指定して、[保存] をクリックします。

ホストの電源投入

リモートからのホストの電源投入

Citrix Hypervisor サーバーの電源投入機能を使用すると、XenCenter や CLI を使ってリモートのホストの電源を投入したり切断（シャットダウン）したりできます。

ホストの電源投入機能を有効にするには、以下のいずれかの電源管理ソリューションが必要です。

- **Wake-on-LAN** が有効なネットワークカード。
- **Dell Remote Access Card (DRAC)**。Citrix Hypervisor で DRAC を使用するには、Dell サプリメンタルパックをインストールしておく必要があります。DRAC をサポートするには、DRAC のサーバーに RACADM コマンドラインユーティリティをインストールして、DRAC およびそのインターフェイスを有効にする必要があります。通常、RACADM は DRAC 管理ソフトウェアに含まれています。詳しくは、Dell 社の DRAC ドキュメントを参照してください。
- **Hewlett-Packard Integrated Lights-Out (iLO)**。Citrix Hypervisor で iLO を使用するには、そのサーバー上の iLO を有効にして、インターフェイスをネットワークに接続する必要があります。詳しくは、HP 社の iLO ドキュメントを参照してください。
- Citrix Hypervisor の電源を投入または切断するための、管理 API に基づいたカスタムスクリプト。詳しくは、次のセクションの「ホストの電源投入機能のカスタムスクリプトを作成する」を参照してください。

電源を自動的に投入または切断できるように XenServer ホストを設定するには、以下の操作を行います：

1. プール内のホストがリモートからの電源制御をサポートしていること（Wake-on-LAN 機能、DRAC または iLO カード、またはカスタムスクリプトが設定されていることなど）を確認します。
2. CLI または XenCenter を使用して、ホスト電源投入機能を有効にします。

CLI を使用してホストの電源投入を管理する

ホスト電源投入機能は、CLI または XenCenter で管理できます。このセクションでは、CLI での管理について説明します。

ホスト電源投入機能は、ホストレベル（つまり各 Citrix Hypervisor ホスト）で有効になります。

この機能を有効にすると、CLI や XenCenter からホストの電源を入れることができます。

CLI を使用してホスト電源投入を有効にするには

次のコマンドを実行します：

```
1 xe host-set-power-on-mode host=<host uuid> \  
2   power-on-mode=("","wake-on-lan", "iLO", "DRAC","custom") \  
3   power-on-config=key:value
```

iLO および DRAC では、シークレット機能を使用している場合、`power_on_ip` キーでパスワードを指定します。詳しくは、「[シークレット](#)」を参照してください。

CLI を使用してホストの電源をリモートから投入するには

次のコマンドを実行します：

```
1 xe host-power-on host=<host uuid>
```

ホスト電源投入機能のカスタムスクリプトを作成する

デフォルトでサポートされるプロトコル（Wake-On-Ring や Intel Active Management Technology など）をサポートしない Citrix Hypervisor ホストの電源をリモートから投入するには、カスタムの Linux Python スクリプトを作成します。ただし、iLO、DRAC、および Wake-On-LAN ソリューション用のカスタムスクリプトを作成することもできます。

このセクションでは、Citrix Hypervisor API コール `host.power_on` のキー/値ペアを使用したホスト電源投入用カスタムスクリプトの作成について説明します。

カスタムスクリプトは、Citrix Hypervisor の電源の制御が必要なときにコマンドラインから実行する必要があります。また、XenCenter でスクリプトの実行を指定し、XenCenter UI 機能を使用して操作することもできます。

Citrix Hypervisor API については、[開発者用のドキュメント](#) Web サイトで公開されている Citrix Hypervisor Management API（英文）を参照してください。

警告:

/etc/xapi.d/plugins/ディレクトリにインストールされるデフォルトのスクリプトを変更することはできません。新しく作成したスクリプトをこのディレクトリに追加することはできますが、Citrix Hypervisor に付属のスクリプトは編集しないでください。

キー/値ペア

ホスト電源投入機能を使用するには、`host.power_on_mode`キーと`host.power_on_config`キーを設定します。値については、後のセクションを参照してください。

次の API コールを使用すると、これらのフィールドを一度に設定することもできます:

```
1 void host.set_host_power_on_mode(string mode, Dictionary<string,string> config)
```

host.power_on_mode

- 定義: 電源管理ソリューションの種類 (Dell DRAC など) を指定するキー/値ペアを含みます。
- 設定可能な値:
 - 空文字。電源管理を無効にします。
 - iLO: HP iLO を示します。
 - DRAC: Dell DRAC を示します。DRAC を使用するには、Dell サプリメンタルパックをインストールしておく必要があります。
 - wake-on-lan: Wake on LAN を示します。
 - そのほかの名前 (カスタムの電源投入スクリプトの指定)。このオプションでは、カスタムの電源管理スクリプトを指定できます。
- 種類: 文字列

host.power_on_config

- 定義: 電源投入モードを指定するキー/値ペアを含みます。iLO および DRAC に関する追加情報を指定します。
- 設定可能な値:
 - 電源管理ソリューションの種類として iLO または DRAC を指定する場合は、このキーで以下のいずれかの値を指定します。
 - * `power_on_ip`: 電源管理カードとの通信で使用される IP アドレスです。iLO または DRAC が構成されたネットワークインターフェイスのドメイン名を入力することもできます。

- * `power_on_user`: 管理プロセッサに関連付けられた iLO または DRAC のユーザー名です。工場出荷時のものから変更されている場合があります。
 - * `power_on_password_secret`: セキュリティを保護するシークレット機能を使用してパスワードを指定します。
- シークレット機能を使用してパスワードを保存するには、「`power_on_password_secret`」キーを指定します。詳しくは、「[シークレット](#)」を参照してください。
- 種類: マップ (文字列, 文字列)

サンプルスクリプト

このサンプルスクリプトでは、Citrix Hypervisor API をインポートし、自身をカスタムスクリプトとして定義し、さらにリモートから制御するホストに特定のパラメータを渡します。カスタムスクリプトでは、常に `session` パラメータを定義する必要があります。

このスクリプトの結果は、実行に失敗した場合のみ表示されます。

```
1 import XenAPI
2 def custom(session,remote_host,
3 power_on_config):
4 result="Power On Not Successful"
5 for key in power_on_config.keys():
6 result=result+' '
7 key=' '+key+' '
8 value=' '+power_on_config[key]
9 return result
```

注:

作成したスクリプトは、拡張子 `.py` で `/etc/xapi.d/plugins` ディレクトリに保存します。

Citrix Hypervisor サーバーとリソースプールとの通信

Citrix Hypervisor では、管理 API トラフィックの暗号化に TLS プロトコルが使用されます。Citrix Hypervisor と管理 API クライアント (またはアプライアンス) との間の通信で、デフォルトで TLS 1.2 プロトコルが使用されるようになりました。ただし、管理 API クライアントまたはアプライアンスが TLS 1.2 を使用して通信できない場合は、それ以前のプロトコルが通信に使用される場合があります。

Citrix Hypervisor では、次の暗号の組み合わせが使用されます:

-TLS_RSA_WITH_AES_128_CBC_SHA256

-TLS_RSA_WITH_AES_256_CBC_SHA

-TLS_RSA_WITH_AES_128_CBC_SHA

-TLS_RSA_WITH_RC4_128_SHA

-TLS_RSA_WITH_RC4_128_MD5

-TLS_RSA_WITH_3DES_EDE_CBC_SHA

また、Citrix Hypervisor では、**TLS 1.2** のみによる通信を許可するようにホストまたはリソースプールを構成できます。このオプションでは、TLS 1.2 プロトコルを使用した Citrix Hypervisor と管理 API クライアント（またはアプライアンス）との通信が許可されます。TLS 1.2 のみのオプションでは、**TLS_RSA_WITH_AES_128_CBC_SHA256** の暗号の組み合わせが使用されます。

警告:

Citrix Hypervisor プールと通信するすべての管理 API クライアントおよびアプライアンスに TLS 1.2 との互換性があることを確認してから、**[TLS 1.2 のみ]** をクリックしてください。

Citrix Hypervisor プールの IGMP スヌーピングを有効にする

Citrix Hypervisor マルチキャストトラフィックをすべてのゲスト仮想マシンに送信すると、ホストデバイスは想定外のパケットを処理する必要があるため、不必要な負荷が発生することになります。IGMP スヌーピングを有効にすると、ローカルネットワーク上のホストは明示的に参加していないマルチキャストグループのトラフィックを受信しなくなるため、マルチキャストのパフォーマンスが向上します。IGMP スヌーピングは、IPTV のように帯域幅を大幅に消費する IP マルチキャストアプリケーションの場合、特に有効です。

リソースプールの IGMP スヌーピングを有効にするには、XenCenter または CLI を使用します。XenCenter を使用して IGMP スヌーピングを有効にするには、**[プールプロパティ]** で **[ネットワークオプション]** を選択します。xe コマンドについては、[pool-igmp-snooping](#) を参照してください。

注:

- IGMP スヌーピングは、ネットワークのバックエンドが Open vSwitch を使用している場合のみ使用できます。
- この機能をプールで有効にする場合、物理スイッチの 1 つで IGMP クエリアを有効にすることが必要なこともあります。これを有効にしないと、サブネットワークのマルチキャストがブロードキャストにフォールバックし、Citrix Hypervisor のパフォーマンスが低下する可能性があります。
- IGMP v3 を実行しているプールでこの機能を有効にすると、仮想マシンの移行またはネットワークボンディングのフェイルオーバーによって IGMP のバージョンが v2 に切り替わることがあります。
- GRE ネットワークでこの機能を有効にするには、GRE ネットワークに IGMP クエリアを設定する必要があります。または、物理ネットワークから GRE ネットワークに IGMP クエリメッセージを転送することもできます。これをしない場合、GRE ネットワーク内のマルチキャストトラフィックがブロックされません。

クラスター化プール

December 30, 2019

クラスターリングは、GFS2 ストレージリポジトリを使用するリソースプールに必要な、追加機能を提供します。GFS2 について詳しくは、「[ストレージの構成](#)」を参照してください。

クラスターは、クラスター化されていないプールよりも密接に接続され協調する、Citrix Hypervisor ホストのプールです。クラスター内のホストは、選択したネットワーク上で互いに一定の通信を維持します。クラスター内のすべてのホストは、クラスター内のすべてのホストの状態を認識しています。このホスト協調により、クラスターは GFS2 ストレージリポジトリのコンテンツへのアクセスを制御できます。

クォーラム

クラスター内の各ホストは、クラスター内のホストの少なくとも半分（それ自体を含む）と常に通信している必要があります。この状態は、クォーラムを持つホストと呼ばれます。

奇数のプールのクォーラム値は、クラスター内のホストの合計数に 1 を加えたものの半分です： $(n + 1) / 2$ 。偶数のプールのクォーラム値は、クラスター内のホストの合計数の半分です： $n/2$ 。

偶数のプールの場合、実行中のクラスターを正確に半分に分けることができます。実行中のクラスターは、クラスターのどちらの半分が自己隔離し、クラスターのどちらの半分がクォーラムを持つかを決定します。偶数のクラスター化プールにコールドスタートから電源を投入する場合は、ホストがクォーラムを持つ前に、 $(n/2) + 1$ 台のホストを使用できるようにする必要があります。ホストがクォーラムを持つと、クラスターがアクティブになります。

ホストがクォーラムを持たない場合、そのホストは自己隔離します。

自己隔離

ホストは、クォーラムを持たないことを検出すると、数秒で自己隔離します。ホストは自己隔離すると、すぐに再起動します。ホストはハードシャットダウンを行うので、ホスト上で実行されているすべての仮想マシンが強制終了されます。高可用性を使用するクラスター化プールでは、Citrix Hypervisor は、ほかのプールメンバーでのその再起動構成に従って仮想マシンを再起動します。自己隔離されたホストは再起動され、クラスターに再び参加しようとします。

クラスター内の稼働中ホストの数がクォーラム値より小さくなると、残りのすべてのホストがクォーラムを失います。

理想的なシナリオでは、クラスター化プールには、クォーラムに必要な数より多くの稼働中ホストが常に存在し、Citrix Hypervisor が隔離することはありません。このシナリオをより実現可能にするには、クラスター化プールの設定時に次の推奨事項を考慮してください：

- 適切なハードウェア冗長性を確保します。

- クラスターネットワークに専用のボンディングネットワークを使用します。ボンディングされた NIC が必ず同じ L2 セグメント上にあるようにします。詳しくは、「[ネットワーク](#)」を参照してください。
- プールと GFS2 ストレージリポジトリとの間のストレージマルチパスを構成します。詳しくは、「[ストレージのマルチパス](#)」を参照してください。
- クラスター化プールで高可用性を構成します。クラスター化プールでは、ハートビートストレージリポジトリは GFS2 ストレージリポジトリである必要があります。詳しくは、「[高可用性](#)」を参照してください。

クラスター化プールを作成する

開始前に、次の前提条件が満たされていることを確認してください：

- クラスター化プール内のすべての Citrix Hypervisor サーバーには、少なくとも 2GiB のコントロールドメインメモリが必要です。
- クラスター内のすべてのホストは、クラスターネットワークに静的 IP アドレスを使用する必要があります。
- クラスタリングを使用するのは、プールが 3 つ以上のホストを含む場合だけにすることをお勧めします。これは、2 つのホストを含むプールではプール全体の自己隔離で問題が発生しやすいためです。
- プール内のホスト間にファイアウォールがある場合は、ホストが次のポートを使用してクラスターネットワーク上で通信できることを確認してください：
 - TCP: 8892、21064
 - UDP: 5404、5405

詳しくは、「[Communication Ports Used by Citrix Technologies](#)」を参照してください。

- 既存のプールをクラスタリングする場合は、高可用性が無効になっていることを確認してください。クラスタリングが有効になった後、高可用性を再度有効にできます。

必要な場合は、XenCenter を使用してプールにクラスタリングを設定することもできます。詳しくは、[XenCenter 製品ドキュメント](#)を参照してください。

xe CLI (コマンドラインインターフェイス) を使用してクラスター化プールを作成するには：

1. ボンディングネットワークを作成して、クラスタリングネットワークとして使用します。プールマスターにする Citrix Hypervisor サーバーで、以下の手順を実行します：
 - a) Citrix Hypervisor サーバーのコンソールを開きます。
 - b) 次のコマンドを使用して、リソースプールに名前を付けます：

```
1 xe pool-param-set name=label="New Pool" uuid=<pool_uuid>
```

- c) 次のコマンドを使用して、NIC ボンディングで使用するネットワークを作成します：

```
1 xe network-create name=label=bond0
```

これにより、新しいネットワークの UUID が返されます。

- d) 次のコマンドを使用して、ボンディングに使用する PIF の UUID を見つけます：

```
1 xe pif-list
```

- e) アクティブ/アクティブモード、アクティブ/パッシブモード、または LACP ボンディングモードのいずれかで、ボンディングしたネットワークを作成します。使用するボンディングモードに応じて、以下のいずれかのアクションを実行します：

- アクティブ/アクティブモードのボンディング（デフォルト）を作成するには、`bond-create` コマンドを使用します。パラメーターをコンマで区切って、新しく作成されたネットワーク UUID と、ボンディングする PIF の UUID を指定します：

```
1 xe bond-create network-uuid=<network_uuid> /  
2   pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<  
   pif_uuid_4>
```

ボンディングを構成する NIC の数に応じて、2 つまたは 4 つの UUID を指定してください。これにより、ボンディングの UUID が返されます。

- アクティブ/パッシブモードまたは LACP モードのボンディングを作成するには、上記と同じ構文に `mode` パラメータを追加して、`lacp` または `active-backup` を指定します：

```
1 xe bond-create network-uuid=<network_uuid> pif-uuids=<  
   pif_uuid_1>, /  
2   <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /  
3   mode=balance-slb | active-backup | lacp
```

プールマスターでボンディングしたネットワークを作成した後、他の Citrix Hypervisor サーバーをプールに追加すると、ネットワークとボンディングの情報が自動的に追加するサーバーに複製されます。

詳しくは、「[ネットワーク](#)」を参照してください。

2. 少なくとも 3 台の Citrix Hypervisor サーバーのリソースプールを作成します。

プールメンバー（マスターではない）である Citrix Hypervisor の各サーバーで、次の手順を繰り返します：

- a) Citrix Hypervisor サーバーのコンソールを開きます。
- b) 次のコマンドを使用して、Citrix Hypervisor サーバーをプールマスターのプールに参加させます：

```
1 xe pool-join master-address=master_address master-username=  
   administrators_username master-password=password
```

`master-address` パラメーターの値は、プールマスターである Citrix Hypervisor サーバーの完全修飾ドメイン名に設定する必要があります。`password` にはプールマスターのインストール時に設定した管理者パスワードを指定します。

詳しくは、「[ホストとリソースプール](#)」を参照してください。

3. このネットワークに属するすべての PIF について、`disallow-unplug=true`を設定します。

a) 次のコマンドを使用して、ネットワークに属する PIF の UUID を見つけます：

```
1 xe pif-list
```

b) リソースプール内の Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

4. プールでクラスタリングを有効にします。リソースプール内の Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe cluster-pool-create network-uuid=<network_uuid>
```

前の手順で作成したボンディングしたネットワークの UUID を入力します。

クラスタ化プールを管理する

クラスタ化プールを管理する場合は、次の方法で、プールがクォーラムを失うリスクを軽減できます。

ホストが正常にシャットダウンされるようにする

ホストは、正常にシャットダウンされると、再起動されるまで一時的にクラスタから削除されます。ホストは、シャットダウンされている間はクラスタのクォーラム値にカウントされません。そのホストがないことで他のホストがクォーラムを失うことはありません。

ただし、ホストは、強制的または予期せずにシャットダウンされた場合、オフラインになる前にクラスタから削除されることはありません。このホストは、クラスタのクォーラム値にカウントされます。シャットダウンされると、他のホストがクォーラムを失う可能性があります。

メンテナンスモードを使用する

ホスト上で何かを実行することでホストがクォーラムを失う可能性がある場合は、その前に、ホストをメンテナンスモードにしてください。ホストがメンテナンスモードの場合、実行中の仮想マシンはプール内の別のホストに移行されます。また、そのホストがプールマスタであった場合、その役割はプール内の別のホストに渡されます。操作によってメンテナンスモードのホストが自己隔離した場合でも、仮想マシンを失うことや、プールへの XenCenter の接続が失われることはありません。

メンテナンスモードのホストは、以降もクラスタのクォーラム値にカウントされます。

ホストがメンテナンスモードの場合は、クラスター化プールに含まれるそのホストの IP アドレスのみを変更できます。ホストの IP アドレスを変更すると、そのホストはクラスターから離れることになります。IP アドレスが正常に変更されると、そのホストはクラスターに再び参加します。ホストがクラスターに再び参加した後、メンテナンスモードを解除できます。

自己隔離しているかオフラインになっているホストを回復する

自己隔離されているホストを回復することは重要です。これらのクラスターメンバーは、オフラインになっている間は、クラスターのクォーラム数にカウントされ、接続可能なクラスターメンバーの数が減少します。この状況では、後続のホスト障害が発生することでクラスターがクォーラムを失い完全にシャットダウンされるリスクが高まります。

クラスター内にオフラインのホストがあると、特定の操作を実行できなくなります。クラスター化プールでは、プールのメンバーすべてがプールメンバーシップのすべての変更に同意しないと、変更は成功しません。クラスターメンバーが接続不可の場合は、Citrix Hypervisor により、クラスターメンバーシップを変更する操作（ホストの追加や削除など）が行えなくなります。

ホストを停止とマークする

オフラインのホストを回復できない場合は、それらをクラスターに対して停止とマークすることができます。ホストを停止とマークすると、それらがクラスターから永続的に削除されます。ホストが停止としてマークされると、それらはクォーラム値にカウントされなくなります。

制約

- クラスター化プールでは、プールあたり 16 台までのホストのみがサポートされます。
- ネットワークが管理とクラスタリングの両方に使用されている場合は、クラスターを再作成せずに管理ネットワークを分離することはできません。
- XenCenter を使用してクラスターネットワークの IP アドレスを変更するには、クラスタリングと GFS2 を一時的に無効にする必要があります。
- クラスターが稼働中で、クラスターに実行中の仮想マシンがある間は、クラスタリングネットワークのボンディングを変更しないでください。この操作により、クラスターが隔離される可能性があります。
- クラスタリングが有効になっているホストが少なくとも 1 つ含まれるクラスタリングネットワークで、IP アドレスの競合（IP アドレスが同じホストが複数存在）が発生した場合、競合しているホストが隔離されないことがあります。この問題を解決するには、IP アドレスの競合を解決します。

ユーザーの管理

January 20, 2020

ユーザー、グループ、役割、および権限を定義することで、Citrix Hypervisor サーバーやリソースプールにアクセスできるユーザーや実行可能な操作を制御できます。

Citrix Hypervisor の初回インストール時に、1つの管理者ユーザーアカウントが Citrix Hypervisor に自動的に追加されます。このアカウントはローカルスーパーユーザー（LSU）または root と呼ばれ、Citrix Hypervisor によりローカルに認証されるものです。

ローカルスーパーユーザー（root）は特別なシステム管理用アカウントであり、すべての権限を持ちます。Citrix Hypervisor では、ローカルスーパーユーザーは、インストールでのデフォルトのアカウントです。Citrix Hypervisor は、ローカルスーパーユーザーアカウントを認証します。ローカルスーパーユーザーは、外部の認証サービスを必要としません。このため、外部の認証サービスに障害が生じた場合でも、ローカルスーパーユーザーとしてログインすればシステムを管理できます。ローカルスーパーユーザーは、SSH を使用して物理 Citrix Hypervisor ホストに常にアクセスできます。

ほかのユーザーを作成するには、XenCenter の [ユーザー] タブまたは xe CLI を使用して Active Directory アカウントを追加します。Active Directory を使用しない環境では、ローカルスーパーユーザーのみを使用します。

注:

Citrix Hypervisor で新しく作成したユーザーには、デフォルトで RBAC 役割が割り当てられません。このため、ほかの管理者により役割が割り当てられるまで、これらのユーザーは Citrix Hypervisor プールにアクセスできません。

これらの権限は、「Active Directory 認証の使用」セクションで説明しているように、役割を通じて付与されます。

Active Directory でユーザーを認証する

XenServer ホストやプールに対して複数のユーザーアカウントを使用するには、Active Directory ユーザーアカウントで認証する必要があります。Active Directory アカウントでは、Citrix Hypervisor のユーザーが Windows ドメインの資格情報でプールにログインできます。

ユーザーアカウントに基づいてさまざまなアクセスレベルを設定するには、Active Directory 認証を有効にし、ユーザーアカウントを追加し、それらのアカウントに役割を割り当てます。

Active Directory アカウントを持つ管理者は、xe CLI を使用でき（適切な `-u` および `-pw` 引数を指定）、XenCenter を使用してホストに接続することもできます。認証はリソース単位プールベースで行われます。

サブジェクトは、ユーザーアカウントへのアクセスを制御します。Citrix Hypervisor のサブジェクトは、ディレクトリサーバー上のエンティティ（ユーザーまたはグループ）にマップされます。外部認証を有効にすると、Citrix Hypervisor で、セッションを作成するときに使用された資格情報がまずローカルルートの資格情報と照合され、次にサブジェクトリストと照合されます。アクセスを許可するには、そのユーザーまたはグループのサブジェクトエントリを作成します。XenCenter または xe CLI を使用してサブジェクトエントリを作成できます。

Active Directory やユーザーアカウントに関する表記が、XenCenter と Citrix Hypervisor CLI で異なる点に注意してください: XenCenter 用語 Citrix Hypervisor CLI 用語ユーザーサブジェクト追加ユーザー追加サブジェクト

Citrix Hypervisor は Linux ベースのシステムですが、Citrix Hypervisor では Citrix Hypervisor ユーザーアカウントとして Active Directory アカウントを使用することができます。このため、Active Directory 資格情報が Active Directory ドメインコントローラに渡されます。

Citrix Hypervisor に Active Directory を追加すると、Active Directory のユーザーとグループが Citrix Hypervisor のサブジェクトになります。XenCenter では、サブジェクトはユーザーと呼ばれます。ユーザーおよびグループは、Citrix Hypervisor にサブジェクトを登録するときに、ログオン時に、Active Directory を使用することで認証されます。ユーザーおよびグループは、ドメイン名を使用してユーザー名を修飾する必要はありません。

ユーザー名を修飾するには、ダウンレベルログオン名形式で入力する必要があります。例: `mydomain\myuser`。

注:

ユーザー名を修飾しない場合、XenCenter では、デフォルトで、Active Directory ドメインユーザーでのログインが試行されます。ただし、ローカルスーパーユーザーアカウントでログインする場合、XenCenter は常にローカルで（つまり Citrix Hypervisor ホスト上で）認証を試行します。

外部認証プロセスは、以下のように機能します:

1. Citrix Hypervisor ホストに接続するときに提供された資格情報が Active Directory ドメインコントローラに渡され、認証が要求されます。
2. Active Directory ドメインコントローラが、その資格情報を確認します。資格情報が無効な場合は、ここで認証に失敗します。
3. 資格情報が有効な場合は、Active Directory ドメインコントローラに照会され、その資格情報に関連付けられているサブジェクト識別子およびグループメンバシップが取得されます。
4. 取得したサブジェクト識別子が Citrix Hypervisor に格納されているものと一致した場合は、認証が正常に行われます。

ドメインに参加した際、プールの Active Directory 認証を有効にします。これにより、そのドメイン（および信頼関係のあるドメイン）のユーザーのみがリソースプールに接続できるようになります。

注:

DHCP が設定されたネットワーク PIF の DNS 設定を手作業で更新することはサポートされません。これにより、Active Directory の統合に問題が生じ、ユーザー認証に失敗することがあります。

Active Directory 認証を設定する

Citrix Hypervisor では、Windows Server 2008 またはそれ以降の Active Directory サーバーがサポートされません。

Citrix Hypervisor サーバーで Active Directory を認証するには、（相互運用性が有効な）Active Directory サーバーとその Citrix Hypervisor サーバーが同じ DNS サーバーを使用している必要があります。

Active Directory サーバーと DNS サーバーが同じマシンである場合もあります。これは、DHCP を使用して IP ア

ドレス、および DNS サーバーの一覧を Citrix Hypervisor サーバーに提供することで実現できます。または、PIF オブジェクト内の値を設定することや、手動の静的構成の使用時にインストーラーを使用することもできます。

DHCP を有効にしてホスト名を割り当てることをお勧めします。ホスト名 `localhost` または `linux` をホストに割り当てないでください。

警告:

Citrix Hypervisor 環境内では、一意の Citrix Hypervisor サーバー名を使用する必要があります。

以下の点に注意してください:

- Citrix Hypervisor では、ホスト名に基づいた Active Directory エントリが Active Directory データベースに格納されます。同じホスト名を持つ 2 つの Citrix Hypervisor サーバーが同じ Active Directory ドメインに属している場合、2 つ目の Citrix Hypervisor は 1 つ目の Citrix Hypervisor の Active Directory エントリを上書きします。上書きは、ホストが同じプールに属しているか異なるプールに属しているかにかかわらず行われます。これにより、1 つ目の Citrix Hypervisor での Active Directory 認証が機能しなくなる可能性があります。

異なる Active Directory ドメインに属している Citrix Hypervisor サーバーでは、同じホスト名を使用できません。

- Active Directory で比較されるのは UTC 時間なので、異なるタイムゾーンに属している Citrix Hypervisor サーバーは同じ Active Directory ドメインに追加できます。時計が同期するように、Citrix Hypervisor プールと Active Directory サーバーで同じ NTP サーバーを使用できます。
- リソースプールで複数の認証方法を使用することはサポートされていません。プール内の一部のホストでのみ Active Directory 認証を有効にして、ほかのホストで無効にすることはできません。
- Citrix Hypervisor の Active Directory 統合機能では、Active Directory サーバーとの通信に Kerberos プロトコルが使用されます。このため、Citrix Hypervisor では、Kerberos プロトコルが無効な Active Directory サーバーはサポートされていません。
- Active Directory を使用して正しく外部認証が行われるようにするには、Citrix Hypervisor サーバーの時計が Active Directory サーバーと同期している必要があります。Citrix Hypervisor を Active Directory ドメインに追加するときに時計が同期しているかどうかをチェックされ、同期していないと認証に失敗します。

警告:

ホスト名は、63 文字以下の英数字で指定します。ただし、数字のみのホスト名を使用しないでください。

Active Directory 認証を有効にした後にプールにサーバーを追加すると、そのサーバー上の Active Directory 設定を確認するメッセージが表示されます。追加するサーバーの資格情報を入力するときは、サーバーをドメインに追加するための特権を持つ Active Directory 資格情報を使用します。

Active Directory の統合

Citrix Hypervisor からドメインコントローラーへのアクセスが遮断されないように、以下のファイアウォールポートが送信トラフィック用に開放されていることを確認してください。

ポート	プロトコル	使用
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS ネームサービス
139	TCP	NetBIOS セッション (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	マシンパスワードの変更
3268	TCP	グローバルカタログ検索

注:

- Linux コンピュータ上で *iptables* を使用してファイアウォール規則を確認するには、次のコマンドを実行します: `iptables -nL`。
- Citrix Hypervisor では、Active Directory サーバーでの Active Directory ユーザーの認証、および Active Directory サーバーとの通信の暗号化に PowerBroker Identity Services (PBIS) が使用されます。

Citrix Hypervisor による **Active Directory** 統合でのマシンアカウントパスワードの管理

Windows クライアントマシンと同様に、PBIS では、マシンアカウントパスワードが自動的に更新されます。PBIS では、30 日ごとに、または Active Directory サーバーのマシンアカウントパスワード更新ポリシーで指定されたとおりに、パスワードが更新されます。

リソースプールの外部認証を有効にする

Active Directory による外部認証は、XenCenter または以下の CLI コマンドを使用して設定します。

```
1 xe pool-enable-external-auth auth-type=AD \
2   service-name=full-qualified-domain \
3   config:user=username \
```

```
4 config:pass=password
```

指定されたユーザーには `Add/remove computer objects or workstations` の特権が必要です。これはドメイン管理者のデフォルトです。

Active Directory および Citrix Hypervisor サーバーが使用するネットワークで DHCP を使用しない場合は、以下の方法で DNS を設定します：

1. 非完全修飾ドメイン名エントリを解決できるように、ドメインの DNS サフィックスの検索順を設定します：

```
1 xe pif-param-set uuid=pif_uuid_in_the_dns_subnetwork \  
2 "other-config:domain=suffix1.com suffix2.com suffix3.com"
```

2. Citrix Hypervisor サーバー上で、使用する DNS サーバーを設定するには、次のコマンドを実行します：

```
1 xe pif-reconfigure-ip mode=static dns=dns host ip=ip \  
2 gateway=gateway netmask=netmask uuid=uuid
```

3. DNS サーバーと同じネットワーク上にある PIF を使用するように管理インターフェイスを手動で設定します：

```
1 xe host-management-reconfigure pif-uuid=pif_in_the_dns_subnetwork
```

注：

外部認証はホストごとのプロパティです。ただし、プール単位で外部認証を有効または無効にすることをお勧めします。プール単位での設定では、Citrix Hypervisor が、特定のホストで認証を有効にしたときに発生する障害に対処できます。また Citrix Hypervisor は、プール全体で一貫した構成となるように、必要な変更をロールバックします。 `host-param-list` コマンドを実行して、ホストの外部認証が有効かどうかを確認できます。

Active Directory 認証を無効にするには、XenCenter を使用するか、次の `xe` コマンドを実行します：

```
1 xe pool-disable-external-auth
```

ユーザー認証

ほかのユーザーが Citrix Hypervisor サーバーにアクセスできるようにするには、そのユーザーまたはグループ用のサブジェクトを追加する必要があります。(推移的グループメンバーシップも通常の方法でチェックされます。たとえば、グループAにグループBが含まれ、`user 1`がグループBのメンバーである場合に、グループAのサブジェクトを追加すると、`user 1`へのアクセスが許可されます)。Active Directory でユーザー権限を管理する場合は、単一のグループを作成してから、そのグループのユーザーを追加または削除できます。または、Citrix Hypervisor で個々のユーザーを追加および削除することや、認証要件に応じてユーザーとグループの組合せを追加および削除することができます。次のセクションで説明するように、XenCenter から、または CLI を使用して、サブジェクトリストを管理できます。

ユーザーを認証するとき、資格情報は最初にローカルルートアカウントと照合され、Active Directory サーバーに障害が発生したシステムを回復できます。資格情報（ユーザー名とパスワード）が一致しない場合は、Active Directory サーバーに対して認証要求が行われます。認証が成功すると、ユーザーの情報が取得され、ローカルのサブジェクトリストに対して検証されます。認証が失敗した場合、アクセスは拒否されます。サブジェクトリストでの検証は、そのユーザー、またはそのユーザーの推移的グループメンバシップのグループがリスト上に見つかりと成功します。

注:

Active Directory グループにプール管理者の役割を割り当ててホストへの SSH アクセスを許可する場合、その AD グループのユーザー数は 500 以下である必要があります。

Active Directory サブジェクトを Citrix Hypervisor に追加するには:

```
1 xe subject-add subject-name=entity_name
```

entity_name は、アクセスを付与するユーザーまたはグループの名前です。明確にする必要がない限り、エンティティのドメインを含めることができます（たとえば、「user1」ではなく「xendt\user1」）、動作は同じです。

ユーザーのサブジェクト識別子を確認します。サブジェクト識別子は、ユーザー、またはそのユーザーが属しているグループの名前です。グループを削除すると、ユーザーが明示的に指定してある場合を除き、そのグループに属しているすべてのユーザーのアクセスが無効になります。ユーザーのサブジェクト識別子を確認するには、`subject list` コマンドを使用します:

```
1 xe subject-list
```

このコマンドでは、すべてのユーザーの一覧が表示されます。

サブジェクトリストにフィルタを適用する場合、たとえば、`testad` ドメイン内のユーザー `user1` のサブジェクト識別子を検索するには、次のコマンドを実行します:

```
1 xe subject-list other-config:subject-name='testad\user1'
```

取得したサブジェクト識別子を指定し、`subject-remove` コマンドを使用してユーザーを削除します:

```
1 xe subject-remove subject-uuid=subject_uuid
```

このユーザーの実行中のセッションを終了できます。詳しくは、「*CLI* を使用してすべての認証済みセッションを終了するには」および「*CLI* を使用して特定ユーザーのセッションを終了するには」を参照してください。実行中のセッションを終了しないと、そのユーザーがセッションからログアウトするまでアクセスできてしまうことに注意してください。

Citrix Hypervisor サーバーやリソースプールへのアクセスが許可されているユーザーやグループを確認するには、次のコマンドを実行します:

```
1 xe subject-list
```

ユーザーのアクセスを削除する

ユーザーが認証されると、そのセッションを終了するか、ほかの管理者がそのユーザーのセッションを終了するまで、ホストへのアクセスが保持されます。ユーザーをサブジェクトリストから削除したり、アクセスが付与されたグループから削除したりしても、実行中のセッションが無効になるわけではありません。ユーザーは、XenCenter または作成済みのほかの API セッションを使用して引き続きプールにアクセスできます。XenCenter および CLI では、個々のセッション、またはアクティブなすべてのセッションを強制終了できます。XenCenter でこれを行う方法については、[XenCenter ドキュメント](#)を参照してください。次のセクションでは、CLI を使用する方法について説明します。

CLI を使用してすべての認証済みセッションを終了する

xe を使用してすべての認証済みセッションを終了するには、次の CLI コマンドを実行します：

```
1 xe session-subject-identifier-logout-all
```

CLI を使用して特定ユーザーのセッションを終了する

1. 対象ユーザーのサブジェクト識別子を確認します。サブジェクト識別子を確認するには、`session-subject-identifier-list` または `subject-list xe` コマンドを使用します。最初のコマンドは、セッションを持っているユーザーを表示します。2 つ目のコマンドではすべてのユーザーが表示されますが、フィルターを適用できます。たとえば、`xe subject-list other-config:subject-name=xendt\\user1` のようなコマンドを使用します。シェルによってはこのようにバックslash を 2 つ入力します。
2. 取得したサブジェクト識別子をパラメータとして指定して、`session-subject-logout` コマンドを実行します。例：

```
1 xe session-subject-identifier-logout subject-identifier=subject_id
```

Active Directory ドメインからプールを削除する

警告：

ドメインからホストやプールを削除すると、Active Directory の資格情報でログインした管理者ユーザーが切断されます。

リソースプールでの Active Directory 認証を無効にするには、XenCenter を使用して Active Directory ドメインからプールを削除します。詳しくは、[XenCenter ドキュメント](#)を参照してください。または、必要に応じてプールの UUID を指定し、`pool-disable-external-auth` コマンドを実行します。

注:

リソースプールを Active Directory ドメインから削除しても、Active Directory データベースからホストオブジェクトが削除されることはありません。無効なホストエントリを削除する方法については、[Microsoft 社のサポート文書](#)を参照してください。

役割ベースのアクセス制御

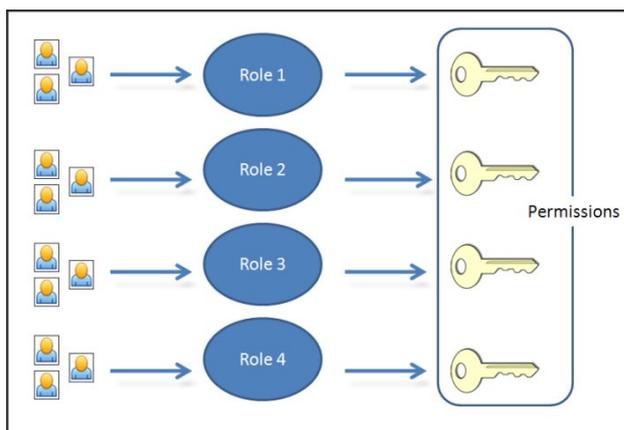
December 30, 2019

Citrix Hypervisor の役割ベースのアクセス制御 (RBAC: Role Based Access Control) 機能では、特定のユーザー (つまり XenServer 管理者) に役割を割り当てて、Citrix Hypervisor へのアクセスや実行可能な管理タスクを制御できます。この機能では、ユーザー (またはグループ) が Citrix Hypervisor の管理タスクの定義済みセットである「役割」にマップされ、この役割に基づいて、特定の管理タスクを実行するために必要な Citrix Hypervisor ホストへのアクセス許可が決定されます。

管理者にはアクセス許可は直接割り当てられず、そのユーザーアカウントまたはグループアカウントに割り当てられた役割によりアクセス許可が付与されます。このため、管理者を適切な役割に割り当てるのが個々のアクセス許可の管理になり、管理者アカウントの管理が簡単になります。管理者のアカウントおよび役割のリストは、Citrix Hypervisor により保持されます。

役割ベースのアクセス制御により、異なるグループに属する管理者に異なるアクセス許可を付与できます。これにより、十分な経験のない管理者による不適切な変更を防ぐことができます。

役割ベースのアクセス制御には、法規制の順守と監査のため監査ログ機能も用意されています。



役割ベースのアクセス制御では、認証サービスとして Active Directory が使用されます。Citrix Hypervisor は、認証されたユーザーの一覧を Active Directory のユーザーおよびグループアカウントに基づいて管理します。このため、役割を割り当てるには、事前にリソースプールをドメインに追加して、Active Directory アカウントを追加しておく必要があります。

ローカルスーパーユーザー (root) は特別なシステム管理用アカウントであり、すべての権限およびアクセス許可を持ちます。ローカルスーパーユーザーは、Citrix Hypervisor をインストールするときのデフォルトのアカウントです。このアカウントは Citrix Hypervisor により認証され、外部の認証サービスは使用されません。このため、外部の認証サービスに障害が生じた場合でも、ローカルスーパーユーザーとしてログインすればシステムを管理できます。ローカルスーパーユーザーは、SSH を使用して Citrix Hypervisor 物理ホストに常にアクセスできます。

役割ベースのアクセス制御の基本的な手順

次のセクションでは、役割ベースのアクセス制御を有効にしてユーザーやグループに役割を割り当てるための手順について説明します：

1. ドメインに参加する。詳しくは、「[リソースプールの外部認証を有効にする](#)」を参照してください。
2. Active Directory のユーザーまたはグループをプールに追加する。追加したユーザーやグループはサブジェクトになります。詳しくは、「[RBAC にサブジェクトを追加するには](#)」を参照してください。
3. サブジェクトに RBAC の役割を割り当てる (または変更する)。詳しくは、「[新しいサブジェクトに RBAC の役割を割り当てるには](#)」を参照してください。

RBAC 役割とアクセス権

March 12, 2020

役割

Citrix Hypervisor には、以下の 6 つの役割が用意されています。

- プール管理者 (*Pool Admin*)： ローカルスーパーユーザー (root) と同レベルの管理者で、すべての操作を実行できます。

注：

ローカルスーパーユーザー (root) には、「プール管理者」の役割が適用されます。つまり、プール管理者にはローカルスーパーユーザーと同じ権限が設定されます。

- プールオペレータ (*Pool Operator*)： 管理者ユーザーを追加/削除したり役割を変更したりすることはできませんが、そのほかのすべての管理タスクを実行できます。ホストやプールの管理 (ストレージの作成、プールの作成、ホストの管理など) に特化した役割です。
- 仮想マシンパワー管理者 (*VM Power Admin*)： 仮想マシンを作成して管理できます。仮想マシンオペレータに仮想マシンを提供することに特化した役割です。

- 仮想マシン管理者 (*VM Admin*): 仮想マシンパワー管理者に似ていますが、仮想マシンを移行したりスナップショットを作成したりすることはできません。
- 仮想マシンオペレータ (*VM Operator*): 仮想マシン管理者に似ていますが、仮想マシンを作成したり破棄したりすることはできません。ただし、ライフサイクル操作を開始したり終了したりすることは許可されます。
- 読み取りのみ (*Read Only*): リソースプールとパフォーマンスのデータを表示することしかできません。

警告:

Active Directory グループにプール管理者の役割を割り当ててホストへの SSH アクセスを許可する場合、その Active Directory グループのメンバー数は 500 以下である必要があります。

各役割で許可されるタスクについて詳しくは、次のセクションの「RBAC 役割の定義とアクセス権」を参照してください。

Citrix Hypervisor で管理者ユーザーを作成した後で役割を割り当てないと、そのアカウントは使用できません。Citrix Hypervisor では役割が自動的に割り当てられません。このため、ほかの管理者により役割が割り当てられるまで、これらのユーザーは Citrix Hypervisor プールにアクセスできません。

1. サブジェクトに割り当てる役割を変更します。これを行うには役割の割り当て/変更権限が必要であり、この権限はプール管理者のみに付与されます。
2. そのユーザーのグループメンバシップを変更して、必要な役割が割り当てられている Active Directory グループにユーザーを追加します。

RBAC 役割の定義とアクセス権

次の表は、各役割で使用可能な権限をまとめたものです。各アクセス権について詳しくは、「アクセス権の定義」を参照してください。

アクセス権	プール管理者	プールオペレーター	VM パワー管理者	VM 管理者	VM オペレーター	読み取り専用
役割の割り当て/変更	<input checked="" type="checkbox"/>					
物理サーバーのコンソールへのログイン (SSH および XenCenter の使用)	<input checked="" type="checkbox"/>					
サーバーのバックアップ/復元	<input checked="" type="checkbox"/>					

アクセス権	プール管理者	プールオペレーター	VM パワー管理者	VM 管理者	VM オペレーター	読み取り専用
OVF/OVA パッケージとディスクイメージのインポート/エクスポート	☑					
ソケットごとのコア数の設定	☑	☑	☑	☑		
Citrix Hypervisor Conversion Manager による仮想マシンの変換	☑					
スイッチポートのロック	☑	☑				
マルチパス	☑	☑				
接続中のユーザーのログアウト	☑	☑				
アラートの作成と解除	☑	☑				
任意のユーザーのタスクのキャンセル	☑	☑				
プール管理	☑	☑				
ライブマイグレーション	☑	☑	☑			
ストレージライブマイグレーション	☑	☑	☑			
高度な仮想マシン操作	☑	☑	☑			

アクセス権	プール管理者	プールオペレーター	VM 管理者	VM パワー管理者	VM オペレーター	読み取り専用
仮想マシンの作成/破棄操作	☑	☑	☑	☑		
仮想マシンの CD メディアの変更	☑	☑	☑	☑	☑	
仮想マシンの電源状態の変更	☑	☑	☑	☑	☑	
仮想マシンコンソールの表示	☑	☑	☑	☑	☑	
XenCenter の表示管理操作	☑	☑	☑	☑	☑	
自分のタスクのキャンセル	☑	☑	☑	☑	☑	☑
監査ログの表示	☑	☑	☑	☑	☑	☑
プールへの接続およびすべてのプールメタデータの読み取り	☑	☑	☑	☑	☑	☑
仮想 GPU の構成	☑	☑				
仮想 GPU 構成の表示	☑	☑	☑	☑	☑	☑
構成ドライブへのアクセス (CoreOS VM のみ)	☑					
コンテナ管理	☑					

アクセス権	プール管理者	プールオペレーター	VM 管理者	VM パワー管理者	VM オペレーター	読み取り専用
スケジュールされたスナップショット (既存のスナップショット スケジュールに仮想マシンを追加/削除)	☑	☑	☑			
スケジュールされたスナップショット (スナップショットスケジュールを追加/変更/削除)	☑	☑				
ヘルスチェックの構成	☑	☑				
ヘルスチェックの結果と設定の表示	☑	☑	☑	☑	☑	☑
変更ブロック追跡の構成	☑	☑	☑	☑		
変更ブロックの一覧作成	☑	☑	☑	☑	☑	
PVS アクセラレータの構成	☑	☑				
PVS アクセラレータ構成の表示	☑	☑	☑	☑	☑	☑

アクセス権の定義

役割の割り当て/変更:

- ユーザーの追加/削除
- ユーザーアカウントの役割の追加/削除
- Active Directory 統合機能の有効化および無効化（ドメインへの追加）

この権限により、あらゆる権限が付与されたり、あらゆるタスクを実行できるようになります。

警告： Active Directory 統合機能および Active Directory から追加されたすべてのサブジェクトの無効化が許可されます。

サーバーコンソールへのログイン：

- SSH を使用したサーバーコンソールへのアクセス
- XenCenter を使用したサーバーコンソールへのアクセス

警告： ルートシェルにアクセスできるため、RBAC を含むシステム全体の再設定が独断的に可能になります。

サーバーのバックアップ/復元、仮想マシンの作成/破棄操作：

- サーバーのバックアップおよび復元
- プールメタデータのバックアップおよび復元

バックアップからの復元が許可されるため、RBAC 構成の変更を元に戻すことが可能です。

OVF/OVA パッケージとディスクイメージのインポート/エクスポート：

- OVF および OVA パッケージのインポート
- ディスクイメージのインポート
- OVF/OVA パッケージとしてのエクスポート

ソケットごとのコア数の設定：

- 仮想マシンに割り当てる仮想 CPU のソケットごとのコア数の設定

仮想マシンの仮想 CPU のトポロジを指定するための権限です。

Citrix Hypervisor Conversion Manager による仮想マシンの変換：

- VMware 仮想マシンの Citrix Hypervisor 仮想マシンへの変換

VMware の仮想マシンを Citrix Hypervisor 用に変換できます。これにより、VMware のワークロードを Citrix Hypervisor 環境に移行できます。

スイッチポートロック：

- ネットワークトラフィックの制御

特定のネットワーク上のトラフィックをすべてブロック（デフォルト）したり、特定の IP アドレス以外の送信トラフィックをブロックしたりできます。

マルチパス：

- マルチパスの有効化
- マルチパスの無効化

接続中のユーザーのログアウト:

- ログインしているユーザーの切断

アラートの作成/解除:

- リソースの使用量が特定のしきい値に達したときに XenCenter で生成されるアラートの構成
- [アラート] ビューのすべてのアラートの削除

警告: プール全体のアラートの解除が許可されます。

注: アラートの表示許可は、プールへの接続およびすべてのプールメタデータの読み取り権限に含まれます。

任意のユーザーのタスクのキャンセル:

- 任意のユーザーによるタスクのキャンセル

だれが実行したタスクかにかかわらず、実行中の Citrix Hypervisor タスクをキャンセルできます。

プール管理:

- プールプロパティ (名前、デフォルト SR) の設定
- クラスタ化プールを作成する
- 高可用性の有効化、無効化、および構成
- 各仮想マシンの再起動優先度の設定
- 障害回復の構成、フェイルオーバー、フェイルバック、およびフェイルオーバーテストの実行
- ワークロードバランス (WLB) の有効化、無効化、および構成
- プールへのサーバーの追加とプールからの削除
- メンバーのマスターへの変換
- マスターアドレスの指定
- マスターアドレスのメンバーへの通知
- 新しいマスターの指定
- プールおよびサーバー証明書の管理
- パッチの適用
- サーバープロパティの設定
- サーバーのログ機能の構成
- サーバーの有効化および無効化
- サーバーのシャットダウン、再起動、および電源投入
- ツールスタックの再起動
- システム状態のレポート
- ライセンスの適用
- すべての仮想マシンのほかのサーバー上へのライブマイグレーション (保守モード、または高可用性での操作)
- サーバーの管理インターフェイスおよびセカンダリインターフェイスの設定
- サーバー管理の無効化
- クラッシュダンプの削除
- ネットワークの追加、変更、および削除

- PBD/PIF/VLAN/ボンディング/ストレージリポジトリの追加、変更、および削除
- シークレットの追加、削除、および取得

プール管理に必要なすべてのタスクに対する許可が含まれます。

注: 管理インターフェイスが機能していない場合、ローカルの root でのログイン以外は認証されません。

ライブマイグレーション:

- 2つのホストが共有するストレージ上にある仮想マシンを、1つのホストから別のホストに移行

ストレージライブマイグレーション:

- 仮想マシンが2つのホスト間で共有されているストレージ上にない場合、1つのホストから別のホストに移行
- ストレージリポジトリ間での仮想ディスク (VDI) の移動

高度な仮想マシン操作:

- 仮想マシンメモリの調整 (動的メモリ制御)
- メモリを含んだスナップショット作成、スナップショット作成、および仮想マシンのロールバック
- 仮想マシンの移行
- 仮想マシンの起動 (物理サーバーの指定を含む)
- 仮想マシンの再開

Citrix Hypervisor により選択されたサーバーとは異なるサーバー上での仮想マシンの起動操作が許可されます。

仮想マシンの作成/破棄操作:

- インストールまたは削除
- 仮想マシンの複製/コピー
- 仮想ディスク/CD デバイスの追加、削除、および構成
- 仮想ネットワークデバイスの追加、削除、および構成
- XVA ファイルのインポート/エクスポート
- 仮想マシン構成の変更
- サーバーのバックアップ/復元

注:

仮想マシン管理者の役割では、XVA ファイルを共有ストレージリポジトリがあるプールにのみインポートできます。仮想マシン管理者の役割には、XVA ファイルをホストや共有ストレージのないプールにインポートする権限はありません。

仮想マシンの **CD** メディアの変更:

- CD のイジェクト
- CD の挿入

OVF/OVA パッケージのインポート/エクスポートとディスクイメージのインポート

仮想マシンの電源状態の変更:

- 仮想マシンの起動（自動配置）
- 仮想マシンのシャットダウン
- 仮想マシンの再起動
- 仮想マシンの一時停止
- 仮想マシンの再開（自動配置）

サーバーを指定した仮想マシンの起動、再開、および移行は高度な仮想マシン操作に含まれ、このアクセス権では許可されません。

仮想マシンコンソールの表示:

- 仮想マシンコンソールの表示と操作

サーバーコンソールにはアクセスできません。

XenCenter の表示管理操作:

- グローバル XenCenter フォルダーの作成および変更
- グローバル XenCenter カスタムフィールドの作成および変更
- グローバル XenCenter 検索クエリの作成および変更

フォルダ、カスタムフィールド、および検索クエリは、そのプールにアクセスするすべての管理者ユーザーで共有されます。

自分のタスクのキャンセル:

- 自分で実行したタスクのキャンセル

監査ログの表示:

- Citrix Hypervisor 監査ログのダウンロード

プールへの接続およびすべてのプールメタデータの読み取り:

- プールへのログイン
- プールメタデータの表示
- パフォーマンスの履歴データの表示
- ログインユーザーの表示
- ユーザーおよび役割の表示
- メッセージの表示
- イベントの登録および受信

仮想 **GPU** の構成:

- プールレベルの割り当てポリシーの指定
- 仮想マシンへの仮想 GPU の割り当て
- 仮想マシンからの仮想 GPU の割り当て解除
- 許可される仮想 GPU の種類の変更
- GPU グループの作成、破棄、または割り当て

仮想 **GPU** 構成の表示:

- GPU 情報、GPU の割り当てポリシー、および仮想 GPU の割り当ての表示

構成ドライブへのアクセス (**CoreOS VM** のみ):

- 仮想マシンの構成ドライバーへのアクセス
- クラウド構成パラメーターの変更

コンテナ管理:

- 起動
- 停止
- 一時停止
- 再開
- コンテナに関するアクセス情報

スケジュールされたスナップショット:

- 既存のスナップショットスケジュールに仮想マシンを追加
- 既存のスナップショットスケジュールから仮想マシンを削除
- スナップショットスケジュールを追加
- スナップショットスケジュールを変更
- スナップショットスケジュールを削除

ヘルスチェックの構成:

- ヘルスチェックの有効化
- ヘルスチェックの無効化
- ヘルスチェック設定の更新
- サーバーの状態レポートの手動アップロード

ヘルスチェックの結果と設定の表示:

- ヘルスチェックのアップロード結果の表示
- ヘルスチェックの登録設定の表示

変更ブロック追跡の構成:

- 変更ブロック追跡の有効化
- 変更ブロック追跡の無効化
- スナップショットに関連付けられたデータを破棄してメタデータを保持
- VDI の NBD 接続情報を取得

変更ブロック追跡は、ライセンスが適用された Citrix Hypervisor Premium Edition インスタンスでのみ有効にできます。

変更ブロックの一覧作成:

- 2 つの VDI スナップショットを比較し、スナップショット間で変更されたブロックの一覧を作成します。

PVS アクセラレータの構成:

- PVS アクセラレータの有効化
- PVS アクセラレータの無効化
- (PVS アクセラレータ) キャッシュ構成のアップデート
- (PVS アクセラレータ) キャッシュ構成の追加または削除

PVS アクセラレータ構成の表示:

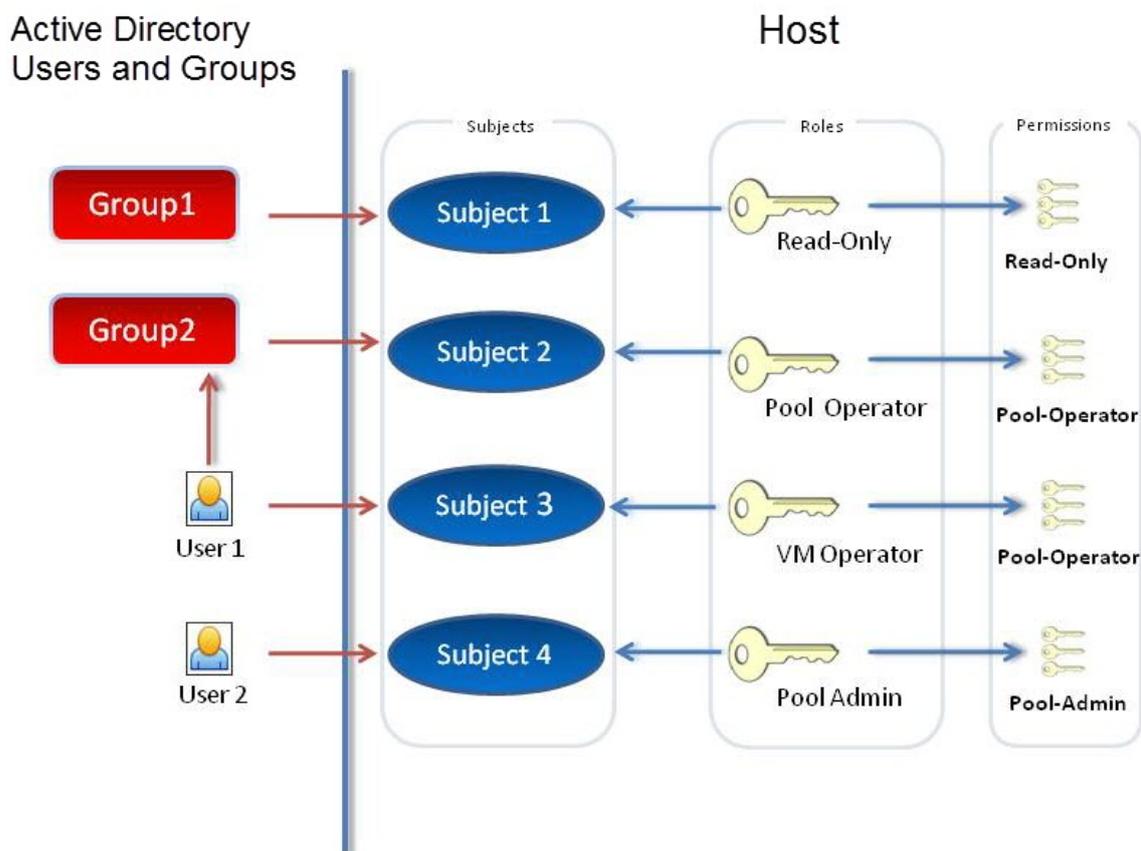
- PVS アクセラレータの状態の表示

注:

読み取り専用の役割では、昇格用の資格情報を入力しても、XenCenter のフォルダにリソースを移動できない場合があります。この問題が発生した場合は、より権限の強いユーザーアカウントで XenCenter にログインし直してから再試行してください。

Citrix Hypervisor によってユーザーに適用される役割の決定プロセス

1. Active Directory サーバーがサブジェクトを認証します。認証時に、そのサブジェクトがほかの Active Directory グループに属しているかどうかチェックされます。
2. Citrix Hypervisor が、そのサブジェクト、および所属する Active Directory グループにどの役割が割り当てられているかを検証します。
3. サブジェクトが複数の Active Directory グループに属している場合は、割り当てられている役割のすべてのアクセス許可がそのサブジェクトに継承されます。



CLI での RBAC の使用

March 12, 2020

RBAC xe CLI コマンド

役割とサブジェクトを操作するには、次のコマンドを使用します。

使用可能な役割の一覧を表示するには

次のコマンドを実行します: `xe role-list`

これにより、次のような、現在定義されている役割の一覧が表示されます。

```
1    uuid( RO ): 0165f154-ba3e-034e-6b27-5d271af109ba
```

```
2 name ( R0): pool-admin
3 description ( R0): The Pool Administrator role has full access to
4 all
5 features and settings, including accessing Dom0 and managing
6 subjects,
7 roles and external authentication
8
9 uuid ( R0): b9ce9791-0604-50cd-0649-09b3284c7dfd
10 name ( R0): pool-operator
11 description ( R0): The Pool Operator role manages host- and pool-
12 wide resources,
13 including setting up storage, creating resource pools and managing
14 patches, and
15 high availability (HA).
16
17 uuid( R0): 7955168d-7bec-10ed-105f-c6a7e6e63249
18 name ( R0): vm-power-admin
19 description ( R0): The VM Power Administrator role has full access
20 to VM and
21 template management and can choose where to start VMs and use the
22 dynamic memory
23 control and VM snapshot features
24
25 uuid ( R0): aaa00ab5-7340-bfbc-0d1b-7cf342639a6e
26 name ( R0): vm-admin
27 description ( R0): The VM Administrator role can manage VMs and
28 templates
29
30 uuid ( R0): fb8d4ff9-310c-a959-0613-54101535d3d5
31 name ( R0): vm-operator
32 description ( R0): The VM Operator role can use VMs and interact
33 with VM consoles
34
35 uuid ( R0): 7233b8e3-eacb-d7da-2c95-f2e581cdbf4e
36 name ( R0): read-only
37 description ( R0): The Read-Only role can log in with basic read-
38 only access
```

注:

役割の一覧は固定的であり、追加、削除、および変更はできません。

現在のサブジェクトの一覧を表示するには

次のコマンドを実行します。

```
1 xe subject-list
```

これにより、次のような、Citrix Hypervisor ユーザー、UUID、および割り当てられている役割の一覧が表示されます：

```
1  uuid ( R0): bb6dd239-1fa9-a06b-a497-3be28b8dca44
2  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2244
3  other-config (MRO): subject-name: example01\user_vm_admin; subject-
   upn: \
4  user_vm_admin@XENDT.NET; subject-uid: 1823475908; subject-gid:
   1823474177; \
5  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2244;
   subject-gecos: \
6  user_vm_admin; subject-displayname: user_vm_admin; subject-is-
   group: false; \
7  subject-account-disabled: false; subject-account-expired: false;
   \
8  subject-account-locked: false;subject-password-expired: false
9  roles (SR0): vm-admin
10
11  uuid ( R0): 4fe89a50-6a1a-d9dd-afb9-b554cd00c01a
12  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2245
13  other-config (MRO): subject-name: example02\user_vm_op; subject-upn
   : \
14  user_vm_op@XENDT.NET; subject-uid: 1823475909; subject-gid:
   1823474177; \
15  subject-sid: S-1-5-21-1539997073-1618981536-2562117463-2245; \
16  subject-gecos: user_vm_op; subject-displayname: user_vm_op; \
17  subject-is-group: false; subject-account-disabled: false; \
18  subject-account-expired: false; subject-account-locked: \
19  false; subject-password-expired: false
20  roles (SR0): vm-operator
21
22  uuid ( R0): 8a63fbf0-9ef4-4fef-b4a5-b42984c27267
23  subject-identifier ( R0): S
   -1-5-21-1539997073-1618981536-2562117463-2242
24  other-config (MRO): subject-name: example03\user_pool_op; \
25  subject-upn: user_pool_op@XENDT.NET; subject-uid: 1823475906; \
26  subject-gid: 1823474177; subject-s id:
```

```
27 S-1-5-21-1539997073-1618981536-2562117463-2242; \  
28 subject-gecos: user_pool_op; subject-displayname: user_pool_op; \  
29 subject-is-group: false; subject-account-disabled: false; \  
30 subject-account-expired: false; subject-account-locked: \  
31 false; subject-password-expired: false \  
32 roles (SR0): pool-operator
```

RBAC にサブジェクトを追加するには

既存の Active Directory ユーザーに RBAC の役割を割り当てるには、Citrix Hypervisor でそのユーザーアカウントまたは適切なグループアカウントのサブジェクトインスタンスを作成します。

次のコマンドを実行して、新しいサブジェクトインスタンスを追加します:

```
1 xe subject-add subject-name=AD user/group
```

新しいサブジェクトに **RBAC** の役割を割り当てるには

サブジェクトを作成したら、それに RBAC の役割を割り当てます。役割は UUID または名前で指定します:

次のコマンドを実行します:

```
1 xe subject-role-add uuid=subject uuid role-uuid=role_uuid
```

または

```
1 xe subject-role-add uuid=subject uuid role-name=role_name
```

たとえば、次のコマンドでは、UUID が b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 のサブジェクトにプール管理者の役割が割り当てられます:

```
1 xe subject-role-add uuid=b9b3d03b-3d10-79d3-8ed7-a782c5ea13b4 role-name  
=pool-admin
```

サブジェクトに割り当てられている **RBAC** の役割を変更するには

ユーザーの役割を変更するには、既存の割り当てを解除してから新しい役割を割り当てる必要があります:

次のコマンドを実行します:

```
1 xe subject-role-remove uuid=subject_uuid role-name=role_name_to_remove  
2 xe subject-role-add uuid=subject_uuid role-name=role_name_to_add
```

新しい役割を有効にするには、そのユーザーをいったんログアウトしてから再ログインする必要があります（この操作には「アクティブなユーザー接続のログアウト」権限が必要であり、この権限はプール管理者とプールオペレータに付与されます）。

警告:

プール管理者サブジェクトを追加または削除すると、このサブジェクトの SSH セッションがプール内の全ホストで有効または無効になるまでに数秒の遅延が生じる場合があります。

監査

役割ベースのアクセス制御の監査ログには、ログインしたユーザーにより実行されたすべての管理タスクが記録されます。

- 記録される各メッセージには、そのタスクを実行した管理者のサブジェクト ID およびユーザー名が記録されます。
- 許可されていない操作を実行しようとした場合は、その操作が記録されます。
- 成功した操作も記録されます。操作に失敗した場合はそのエラーコードが記録されます。

監査ログの **xe CLI** コマンド

以下のコマンドにより、そのプールの RBAC 監査ファイルのすべての記録がファイルとしてダウンロードされます。オプションの `since` パラメータを指定すると、その日時以降の記録のみがダウンロードされます。

```
1 xe audit-log-get [since=timestamp] filename=output filename
```

プールからすべての監査記録を取得するには

次のコマンドを実行します。

```
1 xe audit-log-get filename=/tmp/auditlog-pool-actions.out
```

特定の日時（ミリ秒単位）以降の監査記録を取得するには

次のコマンドを実行します。

```
1 xe audit-log-get since=2009-09-24T17:56:20.530Z \  
2 filename=/tmp/auditlog-pool-actions.out
```

特定の日時（分単位）以降の監査記録を取得するには

次のコマンドを実行します。

```
1 xe audit-log-get since=2009-09-24T17:56Z \  
2     filename=/tmp/auditlog-pool-actions.out
```

ネットワーク

March 12, 2020

このセクションでは、Citrix Hypervisor のネットワーク、VLAN、および NIC ボンディングなどについて説明します。また、ネットワーク設定の管理やトラブルシューティングについても説明します。

重要:

vSwitch は Citrix Hypervisor のデフォルトのネットワークスタックです。「vSwitch ネットワーク」の指示に従って、Linux ネットワークスタックを構成してください。

Citrix Hypervisor のネットワークの概念について理解している場合は、「[ネットワークの管理](#)」に進んで次のセクションを参照してください:

- スタンドアロン Citrix Hypervisor サーバーでのネットワークの作成
- Citrix Hypervisor サーバー間でのプライベートネットワークの作成
- リソースプール内の Citrix Hypervisor サーバーでのネットワークの作成
- スタンドアロンまたはリソースプール内の Citrix Hypervisor サーバーでの VLAN の作成
- スタンドアロン Citrix Hypervisor サーバーでのボンディングの作成
- リソースプール内の Citrix Hypervisor サーバーでのボンディングの作成

注:

「管理インターフェイス」という用語は、管理トラフィックを伝送する IP 対応 NIC を示すために使用されません。「セカンダリインターフェイス」という用語は、ストレージトラフィック用に構成された IP 対応 NIC を示すために使用されます。

サポートされるネットワーク

Citrix Hypervisor では、各ホストで最大 16 個の物理ネットワークインターフェイス（または最大 4 組のボンディングネットワークインターフェイス）がサポートされ、各仮想マシンで最大 7 個の仮想ネットワークインターフェイスがサポートされます。

注:

Citrix Hypervisor では、xe コマンドラインインターフェイス (CLI) による、NIC の自動設定と管理機能が提供されます。ホストネットワーク構成ファイルを直接編集しないでください。

vSwitch ネットワーク

コントローラアプライアンスを使用すると、vSwitch ネットワークで OpenFlow がサポートされ、ACL (Access Control List: アクセス制御リスト) などの追加機能が提供されます。Citrix Hypervisor vSwitch のコントローラアプライアンスは、vSwitch コントローラと呼ばれます。vSwitch Controller を使用すると、GUI を通じてネットワークを監視できます。vSwitch コントローラでは、以下の機能が提供されます。

- セキュリティポリシーによる、仮想マシンへのトラフィック出入力の詳細なフロー制御
- 仮想ネットワーク環境で行われるすべてのトラフィックの動作およびパフォーマンスの視覚化

vSwitch により、仮想化されたネットワーク環境における IT 管理が大幅に簡略化されます。仮想マシンがリソースプール内のある物理ホストから別の物理ホストに移行した場合でも、すべての仮想マシン構成と統計は仮想マシンにバインドされたままとなります。詳しくは、「[vSwitch と Controller](#)」を参照してください。

使用されているネットワークスタックを確認するには、次のコマンドを実行します:

```
1 xe host-list params=software-version
```

コマンドの出力で、`network_backend`の行を確認します。ネットワークスタックとして vSwitch が使用されている場合は、次のように出力されます:

```
1 network_backend: openvswitch
```

ネットワークスタックとして Linux ブリッジが使用されている場合は、次のように出力されます:

```
1 network_backend: bridge
```

Linux ネットワークスタックに戻すには、次のコマンドを実行します:

```
1 xe-switch-network-backend bridge
```

このコマンドの実行後、ホストを再起動する必要があります。

警告:

Linux ネットワークスタックでは OpenFlow がサポートされず、サーバー間のプライベートネットワークを作成することはできません。Citrix Hypervisor vSwitch Controller では、Linux ネットワークスタックは管理されません。

Citrix Hypervisor のネットワーキングの概要

ここでは、Citrix Hypervisor 環境でのネットワークに関する一般的な概念について説明します。

Citrix Hypervisor では、インストール中に物理 NIC ごとにネットワークが作成されます。サーバーをプールに追加すると、デフォルトのネットワークがマージされます。これは、同じデバイス名を持つすべての物理 NIC が必ず同じネットワークに接続されるようにするためです。

通常は、内部ネットワークを作成する場合、既存の NIC を使用して新しい VLAN を設定する場合、または NIC ボンディングを作成する場合にのみ、新しいネットワークを追加します。

Citrix Hypervisor では、4 種類のネットワークを設定できます。

- 外部ネットワークには、物理ネットワークインターフェイスが関連付けられています。外部ネットワークは、仮想マシンと、そのネットワークに接続された物理ネットワークインターフェイスとの間のブリッジを提供します。外部ネットワークを使用すると、仮想マシンは、サーバーの物理 NIC を通じて使用可能なリソースに接続できます。
- ボンディングしたネットワークでは複数の NIC を 1 つの仮想的な NIC としてボンディングして、仮想マシンとネットワークの間に単一の高性能チャネルを作成します。
- 単一サーバーのプライベートネットワークは、物理ネットワークインターフェイスに関連付けられていません。単一サーバーのプライベートネットワークは、そのホスト上の仮想マシン間での接続のみを提供します。外部には接続できません。
- サーバー間のプライベートネットワークは単一サーバーのプライベートネットワークの概念をリソースプールレベルに拡張したもので、vSwitch を使用することで同一リソースプール内の仮想マシン間での通信が可能になります。

注:

ネットワークの設定オプションには、スタンドアロン Citrix Hypervisor サーバーとリソースプールで、動作が異なるものがあります。このセクションでは、スタンドアロンホストとリソースプールの両方に適用される一般情報と、スタンドアロンホストおよびリソースプールに特有な情報について説明します。

ネットワークオブジェクト

このセクションでは、ネットワークエンティティを表すサーバー側ソフトウェアオブジェクトとして、以下のオブジェクトを使用します。

- *PIF (Physical Interface)* は、ホスト上の物理ネットワークインターフェイスを表します。PIF オブジェクトは、名前と説明、UUID、対応する NIC のパラメータ、および接続先のネットワークとサーバーという属性を持ちます。
- *VIF (Virtual Interface)* は、仮想マシン上の仮想インターフェイスを表します。VIF オブジェクトは、名前と説明、UUID、および接続先のネットワークと仮想マシンという属性を持ちます。

- ネットワークは、ホストの仮想イーサネットスイッチです。ネットワークオブジェクトは、名前と説明、UUID、および接続先の VIF と PIF の集合という属性を持ちます。

XenCenter および xe CLI を使用すると、ネットワークオプションを設定できます。管理操作に使用する NIC を制御することや、VLAN や NIC ボンディングなどの高度なネットワーク機能を作成することができます。

ネットワーク

各 Citrix Hypervisor サーバーには、1 つまたは複数のネットワークがあり、それらは仮想イーサネットスイッチです。PIF に関連付けられていないネットワークは、内部とみなされます。内部ネットワークは、同一 Citrix Hypervisor サーバー上の仮想マシン間の接続のみに使用され、外部との接続はできません。PIF に関連付けられたネットワークは、外部とみなされます。外部ネットワークは、VIF と、ネットワークに接続された PIF との間のブリッジを提供し、PIF の NIC 経由で外部ネットワーク上のリソースへの接続を可能にします。

VLAN

VLAN では、IEEE 802.1Q 標準で定義されるように、単一の物理ネットワークで複数の論理ネットワークをサポートできます。Citrix Hypervisor サーバーでは VLAN をさまざまな方法で使用できます。

注:

リソースプール、スタンドアロンホスト、そして NIC ボンディングの使用/不使用などの構成の違いにより、サポートされる VLAN 設定が異なることはありません。

仮想マシンでの VLAN の使用

802.1Q VLAN のトランクポートとして設定されているスイッチポートと Citrix Hypervisor の VLAN 機能を使用して、ゲストの仮想ネットワークインターフェイス (VIF) を特定の VLAN に接続できます。この場合、Citrix Hypervisor サーバーがゲストの VLAN タグ付けとタグ解除を実行します。

Citrix Hypervisor VLAN は、指定された VLAN タグに対応する VLAN インターフェイスを表す追加の PIF オブジェクトによって表されます。物理 NIC を表す PIF に Citrix Hypervisor ネットワークを接続して、NIC 上のすべてのトラフィックを確認できます。または、VLAN を表す PIF にネットワークを接続して、指定された VLAN タグを持つトラフィックのみを確認できます。VLAN 0 でネイティブ VLAN トラフィックのみにアクセスするようにネットワークを接続することもできます。

スタンドアロンまたはリソースプール内の Citrix Hypervisor サーバーでの VLAN の作成手順については、「[VLAN を作成する](#)」を参照してください。

管理インターフェイスでの VLAN の使用

トランクポートまたはアクセスモードポートとして設定されたスイッチポートを使用して、VLAN 上で管理インターフェイスを構成することができます。XenCenter または xe CLI を使って VLAN をセットアップし、管理インターフェイスとして使用します。詳しくは、「[管理インターフェイス](#)」を参照してください。

管理インターフェイスでの VLAN の使用

トランクポートまたはアクセスモードポートとして設定されたスイッチポートを使用して、VLAN 上で管理インターフェイスを構成することができます。XenCenter または xe CLI を使って VLAN をセットアップし、管理インターフェイスとして使用します。詳しくは、「[管理インターフェイス](#)」を参照してください。

ストレージ専用 NIC での VLAN の使用

ストレージ専用 NIC は、管理インターフェイスに関する前のセクションで説明したように、ネイティブ VLAN ポートまたはアクセスモードポートを使用するように設定できます。ストレージ専用 NIC は、IP 対応 NIC またはセカンダリインターフェイスとも呼ばれます。仮想マシンに関する前のセクションで説明したように、トランクポートと Citrix Hypervisor VLAN を使用するようにストレージ専用 NIC を設定できます。詳しくは、「[ストレージ専用 NIC を設定する](#)」を参照してください。

管理インターフェイスとゲスト VLAN を単一のホスト NIC にまとめる

単一のスイッチポートをトランク VLAN とネイティブ VLAN の両方と組み合わせることができます。これにより、1 つのホスト NIC を（ネイティブ VLAN 上の）管理インターフェイス用に使用したり、ゲスト VIF を特定の VLAN ID に接続するために使用したりできます。

ジャンボフレーム

ジャンボフレームは、ストレージトラフィックのパフォーマンスを最適化するために使用される機能です。ジャンボフレームは、1,500 バイトを超えるペイロードを含むイーサネットフレームです。通常、スループットの向上、システムバスメモリの負荷や CPU オーバーヘッドの低減を実現するために使用されます。

注:

Citrix Hypervisor では、プール内のすべてのホスト上で、ネットワークスタックとして vSwitch が使用されている場合にのみジャンボフレームがサポートされます。

ジャンボフレームを使用するための要件

ジャンボフレームを使用するには、以下の点に注意してください:

- ジャンボフレームは、プールレベルで設定されます
- プール内のすべてのホスト上で、ネットワークバックエンドとして vSwitch を設定する必要があります
- サブネット上のすべてのデバイスがジャンボフレームを使用するように設定する必要があります

- ジャンボフレームは専用のストレージネットワーク上で有効にします (推奨)
- 管理ネットワーク上でジャンボフレームを有効にする設定はサポートされていません
- 仮想マシンでのジャンボフレームの使用はサポートされていません

ジャンボフレームを使用する場合は、MTU (Maximum Transmission Unit: 最大転送単位) の値を 1500 から 9216 の範囲で指定します。XenCenter または xe CLI を使用して MTU を設定できます。

NIC ボンディング

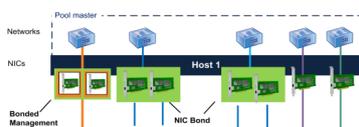
NIC ボンディングは、NIC チーミングと呼ばれることもあります。管理者は、複数の NIC を束ねて、Citrix Hypervisor サーバーの耐障害性や帯域幅を向上させることができます。NIC ボンディングは論理的には 1 つのネットワークカードとして機能し、ボンディングされたすべての NIC は MAC アドレスを共有します。

ボンディングされた NIC の一方に障害が発生すると、ホストのネットワークトラフィックは自動的に他方の NIC 経由で転送されます。Citrix Hypervisor では、最大で 8 組のボンディングネットワークがサポートされます。

Citrix Hypervisor では、アクティブ/アクティブモード、アクティブ/パッシブモード、および LACP ボンディングモードがサポートされます。ボンディングを構成できる NIC の数やサポートされるボンディングモードは、使用するネットワークスタックにより異なります。

- LACP ボンディングは、vSwitch でのみ使用できます。アクティブ/アクティブモードおよびアクティブ/パッシブモードのボンディングは、vSwitch および Linux ブリッジの両方で使用できます。
- ネットワークスタックとして vSwitch を使用する場合は、最大で 4 つの NIC を使用してボンディングを作成できます。
- Linux ブリッジネットワークスタックの場合、ボンディングを構成できる NIC は 2 つまでです。

次の図では、管理インターフェイスとして NIC ボンディングが使用されています。Citrix Hypervisor は、管理用トラフィックにこの NIC ボンディングを使用します。



すべてのボンディングモードで、フェイルオーバー機能が提供されます。ただし、すべての NIC をすべての種類のトラフィック用にアクティブに使用するモードは一部のみです。Citrix Hypervisor では、以下の種類のトラフィックで NIC ボンディングを使用できます：

- 通常の **NIC** (非管理用)：Citrix Hypervisor が仮想マシントラフィックのみに使用している NIC をボンディングできます。これらの NIC を結合すると、回復性が提供されるだけでなく、NIC 間の複数の仮想マシンからのトラフィックのバランスも調整されます。
- 管理インターフェイス：管理インターフェイスをほかの NIC とボンディングして、障害発生時に管理トラフィックが 2 つ目の NIC にフェイルオーバーされるように設定できます。アクティブ/アクティブモードでは管理インターフェイスの負荷を分散させることはできませんが、LACP (Link Aggregation Control Protocol)

モードでは可能です。ボンディングされた NIC に VLAN を作成し、ホスト管理インターフェイスをその VLAN に割り当てることができます。

- セカンダリインターフェイス: セカンダリインターフェイス (ストレージ用のインターフェイスなど) として割り当てた NIC をボンディングできます。ただし、多くの iSCSI ソフトウェアイニシエータストレージでは、負荷分散を提供しない NIC ボンディングではなく、マルチパス構成を使用することをお勧めしています。詳しくは、『*Designing Citrix Hypervisor Network Configurations*』を参照してください。

このセクションでは、iSCSI および NFS のトラフィックに対して「IP ベースのストレージトラフィック」という語を使用します。

VIF で既に使用されているインターフェイスを使用してボンディングを作成できます: この場合、仮想マシントラフィックが自動的にそのボンディングインターフェイスに移行されます。

Citrix Hypervisor では、追加の PIF は NIC ボンディングを表します。Citrix Hypervisor NIC ボンディングは、それを構成する物理デバイス (PIF) を完全に包括します。

注:

- 単一の NIC を使ってボンディングを作成することはサポートされません。
- NIC ボンディングは、FCoE トラフィックを処理する NIC でサポートされません。

IP アドレッシングの要点

NIC ボンディングの IP アドレスは、以下のように割り当てられます:

- 管理ネットワークおよびストレージネットワーク
 - 管理インターフェイスやセカンダリインターフェイスをボンディングする場合、単一の IP アドレスが割り当てられます。つまり、個々の NIC は IP アドレスを持たず、Citrix Hypervisor では、2 つの NIC が単一の論理接続として使用されます。
 - 仮想マシン以外のトラフィック用に NIC ボンディングを使用する場合 (共有ネットワークストレージや管理用 XenCenter への接続など) は、ボンディングに IP アドレスを設定します。管理インターフェイスやセカンダリインターフェイスの作成により既に NIC に IP アドレスが割り当てられている場合は、その NIC を使ってボンディングを作成すると自動的にその IP アドレスが割り当てられます。
 - IP アドレスが割り当てられていない NIC と管理インターフェイスやセカンダリインターフェイスでボンディングを作成すると、管理インターフェイスまたはセカンダリインターフェイスの IP アドレスが割り当てられます。
 - タグ付き VLAN 管理インターフェイスと他のインターフェイスをボンディングすると、ボンディングされた NIC 上に管理 VLAN が作成されます。
- 仮想マシンネットワーク: 仮想マシントラフィック用に NIC ボンディングを使用する場合、そのボンディングに IP アドレスを設定する必要はありません。これは、ボンディングが、IP アドレスが不要な OSI モデルのレイヤ 2 (データリンクレイヤ) で動作するためです。仮想マシンの IP アドレスは、VIF に割り当てられます。

ボンディングの種類

Citrix Hypervisor では、3 種類の NIC ボンディングがサポートされます。ボンディングの種類は、XenCenter または CLI コマンドを使用して設定します。

- アクティブ/アクティブモードでは、ボンディングされた NIC 間で仮想マシントラフィックが分散されま
す。「アクティブ/アクティブボンディング」を参照してください。
- アクティブ/パッシブモードでは、一方の NIC のみがトラフィックに使用されます。「アクティブ/パッシブボ
ンディング」を参照してください。
- LACP (Link Aggregation Control Protocol) モードでは、スイッチとサーバー間で NIC のアクティブ/ス
タンバイが決定されます。「LACP ボンディング」を参照してください。

注:

ボンディングは [アップ遅延] が 31,000 ミリ秒、[ダウン遅延] が 200 ミリ秒で設定されます。[アップ遅延] の値が大きいのは、一部のスイッチでポートが有効になるまでに時間がかかるためです。このように設定しないと、リンクが障害から復旧したとき、スイッチでトラフィックを転送できるようになる前に、ボンドによりそのリンクへトラフィックが再配分される可能性があります。両方の接続を別のスイッチに移動するには、第 1 の接続を移動してから 31 秒間待機して、その接続の使用が再開されてから、第 2 の接続を移動します。Up Delay の変更については、ボンディングのアップ遅延の変更を参照してください。

ボンディングの状態

Citrix Hypervisor では、各ホストのボンディングの状態がイベントログに記録されます。イベントログには、ボンディングを構成する NIC の障害や障害から回復などの情報が記録されます。同様に、以下のコマンドで `links-up` パラメータを使用して、ボンディングの状態を確認することもできます。

```
1 xe bond-param-get uuid=bond_uuid param-name=links-up
```

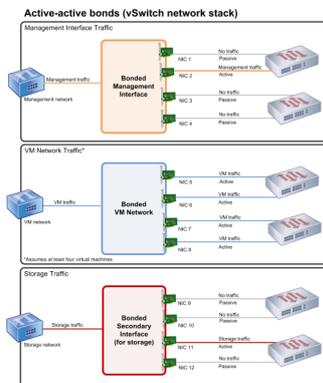
Citrix Hypervisor では、ボンディングの状態が約 5 秒ごとに確認されます。このため、ボンディングの複数の NIC に 5 秒以内に相次いで障害が発生すると、次の状態チェックまで障害がログに記録されない場合があります。

ボンディングのイベントログは、XenCenter の [ログ] タブに表示されます。XenCenter を実行していない場合は、各ホストの `/var/log/xensource.log` にもログが記録されます。

アクティブ/アクティブボンディング

アクティブ/アクティブモードの NIC ボンディングを仮想マシントラフィックで使用すると、トラフィックが両方の NIC で同時に送信されます。一方、管理トラフィックでアクティブ/アクティブモードを使用すると、1 つの NIC でトラフィックが送信され、もう 1 つの NIC は障害発生時まで使用されません。アクティブ/アクティブモードは、Linux ブリッジおよび vSwitch ネットワークスタック環境でのデフォルトの NIC ボンディングです。

ネットワークスタックとして Linux ブリッジを使用する場合、ボンディングを構成できる NIC は 2 つまでです。ネットワークスタックとして vSwitch を使用する場合、最大で 4 つの NIC を使用してアクティブ/アクティブモードのボンディングを作成できます。ただし、アクティブ/アクティブモードで 3 つまたは 4 つの NIC を使用する利点は、仮想マシントラフィックでしか発揮されません（次の図参照）。



Citrix Hypervisor では、ボンディングに複数の MAC アドレスが関連付けられている場合のみ、複数の NIC にトラフィックを送信できます。Citrix Hypervisor は、VIF の仮想 MAC アドレスに基づいて、トラフィックを分散します。つまり、以下のようになります。

- 仮想マシントラフィック：仮想マシン（ゲスト）トラフィックのみに使用される NIC ボンディングでは、すべての NIC がアクティブになり、仮想マシントラフィックが分散されます。ただし、個別の VIF のトラフィックが複数の NIC に分散されることはありません。
- 管理トラフィックまたはストレージトラフィック：複数の NIC が同時にアクティブになることはありません。アクティブな NIC に障害が発生した場合のみ、ほかの NIC がアクティブになります。管理インターフェイスまたはセカンダリインターフェイスにボンディングを使用すると、トラフィックは分散されませんが耐障害性が提供されます。
- 混合トラフィック：NIC ボンディングで IP ベースのストレージトラフィックと仮想マシントラフィックの両方が送信される場合は、仮想マシントラフィックおよびコントロールドメイントラフィックのみが分散されます。コントロールドメインは実質的に仮想マシンであるため、ほかの仮想マシンと同じように NIC を使用します。Citrix Hypervisor では、仮想マシントラフィックと同じしくみでコントロールドメインのトラフィックが分散されます。

トラフィックの分散

Citrix Hypervisor は、パケット送信元の MAC アドレスに基づいてトラフィックを複数の NIC に分散します。管理トラフィックの場合、送信元の MAC アドレスは 1 つなので、アクティブ/アクティブモードでは 1 つの NIC のみを使用され、トラフィックは分散されません。以下の 2 つの要素に基づいてトラフィックが分散されます。

- トラフィックを送信する側と受信する側の仮想マシンおよび VIF
- 送信されるデータの量（キロバイト）

Citrix Hypervisor では、各 NIC で送受信されるデータの量がキロバイト単位で評価されます。一方の NIC で送信されるデータ量が他方の NIC の量を超えると、Citrix Hypervisor によって VIF と NIC の関連付けがリバランスされます。VIF の全負荷が転送されます。1 つの VIF の負荷が 2 つの NIC 間で分割されることはありません。

アクティブ/アクティブモードの NIC ボンディングでは、複数の仮想マシンからのトラフィックが分散されますが、単一仮想マシンに対して 2 つの NIC によるスループットを提供することはできません。VIF は、ボンディングを構成する 2 つの NIC を同時に使用することはありません。Citrix Hypervisor でトラフィックのリバランスが定期的に行われる間、ボンディング内の特定の NIC に VIF が固定的に割り当てられることはありません。

アクティブ/アクティブモードは、SLB (Source Level Balancing) ボンディングと呼ばれることもあります。Citrix Hypervisor では、ボンディングされたネットワークインターフェイス間の負荷が SLB により分散されます。SLB はオープンソースの ALB (Adaptive Load Balancing) モードに由来し、ALB 機能を再利用して NIC 間で負荷を動的に再分配します。

このとき、各スレーブ (インターフェイス) に流れるバイト数は、定期的を追跡されます。新しい送信元の MAC アドレスを含んだパケットは、送信されると、負荷の低い方のスレーブインターフェイスに割り当てられます。トラフィックの再分配は、一定の間隔で行われます。

各 MAC アドレスは対応する負荷を持ち、Citrix Hypervisor は仮想マシンが送受信するデータ量に応じてその負荷全体をほかの NIC にリバランスします。アクティブ/アクティブモードでは、1 つの仮想マシンからのすべてのトラフィックを単一 NIC で送信できます。

注:

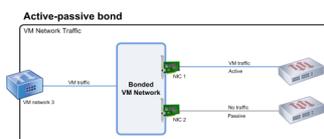
アクティブ/アクティブモードのボンディングでは、802.3ad (LACP) または EtherChannel 用のスイッチサポーターが不要です。

アクティブ/パッシブボンディング

アクティブ/パッシブボンディングでは、1 つの NIC のみにトラフィックがルーティングされます。アクティブな NIC がネットワーク接続を失うと、トラフィックはボンディング内の他の NIC にフェイルオーバーされます。アクティブ/パッシブボンディングでは、トラフィックはアクティブ NIC 経由でルーティングされます。アクティブな NIC に障害が発生すると、トラフィックはパッシブ NIC に移ります。

アクティブ/パッシブモードの NIC ボンディングは、Linux ブリッジおよび vSwitch ネットワークスタック環境で使用できます。ネットワークスタックとして Linux ブリッジを使用する場合、ボンディングを構成できる NIC は 2 つまでです。ネットワークスタックとして vSwitch を使用する場合は、最大で 4 つの NIC を使用してボンディングを作成できます。ただし、アクティブ/パッシブモードでは、ボンディングを構成する NIC のうちアクティブになるのは 1 つのみで、すべての種類のトラフィックで負荷分散は提供されません。

次の図では、2 つの NIC でアクティブ/パッシブモードのボンディングを構成しています。



アクティブ/アクティブモードは、Citrix Hypervisor のデフォルトのボンディング設定です。CLI を使用してボンディングを設定する場合は、アクティブ/パッシブモードのパラメータを指定する必要があります。それ以外の場合は、アクティブ/アクティブボンディングが作成されます。管理トラフィックやストレージトラフィック用のネットワークに必ずアクティブ/パッシブモードを使用しなければならないわけではありません。

回復性を考慮すると、アクティブ/パッシブモードが適切である場合があります。アクティブ/パッシブモードでは、トラフィックに使用される NIC が頻繁には変更されません。同様に、このモードでは 2 つのスイッチを使用して冗長性を向上できますが、スタック構成は必要はありません。管理スイッチに障害が発生した場合に、スタック構成のスイッチが単一障害点になる可能性があります。

アクティブ/パッシブモードのボンディングでは、802.3ad (LACP) または EtherChannel 用のスイッチサポートが不要です。

トラフィックの負荷分散が不要な場合、または一方の NIC にのみトラフィックを送信したい場合は、アクティブ/パッシブモードのボンディングを使用します。

重要:

VIF を作成した後やリソースプールが実務環境で動作している場合は、NIC ボンディングの作成や変更を慎重に行う必要があります。

LACP ボンディング

LACP (Link Aggregation Control Protocol) ボンディングでは、複数のポートをグループ化して単一の論理チャネルとして使用します。LACP ボンディングでは、フェイルオーバーが提供されます。また、より多くの帯域幅を使用できるようになります。

ほかのボンディングモードとは異なり、LACP ボンディングを使用するには送信側および受信側での設定が必要です：つまり、ホスト上でボンディングを作成して、スイッチ上の各ボンディングに LAG (Link Aggregation Group: リンクアグリゲーショングループ) を作成します。「LACP ボンディングのスイッチ構成」を参照してください。LACP ボンディングを使用するには、ネットワークスタックとして vSwitch を設定する必要があります。また、IEEE 802.3ad 標準をサポートするスイッチを使用する必要があります。

アクティブ/アクティブ SLB ボンディングと LACP ボンディングの比較:

アクティブ/アクティブ **SLB** ボンディング

長所:

- ハードウェア互換性リストに記載されているすべてのスイッチで使用できます。
- スタック構成をサポートしないスイッチを使用できます。
- 4 つの NIC でボンディングを構成できます。

注意事項:

- 適切な負荷分散のためには、1 つの VIF につき 1 つ以上の NIC が必要です。

- ストレージトラフィックや管理トラフィックを複数の NIC に分散させることはできません。
- 負荷分散が提供されるのは、複数の MAC アドレスが割り当てられている場合のみです。

LACP ボンディング

長所:

- すべての種類のトラフィックですべての NIC が同時にアクティブになります。
- 送信元の MAC アドレスに依存せずにトラフィックが分散されるため、すべての種類のトラフィックで負荷分散が提供されます。

注意事項:

- IEEE 802.3ad 標準をサポートするスイッチを使用する必要があります。
- スイッチ側での設定が必要です。
- vSwitch での使用のみがサポートされています。
- 単一スイッチまたはスタック構成のスイッチが必要です。

トラフィックの分散

Citrix Hypervisor では、2 種類の LACP ボンディングハッシュがサポートされています。ハッシュとは、NIC およびスイッチがトラフィックを分散する方式です。1 つは送信元および送信先の IP アドレスとポート番号に基づいてトラフィックを分散するもので、もう 1 つは送信元の MAC アドレスに基づいてトラフィックを分散するものです。

ハッシュの種類およびトラフィックの形式によっては、アクティブ/アクティブモードのボンディングよりも効率的にトラフィックを分散できます。

注:

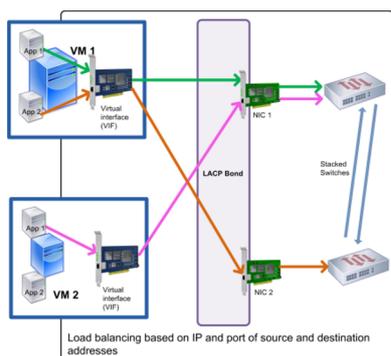
管理者は、ホストおよびスイッチ上で送信トラフィックと受信トラフィックを個別に設定します。ただし、これらの設定はホストとスイッチで異なっても構いません。

送信元/送信先のポートと **IP** による負荷分散。

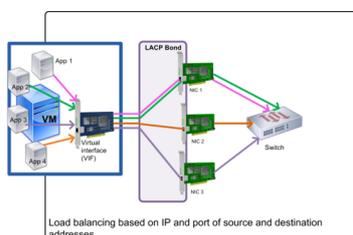
これは、LACP ボンディングのデフォルトのハッシュアルゴリズムです。送信元または送信先の IP やポートが異なる場合、1 つのゲストからのトラフィックを 2 つの NIC に分散できます。

たとえば、仮想マシン上で複数のアプリケーションを実行して、それらのアプリケーションが異なる IP またはポートを使用する場合、このハッシュアルゴリズムによりトラフィックが分散されます。トラフィックを分散することで、ゲストは総スループットを使用できるようになります。この場合、1 つの仮想マシンで複数 NIC の総合スループットを使用できるようになります。

次の図のように、1 つの仮想マシン上で実行される 2 つの異なるアプリケーションのトラフィックをそれぞれ異なる NIC に分散できます。



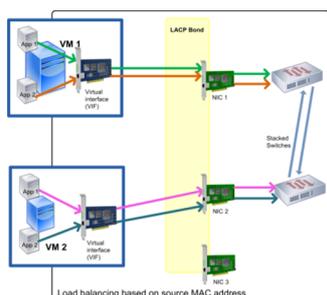
送信元および送信先の IP アドレスとポート番号に基づいた LACP ボンディングは、単一仮想マシン上の 2 つのアプリケーションのトラフィック負荷を分散させる場合に使用します。たとえば、3 つの NIC によるボンディングを単一の仮想マシンだけで使用する場合はこのオプションを使用します。



このハッシュアルゴリズムでは、送信元の IP アドレス、送信元のポート番号、送信先の IP アドレス、送信先のポート番号、および送信元の MAC アドレスという 5 つの要素により、トラフィックの分散方法が決定されます。

送信元の **MAC** アドレスによる負荷分散。

このタイプの負荷分散は、同じホスト上に複数の仮想マシンがある場合にうまく機能します。このボンディングでは、送信元の仮想マシンの MAC アドレスに基づいてトラフィックが分散されます。Citrix Hypervisor は、アクティブ/アクティブモードのボンディングと同じアルゴリズムでトラフィックを送信します。同一仮想マシンからのトラフィックが複数の NIC に分散されることはありません。このため、VIF の数が NIC よりも少ない場合、このハッシュアルゴリズムは適していません。トラフィックを複数の NIC に分散できないため、適切な負荷分散は提供されません。



スイッチ設定

必要な冗長性の程度に応じて、ボンディングした NIC を同じスイッチに接続したり、スタック構成のスイッチに個別に接続したりできます。2 つの NIC を異なるスイッチに接続した場合、一方の NIC やスイッチに障害が発生した場合に、他方の NIC にフェイルオーバーされます。スイッチを追加することで、以下のように単一障害点を排除できます。

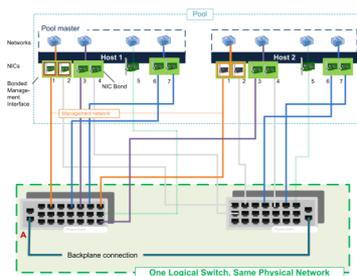
- ボンディングした管理インターフェイスの一方のリンクで 2 台目のスイッチに接続している場合、そのスイッチに障害が発生しても管理ネットワークは切断されず、ホスト間の通信も中断されません。
- すべてのトラフィックの種類で、他方の NIC またはスイッチに障害が発生しても、他方の NIC やスイッチにフェイルオーバーされるため、仮想マシンのネットワーク接続は維持されます。

LACP ボンディングの NIC を複数のスイッチに接続する場合は、スタック構成のスイッチを使用します。「スタック構成のスイッチ」とは、単一の論理スイッチとして動作する複数の物理スイッチの構成を指します。複数のスイッチを物理的に接続して、スイッチの管理ソフトウェアを使用してそれらが単一の論理スイッチユニットとして動作するように設定する必要があります。通常、スイッチのスタック構成はスイッチベンダ独自の機能拡張で提供され、ベンダによっては異なる名称が使用されている場合があります。

注:

アクティブ/アクティブモードのボンディングの問題を解決するには、スイッチをスタック構成にする必要があります。アクティブ/パッシブモードのボンディングでは、スタック構成のスイッチを使用する必要はありません。

次の図は、ボンディングされた NIC のケーブルとネットワーク構成を一致させる方法を示しています。



LACP ボンディングのスイッチ構成

スイッチ構成の詳細はベンダごとに異なるので、LACP ボンディングでのスイッチ構成には以下の考慮事項があります。

- LACP および IEEE 802.3ad 標準をサポートするスイッチを使用する必要があります。
- スイッチ上で LAG を作成するときに、全ホストの LACP ボンディングの数だけ LAG を作成する必要があります。たとえば、5 台のホストで構成されるプールで、各ホストの NIC 4 と NIC 5 で LACP ボンディングを作成した場合は、スイッチ上に 5 つの LAG を作成します。ホストの NIC に対応するポートのグループに 1 つの LAG を作成し、必要に応じて VLAN ID を追加します。
- Citrix Hypervisor の LACP ボンディングでは、LAG のスタティックモードを無効にする必要があります。

「スタック構成」で説明したように、LACP ボンディングの NIC を複数のスイッチに接続する場合は、スタック構成のスイッチを使用する必要があります。

セットアップ後のネットワークの初期設定

Citrix Hypervisor サーバーのネットワーク設定は、ホストの初回インストール時に行います。IP アドレス設定 (DHCP/静的)、管理インターフェイス用の NIC、ホスト名などのオプションは、インストール時に指定した値に基づいて設定されます。

複数の NIC を持つホストのインストール後の設定内容は、インストール時に管理用として選択した NIC によって異なります。

- ホストの NIC ごとに PIF が作成される。
- 管理インターフェイスとして選択した NIC の PIF は、インストール時に指定したオプションで IP アドレスが設定される。
- 各 PIF に対してネットワークが作成される (network 0、network 1 など)。
- 各ネットワークは個別の PIF に接続される。
- IP アドレス指定オプションは、管理インターフェイスとして使用される PIF 以外のすべての PIF に対して未設定のままである。

単一の NIC を持つホストでは、インストール後に次の内容が設定されます：

- その NIC に対応する単一の PIF が作成される。
- インストール中に指定したオプションで PIF の IP アドレスが設定され、ホストの管理が可能になる。
- その PIF がホスト管理用に設定される。
- 単一のネットワーク、network 0 が作成される。
- network 0 は PIF に接続され、仮想マシンへの外部からの接続が有効になる。

タグ付き VLAN ネットワーク上で Citrix Hypervisor をインストールした後、構成は次のようになります：

- ホストの NIC ごとに PIF が作成される。
- NIC でタグ付き VLAN の管理インターフェイスとして選択された PIF には、インストール時に指定したオプションで IP アドレスが設定される。
- 各 PIF に対してネットワークが作成される (network 1、network 2 など)。追加の VLAN ネットワークが作成される (たとえば、VLAN<TAG> 上の eth0 に関連付けられた、プール全体にわたるネットワーク用)。
- 各ネットワークは個別の PIF に接続される。その VLAN PIF がホスト管理用に設定される。

いずれの場合も、上記のネットワーク設定により、ほかのコンピュータ上の XenCenter、xe CLI、およびそのほかの管理ソフトウェアから、管理インターフェイスの IP アドレスを使用して Citrix Hypervisor サーバーに接続できるようになります。また、これらの設定により、ホスト上で作成された仮想マシンに対して外部ネットワーク機能が提供されます。

Citrix Hypervisor のインストールでは、管理操作用の PIF に対してのみ、IP アドレスが設定されます。仮想マシンの外部ネットワークは、仮想イーサネットスイッチとして動作するネットワークオブジェクトを使用して、PIF から VIF へのブリッジによって実現されます。

VLAN、NIC ボンディング、およびストレージトラフィック専用 NIC の設定などのネットワーク機能に必要な手順は、後続のセクションで説明します。

ネットワーク設定の変更

network オブジェクトを変更することで、ネットワーク設定を変更できます。つまり、network オブジェクトまたは VIF を指定してコマンドを実行します。

network オブジェクトの変更

ネットワークのフレームサイズ (MTU)、name-label、name-description、purpose などの設定を変更できます。値を変更するには、xe network-param-set コマンドとその関連パラメータを使用します。

network-param-set コマンドを実行するときは、uuid パラメータを必ず指定する必要があります。

オプションのパラメータは次のとおりです：

- 「default_locking_mode」を参照してください。「クラウド環境で VIF のロックモードを簡単に設定する」を参照してください。
- name-label
- name-description
- MTU
- 「purpose」を参照してください。「ネットワークに目的を追加する。」を参照してください。
- other-config

パラメータの値が指定されていない場合、パラメータは null 値に設定されます。マップパラメータのキーと値は、map-param:key=value 形式で指定します。

ボンディングのアップ遅延の変更

障害発生後にそのリンクにトラフィックが再配分されるのを避けるため、ボンディングのアップ遅延値としてデフォルトで 31,000 ミリ秒が設定されます。この比較的大きな Up Delay 値は、アクティブ/アクティブモードだけでなく、すべてのボンディングモードで重要な意味を持ちます。

ただし、必要に応じてこの値を変更を変更することができます。

次のコマンドを実行して、Up Delay 値をミリ秒単位で指定します：

```
1 xe pif-param-set uuid=<uuid of bond master PIF> other-config:bond-updelay=<delay in ms>
```

次のコマンドを実行して、物理インターフェイスをアンプラグして再プラグします。これにより、変更が有効になります：

```
1 xe pif-unplug uuid=<uuid of bond master PIF>
```

```
1 xe pif-plug uuid=<uuid of bond master PIF>
```

ネットワークの管理

March 12, 2020

ここで説明するネットワーク設定手順は、スタンドアロンホストとリソースプール内のホストとで異なります。

サーバー間のプライベートネットワーク

以前のバージョンの Citrix Hypervisor では、同一ホスト上の仮想マシン間でのみ通信が可能な「単一サーバーのプライベートネットワーク」を作成できました。このバージョンでは、この単一サーバーのプライベートネットワークの概念をリソースプールレベルに拡張するサーバー間のプライベートネットワークを作成できます。このプライベートネットワークでは、同一リソースプール内の仮想マシン間での通信が可能です。サーバー間のプライベートネットワークは、単一サーバーのプライベートネットワークの独立性と、リソースプール全体での接続性を兼ね備えています。このネットワークでは、による仮想マシンのライブマイグレーションなどのアジリティ機能も使用できます。

サーバー間のプライベートネットワークは、外部ネットワークから隔離されます。プライベートネットワークに接続していない仮想マシンでは、このネットワーク上にトラフィックを送受信できません。これは、その仮想マシンがほかの仮想マシンと同じ物理ホスト上にあり、同じ PIF（物理ネットワークインターフェイス）上のネットワークに VIF が接続されている場合にも当てはまります。VLAN でも同様の機能が提供されますが、サーバー間のプライベートネットワークで GRE（Generic Routing Encapsulation）IP トンネリングプロトコルを使用すると、物理スイッチファブリックを設定しなくても、ネットワークを隔離させることができます。

プライベートネットワークでは、物理スイッチファブリックを使用しなくても、以下の特長が提供されます。

- 単一サーバーのプライベートネットワークと同様の独立したネットワークを構築できる。
- リソースプール内の複数ホスト間で仮想マシンを移行できる。
- ライブマイグレーションなどの機能との互換性

サーバー間のプライベートネットワークは、NIC に IP アドレスを割り当てる必要があるため、管理インターフェイスまたはセカンダリインターフェイス上に作成する必要があります。IP アドレスが割り当てられた任意の NIC を使用してこのネットワークを作成できます。サーバー間のプライベートネットワークをセカンダリインターフェイス上に作成する場合は、このインターフェイスが隔離されたサブネットに属している必要があります。

管理インターフェイスやほかのセカンダリインターフェイスが同じサブネットに属していると、ネットワークトラフィックが正しくルーティングされません。

注:

サーバー間のプライベートネットワークを作成するには、次の条件が満たされている必要があります:

- リソースプール内のすべてのホストで Citrix Hypervisor 6.0 以降が動作している。
- リソースプール内のすべてのホストで、ネットワークスタックとして vSwitch が使用されている。
- vSwitch コントローラが実行されており、リソースプールが追加されている (vSwitch 接続に必要な初期化および構成タスクを行う vSwitch Controller がリソースプールに設定されている)。
- サーバー間のプライベートネットワークは、管理インターフェイスとして設定された NIC 上で作成する必要があります。この管理インターフェイスには、サーバー間のプライベートネットワーク用に作成した、異なるサブネット上のセカンダリインターフェイス (IP が有効な PIF) も含まれます。

vSwitch の設定について詳しくは、「[vSwitch と Controller](#)」を参照してください。プライベートネットワークを作成する方法については、XenCenter ドキュメントの「[Citrix Hypervisor のネットワークについて](#)」を参照してください。

スタンドアロンホストでのネットワークの作成

ホストのインストール時に各 PIF に対して外部ネットワークが作成されるため、追加のネットワーク作成が必要になるのは、通常以下の場合のみです:

- プライベートネットワークを使用する。
- VLAN や NIC ボンディングなどの高度な機能を使用する。

XenCenter を使用してネットワークを追加または削除する方法については、XenCenter ドキュメントの「[新しいネットワークの追加](#)」を参照してください。

Citrix Hypervisor サーバーのテキストコンソールを開きます。

次の `network-create` コマンドを実行してネットワークを作成します。これにより、新規に作成したネットワークの UUID が返されます:

```
1 xe network-create name=label=mynetwork
```

この時点で、このネットワークは PIF に接続されていないため、内部ネットワークです。

リソースプールでのネットワークの作成

リソースプール内のすべての Citrix Hypervisor サーバーで、同数の物理 NIC が装着されている必要があります。ただし、この要件はホストをプールに追加するときの絶対条件ではありません。

リソースプール内のすべてのホストでネットワークの共通セットが共有されるため、プール内のすべての Citrix Hypervisor サーバーで、同じ物理ネットワーク設定を使用することが重要です。個々のホスト上の PIF は、デバイス名に基づいたプール全体のネットワークに接続されます。たとえば、eth0 NIC を持つすべての Citrix Hypervisor サーバーでは、それに対応する PIF がプール全体の `Network 0` ネットワークに接続されます。eth1 NIC を持つホストも同様に `Network 1` ネットワークに接続され、プール内の 1 つ以上の Citrix Hypervisor サーバーに装着されたほかの NIC も同様にネットワークに接続されます。

リソースプール内の Citrix Hypervisor サーバーで NIC の数が異なると、複雑な状況になります。その理由は、一部のプールネットワークが一部のホストに対して有効にならないためです。たとえば、リソースプール内にホスト `host1` とホスト `host2` があり、`host1` に 4 つの NIC が装着されており、`host2` に 2 つの NIC が装着されている場合、eth0 と eth1 に対応する PIF に接続されたネットワークだけが `host2` 上で有効になります。つまり、`host1` 上の仮想マシンが eth2 と eth3 のネットワークに接続された 2 つの VIF を持つ場合、この仮想マシンは `host2` 上に移行できなくなります。

VLAN の作成

リソースプール内の複数のホストで使用する VLAN を作成するには、`pool-vlan-create` コマンドを実行します。これにより VLAN が作成され、必要な PIF がプール内の各ホスト上で作成され、プラグされます。詳しくは、「[pool-vlan-create](#)」を参照してください。

Citrix Hypervisor サーバーのコンソールを開きます。

次のコマンドを実行して、VLAN で使用するネットワークを作成します。これにより、新しいネットワークの UUID が返されます。

```
1 xe network-create name=label=network5
```

次の `pif-list` コマンドを実行して、目的の VLAN タグをサポートする物理 NIC に対応している PIF の UUID を確認します。これにより、既存の VLAN を含む、すべての PIF の UUID とデバイス名が返されます。

```
1 xe pif-list
```

新しい VLAN に接続するすべての仮想マシンで、目的の物理 PIF および VLAN タグを指定する VLAN オブジェクトを作成します。これにより、新しい PIF が作成され、指定したネットワークにプラグされます。また、新しい PIF オブジェクトの UUID が返されます。

```
1 xe vlan-create network-uuid=network_uuid pif-uuid=pif_uuid vlan=5
```

仮想マシンの VIF を新しいネットワークに接続します。詳しくは、「[スタンドアロンホストでネットワークを作成する](#)」を参照してください。

スタンドアロンホストでの NIC ボンディングの作成

NIC ボンディングを作成する場合、XenCenter を使用することをお勧めします。詳しくは、「[NIC の構成](#)」を参照してください。

ここでは、xe CLI を使用して、リソースプールに属していない、スタンドアロン Citrix Hypervisor サーバーの NIC ボンディングを作成します。リソースプール内の Citrix Hypervisor サーバーで NIC ボンディングを作成する方法については、「[リソースプールでの NIC ボンディングの作成](#)」を参照してください。

NIC ボンディングの作成

管理インターフェイスで NIC ボンディングを使用する場合、管理インターフェイスで使用している PIF/NIC をボンディング PIF に移動する必要があります。管理インターフェイスが自動的にボンディングの PIF に移動します。

1. 次の `network-create` コマンドを実行して、NIC ボンディングで使用するネットワークを作成します。これにより、新しいネットワークの UUID が返されます。

```
1 xe network-create name=label=bond0
```

2. 次の `pif-list` コマンドを実行して、ボンディングに使用する PIF の UUID を検出します:

```
1 xe pif-list
```

3. 次のいずれかを行います:

- アクティブ/アクティブモードのボンディング (デフォルト) を作成するには、`bond-create` コマンドを使用します。パラメーターをコマンドで区切って、新しく作成されたネットワーク UUID と、ボンディングする PIF の UUID を指定します:

```
1 xe bond-create network-uuid=network_uuid /  
2     pif-uuids=pif_uuid_1,pif_uuid_2,pif_uuid_3,pif_uuid_4
```

ボンディングを構成する NIC の数に応じて、2 つまたは 4 つの UUID を指定してください。これにより、ボンディングの UUID が返されます。

- アクティブ/パッシブモードまたは LACP モードのボンディングを作成するには、上記と同じ構文に `mode` パラメーターを追加して、`lACP` または `active-backup` を指定します:

```
1 xe bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1  
    , /  
2     pif_uuid_2,pif_uuid_3,pif_uuid_4 /  
3     mode=balance-slb | active-backup | lACP
```

ボンディングの **MAC** アドレス制御

管理インターフェイスで NIC ボンディングを作成するということは、その管理インターフェイスで使用している PIF/NIC が、ボンディングに含まれることを意味します。ホストで DHCP を使用する場合、ボンディングの MAC アドレスは使用中の PIF/NIC のものと同じになり、管理インターフェイスの IP アドレスはボンディング作成後も保持されます。

管理インターフェイスとして使用している NIC と異なる MAC アドレスをボンディングに設定することもできますが、ボンディングが有効になって MAC アドレスや IP アドレスが変更されたときに、そのホストとの既存のネットワークセッションが切断されます。

ボンディングの MAC アドレスは、以下の 2 つの方法で制御できます。

- `bond-create` コマンドで `mac` パラメーターを指定します。このパラメーターを使用して、ボンディングの MAC アドレスを任意のアドレスに設定できます。
- 管理インターフェイスのボンディングで `mac` パラメータを指定しない場合、Citrix Hypervisor ではその管理インターフェイスの MAC アドレスが使用されます。そのほかの管理インターフェイスのボンディングでは、その管理インターフェイスの MAC アドレス（および IP アドレス）が使用されます。非管理インターフェイスのボンディングでは、最初の NIC の MAC アドレスが使用されます。

NIC ボンディングを元に戻す

Citrix Hypervisor サーバーのボンディングを解除する場合は、`bond-destroy` コマンドにより「プライマリスレーブ」が自動的に管理インターフェイスとして使用されます。このため、すべての VIF が管理インターフェイスに移動します。ホストの管理インターフェイスがタグ付き VLAN にボンディングされたインターフェイス上にある場合、`bond-destroy` を実行すると、管理 VLAN はプライマリスレーブに移行します。

「プライマリスレーブ」とは、ボンディング作成時に MAC アドレスおよび IP 設定の元になった PIF を指します。2 つの NIC をボンディングする場合、以下のようにプライマリスレーブが決定されます。

1. ボンディングの一方が管理インターフェイスの場合はその NIC。
2. 管理インターフェイスが含まれないボンディングの場合は IP アドレスを持つ NIC。
3. それ以外の場合は最初の NIC。最初の NIC は、次のコマンドで確認できます。

```
1 xe bond-list params=all
```

リソースプールでの **NIC** ボンディングの作成

リソースプールでの NIC ボンディングの作成は、リソースプールにホストを追加したり仮想マシンを作成したりした後ではなく、リソースプールの初期作成時に行ってください。これにより、プールに追加するホストにボンディング設定が自動的に適用されるため、必要な手順を減らすことができます。

既存のプールに NIC ボンディングを作成する場合、以下のいずれかが必要です。

- CLI でプールマスタ上にボンディングを作成し、さらにほかのホスト上にボンディングを作成する。
- CLI でプールマスタ上にボンディングを作成し、ほかのホストを再起動する。これにより、プールマスタの設定がすべてのホストに継承されます。
- XenCenter でプールマスタ上にボンディングを作成する。プールマスタのネットワーク設定が XenCenter によりすべてのホストに同期されます。ホストの再起動も不要です。

操作が簡単であり、設定ミスを防ぐためにも、XenCenter を使用して NIC ボンディングを作成することをお勧めします。詳しくは、「[NIC の構成](#)」を参照してください。

ここでは、xe CLI を使用して、リソースプール内の Citrix Hypervisor サーバーの NIC ボンディングを作成します。スタンドアロンホストで NIC ボンディングを作成する方法については、「[スタンドアロンホストでの NIC ボンディングの作成](#)」を参照してください。

警告:

高可用性機能が有効な場合は、ネットワークボンディングを作成しないでください。ボンディングの作成処理により、実行中の高可用性ハートビートが阻害されて、ホストの自己隔離（つまりシャットダウン）を引き起こします。ホストが正しく再起動しなくなり、復元するには `host-emergency-ha-disable` コマンドを実行する必要がある場合があります。

マスターにするホストを選択します。XenServer ホストは、デフォルトで名前のないリソースプールに属します。リソースプールを作成するには、次のコマンドを実行して、名前のないリソースプールに名前を設定します。

```
1 xe pool-param-set name=label="New Pool" uuid=pool_uuid
```

NIC ボンディングの作成の手順に従って、NIC ボンディングを作成します。

プールに追加するホストでコンソールを開き、次のコマンドを実行します。

```
1 xe pool-join master-address=host1 master-username=root master-password=  
password
```

ネットワークとボンディングの情報が、新しいホストに自動的に複製されます。管理インターフェイスが、元のホスト上の NIC からボンディングの PIF に移動します。これにより、このボンディング全体が管理インターフェイスとして動作します。

次の `host-list` コマンドを実行して、そのホストの UUID を確認します:

```
1 xe host-list
```

警告:

高可用性機能が有効な場合は、ネットワークボンディングを作成しないでください。ボンディングの作成処理により、実行中の高可用性ハートビートが阻害されて、ホストの自己隔離（つまりシャットダウン）を引き起こ

します。ホストが正しく再起動しなくなり、復元するには `host-emergency-ha-disable` コマンドを実行する必要がある場合があります。

ストレージ専用 NIC の設定

ストレージなどの特定機能専用の NIC を設定するには、XenCenter または xe CLI を使用してその NIC に IP アドレスを割り当てます。NIC に IP アドレスを割り当てると、セカンダリインターフェイスが作成されます (IP アドレスが割り当てられる NIC のうち、Citrix Hypervisor を管理するために使用される管理インターフェイスを「管理インターフェイス」と呼びます)。

セカンダリインターフェイスに特定の機能を割り当てる場合、適切なネットワーク設定を行う必要があります。これは、NIC がほかの用途に使用されないようにするためです。NIC をストレージトラフィック専用にするには、ストレージターゲットにその NIC からしかアクセスできないように、NIC、ストレージターゲット、スイッチ、および VLAN を設定する必要があります。つまり、ストレージ用の NIC で送信するトラフィックを、物理的な構成や IP アドレスの設定により制限します。これにより、その NIC にほかのトラフィック (管理トラフィックなど) が送信されることを防ぎます。

ストレージトラフィック用のセカンダリインターフェイスを作成するには、次の条件を満たす IP アドレスを割り当てる必要があります:

- 使用する記憶域コントローラーと同じサブネットに属し、
- ほかのセカンダリインターフェイスや管理インターフェイスとは異なるサブネットに属しています。

複数のセカンダリインターフェイスを作成する場合は、各インターフェイスが個別のサブネットに属している必要があります。たとえば、ストレージトラフィック用のセカンダリインターフェイスを 2 つ追加する場合、3 つの異なるサブネットに属する IP アドレスが必要です。つまり、管理インターフェイスのサブネット、1 つ目のセカンダリインターフェイスのサブネット、および 2 つ目のセカンダリインターフェイスのサブネットです。

ストレージトラフィックの耐障害性を高めるためにボンディングを使用する場合は、Linux ブリッジボンディングではなく LACP を使用することを検討してください。LACP ボンディングを使用するには、ネットワークスタックとして vSwitch を設定する必要があります。詳しくは、「[vSwitch ネットワーク](#)」を参照してください。

注:

iSCSI または NFS のストレージリポジトリで使用するセカンダリインターフェイスの NIC を選択する場合、その NIC の IP サブネットが管理インターフェイスからルーティングできない隔離されたものである必要があります。ネットワークが隔離されていない場合、ホストを再起動した後のネットワークインターフェイスの初期化順序によっては、管理インターフェイスを経由してストレージトラフィックが送信される可能性があります。

PIF が別のサブネット上にあること、またはその PIF 経由で目的のトラフィックが転送されるようにネットワークトポロジに適したルーティングが設定されていることを確認します。

次のコマンドを実行して、その PIF の IP 設定を行います。このコマンドでは、`mode` パラメーターに適切な値を設定し、静的 IP アドレスを使用する場合はそのアドレス、ネットマスク、ゲートウェイ、および DNS のパラメーターを設定します:

```
1 xe pif-reconfigure-ip mode=DHCP | Static uuid=pif-uuid
```

次のコマンドを実行して、PIF の `disallow-unplug` パラメーターを `true` に設定します。

```
1 xe pif-param-set disallow-unplug=true uuid=pif-uuid
```

```
1 xe pif-param-set other-config:management_purpose="Storage" uuid=pif-  
  uuid
```

管理インターフェイスからもルーティングされるストレージ用のセカンダリインターフェイスを設定するには、以下の2つの選択肢があります（ただし、この構成は推奨されません）。

- ホストの再起動後に、セカンダリインターフェイスが正しく設定されていることを確認し、`xe pbd-unplug` コマンドと `xe pbd-plug` コマンドを使用してストレージ接続を再初期化します。これによりストレージ接続が再起動し、正しいインターフェイスにルーティングされます。
- または、`xe pif-forget` コマンドを使用してそのインターフェイスを Citrix Hypervisor データベースから消去し、コントロールドメイン内で手作業でインターフェイスを設定します。`xe pif-forget` コマンドの使用は上級者向けであり、Linux ネットワークの設定方法に関する理解が必要です。

SR-IOV 対応 NIC の使用

SR-IOV (Single Root I/O Virtualization) とは、単一の PCI デバイスを物理システム上で複数の PCI デバイスとして仮想化する技術です。実際の物理デバイスは物理機能 (PF) と呼ばれ、その他は仮想機能 (VF) と呼ばれます。ハイパーバイザーは、仮想マシン (VM) に1つまたは複数の VF を割り当てることができます。ゲストは、直接割り当てられているようにデバイスを使用できます。

1つまたは複数の NIC VF を仮想マシンに割り当てると、ネットワークトラフィックが仮想スイッチをバイパスできます。このように設定すると、各仮想マシンが NIC を直接使用しているかのように動作するため、処理のオーバーヘッドが軽減されてパフォーマンスが向上します。

SR-IOV の利点

SR-IOV VF は VIF よりも優れたパフォーマンスを提供します。同じ NIC を経由する (Citrix Hypervisor ネットワークスタックをバイパス) 異なる仮想マシンからのトラフィックをハードウェアベースで分離できます。

この機能を使用することで、以下のことを実行できます：

- SR-IOV をサポートする NIC で SR-IOV を有効にします。
- SR-IOV をサポートする NIC で SR-IOV を無効にします。
- SR-IOV VF を VF リソースプールとして管理します。

- 仮想マシンに SR-IOV VF を割り当てます。
- SR-IOV VF を構成します (MAC アドレス、VLAN、レートなど)。
- SR-IOV が Automated Certification Kit の一部としてサポートされているかを確認するテストを実行します。

システム構成

SR-IOV をサポートするには、ハードウェアプラットフォームを正しく構成する必要があります。次の技術が必要です:

- I/O MMU 仮想化 (AMD-Vi および Intel VT-d)
- Alternative Routing ID Interpretation (ARI)
- Address Translation Services (ATS)
- Access Control Services (ACS)

前述のテクノロジーを有効にするように BIOS を構成する方法については、システム付属のマニュアルを参照してください。

NIC での SR-IOV ネットワーク有効化

XenCenter で、[ネットワーク] タブの [新規ネットワーク] ウィザードを使用して、NIC 上に SR-IOV ネットワークを作成して有効にします。

仮想インターフェイス (仮想マシンレベル) への SR-IOV ネットワーク割り当て

XenCenter の仮想マシンレベルで、[ネットワーク] タブの [仮想インターフェイスの追加] ウィザードを使用して、この仮想マシンの仮想インターフェイスとして SR-IOV 対応ネットワークを追加します。詳しくは、「[新しいネットワークの追加](#)」を参照してください。

サポートされている NIC およびゲスト

サポートされているハードウェアプラットフォームと NIC の一覧については、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。特定のゲストが SR-IOV をサポートしているかを判断するには、ベンダーが提供するマニュアルを参照してください。

制限事項

- 特定の NIC がレガシードライバー（Intel I350 ファミリーなど）を使用する場合、これらのデバイスで SR-IOV を有効または無効にするには、ホストを再起動する必要があります。
- SR-IOV では HVM ゲストのみがサポートされています。
- 異なる種類の NIC があるプールレベルの SR-IOV ネットワークはサポートされていません。
- NIC のハードウェアの制限により、同じ NIC の SR-IOV VF と通常の VIF が互いに通信できない場合があります。有効にするには、通信が VF から VF または VIF から VIF へのパターンであり、VF から VIF へのパターンではないことを確認してください。
- 一部の SR-IOV VF の QoS（サービス品質）設定は、ネットワーク速度の制限をサポートしていないため、有効になりません。
- ライブマイグレーション、サスペンド、チェックポイントの実行は、SR-IOV VF を使用する仮想マシンではサポートされていません。
- SR-IOV VF はホットプラグをサポートしていません。
- レガシー NIC ドライバーを使用した一部の NIC では、ホストの再起動後 NIC が SR-IOV を有効にできない場合、再起動が必要なことがあります。
- 以前のリリースで作成された仮想マシンでは、XenCenter のこの機能を使用できません。
- 仮想マシンに SR-IOV VF がある場合、ライブマイグレーションが必要な機能は使用できません。これは、仮想マシンが物理的な SR-IOV 対応 NIC の VF に直接関連付けられるためです。SR-IOV VF で送信される仮想マシンネットワークトラフィックは、vSwitch をバイパスします。このため、ACL や QoS（サービス品質）などの機能を使用できません。
- ハードウェア制限：ハイパーバイザーから機能レベルリセット（FLR）の実行を要求された場合、SR-IOV 機能は Controller を使用してデバイスの機能を 100 ミリ秒以内に初期状態にリセットします。
- SR-IOV は、高可用性を活用する環境で使用できます。ただし、容量計画では SR-IOV は考慮されません。SR-IOV VF が割り当てられた仮想マシンは、適切なリソースを持つプール内にホストがある場合、ベストエフォート方式で再起動します。これらのリソースには、適切なネットワーク上で有効になっている SR-IOV、および空き VF が含まれます。

レガシードライバー用の **SR-IOV VF** の構成

通常、NIC がサポートできる VF の最大数は自動的に決定されます。レガシードライバー（Intel I350 ファミリーなど）を使用する NIC では、ドライバーモジュール構成ファイル内で制限が定義されているため、手動で調整する必要があります。最大値に設定するには、エディターを使用してファイルを開き、次の行を変更します。

```
1 ## VFs-maxvfs-by-user:
```

例えば、igb ドライバの最大 VF を 4 に設定するには、`/etc/modprobe.d/igb.conf`を次のように編集します：

```
1 ## VFs-param: max_vfs
2 ## VFs-maxvfs-by-default: 7
3 ## VFs-maxvfs-by-user: 4
4 options igb max_vfs=0
```

注：

- 値は `VFs-maxvfs-by-default` 行の値以下にする必要があります。
- これらのファイルの他の行は変更しないでください。
- 変更は SR-IOV を有効にする前に行う必要があります。

CLI

SR-IOV ネットワークの作成、削除、表示、および SR-IOV VF の仮想マシンへの割り当てについては、「[SR-IOV コマンド](#)」を参照してください。

出力データレート (QoS) の制御

仮想マシンが 1 秒間に送信可能な出力データ量を仮想インターフェイス (VIF) に設定して、QoS (Quality of Service: サービス品質) を制御できます。この QoS 値は、出力パケットの最大転送レートを 1 秒あたりのキロバイト単位で設定します。

この値で制御されるのは、仮想マシンからの出力 (送信) 転送レートのみです。仮想マシンの受信データ量は制限されません。受信データ量を制御する場合、ネットワークレベル (スイッチなど) で入力パケットを制限することをお勧めします。

VIF の QoS 値を設定するには、リソースプールのネットワークスタック構成に応じて、vSwitch Controller または Citrix Hypervisor (XenCenter または CLI による) を使用します。

vSwitch

構成方法は次のとおりです：

- **vSwitch Controller** - ネットワークスタックとして vSwitch を使用する場合は、これが最適な設定方法です。vSwitch スタックが使用される環境では、XenCenter の QoS オプションを使用できません。
- **xe コマンド** - `xe` コマンドで QoS 転送レートを設定することもできます。後述の例を参照してください。ただし、vSwitch コントローラのユーザーインターフェイスを使用した方が詳細に制御できます。

Linux ブリッジ

設定方法:

- **XenCenter** - [仮想インターフェイスプロパティ] ダイアログボックスで、QoS 転送レートの上限值を設定できます。
- **xe** コマンド - **xe** コマンドで QoS 転送レートを設定することもできます。後のセクションを参照してください。

重要:

ネットワークスタックとして vSwitch を使用する環境で、意図せず vSwitch Controller と Citrix Hypervisor サーバーのそれぞれに QoS 値を設定してしまうことがあります。この場合、Citrix Hypervisor によって低い方の転送レートで出力トラフィックが制御されます。

QoS の CLI コマンドの例:

以下の例では、`vif-param-set` コマンドを使用して VIF の最大転送レートを毎秒 100 キロバイトに設定しています:

```
1 xe vif-param-set uuid=vif_uuid qos_algorithm_type=ratelimit
2 xe vif-param-set uuid=vif_uuid qos_algorithm_params:kbps=100
```

注:

vSwitch Controller を使用する場合、CLI コマンドではなく vSwitch Controller で最大転送レートを設定することをお勧めします。vSwitch Controller での設定方法については、「[vSwitch と Controller](#)」を参照してください。

ネットワーク設定オプションの変更

ここでは、Citrix Hypervisor サーバーのネットワーク設定を変更する方法について説明します。これには以下のタスクが含まれます:

- ホスト名 (DNS 名) を変更する。
- DNS サーバーを追加または削除する。
- IP アドレスを変更する。
- 管理インターフェイスとして使用する NIC を変更する。
- サーバーに新しい物理 NIC を追加する。
- ネットワークに目的を追加する。
- ARP フィルタを有効にする (スイッチポートのロック)。

ホスト名

システムのホスト名 (DNS 名) はプール全体のデータベースに定義され、次の `xe host-set-hostname-live` コマンドで変更できます:

```
1 xe host-set-hostname-live host-uuid=host_uuid host-name=host-name
```

新しいホスト名は、コントロールドメインのホスト名にも自動的に反映されます。

DNS サーバー

Citrix Hypervisor サーバーの IP アドレス設定に DNS サーバーを追加したり削除したりするには、`pif-reconfigure-ip` コマンドを使用します。たとえば、静的 IP を持つ PIF の場合:

```
1 pif-reconfigure-ip uuid=pif_uuid mode=static DNS=new_dns_ip
```

スタンドアロンホストでの IP アドレス設定の変更

ネットワークインターフェイスの設定は、`xe CLI` を使用して変更できます。ネットワーク設定スクリプトを直接編集することは避けてください。

PIF の IP アドレス設定を変更するには、`pif-reconfigure-ip` コマンドを使用します。`pif-reconfigure-ip` コマンドで使用可能なオプションについて詳しくは、「[pif-reconfigure-ip](#)」を参照してください。リソースプール内のホストの IP アドレスを変更する方法については、次のセクションを参照してください。

リソースプールでの IP アドレス設定の変更

リソースプール内の Citrix Hypervisor サーバーには、管理やプール内のほかのホストとの通信に使用する単一の管理 IP アドレスがあります。管理インターフェイスの IP アドレスの変更手順は、プールマスタとそれ以外のホストで異なります。

注:

サーバーの IP アドレスやその他のネットワークパラメーターを変更するときは注意が必要です。環境のネットワークポートロジや変更内容によっては、ネットワークストレージへの接続が切断される場合があります。この問題が発生した場合は、XenCenter の [ストレージ] > [修復] コマンドや、CLI の `pbd-plug` コマンドを使用してストレージを再プラグする必要があります。この理由から、仮想マシンをほかのホストに移行してから、IP アドレス設定を変更することをお勧めします。

次の `pif-reconfigure-ip` コマンドを実行して、IP アドレスを設定します。`pif-reconfigure-ip` コマンドで使用可能なオプションについて詳しくは、「[pif-reconfigure-ip](#)」を参照してください:

```
1 xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

次の`host-list`コマンドを実行して、プール内のほかのすべての Citrix Hypervisor サーバーが認識されることを確認します（メンバホストがプールマスタに正しく再接続されたことを示します）:

```
1 xe host-list
```

プールマスタとして動作する Citrix Hypervisor サーバーの IP アドレスを変更する場合は、追加の手順が必要です。これは、各プールメンバーがプールマスタと通信するときに、変更前の古い IP アドレスが使用されるため、IP アドレスが変更されると、プールマスタとどのように接続すればよいかわからなくなるためです。

可能な場合は、リソースプールの運用中に変更される可能性が低い IP アドレスをプールマスタに割り当ててください。

次の`pif-reconfigure-ip`コマンドを実行して、IP アドレスを設定します:

```
1 xe pif-reconfigure-ip uuid=pif_uuid mode=DHCP
```

プールマスタの IP アドレスが変更され、メンバホストが接続できなくなると、すべてのメンバホストが緊急モードに切り替わります。

プールマスタ上で、次の`pool-recover-slaves`コマンドを実行します。これにより、プールマスタが各メンバホストと通信し、プールマスタの新しい IP アドレスが通知されます:

```
1 xe pool-recover-slaves
```

管理インターフェイス

複数の NIC が装着されたコンピュータに Citrix Hypervisor をインストールすると、管理インターフェイスとして使用される NIC が 1 つ選択されます。管理インターフェイスは、XenCenter とそのホスト間の通信、およびホストどうしの通信で使用されます。

次の`pif-list`コマンドを実行して、管理インターフェイスとして使用する NIC の PIF を確認します。このコマンドにより、各 PIF の UUID が返されます。

```
1 xe pif-list
```

次の`pif-param-list`コマンドを実行して、管理インターフェイスとして使用する PIF の IP アドレス設定を確認します。必要な場合は、`pif-reconfigure-ip`コマンドを使用して、その PIF の IP アドレス設定を変更します。

```
1 xe pif-param-list uuid=pif_uuid
```

次の`host-management-reconfigure`コマンドを実行して、管理インターフェイスとして使用する PIF を変更します。このホストがリソースプールに属している場合は、プールマスタ上のコンソールでこのコマンドを実行する必要があります。

```
1 xe host-management-reconfigure pif-uuid=pif_uuid
```

次の`network-list`コマンドを実行して、プールのすべてのホストで管理インターフェイスとして使用される NIC の PIF を確認します。このコマンドには、プール全体のネットワーク UUID が返されます。

```
1 xe network-list
```

`network-param-list`コマンドを使用して、リソースプールのすべてのホストの PIF UUID を取得します。次の`pif-param-list`コマンドを実行して、管理インターフェイスとして使用する PIF の IP アドレス設定を確認します。必要な場合は、`pif-reconfigure-ip`コマンドを使用して、その PIF の IP アドレス設定を変更します。

```
1 xe pif-param-list uuid=pif_uuid
```

次の`pool-management-reconfigure`コマンドを実行して、ネットワーク一覧で管理インターフェイスとして使用される PIF を変更します。

```
1 xe pool-management-reconfigure network-uuid=network_uuid
```

管理アクセスの無効化

管理コンソールへのリモートアクセスを完全に無効にするには、`host-management-disable`コマンドを使用します。

警告:

管理インターフェイスを無効にした場合、物理ホストコンソールにログインして管理タスクを行う必要があります。管理インターフェイスを無効にすると、XenCenter などの外部インターフェイスは機能しなくなります。

物理 NIC の新規追加

Citrix Hypervisor サーバーへの物理 NIC のインストールは、通常の手順で行います。ホストの再起動後、xe CLI コマンド`pif-scan`を実行して、新しい NIC 用の PIF オブジェクトを作成します。

物理 NIC の削除

NIC を削除する前に、対応する PIF の UUID を確認してください。Citrix Hypervisor サーバーから通常の方法で物理 PIF を削除します。ホストの再起動後、xe CLI コマンド`pif-forget uuid=<UUID>`を実行して、PIF オブジェクトを破棄します。

ネットワークへの目的の追加

ネットワーク目的は、ネットワークにさらに機能を追加するために使用できます。例えば、ネットワークを使用して NBD 接続を確立する機能です。

ネットワーク目的を追加するには、`xe network-param-add` コマンドを使用します：

```
1 xe network-param-add param-name=purpose param-key=purpose uuid=network-  
  uuid
```

ネットワーク目的を削除するには、`xe network-param-remove` コマンドを使用します：

```
1 xe network-param-remove param-name=purpose param-key=purpose uuid=  
  network-uuid
```

現在、ネットワーク目的で使用可能な値は `nbd` と `insecure_nbd` です。詳しくは、[Citrix Hypervisor Changed Block Tracking Guide \(英語\)](#) を参照してください。

スイッチポートロックの使用

Citrix Hypervisor のスイッチポートロック機能を使用すると、仮想マシンが MAC アドレスや IP アドレスを偽装できなくなり、不明な仮想マシンからの悪意のあるトラフィックを制御できるようになります。ポートロックコマンドでは、特定のネットワーク上のトラフィックをすべてブロック（デフォルト）したり、特定の IP アドレスからのトラフィック以外をブロックしたりできます。

クラウドサービスプロバイダでスイッチポートロック機能を使用すると、内部脅威に対するセキュリティを強化できます。仮想マシンがインターネットのパブリックな IP アドレスを使用するクラウド環境では、なりすましなどに対するセキュリティ対策を施して、クラウドのテナントがほかの仮想マシンを攻撃することを防ぐ必要があります。

スイッチポートロック機能を使用すると、すべてのテナントや仮想マシンで同じレイヤ 2 ネットワークを使用して、ネットワーク設定をシンプルにできます。

ポートロックコマンドの機能の 1 つに、信頼できない仮想マシンからのトラフィックを制限して、その仮想マシンが MAC アドレスや IP アドレスを偽装することを不可能にするものがあります。これにより、以下の行為を制限できます。

- Citrix Hypervisor の管理者が許可していない MAC アドレスや IP アドレスを偽装する。
- ほかの仮想マシンのトラフィックを傍受、なりすまし、または妨害する。

要件

- Citrix Hypervisor のスイッチポートロック機能は、Linux ブリッジおよび vSwitch ネットワークスタックでサポートされます。

- 役割ベースのアクセス制御（RBAC）を使用する環境でこの機能を設定するには、プールオペレータまたはプール管理者以上の権限を持つアカウントでログインする必要があります。RBAC を使用しない環境では、プールのルートのルートアカウントでログインする必要があります。
- ポートロックコマンドは、オンラインおよびオフラインのネットワークに対して実行できます。
- Windows 仮想マシンで切断されたネットワークアイコンを表示するには、Citrix VM Tools をインストールする必要があります。

注

スイッチポートロック構成がない場合は、VIF は「network_default」に設定され、ネットワークは「unlocked」に設定されます。

vSwitch コントローラやその他のサードパーティコントローラを使用する環境でスイッチポートロックを設定することはサポートされません。

スイッチポートロックを設定しても、以下の行為は制限されません。

- ほかのテナントやユーザーに対して IP レベルの攻撃をする。ただし、そのクラウド内のほかのテナントやユーザーになりすましたり、ほかのユーザーのトラフィックを傍受したりする IP レベル攻撃は、スイッチポートロックで防御できます。
- ネットワークリソースを過度に消費する。
- 通常のスイッチフラディングの手段（ブロードキャスト MAC アドレスまたは不明な送信先 MAC アドレスを使用するなど）を使用して、ほかの仮想マシン宛てのトラフィックを受信する。

同様に、スイッチポートロックを設定しても、仮想マシンからのトラフィックの送信先は制限されません。

実装における注意事項

スイッチポートロック機能は、コマンドラインまたは Citrix Hypervisor API を使って実装できます。特に、大規模な環境では、API を使って自動化することが一般的です。

例

ここでは、スイッチポートロック機能を使用してさまざまな攻撃から環境を保護する方法について、例を挙げて説明します。これらの例で、「VM-c」は悪意のあるテナント（Tenant C）が使用している仮想マシンを表します。「VM-a」および「VM-b」は、通常のテナントが使用している仮想マシンを表します。

例 1: スイッチポートロックによる **ARP** スプーフィングからの保護:

ARP スプーフィングとは、攻撃者が自分の MAC アドレスを別のノードの IP アドレスに関連付けようとすることです。ARP スプーフィングにより、ノードのトラフィックが攻撃者に送信される可能性があります。攻撃者はこの目標を達成するために、偽の（なりすまされた）ARP メッセージをイーサネット LAN に送信します。

シナリオ:

VM-a が VM-b の IP アドレスを指定して VM-b に IP トラフィックを送信します。VM-c の攻撃者は、ARP スプーフィングを使用して VM-b になりすまします。

1. VM-c から、推測的な ARP 応答のストリームが VM-a に送信されます。これらの ARP 応答では、VM-c の MAC アドレス (c_MAC) と VM-b の IP アドレス (b_IP) との関連付けが偽装されます。

結果: 管理者がスイッチポートロック機能を有効にしたため、偽装が無効になり、これらのパケットはすべてドロップします。

2. VM-b から VM-a への ARP 応答により、VM-b の MAC アドレス (b_MAC) が VM-b の IP アドレス (b_IP) に関連付けられます。

結果: VM-a が VM-b の ARP 応答を受信します。

例 2: IP アドレススプーフィングからの保護:

IP アドレススプーフィングは、ソース IP アドレスが偽装されたインターネットプロトコル (IP) パケットを作成することで、パケットの本当の IP アドレスを隠す手法です。

シナリオ:

攻撃者 (Tenant C) が自分のホスト (Host-C) を使用してリモートシステムにサービス拒否攻撃をしかけ、自分の ID を偽装しようとします。

試行 1:

Tenant C が Host-C の IP アドレスと MAC アドレスとして、VM-a のもの (a_IP と a_MAC) を設定します。Tenant C は、Host-C からリモートシステムに IP トラフィックを送信します。

結果: Host-C からのパケットはドロップします。これは、管理者がスイッチポートロック機能を有効にしたためです。これにより偽装が無効になり、Host-C からのパケットがドロップします。

試行 2:

Tenant C が Host-C の IP アドレスとして、VM-a のもの (a_IP) を設定し、元の c_MAC は保持します。

Tenant C は、Host-C からリモートシステムに IP トラフィックを送信します。

結果: Host-C からのパケットはドロップします。これは、管理者がスイッチポートロック機能を有効にしたためです。これにより、偽装が無効になります。

例 3: Web ホスト:

シナリオ:

山田氏はインフラストラクチャ管理者です。

彼のテナント (Tenant B) は自分の仮想マシン VM-b で複数の Web サイトをホストしています。各 Web サイトでは、同一仮想ネットワークインターフェイス (VIF) 上でホストされる個別の IP アドレスが必要です。

山田氏は Host-B の VIF を再設定して、この VIF が単一 MAC アドレスと複数 IP アドレスを保持するように変更します。

スイッチポートロック機能のしくみ

スイッチポートロック機能により、以下の 2 つのレベルでパケットフィルタを制御できます。

- **VIF レベル:** VIF 上での設定により、パケットがどのようにフィルタされるかが決定されます。仮想マシンからのすべてのトラフィックをブロックしたり、その VIF に関連付けられている IP アドレスを使用したトラフィックだけを送信したり、その VIF が接続しているネットワーク上のすべての IP アドレスにトラフィックを送信したりできます。
- **ネットワークレベル:** Citrix Hypervisor ネットワークにより、パケットがどのようにフィルタされるかが決定されます。VIF のロックモードを `network_default` に設定すると、ネットワークレベルのロック設定に基づいて許可されるトラフィックが決定されます。

使用するネットワークスタックにかかわらず、この機能は同じしくみで動作します。ただし、後続のセクションで説明するように、Linux ブリッジでは IPv6 でのスイッチポートロックが完全にはサポートされません。

VIF のロックモード

Citrix Hypervisor のスイッチポートロック機能では、VIF に 4 つのロックモードを設定できます。これらのロックモードは、実行中の仮想マシンに接続されている VIF に対してのみ適用されます。

![この図は、ネットワークのロックモードが「unlocked」に設定されているときの VIF のロックモードを示しています。左の図では、VIF のロックモードが「network_default」に設定されており、仮想マシンからのトラフィックはフィルタされません。中央の図では、VIF のロックモードが「disabled」に設定されており、すべての送受信パケットがブロックされます。右の図では、VIF のロックモードが「locked」に設定されており、正しい MAC アドレスおよび IP アドレスを含んでいるパケットだけが送信されます。](/en-us/citrix-hypervisor/media/vif-switch-port-locking-modes.png)

- **Network_default:** VIF のロックモードを `network_default` に設定すると、Citrix Hypervisor はネットワークの `default-locking-mode` パラメーターに基づいてその VIF を介したパケットをフィルタします。動作は、関連付けられたネットワークのネットワークデフォルトロックモードパラメーターが無効またはロック解除に設定されているかどうかによって異なります：

- ネットワークのロックモードが `default-locking-mode=disabled` の場合、Citrix Hypervisor によって VIF ですべてのトラフィックをドロップするフィルタ規則が適用されます。

- ネットワークのロックモードが `default-locking-mode=unlocked` の場合、Citrix Hypervisor によって VIF のすべてのフィルタ規則が解除されます。 `default-locking-mode` パラメーターのデフォルト値は `unlocked` です。

`default-locking-mode` パラメーターについては、「[ネットワークコマンド](#)」を参照してください。

ネットワークの `default-locking-mode` パラメーターの設定がそのネットワークに接続している VIF のフィルタ規則に影響するのは、その VIF のロックモードが `network_default` である場合のみです。

注:

VIF がアクティブな場合、そのネットワークの `default-locking-mode` パラメーターを変更することはできません。

- **locked:** VIF のロックモードを `locked` に設定すると、Citrix Hypervisor はその VIF で特定の MAC アドレスおよび IP アドレスとの送受信トラフィックのみを許可します。このモードで IP アドレスが指定されていない場合、仮想マシンはそのネットワーク上の VIF を介してトラフィックを送信できません。

VIF でのトラフィックを許可する IP アドレスを指定するには、IPv4 または IPv6 の IP アドレスを `ipv4_allowed` または `ipv6_allowed` パラメーターで指定します。ただし、Linux ブリッジを使用する環境では、IPv6 アドレスを指定しないでください。

Citrix Hypervisor Linux ブリッジがアクティブな場合でも、IPv6 アドレスを指定すること自体は可能ですが、Citrix Hypervisor ではその IPv6 アドレスでトラフィックをフィルタすることはできません。Linux ブリッジには NDP (Neighbor Discovery Protocol) パケットをフィルタするモジュールがないため、完全な保護を実装できません。このため、NDP パケットを偽造することで仮想マシンが偽装される場合があります。この結果、Linux ブリッジ環境で IPv6 アドレスを指定しても、Citrix Hypervisor によってすべての IPv6 トラフィックがその VIF で許可されてしまいます。IPv6 アドレスを指定しなければ、Citrix Hypervisor によってすべての IPv6 トラフィックがその VIF でドロップされます。

- **unlocked:** すべてのネットワークトラフィックが許可され、その VIF を通過できるようになります。つまり、その VIF で送受信されるトラフィックにいかなるフィルタも適用されません。
- **disabled:** すべてのネットワークトラフィックが禁止され、その VIF を通過できなくなります。つまり、Citrix Hypervisor によって VIF ですべてのトラフィックをドロップするフィルタ規則が適用されます。

スイッチポートロックの設定

ここでは、以下の手順について説明します:

- VIF で特定の IP アドレスのトラフィックだけを許可する。
- 許可する IP アドレスの一覧にほかの IP アドレスを追加する。たとえば、仮想マシンがネットワークに接続されて実行中に、VIF に IP アドレスを追加する場合（たとえば、ネットワークを一時的にオフラインにしている場合）。
- 許可する IP アドレスの一覧から特定の IP アドレスを削除する。

VIF のロックモードを `locked` に設定すると、`ipv4-allowed` または `ipv6-allowed` パラメーターで指定された IP アドレスのトラフィックだけが許可されるようになります。

VIF に複数の IP アドレスが割り当てられることもあるため、これらのパラメータでは、複数の IP アドレスを指定することもできます。

これらの手順は、VIF の接続前および接続後（仮想マシンの起動後）に実行できます。

VIF のロックモードが `locked` に設定されていない場合は、次のコマンドで `locking-mode` パラメーターに `locked` を指定します。

```
1 xe vif-param-set uuid=vif-uuid locking-mode=locked
```

ここで、`vif-uuid`にはVIFのUUIDを指定します。VIFのUUIDを確認するには、そのホスト上で`xe vif-list`コマンドを実行します。`vm-uuid` 仮想マシンのUUID (`vm-uuid`) ごとに各デバイスの一覧が表示され、デバイスIDは、VIFのデバイス番号を示します。

`vif-param-set`コマンドに以下のパラメータを使用して、許可するIPアドレスを指定します。以下のいずれか、または両方を実行します：

- 許可するIPv4 IPアドレスを指定します。次に例を示します：

```
1 xe vif-param-set uuid=vif-uuid ipv4-allowed=comma separated list
  of ipv4-addresses
```

- 許可するIPv6 IPアドレスを指定します。次に例を示します：

```
1 xe vif-param-set uuid=vif-uuid ipv6-allowed=comma separated list
  of ipv6-addresses
```

複数のIPアドレスをコンマで区切って入力できます。

上記の手順で許可されるIPアドレスを指定した後で、そのVIFに許可されるIPアドレスを追加することができます。

`vif-param-add`コマンドに以下のパラメータを使用して、許可するIPアドレスを追加します。以下のいずれか、または両方を実行します：

- IPv4 IPアドレスを指定します。次に例を示します：

```
1 xe vif-param-add uuid=vif-uuid ipv4-allowed=comma separated list
  of ipv4-addresses
```

- IPv6 IPアドレスを指定します。次に例を示します：

```
1 xe vif-param-add uuid=vif-uuid ipv6-allowed=comma separated list
  of ipv6-addresses
```

許可するIPアドレスとして複数のアドレスが指定されている場合は、特定のIPアドレスを削除して、そのアドレスのトラフィックをドロップできます。

`vif-param-remove`コマンドに以下のパラメータを使用して、削除するIPアドレスを指定します。以下のいずれか、または両方を実行します：

- 削除するIPv4 IPアドレスを指定します。次に例を示します：

```
1 xe vif-param-remove uuid=vif-uuid ipv4-allowed=comma separated
  list of ipv4-addresses
```

- 削除する IPv6 IP アドレスを指定します。次に例を示します:

```
1 xe vif-param-remove uuid=vif-uuid ipv6-allowed=comma separated
  list of ipv6-addresses
```

仮想マシンが特定のネットワークでトラフィックを送信したり受信したりできなくする

ここでは、仮想マシンで特定の VIF を介した送受信を禁止します。VIF は特定の Citrix Hypervisor ネットワークに接続するため、この手順を使用して仮想マシンが特定のネットワークを介して通信できないように設定できます。これにより、ネットワーク全体を無効にしなくても、トラフィックの送受信を詳細に制御できるようになります。

CLI コマンドを使用する場合、VIF の接続を解除しなくてもその VIF のロックモードを設定できます。このコマンドでは、実行中の VIF のフィルタ規則を変更できます。ネットワーク接続は許可されているように表示されますが、仮想マシンから送信されるパケットは VIF ですべてドロップされます。

ヒント:

VIF の UUID を確認するには、そのホスト上で `xe vif-list` コマンドを実行します。デバイス ID は、VIF のデバイス番号を示します。

VIF がトラフィックを受信しないようにするには、次のコマンドを実行して、禁止するネットワークに接続している VIF のロックモードを `disabled` に設定します:

```
1 xe vif-param-set uuid=vif-uuid locking-mode=disabled
```

また、XenCenter で VIF を無効にすることもできます。これを行うには、仮想マシンの [ネットワーク] タブでその VIF を選択して、[非アクティブ化] をクリックします。

VIF の IP アドレス制限の解除

VIF のロックモードを元のデフォルトの設定に戻すには、以下の手順に従います。新規に作成する VIF には、Citrix Hypervisor によって「unlocked」のロックモードが設定され、すべての IP アドレスのトラフィックが許可されます。

VIF をロック解除状態に戻すには、VIF のデフォルトのロックモードを `unlocked` に変更します。ロックモードが `unlocked` に設定されていない場合は、次のコマンドを実行します:

```
1 xe vif-param-set uuid=vif_uuid locking-mode=unlocked
```

クラウド環境での VIF ロックモードの簡単設定

クラウド環境では、各 VIF に対してロックモードコマンドを個別に実行せずに、すべての VIF がデフォルトで `disabled` になるように設定できます。これを行うには、ネットワークレベルでパケットのフィルタ規則を変更しま

す。これにより、前のセクション「スイッチポートロック機能のしくみ」で説明したように、パケットがどのようにフィルタされるかが Citrix Hypervisor ネットワークにより決定されるようになります。

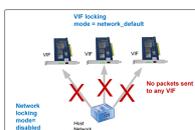
ネットワークの **default-locking-mode** パラメータにより、新しく作成する VIF のデフォルトの動作が決定されます。VIF の **locking-mode** が **network_default** の場合、ネットワークレベルのロックモード (**default-locking-mode**) が参照され、その設定により VIF でパケットの通過を禁止するか許可するかが決定されます。

- **unlocked**: ネットワークの **default-locking-mode** パラメータが **unlocked** の場合、Citrix Hypervisor によってそのネットワークが接続する VIF ですべてのトラフィックが許可されます。
- **disabled**: ネットワークの **default-locking-mode** パラメータが **disabled** の場合、Citrix Hypervisor によってそのネットワークが接続する VIF ですべてのトラフィックをドロップするフィルタ規則が適用されます。

XenCenter や CLI で作成するネットワークの **default-locking-mode** パラメータには、デフォルトで **unlocked** が設定されます。

VIF のロックモードをデフォルト (**network_default**) のままにしておくことで、ネットワークの **default-locking-mode** パラメータでそのネットワークに接続するすべての VIF のフィルタ規則を制御できます。

次の図は、各 VIF の **locking-mode** パラメータがデフォルト値 (**network_default**) の場合に、ネットワークの **default-locking-mode** パラメータの設定がすべての VIF に適用されることを示しています。



たとえば、デフォルトでは、新しく作成される VIF の **locking-mode** は **network_default** に設定されるため、ネットワークの **default-locking-mode** を **disabled** に設定した場合、ロックモードが設定されていないすべての VIF にこの設定が適用されます。この設定を特定の VIF で変更するには、その VIF の **locking-mode** パラメータを変更するか、VIF の **locking-mode** パラメータを明示的に **unlocked** に設定します。これは、特定の仮想マシンを十分に信頼しているため、そのトラフィックをまったくフィルタリングしたくない場合に役立ちます。

ネットワークのデフォルトのロックモード設定を変更するには:

ネットワークを作成した後で、次のコマンドを実行してデフォルトのロックモードを変更します。

```
1 xe network-param-set uuid=network-uuid default-locking-mode=[unlocked|disabled]
```

注:

ネットワークの UUID を確認するには、`xe network-list` コマンドを実行します。このコマンドは、コマンドを実行したホスト上のすべてのネットワークの UUID を表示します。

ネットワークのデフォルトのロックモード設定を確認するには:

以下のいずれかのコマンドを実行します:

```
1 xe network-param-get uuid=network-uuid param-name=default-locking-mode
```

または

```
1 xe network-list uuid=network-uuid params=default-locking-mode
```

VIF トラフィックフィルタリングのネットワーク設定を使用する

Citrix Hypervisor ネットワークの**default-locking-mode**設定に基づいて、そのネットワークに接続する仮想マシン上の VIF のフィルタ規則を制御するには、以下の手順に従います。

1. VIF のロックモードが `network_default` に設定されていない場合は、次のコマンドを実行します:

```
1 xe vif-param-set uuid=vif_uuid locking-mode=network_default
```

2. VIF のロックモードが `unlocked` に設定されていない場合は、次のコマンドを実行します:

```
1 xe network-param-set uuid=network-uuid default-locking-mode=  
unlocked
```

ネットワークのトラブルシューティング

March 12, 2020

ネットワーク設定に問題が生じた場合は、まずコントロールドメインの `ifcfg-*` ファイルを直接変更していないことを確認します。`ifcfg` ファイルは、コントロールドメインのホストエージェントによって直接管理され、変更内容は上書きされます。

ネットワーク障害を診断する

一部のモデルのネットワークカードでは、ベンダーからのファームウェアアップデートを適用しないと、特定の最適化機能を有効にした状態や過負荷状態で正しく動作しない場合があります。仮想マシンへのトラフィックが破損する場合は、まずベンダーから最新のファームウェアアップデートが入手可能かどうか、BIOS をアップデートする必要があるかどうかを確認してください。

ネットワークの問題が解決されない場合は、CLI を使用して物理インターフェイスの受信/送信オフロード最適化機能を無効にします。

警告:

受信/送信オフロード最適化機能を無効にすると、パフォーマンスが低下したり CPU 使用率が増加したりすることがあります。

まず、その物理インターフェイスの UUID を確認します。このとき、次のように、`device`パラメータでデバイスを指定できます:

```
1 xe pif-list device=eth0
```

次に、その PIF に対して次のパラメータを指定して、TX オフロード機能を無効にします。

```
1 xe pif-param-set uuid=pif_uuid other-config:ethtool-tx=off
```

最後に、変更を有効にするために、PIF を再プラグするかホストを再起動します。

緊急時のネットワークリセット

ネットワークの設定に不備があると、ネットワークが切断されます。ネットワーク接続がないと、XenCenter やリモートからの SSH を使って Citrix Hypervisor サーバーにアクセスできなくなります。このような問題が発生した場合は、緊急時のネットワークリセット機能を使用して、ホストのネットワークを簡単に復元およびリセットできます。

この機能は、CLI の `xe-reset-networking` コマンドや、`xsconsole` の **[Network and Management Interface]** セクションで実行できます。

ネットワークが切断される主な原因として、ネットワークインターフェイスの名前を変更したり、ボンディングや VLAN を作成したり、管理インターフェイスを変更したりするときの設定ミスが挙げられます。たとえば、IP アドレスの入力ミスなどです。このユーティリティは、次のシナリオでも実行できます:

- プールのローリングアップグレード、手作業でのアップグレード、Hotfix やドライバのインストール時に接続が切断された場合、または
- プールマスターやメンバホストがプール内のほかのホストと通信できなくなった場合。

ただし、`xe-reset-networking`の機能を使用するのは緊急時のみにしてください。この機能により、そのホストのすべての PIF、ボンディング、VLAN、およびトンネル設定が削除されます。仮想マシンのネットワークや VIF は削除されません。この機能を実行すると、実行中の仮想マシンが強制的にシャットダウンされます。このため、可能な場合は仮想マシンを正しくシャットダウンしておいてください。ネットワークをリセットする前に、管理ネットワークの IP 設定 (DHCP または固定アドレス) を変更できます。

プールマスターでネットワークリセットが必要な場合は、まずプールマスターでネットワークをリセットしてから、プールメンバーでネットワークリセットを適用します。その後で、すべてのプールメンバのネットワークをリセットして、プールのネットワーク設定を統一します。ネットワーク設定の統一がとれていることは、ライブマイグレーションにとって重要な要素です。

注:

ネットワークリセットや `xe host-management-reconfigure` によりプールマスタの IP アドレス（管理インターフェイス）が変更された場合は、そのプール内のすべてのホストでもネットワークリセットを実行する必要があります。これにより、新しい IP アドレスでプールマスタに接続できるようになります。この場合、プールマスタの IP アドレスを正しく指定する必要があります。

高可用性が有効なプールでネットワークリセット機能を使用することはサポートされません。このシナリオでネットワーク設定をリセットするには、まず高可用性を手動で無効にしてから、ネットワークリセットコマンドを実行する必要があります。

ネットワークリセットの検証

ネットワークリセット後の設定モードを指定したら、ホストの再起動後に適用される設定内容が `xsconsole` および CLI に表示されます。変更が必要な場合はここで変更します。これ以降の手順では変更できません。ホストを再起動したら、XenCenter または `xsconsole` を使用して新しいネットワーク設定を確認できます。XenCenter では、ホストの [ネットワーク] タブに新しいネットワーク設定が表示されます。**xsconsole** では、[Network and Management Interface] セクションに表示されます。

注:

緊急時のネットワークリセットは、ほかのプールメンバ上でも実行してください。これにより、プールマスタからボンディング、VLAN、およびトンネルの設定が複製されます。

CLI を使用したネットワークリセット

次の表は、`xe-reset-networking` コマンドで指定できるパラメータの一覧です。

警告:

`xe-reset-networking` コマンドのパラメータは、慎重に使用してください。不適切なパラメータを指定すると、ネットワークの接続や設定が失われることがあります。この場合、パラメータを何も指定せずに `xe-reset-networking` コマンドを再実行することをお勧めします。

プール全体のネットワーク設定をリセットする場合は、まずプールマスタから行い、引き続きすべてのプールメンバのネットワークをリセットしてください。

パラメーター	必須/オプション	説明
<code>-m, --master</code>	オプション	プールマスタの管理インターフェイスの IP アドレスです。デフォルトは、プールマスタで最後に使用されていた IP アドレスです。

パラメーター	必須/オプション	説明
<code>--device</code>	オプション	管理インターフェイスのデバイス名です。デフォルトは、インストール時に指定されたデバイス名です。
<code>--mode=static</code>	オプション	管理インターフェイスの静的 IP アドレスを設定します。以下の 4 つのパラメータを指定します。このパラメータを指定しない場合は、DHCP が使用されます。
<code>--ip</code>	必須、 <code>mode=static</code> の場合	ホストの管理インターフェイスの IP アドレスです。 <code>mode=static</code> の場合にのみ有効です。
<code>--netmask</code>	必須、 <code>mode=static</code> の場合	管理インターフェイスのネットマスクです。 <code>mode=static</code> の場合にのみ有効です。
<code>--gateway</code>	オプション	管理インターフェイスのゲートウェイです。 <code>mode=static</code> の場合にのみ有効です。
<code>--dns</code>	オプション	管理インターフェイスの DNS サーバーです。 <code>mode=static</code> の場合にのみ有効です。
<code>--vlan</code>	オプション	管理インターフェイスの VLAN タグ。デフォルトはインストール時に指定した VLAN タグです。

プールマスタでのコマンド例

ここでは、プールマスタに対して実行するコマンドの例を挙げます：

DHCP 環境でネットワーク設定をリセットするには

```
1 xe-reset-networking
```

静的 IP アドレス環境でネットワーク設定をリセットするには：

```
1 xe-reset-networking --mode= static --ip=ip-address \  
2 --netmask=netmask --gateway=gateway \  
3
```

```
3 --dns=dns
```

初期セットアップ後に別のインターフェイスが管理インターフェイスになった場合に DHCP 設定のネットワークをリセットするには:

```
1 xe-reset-networking --device=device-name
```

初期セットアップ後に別のインターフェイスが管理インターフェイスになった場合に静的 IP 設定のネットワークをリセットするには:

```
1 xe-reset-networking --device=device-name --mode=static \  
2 --ip=ip-address --netmask=netmask \  
3 --gateway=gateway --dns=dns
```

VLAN 上の管理インターフェイスでネットワーク設定をリセットするには:

```
1 xe-reset-networking --vlan=VLAN TAG
```

注:

`reset-network` コマンドは、IP 構成設定とともに使用することもできます。

プールメンバでのコマンド例

プールマスタの例で挙げたすべてのコマンドは、プールメンバにも適用されます。ただし、プールマスタの IP アドレスの指定が必要になる場合があります (IP アドレスが変更された場合など)。

DHCP 環境でネットワーク設定をリセットするには

```
1 xe-reset-networking
```

DHCP 環境で、プールマスタの IP アドレスが変更された場合にネットワーク設定をリセットするには:

```
1 xe-reset-networking --master=master-ip-address
```

静的 IP アドレス環境で、プールマスタの IP アドレスが変更されていない場合にネットワーク設定をリセットするには

```
1 xe-reset-networking --mode=static --ip=ip-address --netmask=netmask \  
2 --gateway=gateway --dns=dns
```

DHCP 環境で、管理インターフェイスとプールマスタの IP アドレスがインストール時の指定から変更された場合にネットワーク設定をリセットするには:

```
1 xe-reset-networking --device=device-name --master=master-ip-address
```

ストレージ

December 30, 2019

このセクションでは、物理ストレージハードウェアを仮想マシン (VM) にマップする方法と、ストレージ関連のタスクを実行するために管理 API で使用されるソフトウェアオブジェクトについて説明します。サポートされている各ストレージタイプの詳細を示すセクションには、次の情報が含まれています：

- CLI を使用した仮想マシン用ストレージの作成手順 (タイプ固有のデバイス構成オプションを使用)
- バックアップ用のスナップショットの生成
- ストレージ管理のベストプラクティス
- 仮想ディスクの QoS (Quality of Service: サービス品質) 設定

ストレージリポジトリ (SR)

ストレージリポジトリ (SR) は、仮想マシンの仮想ディスクイメージ (VDI) が格納される特定のストレージターゲットです。仮想ディスクイメージ (VDI) は、仮想ハードディスクドライブ (HDD) を表す、抽象化されたストレージです。

ストレージリポジトリには柔軟性があり、次のドライブのサポートが組み込まれています：

ローカルで接続：

- IDE
- SATA
- SCSI
- SAS

リモートで接続：

- iSCSI
- NFS
- SAS
- ファイバチャネル

ストレージリポジトリと VDI の抽象化によって、高度なストレージ機能を、それらをサポートするストレージターゲット上で提供できるようになります。たとえば、シンプロビジョニング、VDI スナップショット、高速クローニングなどの高度な機能があります。高度な操作を直接サポートしていないストレージサブシステムの場合、これらの機能を実装するソフトウェアスタックが提供されます。このソフトウェアスタックは、Microsoft の VHD (Virtual Hard Disk: 仮想ハードディスク) 仕様に基づいています。

SR コマンドでは、格納されている個々の VDI の作成、破棄、サイズ変更、複製、接続、および検出を実行できます。

ストレージリポジトリは、永続的なオンディスクデータ構造体です。ブロックデバイスを使用する種類のストレージリポジトリでは、ストレージリポジトリの作成時にそのストレージターゲット上の既存のデータが消去されます。

NFS など、そのほかの種類のストレージリポジトリでは、ストレージレイ上にコンテナが作成されるため、既存のストレージリポジトリは保持されます。

各 Citrix Hypervisor サーバーでは、複数の異なる種類のストレージリポジトリを同時に使用することができます。これらのストレージリポジトリは、ホスト間で共有したり、特定のホスト専用に行ったりできます。共有ストレージは、定義済みのリソースプール内の複数のホスト間でプール（共有）されます。共有されたストレージリポジトリは、プールの各ホストとネットワークで接続されている必要があります。リソースプールでは、すべてのサーバーが少なくとも 1 つの共有ストレージリポジトリを使用している必要があります。共有ストレージを複数のプール間で共有することはできません。

ストレージリポジトリを管理する CLI 操作は、[ストレージリポジトリコマンド](#)で説明します。

仮想ディスクイメージ (VDI)

仮想ディスクイメージ (VDI) は、仮想ハードディスクドライブ (HDD) を表す、抽象化されたストレージです。Citrix Hypervisor における仮想化されたストレージの基本単位です。仮想ディスクイメージは、Citrix Hypervisor サーバーに依存しない永続的なオンディスクオブジェクトです。VDI を管理する CLI 操作は、[VDI \(仮想ディスクイメージ\) コマンド](#)で説明します。データのディスク上の表現は、ストレージリポジトリの種類によって異なります。ストレージリポジトリごとの別個のストレージプラグインインターフェイス (SM API と呼ばれる) でデータが管理されます。

物理ブロックデバイス (PBD)

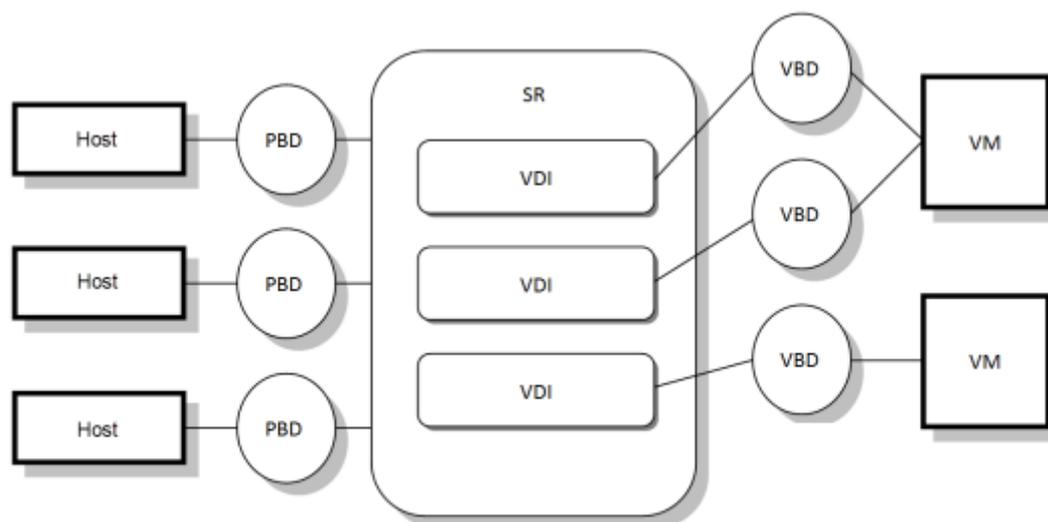
物理ブロックデバイスは、物理サーバーとストレージリポジトリの間のインターフェイスで、ストレージリポジトリをホストにマップするためのコネクタオブジェクトです。PBD には、ストレージターゲットとの接続および対話に使用するデバイス設定フィールドが格納されます。たとえば、NFS デバイス設定には、NFS サーバーの IP アドレスや、Citrix Hypervisor サーバーがマウントするパスの情報が含まれます。PBD オブジェクトにより、ストレージリポジトリと Citrix Hypervisor サーバーとのランタイム接続が管理されます。PBD に関する CLI 操作は、[PBD \(物理ブロックデバイス\) コマンド](#)で説明します。

仮想ブロックデバイス (VBD)

仮想ブロックデバイス (VBD: Virtual Block Device) は、上記の物理ブロックデバイス (PBD) に似たコネクタオブジェクトで、VDI と仮想マシンをマップします。VBD は、VDI を仮想マシンに接続するメカニズムを提供するほか、特定の VDI の QoS (サービス品質) と統計情報、およびその VDI を起動できるかどうかに関するパラメータの微調整が可能です。VBD に関する CLI 操作は、[VBD \(仮想ブロックデバイス\) コマンド](#)で説明します。

ストレージオブジェクトの相関

次の図は、ここで説明したストレージオブジェクトの相関を示しています。



仮想ディスクのデータ形式

一般に、物理ストレージと VDI のマップ形式には、次の種類があります：

1. LUN 上の論理ボリュームベースの VHD： Citrix Hypervisor のデフォルトのブロックベースストレージは、ディスク上に論理ボリュームマネージャーを挿入します。このディスクは、ローカル接続されたデバイス (LVM) か、ファイバチャネル、iSCSI、または SAS 経由の SAN 接続 LUN です。VDI は、このボリュームマネージャ内のボリュームとして表示され、スナップショットおよび複製の参照ノードのシンプロビジョニングが可能な VHD 形式で格納されます。
2. LUN 上のファイルベースの QCOW2： 仮想マシンイメージは、iSCSI ソフトウェアイニシエータまたはハードウェア HBA を介して接続された LUN 上の GFS2 共有ディスクファイルシステム上の、シンプロビジョニングされた QCOW2 形式のファイルとして格納されます。
3. ファイルシステム上のファイルベースの VHD： 仮想マシンイメージは、ローカルの共有されていないファイルシステム (EXT ストレージリポジトリ) または共有された NFS ターゲット (NFS ストレージリポジトリ) 上の、シンプロビジョニングされた VHD 形式のファイルとして格納されます。

VDI の種類

ほとんどの種類のストレージリポジトリでは、VHD 形式の VDI が作成されます。必要に応じて、Raw 形式の VDI を作成できます。このオプションは、xe CLI を使用する場合のみ指定できます。GFS2 ストレージリポジトリの場合は、QCOW2 VDI が作成されます。

VDI が `type=raw` で作成されたかどうかは、`sm-config` マップで確認できます。これらのキーやマップの値は、それぞれ `xe` コマンドの `sr-param-list` と `vdi-param-list` を実行して確認できます。

xe CLI を使用して **Raw** 形式の仮想ディスクを作成する

1. 次のコマンドを実行して、格納先のストレージリポジトリの UUID を指定して VDI を作成します。

```
1 xe vdi-create sr-uuid=sr-uuid type=user virtual-size=virtual-size  
  \  
2 name-label=VDI name sm-config:type=raw
```

2. 新しい仮想ディスクを仮想マシンに接続します。仮想マシン内でディスクツールを使用してパーティション作成およびフォーマットを行うか、新しいディスクを作成します。仮想ディスクを仮想マシンにマップする VBD を作成するには、`vbd-create` コマンドを使用します。

VDI の形式を変換する

VDI の Raw 形式と VHD 形式を直接変換することはできません。その代わりに、VDI (上記の Raw 形式、または VHD) を作成して、既存のボリュームからデータをコピーします。xe CLI を使用して、新しい VDI の仮想サイズがコピー元の VDI 以上であることを確認します。これを行うには、`vdi-param-list` コマンドの使用などにより、`virtual-size` フィールドを確認します。次に、この新しい VDI を仮想マシンに接続して、その仮想マシン内で適切なツールを使用してデータの直接ブロックコピーを行います。たとえば、Windows の標準ディスク管理ツールや Linux の `dd` コマンドです。新しいボリュームが VHD ボリュームの場合は、ディスクへの空セクタの書き込みを防ぐことができるツールを使用します。この操作により、基礎となるストレージリポジトリで領域が最適に使用されるようになります。ファイルベースのコピーを使用するほうが適切な場合があります。

VHD ベースおよび **QCOW2** ベースの **VDI**

VHD および QCOW2 イメージをチェーン化して、2 つの VDI で共通のデータを共有できます。VHD または QCOW2 ベースの仮想マシンを複製する場合、複製時にディスク上に存在したデータを複製元と複製先の仮想マシンが共有します。その後、各仮想マシンは異なるコピーオンライトバージョンの VDI で個別の変更を行います。この機能により、そのような仮想マシンをテンプレートからすぐに複製できるようになり、新しい仮想マシンのプロビジョニングと展開が容易になります。

仮想マシンやその VDI の複製を繰り返すと、チェーン化された VDI がツリー状になります。Citrix Hypervisor では、チェーン内の VDI の 1 つを削除すると、それによって不要になる VDI が削除されます。この結合プロセスは、非同期的に実行されます。解放されるディスク容量や処理に必要な時間は、VDI のサイズと共有データの量によって異なります。

VHD 形式と QCOW2 形式の両方で、シンプロビジョニングがサポートされています。仮想マシンがデータをディスクに書き込むときに、イメージファイルが自動的に細かいチャンクに拡張されます。ファイルベースの VHD と GFS2 ベースの QCOW2 の場合、この手法では、実際に仮想マシンイメージファイルに書き込まれているデータ分の領域しか物理ストレージ上で消費されないという大きな利点があります。LVM ベースの VHD では、基礎となる論理ボリュームコンテナのサイズを VDI の仮想サイズに合わせる必要があります。ただし、スナップショットまたはクローンが

発生すると、基になるコピーオンライトインスタンスディスク上の未使用領域が再利用されます。これら 2 つの動作の違いを次に説明します：

- LVM ベースの VHD イメージの場合、チェーン内の差分ディスクノードは、ディスクに書き込まれた分だけデータを使用します。ただし、リーフノード (VDI クローン) は、ディスクの仮想サイズまで完全に拡張されたままとなります。スナップショットリーフノード (VDI スナップショット) は、不使用时は縮小されたままで、その割り当てが保持されるように読み取り専用で接続できます。読み取り/書き込み形式で接続されたスナップショットノードは、接続時に完全に拡張され、接続解除時に縮小されます。
- ファイルベースの VHD および GFS2 ベースの QCOW2 イメージの場合、すべてのノードが、書き込まれた分だけデータを使用します。リーフノードファイルは、アクティブに書き込まれるにつれて、データを格納するために拡張されます。つまり、100GB の VDI を仮想マシンに割り当てて、そこにオペレーティングシステムをインストールする場合、その VDI ファイルの物理サイズは、ディスク上のオペレーティングシステムデータといくらかのメタデータのサイズを加算したものであり、100GB ではありません。

単一の VHD または QCOW2 テンプレートから複数の仮想マシンを複製する場合、複製先の各仮想マシン (子 VM) によりチェーンが形成され、新しい変更のみが子 VM に書き込まれます。古いブロックは複製元のテンプレート (親) から直接読み取られます。その子 VM をテンプレートに変換して、さらにその複製を作成すると、親、子、孫のチェーンが形成されることになり、パフォーマンスが低下します。Citrix Hypervisor では、最大チェーン長である 30 がサポートされています。正当な理由なくこの上限に近づかないようにしてください。パフォーマンスを低下させずに仮想マシンの複製を作成するには、XenCenter または `vm-copy` コマンドを使用して仮想マシンをコピーします。これにより、チェーンは 0 にリセットされます。

結合に関する VHD 特有の注意事項

ストレージリポジトリに対して同時に実行される結合プロセスは、1 つのみです。また、このプロセススレッドはストレージリポジトリのマスタホスト上で実行されます。

プール内のマスタサーバー上で重要な仮想マシンを実行している場合は、以下の手順で、入出力が低速になる可能性を軽減できます：

- ストレージリポジトリマスタでないホストに仮想マシンを移行します。
- ディスク入出力の優先度を高くして、スケジューラを設定します。詳しくは、「[仮想ディスクの QoS 設定](#)」を参照してください。

ストレージリポジトリの形式

December 30, 2019

ストレージリポジトリを作成するには、XenCenter の [新規ストレージリポジトリ] ウィザードを使用します。このウィザードには、ストレージリポジトリの設定に必要な核手順が表示されます。また、CLI の `sr-create` コマン

ドを使用することもできます。 `sr-create` コマンドでは、ストレージサブストレート上にストレージリポジトリを作成します（既存のデータが消去されることがあります）。また、ストレージリポジトリ API オブジェクトとそれに対応する物理ブロックデバイスレコードを作成します。これにより、仮想マシンでそのストレージリポジトリを使用できるようになります。ストレージリポジトリが作成されると、物理ブロックデバイスが自動的にプラグされます。ストレージリポジトリの `shared=true` フラグを設定した場合は、物理ブロックデバイスレコードが作成され、リソースプール内のすべての Citrix Hypervisor にプラグされます。

IP ベースのストレージ（iSCSI または NFS）を作成する場合は、ストレージネットワークとして管理トラフィック用の NIC を使用したり、ストレージトラフィック用の NIC を作成してそれを使用したりできます。NIC に IP アドレスを割り当てる方法については、[ストレージ専用 NIC の設定](#) を参照してください。

Citrix Hypervisor のすべての種類のストレージリポジトリで、VDI のサイズ変更、高速複製、およびスナップショットがサポートされます。LVM タイプのストレージリポジトリ（ローカル、iSCSI、および HBA）では、スナップショットおよび非表示親ノード用のシンプロビジョニングが提供されます。そのほかの種類のストレージリポジトリ（EXT3、NFS、GFS2）では、アクティブな仮想ディスクを含め、完全なシンプロビジョニングがサポートされます。

警告:

VDI スナップショットなど、仮想マシンに接続されていない VHD VDI は、デフォルトのシンプロビジョニングで格納されます。VDI を再接続するには、シックプロビジョニングになるのに十分なディスク容量を確保する必要があります。VDI クローンでは、シックプロビジョニングが使用されます。

次の表は、サポートされる最大 VDI サイズの一覧です。

ストレージリポジトリの形式	最大 VDI サイズ
EXT3	2TiB
LVM	2TiB
NFS	2TiB
LVMoFCOE	2TiB
LVMoiSCSI	2TiB
LVMoHBA	2TiB
GFS2（iSCSI または HBA を使用）	16TiB

ローカル LVM

この種類のストレージリポジトリは、ローカル接続のボリュームグループ内のディスクを示します。

デフォルトで、Citrix Hypervisor はそれ自身がインストールされた物理ホスト上のローカルディスクを使用します。仮想マシンストレージの管理には、Linux 論理ボリュームマネージャ（LVM）が使用されます。VDI は、指定されたサイズの LVM 論理ボリュームに VHD 形式で実装されます。

LVM のパフォーマンスについての注意事項

スナップショット機能および高速複製機能を LVM ベースのストレージリポジトリで使用すると、このストレージ固有のパフォーマンス上のオーバーヘッドが生じます。パフォーマンスが重視される環境では、Citrix Hypervisor によって、デフォルトの VHD 形式に加えて、Raw 形式での仮想ディスクイメージ (VDI) 作成がサポートされます。ただし、Citrix Hypervisor スナップショット機能は、Raw 形式の VDI ではサポートされません。

警告:

`type=raw` ディスクが接続された仮想マシンのスナップショットを作成しないでください。これを行うと、一部のみのスナップショットが作成されます。この場合、`snapshot-of` フィールドを確認して孤立したスナップショットを識別し、削除できます。

ローカル **LVM** ストレージリポジトリを作成する

XenServer のインストール時に、デフォルトで LVM ストレージリポジトリが作成されます。

次の表は、LVM ストレージリポジトリ用の `device-config` パラメーターの一覧です:

パラメーター名	説明	必須か
デバイス	ストレージリポジトリとして使用するローカルホスト上のデバイス名です。	はい

`/dev/sdb` にローカル LVM ストレージリポジトリを作成する場合は、次のコマンドを実行します。

```
1  xe sr-create host-uuid=valid_uuid content-type=user \
2  name-label="Example Local LVM SR" shared=false \
3  device-config:device=/dev/sdb type=lvm
```

ローカル **EXT3**

EXT3 形式のストレージリポジトリでは、ローカルストレージでシンプロビジョニングが有効になります。ただし、ストレージリポジトリのデフォルトの種類は LVM です。これは、一貫した書き込みパフォーマンスが提供され、ストレージのオーバーコミットを避けることができるためです。EXT3 を使用すると、次のような場合にパフォーマンスの低下が生じることがあります:

- 仮想マシンのライフサイクル操作 (仮想マシンの作成、一時停止、再開など)
- 仮想マシン内での大規模ファイルの作成

ローカルディスク EXT ストレージリポジトリの設定は、常に Citrix Hypervisor CLI を使用して行います。

ローカル **EXT3** ストレージリポジトリ (**ext**) を作成する

次の表は、ext ストレージリポジトリ用の device-config パラメーターの一覧です。

パラメーター名	説明	必須か
デバイス	ストレージリポジトリとして使用するローカルホスト上のデバイス名です。	はい

/dev/sdbにローカル ext ストレージリポジトリを作成する場合は、次のコマンドを実行します：

```
1 xe sr-create host-uuid=valid_uuid content-type=user \
2   name-label="Example Local EXT3 SR" shared=false \
3   device-config:device=/dev/sdb type=ext
```

udev

udevの種類のストレージリポジトリは、udevデバイスマネージャーを使って VDI として接続されたデバイスを示します。

Citrix Hypervisor には、リムーバブルストレージであるudevとして表される、2種類のストレージリポジトリがあります。1つは、Citrix Hypervisor サーバーの物理 CD または DVD ドライブに挿入された CD または DVD です。もう1つは、Citrix Hypervisor サーバーの USB ポートに接続された USB デバイスです。これらのメディアの VDI は、そのディスクまたは USB デバイスの挿入/取り外しにより、接続したり接続解除したりできます。

ISO

この種類のストレージリポジトリは、ISO 形式のファイルとして格納された CD イメージを示します。このストレージリポジトリは、共有 ISO ライブラリの作成に便利です。ISO のライブラリを格納するストレージリポジトリのcontent-typeパラメータはisoである必要があります。

次に例を示します：

```
1 xe sr-create host-uuid=valid_uuid content-type=iso \
2   type=iso name-label="Example ISO SR" \
3   device-config:location=nfs server:path
```

SMB バージョン 3.0 を使用して、Windows ファイルサーバー上に ISO ストレージリポジトリをマウントすることをお勧めします。デフォルトではバージョン 3.0 が選択されています。これは、SMB バージョン 1.0 よりも安全で堅牢だからです。ただし、次のコマンドを使用すると、SMB バージョン 1.0 で ISO ストレージリポジトリをマウントすることができます。

```
1    xe sr-create content-type=iso type=iso shared=true device-config:
      location=valid location
2    device-config:username=username device-config:cifspassword=
      password
3    device-config:type=cifs device-config:vers=Choose either 1.0 or
      3.0 name-label="Example ISO SR"
```

注:

sr-create コマンドの実行時にコマンドラインでパスワードを指定する代わりに、device-config:cifspassword_secret 引数を使用できます。詳しくは、「シークレット」を参照してください。

ソフトウェア iSCSI のサポート

Citrix Hypervisor では、iSCSI LUN の共有ストレージリポジトリがサポートされます。iSCSI は、Open-iSCSI のソフトウェア iSCSI イニシエータまたは iSCSI HBA (Host Bus Adapter: ホストバスアダプタ) によりサポートされます。iSCSI HBA を使用する手順は、ファイバチャネル HBA のものと同じです。両方の手順については、「ファイバチャネル、FCoE、iSCSI HBA または SAS ストレージリポジトリ上の共有 LVM を作成する」を参照してください。

ソフトウェア iSCSI イニシエータによる共有 iSCSI のサポートは、LVM (Logical Volume Manager: 論理ボリュームマネージャ) により実装されています。この機能は、パフォーマンス上、ローカルディスクで LVM 仮想ディスクを使用した場合と同様の長所があります。ソフトウェアベースのホストイニシエータを使用する共有 iSCSI ストレージリポジトリでは、ライブマイグレーションを使用して仮想マシンのアジリティをサポートできます: 仮想マシンはリソースプール内のどの Citrix Hypervisor サーバーでも起動でき、サービスをほとんど停止せずに、ホスト間で仮想マシンを移行できます。

iSCSI ストレージリポジトリは、作成時に指定した LUN 全体を使用し、複数の LUN にまたがることはできません。データバスの初期化と LUN 検出のフェーズの両方で、クライアント認証のために CHAP がサポートされます。

注:

iSCSI LUN のブロックサイズは 512 バイトでなければなりません。

Citrix Hypervisor サーバーでの iSCSI 設定

ネットワーク上で一意に識別されるように、すべて iSCSI イニシエータおよびターゲットに固有の名前を設定する必要があります。各イニシエータは 1 つの iSCSI イニシエータアドレスを持ち、各ターゲットは 1 つの iSCSI ターゲットアドレスを持ちます。これらを総称して、IQN (iSCSI Qualified Names) と呼びます。

Citrix Hypervisor サーバーでは、ホストのインストール時にランダムな IQN で自動的に作成される単一の iSCSI イニシエータがサポートされます。この単一のイニシエータを使用して、同時に複数の iSCSI ターゲットに接続できます。

通常、iSCSI ターゲットは iSCSI イニシエータの IQN リストに基づいてアクセス制御を提供します。このため、Citrix Hypervisor サーバーがアクセスするすべての iSCSI ターゲットおよび LUN で、ホストのイニシエータ IQN からのアクセスが許可されている必要があります。同様に、共有 iSCSI ストレージリポジトリとして使用するターゲットおよび LUN で、リソースプール内のすべてのホストの IQN からのアクセスが許可されている必要があります。

注:

一般的に、アクセス制御を提供しない iSCSI ターゲットでは、データの整合性を保証するために、LUN アクセスがデフォルトで単一イニシエータに制限されます。リソースプール内の複数のサーバーで共有されるストレージリポジトリとして iSCSI LUN を使用する場合は、その LUN で複数のイニシエータからのアクセスが有効になっていることを確認してください。

Citrix Hypervisor サーバーの iSCSI ソフトウェアイニシエータの IQN 値は、XenCenter を使用するか、次の CLI コマンドを実行することにより調整できます:

```
1 xe host-param-set uuid=valid_host_id other-config:iscsi_iqn=new_initiator_iqn
```

警告:

- 各 iSCSI ターゲットおよびイニシエータで、固有の IQN が設定されている必要があります。IQN が重複するとデータの損傷や LUN アクセスの拒否が発生します。
- iSCSI ストレージリポジトリが接続されている Citrix Hypervisor サーバーの IQN を変更しないでください。IQN を変更すると、新規ターゲットや既存のストレージリポジトリに接続できなくなります。

ソフトウェア FCoE ストレージ

ソフトウェア FCoE は、ハードウェアベンダーが FCoE 対応 NIC を組み込み、ハードウェアベースの FCoE と同じメリットを享受することのできる標準フレームワークです。これにより、費用のかかる HBA を使用する必要がなくなります。

ソフトウェア FCoE ストレージを作成する前に、LUN をホストに提供するために必要な設定を手動で完了してください。この設定には、FCoE ファブリックの設定と、SAN のパブリックワールドワイドネーム (PWWN) への LUN の割り当てが含まれます。この設定を完了した後、使用可能な LUN が SCSI デバイスとしてホストの CNA にマウントされます。これにより、ローカルで接続されている SCSI デバイスのように、SCSI デバイスを使用して LUN にアクセスできるようになります。FCoE をサポートするための物理スイッチおよびアレイの構成について詳しくは、ベンダーが提供するドキュメントを参照してください。

注:

ソフトウェア FCoE は、ネットワークバックエンドとして Open vSwitch および Linux ブリッジを使用している場合に使用できます。

ソフトウェア **FCoE** ストレージリポジトリを作成する

ソフトウェア FCoE ストレージリポジトリの作成前に、ホストに接続された FCoE 対応 NIC が存在することを確認してください。

次の表は、FCoE ストレージリポジトリ用の device-config パラメーターの一覧です。

パラメーター名	説明	必須か
SCSIid	作成先 LUN の SCSI バス ID です。	はい

次のコマンドを実行して、共有 FCoE ストレージリポジトリを作成します。

```
1 xe sr-create type=lvmofcoe \  
2 name-label="FCoE SR" shared=true device-config:SCSIid=SCSI_id
```

ハードウェアホストバスアダプタ (HBA)

ここでは、SAS、ファイバチャネル、および iSCSI のホストバスアダプタ (HBA) を管理するために必要な、さまざまな操作について説明します。

QLogic iSCSI HBA セットアップの例

QLogic ファイバチャネル HBA および iSCSI HBA の設定について詳しくは、[Cavium 社の Web サイト](#)を参照してください。

HBA を Citrix Hypervisor サーバーに物理的にインストールしたら、以下の手順で HBA を設定します：

1. HBA の IP ネットワーク構成を設定します。この例では、DHCP と HBA ポート 0 を使用します。特定の IP アドレスやマルチポート HBA を設定する場合は、適切な値を指定します。

```
1 /opt/QLogic_Corporation/SANsurferiCLI/iscli -ipdhcp 0
```

2. 永続的 iSCSI ターゲットを HBA のポート 0 に追加します。

```
1 /opt/QLogic_Corporation/SANsurferiCLI/iscli -pa 0  
iscsi_target_ip_address
```

3. xe sr-probe コマンドを使用して、HBA コントローラを強制的に再スキャンして、使用可能な LUN を表示します。詳しくは、「[ストレージリポジトリをプローブする](#)」および「[ファイバチャネル、FCoE、iSCSI HBA または SAS ストレージリポジトリ上の共有 LVM を作成する](#)」を参照してください。

HBA ベースの **SAS**、ファイバチャネル、または **iSCSI** デバイスエントリを削除する

注:

これらの手順は必須ではありません。パワーユーザーが必要に応じて実行することをお勧めします。

各 HBA ベースの LUN には、対応するグローバルデバイスパスエントリが <SCSIid>-<adapter>:<bus>:<target>:<lun>形式で /dev/disk/by-scsibus にあり、標準デバイスパスが /dev にあります。ストレージリポジトリとして使用されなくなった LUN のデバイスエントリを削除するには、次の手順を実行します:

1. `sr-forget` または `sr-destroy` を使用して、Citrix Hypervisor サーバーデータベースからストレージリポジトリを削除します。詳しくは、[ストレージリポジトリを削除する](#) を参照してください。
2. 適切な LUN およびホストに対する SAN 内のゾーン設定を削除します。
3. `sr-probe` コマンドを使用して、削除する LUN の ADAPTER、BUS、TARGET、および LUN 値を確認します。詳しくは、「[ストレージリポジトリをプローブする](#)」を参照してください。
4. 次のコマンドを実行して、デバイスエントリを削除します。

```
1 echo "1" > /sys/class/scsi_device/adapter:bus:target:lun/device/delete
```

警告:

削除する LUN を間違わないよう、十分注意してください。ホストに必要な LUN (起動用、ルートデバイス用など) を削除してしまうと、ホストが使用不能になります。

共有 **LVM** ストレージ

この種類のストレージリポジトリは、iSCSI (ファイバチャネルまたは Serial Attached SCSI) LUN 上に作成されたボリュームグループ内の論理ボリュームとしてのディスクを示します。

注:

iSCSI LUN のブロックサイズは 512 バイトでなければなりません。

ソフトウェアイニシエータによる **iSCSI** 経由の共有 **LVM** ストレージリポジトリを作成する

次の表は、LVMoiSCSI ストレージリポジトリ用の device-config パラメーターの一覧です:

パラメーター名	説明	必須か
target	ストレージリポジトリをホストする iSCSI ファイラの IP アドレスまたはホスト名です。	はい

パラメーター名	説明	必須か
targetIQN	ストレージリポジトリをホストする iSCSI ファイラの IQN ターゲットアドレスです。	はい
SCSIid	作成先 LUN の SCSI バス ID です。	はい
chapuser	CHAP 認証に使用されるユーザー名です。	いいえ
chappassword	CHAP 認証に使用されるパスワードです。	いいえ
port	ターゲットをクエリするためのネットワークポート番号です。	いいえ
usediscoverynumber	使用する特定の iscsi レコードインデックスです。	いいえ
incoming_chapuser	iSCSI フィルタでホストでの認証に使用されるユーザー名です。	いいえ
incoming_chappassword	iSCSI フィルタでホストでの認証に使用されるパスワードです。	いいえ

iSCSI ターゲット上の特定の LUN に共有 LVMoiscsi ストレージリポジトリを作成する場合は、次のコマンドを実行します。

```

1  xe sr-create host-uuid=valid_uuid content-type=user \
2  name-label="Example shared LVM over iSCSI SR" shared=true \
3  device-config:target=target_ip= device-config:targetIQN=target_iqn=
   \
4  device-config:SCSIid=scsci_id \
5  type=lvmoiscsi

```

ファイバチャネル、**FCoE**、**iSCSI HBA** または **SAS** ストレージリポジトリ上の共有 **LVM** を作成する

LVMoHBA タイプのストレージリポジトリは、XenCenter または xe CLI で作成および管理できます。

次の表は、LVMoHBA ストレージリポジトリ用の device-config パラメーターの一覧です：

パラメーター名	説明	必須か
SCSIid	デバイスの SCSI ID	はい

共有 LVMoHBA ストレージリポジトリを作成するには、リソースプール内の各ホスト上で以下の手順を実行します：

1. リソースプール内の各 Citrix Hypervisor サーバーの LUN にゾーンを定義します。この手順は、使用する SAN 機材により大きく異なるため、詳しくは、SAN のドキュメントを参照してください。
2. 必要に応じて、Citrix Hypervisor サーバーに含まれている以下の HBA コマンドを使用して HBA を設定します：
 - Emulex: `/bin/sbin/ocmanager`
 - QLogic FC: `/opt/QLogic_Corporation/SANsurferCLI`
 - QLogic iSCSI: `/opt/QLogic_Corporation/SANsurferiCLI`

QLogic iSCSI HBA の設定例については、前のセクションの「ハードウェアホストバスアダプタ (HBA)」を参照してください。ファイバチャネルおよび iSCSI の HBA について詳しくは、[Broadcom 社](#)および[Cavium 社](#)の Web サイトを参照してください。

3. `sr-probe`コマンドを使用して、HBA LUN のグローバルデバイスパスを確認します。`sr-probe`コマンドを実行すると、システムにインストールされている HBA が再スキャンされます。これにより、そのホスト用に定義されている新しい LUN がすべて検出され、各 LUN のプロパティが一覧表示されます。対象のホストを指定するには、`host-uuid`パラメータを指定します。

<path>プロパティとして返されるグローバルデバイスパスは、リソースプール内のすべてのホストで共通です。このため、ストレージリポジトリを作成するときに、`device-config:device`パラメータの値としてこのパスを指定する必要があります。

複数の LUN が存在する場合は、<path>プロパティのベンダー、LUN サイズ、LUN シリアル番号、または SCSI ID を使用して LUN を指定します。

```

1  xe sr-probe type=lvmohba \
2  host-uuid=1212c7b3-f333-4a8d-a6fb-80c5b79b5b31
3  Error code: SR_BACKEND_FAILURE_90
4  Error parameters: , The request is missing the device
   parameter, \
5  <?xml version="1.0" ?>
6  <Devlist>
7      <BlockDevice>
8          <path>
9              /dev/disk/by-id/scsi-360
                  a9800068666949673446387665336f
10             </path>
11             <vendor>

```

```
12         HITACHI
13     </vendor>
14     <serial>
15         730157980002
16     </serial>
17     <size>
18         80530636800
19     </size>
20     <adapter>
21         4
22     </adapter>
23     <channel>
24         0
25     </channel>
26     <id>
27         4
28     </id>
29     <lun>
30         2
31     </lun>
32     <hba>
33         qla2xxx
34     </hba>
35 </BlockDevice>
36 <Adapter>
37     <host>
38         Host4
39     </host>
40     <name>
41         qla2xxx
42     </name>
43     <manufacturer>
44         QLogic HBA Driver
45     </manufacturer>
46     <id>
47         4
48     </id>
49 </Adapter>
50 </Devlist>
```

4. プールマスターとして動作するホスト上でストレージリポジトリを作成します。 `sr-probe` コマンドで返された `<path>` プロパティのグローバルデバイスパスを指定します。PBD が作成され、自動的にプール内の各ホストにプラグされます。

```
1 xe sr-create host-uuid=valid_uuid \
```

```
2 content-type=user \  
3 name-label="Example shared LVM over HBA SR" shared=true \  
4 device-config:SCSIid=device_scsi_id type=lvmohba
```

注:

上記の `sr-create` 処理の PBD 作成とプラグ操作を再試行するには、XenCenter の [ストレージ] > [修復] 機能を使用できます。ストレージリポジトリ作成時のゾーン設定がリソースプール内の一部のホストで不正な場合、この機能を使用して解決できます。ストレージリポジトリを削除してから再度作成する代わりに、この機能を使用して、影響を受けているホストのゾーン設定を修正してください。

シンプロビジョニングされた共有 **GFS2** ブロックストレージ

シンプロビジョニングは、事前に VDI の仮想サイズすべてを割り当てるのではなく、仮想ディスクにデータが書き込まれるたびにディスクストレージ領域を VDI に割り当てることによって、ストレージ領域をよりうまく利用します。シンプロビジョニングを使用すると、共有ストレージアレイに必要な領域と総所有コスト (TCO) を大幅に削減できます。

共有ブロックストレージのシンプロビジョニングは、次の場合に特に役立ちます:

- 領域の使用効率を高める必要がある場合。イメージが散在し密に割り当てられていない場合。
- ストレージアレイ上の 1 秒あたりの入出力操作数を減らす必要がある場合。GFS2 ストレージリポジトリは、共有ブロックストレージ上のストレージ読み取りキャッシュをサポートする、一級のストレージリポジトリです。
- 複数の仮想マシンで基本イメージを共有する場合。共有することで個々の仮想マシンのイメージは限られた領域を有効活用できます。
- スナップショットを使用する場合で、各スナップショットがイメージであり、各イメージが散在する場合。
- お使いのストレージは NFS をサポートしておらず、ブロックストレージのみをサポートしています。ストレージが NFS をサポートしている場合は、GFS2 の代わりに NFS を使用することをお勧めします。
- 2TiB を超えるサイズの VDI を作成する場合。GFS2 ストレージリポジトリは、最大 16TiB の VDI をサポートします。

この種類のストレージリポジトリでは、iSCSI または HBA LUN 上に作成されたファイルシステムと同様にディスクが表示されます。GFS2 ストレージリポジトリに保存されている VDI は、QCOW2 イメージ形式で保存されます。

共有 GFS2 ストレージを使用するには、Citrix Hypervisor のリソースプールがクラスタ化されたプールである必要があります。GFS2 ストレージリポジトリを作成する前に、プールでクラスタリングを有効にしてください。詳しくは、「[クラスタ化プール](#)」を参照してください。

クラスタ化プールと GFS2 ストレージリポジトリの間にストレージのマルチパスが設定されていることを確認してください。詳しくは、「[ストレージのマルチパス](#)」を参照してください。

GFS2 タイプのストレージリポジトリは、XenCenter または xe CLI で作成および管理できます。

制約

現在、共有 GFS2 ストレージには次の制約があります：

- VDI が GFS2 ストレージリポジトリ上にある仮想マシンでは、ストレージライブマイグレーションによる仮想マシンの移行はサポートされていません。
- FCoE プロトコルは、GFS2 ストレージリポジトリではサポートされていません。
- トリミングとマッピング解除は、GFS2 ストレージリポジトリではサポートされていません。
- GFS2 ストレージリポジトリおよびこれらのストレージリポジトリ上のディスクでは、パフォーマンス測定値は利用できません。
- 変更ブロック追跡は、GFS2 SR に格納されている VDI ではサポートされません。
- 2TiB を超える VDI を VHD または OVA (Open Virtual Appliance) や OVF (オープン仮想化フォーマット) でエクスポートすることはできません。ただし、VDI が 2TiB を超える仮想マシンは、XVA 形式でエクスポートできます。

注：

クラスタリングが有効になっているホストが少なくとも 1 つ含まれるクラスタリングネットワークで、IP アドレスの競合 (IP アドレスが同じホストが複数存在) が発生した場合、GFS2 ストレージリポジトリ上で操作が停止することがあります。この場合、ホストは隔離されません。この問題を解決するには、IP アドレスの競合を解決します。

ソフトウェアイニシエータによる **iSCSI** 経由の共有 **GFS2** ストレージリポジトリを作成する

XenCenter を使用すると、iSCSI ストレージリポジトリ上に GFS2 を作成できます。詳しくは、XenCenter 製品ドキュメントの「[ソフトウェア iSCSI ストレージ](#)」を参照してください。

または、xe CLI を使用して iSCSI ストレージリポジトリ上に GFS2 を作成することもできます。

次の表は、GFS2 ストレージリポジトリ用の device-config パラメータの一覧です：

パラメーター名	説明	必須か
<code>provider</code>	ブロックプロバイダ実装。この場合は、 <code>iscsi</code> 。	はい
<code>target</code>	ホストする iSCSI ファイラの IP アドレスまたはホスト名	はい
<code>targetIQN</code>	ストレージリポジトリをホストする iSCSI ファイラの IQN ターゲット	はい
<code>SCSIid</code>	デバイスの SCSI ID	はい

`xe sr-probe-ext` コマンドを使用すると、これらのパラメーターに使用するための値を見つけることができます。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 次のコマンドを実行して起動します:

```
1 xe sr-probe-ext type=trfs device-config:provider=iscsi
```

コマンドからの出力では、追加のパラメーターを指定するように求められ、各ステップで使用できる値のリストが示されます。

2. このコマンドを繰り返して、毎回新しいパラメーターを追加します。
3. コマンド出力が `The following SRs were found:` で始まる場合、`xe sr-create` コマンドを実行するときにストレージリポジトリを格納するのに指定した `device-config` パラメーターを使用できます。

iSCSI ターゲットの特定の LUN で共有 GFS2 ストレージリポジトリを作成するには、クラスター化プール内のサーバーで次のコマンドを実行します:

```
1 xe sr-create type=trfs name-label="Example GFS2 SR" --shared \
2   device-config:provider=iscsi device-config:targetIQN=target_iqns \
3   device-config:target=portal_address device-config:SCSIid=scsci_id
```

GFS2 ファイルシステムのマウント時に iSCSI ターゲットにアクセスできない場合、クラスター化されたプール内の一部のホストが隔離される可能性があります。

iSCSI ストレージリポジトリの操作については、「[ソフトウェア iSCSI のサポート](#)」を参照してください。

HBA ストレージリポジトリ上の共有 **GFS2** を作成する

XenCenter を使用すると、HBA ストレージリポジトリ上に GFS2 を作成できます。詳しくは、XenCenter 製品ドキュメントの「[ハードウェア HBA ストレージ](#)」を参照してください。

または、xe CLI を使用して HBA ストレージリポジトリ上に GFS2 を作成することもできます。

次の表は、GFS2 ストレージリポジトリ用の `device-config` パラメーターの一覧です:

パラメーター名	説明	必須か
<code>provider</code>	ブロックプロバイダ実装。この場合は、 <code>hba</code> 。	はい
<code>SCSIid</code>	デバイスの SCSI ID	はい

`xe sr-probe-ext` コマンドを使用すると、SCSIid パラメーターに使用するための値を見つけることができます。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<
  config> sm-config:=<sm_config>
```

1. 次のコマンドを実行して起動します:

```
1 xe sr-probe-ext type=gfs2 device-config:provider=hba
```

コマンドからの出力では、追加のパラメーターを指定するように求められ、各ステップで使用できる値のリストが示されます。

2. このコマンドを繰り返して、毎回新しいパラメーターを追加します。

3. コマンド出力が `The following SRs were found:` で始まる場合、`xe sr-create` コマンドを実行するときにストレージリポジトリを格納するのに指定した `device-config` パラメーターを使用できます。

HBA ターゲットの特定の LUN で共有 GFS2 ストレージリポジトリを作成するには、クラスター化プール内のサーバーで次のコマンドを実行します:

```
1 xe sr-create type=gfs2 name-label="Example GFS2 SR" --shared \
2   device-config:provider=hba device-config:SCSIid=device_scsi_id
```

HBA ストレージリポジトリの操作について詳しくは、「[ハードウェアホストバスアダプタ](#)」を参照してください。

NFS および SMB

では、NFS サーバーの共有 (NFSv4 または NFSv3 をサポート) または SMB サーバーの共有 (SMB 3.0 をサポート) を、仮想ディスクのストレージリポジトリとしてすぐに使用できます。VDI は、Microsoft VHD 形式でのみ格納されます。さらに、これらのストレージリポジトリは共有できるため、共有ストレージリポジトリに格納された VDI で次のことが可能になります。

- リソースプール内のすべての Citrix Hypervisor サーバーでの仮想マシンの起動
- ライブマイグレーションを使用した、サービスをほとんど停止しない、リソースプール内の Citrix Hypervisor サーバー間の仮想マシンの移行

重要:

- SMB 3.0 のサポートは、3.0 プロトコルを使用した共有への接続機能に限定されます。Transparent Failover などの追加の機能は、Citrix Hypervisor 8.1 ではサポートされておらず、アップストリーム Linux カーネルの機能を使用できるかどうか依存します。
- NFSv4 では、`AUTH_SYS` の認証の種類のみがサポートされます。
- SMB ストレージは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。

ファイルベースのストレージリポジトリに格納される VDI は、シンプロビジョニングされます。仮想マシンがデータをディスクに書き込むときにイメージファイルが割り当てられます。これには、実際に仮想マシンイメージファイルに書き込まれているデータ分の領域しかストレージ上で消費されないという大きな利点があります。たとえば、100GB の VDI を仮想マシンに割り当てて、そこにオペレーティングシステムをインストールする場合、オペレーティングシステムデータのサイズがその VDI ファイルの物理サイズに反映され、100GB にはなりません。

VHD ファイルをチェーン化して、2 つの VDI で共通のデータを共有することもできます。ファイルベースの仮想マシンを複製する場合、複製時にディスク上に存在したデータを複製元と複製先の仮想マシンが共有します。その後、各仮想マシンは異なるコピーオンライトバージョンの VDI で個別の変更を行います。この機能により、ファイルベースの仮想マシンをテンプレートからすぐに複製できるようになり、新しい仮想マシンのプロビジョニングと展開が容易になります。

注:

サポートされる VHD チェーンは 30 世代までです。

Citrix Hypervisor のファイルベースのストレージリポジトリおよび VHD の実装では、ファイルサーバーのストレージリポジトリディレクトリを完全に制御できることが前提になっています。VDI の内容を破損する危険があるため、管理者がストレージリポジトリディレクトリの内容を変更することは避けてください。

Citrix Hypervisor は、障害からの高度なデータ保護を維持しながら、不揮発性の RAM を使用して書き込み要求に迅速に回答するエンタープライズクラスのストレージ用に調整されています。たとえば、Citrix Hypervisor では、Network Appliance 社の Data ONTAP 7.3 および 8.1 が動作する FAS2020 および FAS3210 ストレージに対し、広範なテストが実施されています。

警告:

ファイルベースのストレージリポジトリ上の VDI はシンプロビジョニングで作成されるため、ファイルベースのストレージリポジトリ上にすべての VDI に対して十分なディスクスペースがあることを確認する必要があります。Citrix Hypervisor サーバーでは、仮想ディスクの作成時にファイルベースのストレージリポジトリに必要なディスク領域があるかどうかはチェックされません。

共有 **NFS** ストレージリポジトリ (**NFS**) を作成する

NFS ストレージリポジトリを作成するには、NFS サーバーのホスト名または IP アドレスを指定する必要があります。任意のストレージリポジトリを作成可能なパスにストレージリポジトリを作成できます。サーバーによってエクスポートされた、ストレージリポジトリを作成可能なパスの一覧を表示するには、`sr-probe` コマンドを使用します。

Citrix Hypervisor でローエンドなストレージを使用すると、すべての書き込みの応答を待機してから仮想マシンに確認応答を渡すため、時間がかかることがあります。これにより、パフォーマンスが大きく犠牲になります。この問題は、ストレージリポジトリのマウントポイントを非同期モードでエクスポートするようにストレージを設定することで解決できる場合があります。ただし、非同期モードでのエクスポートでは実際にディスク上にない書き込みも認識されるため、障害のリスクを慎重に考慮する必要があります。

注:

指定したパスがプール内のすべてのサーバーにエクスポートされるように NFS サーバーを設定しておく必要があります。この設定を行わない場合、ストレージリポジトリの作成に失敗し、物理ブロックデバイスレコードのプラグに失敗します。

Citrix Hypervisor の NFS 実装では、デフォルトで TCP が使用されます。可能な環境であれば、UDP が使用されるように設定すると、パフォーマンスが向上する場合があります。これを行うには、ストレージリポジトリを作成するときに、`device-config` パラメーター `useUDP=true` を指定します。

次の表は、nfs ストレージリポジトリ用の `device-config` パラメータの一覧です。

パラメーター名	説明	必須か
<code>server</code>	NFS サーバーの IP アドレスまたはホスト名です。	はい
<code>serverpath</code>	ストレージリポジトリを作成する NFS サーバー上の、NFS マウントポイントを含めたパスです。	はい

たとえば、`192.168.1.10:/export1` に共有 NFS ストレージリポジトリを作成する場合は、次のコマンドを実行します:

```
1 xe sr-create content-type=user \
2 name-label="shared NFS SR" shared=true \
3 device-config:server=192.168.1.10 device-config:serverpath=/export1
  type=nfs \
4 nfsversion="3", "4"
```

非共有 NFS ストレージリポジトリを作成する場合は、次のコマンドを実行します。

```
1 xe sr-create host-uuid=host_uuid content-type=user \
2 name-label="Non-shared NFS SR" \
3 device-config:server=192.168.1.10 device-config:serverpath=/export1
  type=nfs \
4 nfsversion="3", "4"
```

共有 **SMB** ストレージリポジトリ (**SMB**) を作成する

SMB ストレージリポジトリを作成するには、SMB サーバーのホスト名または IP アドレス、エクスポートされた共有のフルパス、および適切な資格情報を指定します。

注:

SMB ストレージリポジトリは、ONTAP 8.3 を実行している Network Appliance ストレージおよび Windows Server 2012 R2 でテストされています。

次の表は、SMB ストレージリポジトリ用の device-config パラメーターの一覧です。

パラメーター名	説明	必須か
server	サーバー上の共有へのフルパス	はい
username	共有への RW アクセスを持つユーザーアカウント	オプション
password	ユーザーアカウントのパスワード	オプション

たとえば、192.168.1.10:/share1に共有 SMB ストレージリポジトリを作成する場合は、次のコマンドを実行します:

```
1 xe sr-create content-type=user \
2 name-label="Example shared SMB SR" shared=true \
3 device-config:server=//192.168.1.10/share1 \
4 device-config:username=valid_username device-config:password=
  valid_password type=smb
```

非共有 SMB ストレージリポジトリを作成する場合は、次のコマンドを実行します。

```
1 xe sr-create host-uuid=host_uuid content-type=user \
2 name-label="Non-shared SMB SR" \
3 device-config:server=//192.168.1.10/share1 \
4 device-config:username=valid_username device-config:password=
  valid_password type=smb
```

注:

sr-createコマンドの実行時にコマンドラインでパスワードを指定する代わりに、device-config:password_secret引数を使用できます。詳しくは、「シークレット」を参照してください。

ハードウェア HBA 上の LVM

この種類のストレージリポジトリでは、HBA LUN 上に作成されたボリュームグループ内の論理ボリューム上の VHD としてディスクが表示され、ハードウェアベースの iSCSI または FC のサポートが提供されます。

Citrix Hypervisor サーバーでは、Emulex または QLogic のホストバスアダプタ (HBA) を使ったファイバチャネル SAN がサポートされます。ファイバチャネルの LUN をホストに提供するために必要なファイバチャネルの構成

は、すべて手作業で行う必要があります。この構成には、ストレージデバイス、ネットワークデバイス、および Citrix Hypervisor サーバー内の HBA が含まれます。すべての FC 設定が完了すると、目的の FC LUN の SCSI デバイスが HBA によりホストに提供されます。これにより、ローカルで接続されている SCSI デバイスのように、SCSI デバイスを使用して FC LUN にアクセスできるようになります。

ホスト上に存在する、LUN を持つ SCSI デバイスの一覧を確認するには、`sr-probe` コマンドを使用します。このコマンドでは、新しく追加されたデバイスも認識されます。`sr-probe` で返される SCSI デバイスのパス値は、その LUN にアクセスするすべてのホストで同一です。したがって、リソースプール内のすべてのホストからアクセス可能な共有ストレージリポジトリを作成する場合、この値を使用する必要があります。

QLogic iSCSI HBA に対しても、同じ機能を使用できます。

HBA ベースのファイバチャネルおよび iSCSI の共有ストレージリポジトリを作成する手順については、[ストレージリポジトリを作成する](#)を参照してください。

注:

Citrix Hypervisor では、ファイバチャネルの LUN を仮想マシンに直接マップすることはサポートされていません。HBA ベースの LUN は、ホストにマップして、ストレージリポジトリ内でそれを指定する必要があります。ストレージリポジトリ内の仮想ディスクイメージは、標準のブロックデバイスとして仮想マシンに提供されます。

シンプロビジョニングされた共有 **GFS2** ブロックストレージ

September 11, 2019

シンプロビジョニングは、事前に VDI の仮想サイズすべてを割り当てるのではなく、仮想ディスクにデータが書き込まれるたびにディスクストレージ領域を VDI に割り当てることによって、ストレージ領域をよりうまく利用します。シンプロビジョニングを使用すると、共有ストレージアレイに必要な領域と総所有コスト (TCO) を大幅に削減できます。

共有ブロックストレージのシンプロビジョニングは、次の場合に特に役立ちます:

- 領域の使用効率を高める必要がある場合。イメージが散在し密に割り当てられていない場合。
- ストレージアレイ上の 1 秒あたりの入出力操作数を減らす必要がある場合。GFS2 ストレージリポジトリは、共有ブロックストレージ上のストレージ読み取りキャッシュをサポートする、一級のストレージリポジトリです。
- 複数の仮想マシンで基本イメージを共有する場合。共有することで個々の仮想マシンのイメージは限られた領域を有効活用できます。
- スナップショットを使用する場合で、各スナップショットがイメージであり、各イメージが散在する場合。
- お使いのストレージは NFS をサポートしておらず、ブロックストレージのみをサポートしています。ストレージが NFS をサポートしている場合は、GFS2 の代わりに NFS を使用することをお勧めします。

- 2TiB を超えるサイズの VDI を作成する場合。GFS2 ストレージリポジトリは、最大 16TiB の VDI をサポートします。

この種類のストレージリポジトリでは、iSCSI または HBA LUN 上に作成されたファイルシステムと同様にディスクが表示されます。GFS2 ストレージリポジトリに保存されている VDI は、QCOW2 イメージ形式で保存されます。

前提条件

開始前に、次の前提条件が満たされていることを確認してください：

- クラスター化プール内のすべての Citrix Hypervisor サーバーには、少なくとも 2GiB のコントロールドメインメモリが必要です。
- クラスター内のすべてのホストは、クラスターネットワークに静的 IP アドレスを使用する必要があります。
- クラスタリングを使用するのは、プールが 3 つ以上のホストを含む場合だけにすることをお勧めします。これは、2 つのホストを含むプールではプール全体の自己隔離で問題が発生しやすいためです。
- プール内のホスト間にファイアウォールがある場合は、ホストが次のポートを使用してクラスターネットワーク上で通信できることを確認してください：
 - TCP: 8892、21064
 - UDP: 5404、5405

詳しくは、「[Communication Ports Used by Citrix Technologies](#)」を参照してください。

- 既存のプールをクラスタリングする場合は、高可用性が無効になっていることを確認してください。クラスタリングが有効になった後、高可用性を再度有効にできます。
- リソースプール内に Citrix Hypervisor のすべてのサーバーが表示されている、ブロックベースのストレージデバイスがある。

共有 GFS2 ストレージリポジトリを使用できるようにクラスター化プールを設定する

共有 GFS2 ストレージを使用するには、Citrix Hypervisor のリソースプールがクラスタ化されたプールである必要があります。GFS2 ストレージリポジトリを作成する前に、プールでクラスタリングを有効にしてください。

注：

クラスター化プールは、クラスター化されていないプールと動作が異なります。クラスターの動作について詳しくは、「[クラスター化プール](#)」を参照してください。

必要な場合は、XenCenter を使用してプールにクラスタリングを設定することもできます。詳しくは、[XenCenter 製品ドキュメント](#)を参照してください。

xe CLI (コマンドラインインターフェイス) を使用してクラスター化プールを作成するには：

1. ボンディングネットワークを作成して、クラスタリングネットワークとして使用します。プールマスターにする Citrix Hypervisor サーバーで、以下の手順を実行します:

- a) Citrix Hypervisor サーバーのコンソールを開きます。
- b) 次のコマンドを使用して、リソースプールに名前を付けます:

```
1 xe pool-param-set name-label="New Pool" uuid=<pool_uuid>
```

- c) 次のコマンドを使用して、NIC ボンディングで使用するネットワークを作成します:

```
1 xe network-create name-label=bond0
```

これにより、新しいネットワークの UUID が返されます。

- d) 次のコマンドを使用して、ボンディングに使用する PIF の UUID を見つけます:

```
1 xe pif-list
```

- e) アクティブ/アクティブモード、アクティブ/パッシブモード、または LACP ボンディングモードのいずれかで、ボンディングしたネットワークを作成します。使用するボンディングモードに応じて、以下のいずれかのアクションを実行します:

- アクティブ/アクティブモードのボンディング（デフォルト）を作成するには、`bond-create` コマンドを使用します。パラメーターをコンマで区切って、新しく作成されたネットワーク UUID と、ボンディングする PIF の UUID を指定します:

```
1 xe bond-create network-uuid=<network_uuid> /  
2   pif-uuids=<pif_uuid_1>,<pif_uuid_2>,<pif_uuid_3>,<  
   pif_uuid_4>
```

ボンディングを構成する NIC の数に応じて、2 つまたは 4 つの UUID を指定してください。これにより、ボンディングの UUID が返されます。

- アクティブ/パッシブモードまたは LACP モードのボンディングを作成するには、上記と同じ構文に `mode` パラメータを追加して、`lacp` または `active-backup` を指定します:

```
1 xe bond-create network-uuid=<network_uuid> pif-uuids=<  
   pif_uuid_1>, /  
2   <pif_uuid_2>,<pif_uuid_3>,<pif_uuid_4> /  
3   mode=balance-slb | active-backup | lacp
```

プールマスターでボンディングしたネットワークを作成した後、他の Citrix Hypervisor サーバーをプールに追加すると、ネットワークとボンディングの情報が自動的に追加するサーバーに複製されます。

詳しくは、「[ネットワーク](#)」を参照してください。

2. 少なくとも 3 台の Citrix Hypervisor サーバーのリソースプールを作成します。

プールメンバー（マスターではない）である Citrix Hypervisor の各サーバーで、次の手順を繰り返します：

- a) Citrix Hypervisor サーバーのコンソールを開きます。
- b) 次のコマンドを使用して、Citrix Hypervisor サーバーをプールマスターのプールに参加させます：

```
1 xe pool-join master-address=master_address master-username=
  administrators_username master-password=password
```

`master-address`パラメーターの値は、プールマスターである Citrix Hypervisor サーバーの完全修飾ドメイン名に設定する必要があります。`password`にはプールマスターのインストール時に設定した管理者パスワードを指定します。

詳しくは、「[ホストとリソースプール](#)」を参照してください。

3. このネットワークに属するすべての PIF について、`disallow-unplug=true`を設定します。

- a) 次のコマンドを使用して、ネットワークに属する PIF の UUID を見つけます：

```
1 xe pif-list
```

- b) リソースプール内の Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe pif-param-set disallow-unplug=true uuid=<pif_uuid>
```

4. プールでクラスタリングを有効にします。リソースプール内の Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe cluster-pool-create network-uuid=<network_uuid>
```

前の手順で作成したボンディングしたネットワークの UUID を入力します。

共有 GFS2 ストレージリポジトリへのストレージのマルチパスを設定する

重要：

マルチパスを有効にする前に、以下の事項を確認してください：

- ストレージサーバーで複数のターゲットが使用できる。

たとえば、iSCSI ストレージバックエンドの特定のポータルに対して「sendtargets」を照会した場合、以下のように複数のターゲットが返されます：

```
1 iscsiadm -m discovery --type sendtargets --portal
  192.168.0.161
2 192.168.0.161:3260,1 iqn.strawberry:litchie
```

```
3 192.168.0.204:3260,2 iqn.strawberry:litchie
```

- (iSCSI の場合のみ) コントロールドメイン (dom0) で、マルチパスのストレージにより使用されるサブネットごとに IP アドレスが構成されている。

ストレージへのパスごとに NIC があり、各 NIC に IP アドレスが構成されていることを確認してください。たとえば、ストレージにアクセスする 4 つのパスを作成する場合は、それぞれに IP アドレスが構成された 4 つの NIC が必要です。

- (HBA の場合のみ) 複数の HBA がスイッチファブリックに接続されている。

XenCenter を使用してストレージのマルチパスを設定できます。詳しくは、XenCenter 製品ドキュメントの「[ストレージのマルチパス](#)」を参照してください。

または、xe CLI を使用してストレージのマルチパスを設定するには、クラスター化プール内のすべての Citrix Hypervisor サーバーで次の手順を実行します：

1. Citrix Hypervisor サーバーのコンソールを開きます。
2. 次のコマンドを使用して、サーバー上のすべての PBD をアンプラグします：

```
1 xe pbd-unplug uuid=<pbd_uuid>
```

3. 次のコマンドを使用して、`other-config:multipathing`パラメーターの値を**true**に設定します：

```
1 xe host-param-set other-config:multipathing=true uuid=<server_uuid>
```

4. 次のコマンドを使用して、`other-config:multipathhandle`パラメーターの値を**dmp**に設定します：

```
1 xe host-param-set other-config:multipathhandle=dmp uuid=<server_uuid>
```

5. サーバー上でシングルパスモードで動作しているストレージリポジトリのマルチパスを有効にするには、次の操作を行います：

- そのストレージリポジトリ上の仮想ディスクを使用している、実行中の仮想マシンを移行またはサスペンドします。
- そのストレージリポジトリの PBD をマルチパスで再接続するために、アンプラグして再プラグします：

```
1 xe pbd-unplug uuid=<pbd_uuid>
2 xe pbd-plug uuid=<pbd_uuid>
```

詳しくは、「[ストレージのマルチパス](#)」を参照してください。

共有 **GFS2** ストレージリポジトリを作成する

iSCSI または HBA LUN に共有 GFS2 ストレージリポジトリを作成できます。

iSCSI 経由の共有 **GFS2** ストレージリポジトリを作成する

XenCenter を使用すると、iSCSI ストレージリポジトリ上に GFS2 を作成できます。詳しくは、XenCenter 製品ドキュメントの「[ソフトウェア iSCSI ストレージ](#)」を参照してください。

または、xe CLI を使用して iSCSI ストレージリポジトリ上に GFS2 を作成することもできます。

次の表は、GFS2 ストレージリポジトリ用の device-config パラメータの一覧です：

パラメーター名	説明	必須か
provider	ブロックプロバイダ実装。この場合は、 <code>iscsi</code> 。	はい
target	ホストする iSCSI ファイラの IP アドレスまたはホスト名	はい
targetIQN	ストレージリポジトリをホストする iSCSI ファイラの IQN ターゲット	はい
SCSIid	デバイスの SCSI ID	はい

xe `sr-probe-ext` コマンドを使用すると、これらのパラメーターに使用するための値を見つけることができます。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 次のコマンドを実行して起動します：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=iscsi
```

コマンドからの出力では、追加のパラメーターを指定するように求められ、各ステップで使用できる値のリストが示されます。

2. このコマンドを繰り返して、毎回新しいパラメーターを追加します。
3. コマンド出力が `The following SRs were found:` で始まる場合、xe `sr-create` コマンドを実行するときにストレージリポジトリを格納するのに指定した `device-config` パラメーターを使用できます。

iSCSI ターゲットの特定の LUN で共有 GFS2 ストレージリポジトリを作成するには、クラスター化プール内のサーバーで次のコマンドを実行します：

```
1 xe sr-create type=gfs2 name=label="Example GFS2 SR" --shared \  
2     device-config:provider=iscsi device-config:targetIQN=target_iqns \  
3     device-config:target=portal_address device-config:SCSIid=scsci_id
```

GFS2 ファイルシステムのマウント時に iSCSI ターゲットにアクセスできない場合、クラスター化されたプール内の一部のホストが隔離される可能性があります。

iSCSI ストレージリポジトリの操作について詳しくは、「[ソフトウェア iSCSI のサポート](#)」を参照してください。

HBA ストレージリポジトリ上の共有 GFS2 を作成する

XenCenter を使用すると、HBA ストレージリポジトリ上に GFS2 を作成できます。詳しくは、XenCenter 製品ドキュメントの「[ハードウェア HBA ストレージ](#)」を参照してください。

または、xe CLI を使用して HBA ストレージリポジトリ上に GFS2 を作成することもできます。

次の表は、GFS2 ストレージリポジトリ用の device-config パラメータの一覧です：

パラメーター名	説明	必須か
provider	ブロックプロバイダ実装。この場合は、hba。	はい
SCSIid	デバイスの SCSI ID	はい

xe sr-probe-ext コマンドを使用すると、SCSIid パラメーターに使用するための値を見つけることができます。

```
1 xe sr-probe-ext type=<type> host-uuid=<host_uuid> device-config:=<config> sm-config:=<sm_config>
```

1. 次のコマンドを実行して起動します：

```
1 xe sr-probe-ext type=gfs2 device-config:provider=hba
```

コマンドからの出力では、追加のパラメーターを指定するように求められ、各ステップで使用できる値のリストが示されます。

2. このコマンドを繰り返して、毎回新しいパラメーターを追加します。
3. コマンド出力が **The following SRs were found:** で始まる場合、xe sr-create コマンドを実行するときにストレージリポジトリを格納するのに指定した device-config パラメーターを使用できます。

HBA ターゲットの特定の LUN で共有 GFS2 ストレージリポジトリを作成するには、クラスター化プール内のサーバーで次のコマンドを実行します：

```
1 xe sr-create type=gfs2 name=label="Example GFS2 SR" --shared \  
2   device-config:provider=hba device-config:SCSIid=device_scsi_id
```

HBA ストレージリポジトリの操作について詳しくは、「[ハードウェアホストバスアダプタ](#)」を参照してください。

制約

現在、共有 GFS2 ストレージには次の制約があります：

- VDI が GFS2 ストレージリポジトリ上にある仮想マシンでは、ストレージライブマイグレーションによる仮想マシンの移行はサポートされていません。
- FCoE プロトコルは、GFS2 ストレージリポジトリではサポートされていません。
- トリミングとマッピング解除は、GFS2 ストレージリポジトリではサポートされていません。
- GFS2 ストレージリポジトリおよびこれらのストレージリポジトリ上のディスクでは、パフォーマンス測定値は利用できません。
- 変更ブロック追跡は、GFS2 SR に格納されている VDI ではサポートされません。
- 2TiB を超える VDI を VHD または OVA (Open Virtual Appliance) や OVF (オープン仮想化フォーマット) でエクスポートすることはできません。ただし、VDI が 2TiB を超える仮想マシンは、XVA 形式でエクスポートできます。
- クラスター化プールでは、プールあたり 16 台までのホストのみがサポートされます。
- ネットワークが管理とクラスタリングの両方に使用されている場合は、クラスターを再作成せずに管理ネットワークを分離することはできません。
- XenCenter を使用してクラスターネットワークの IP アドレスを変更するには、クラスタリングと GFS2 を一時的に無効にする必要があります。
- クラスターが稼働中で、クラスターに実行中の仮想マシンがある間は、クラスタリングネットワークのボンディングを変更しないでください。この操作により、クラスターが隔離される可能性があります。
- クラスタリングが有効になっているホストが少なくとも 1 つ含まれるクラスタリングネットワークで、IP アドレスの競合 (IP アドレスが同じホストが複数存在) が発生した場合、競合しているホストが隔離されないことがあります。この問題を解決するには、IP アドレスの競合を解決します。

ストレージリポジトリ (SR) の管理

January 20, 2020

ここでは、さまざまな種類のストレージリポジトリを作成して、Citrix Hypervisor サーバーから使用できるようにする設定例について説明します。また、ライブ VDI マイグレーション機能を含め、ストレージリポジトリの管理に必要なさまざまな操作についても説明します。

ストレージリポジトリを作成する

ここでは、さまざまな種類のストレージリポジトリ (SR) を作成して、Citrix Hypervisor サーバーから使用できるようにする設定例について説明します。これらの例では、CLI を使用してストレージリポジトリを作成します。XenCenter の新規ストレージリポジトリウィザードでの作成方法については、[XenCenter ドキュメント](#)を参照してください。

注:

lvmおよびext3の種類のローカルストレージリポジトリは、xe CLI を使用してのみ作成できます。ただし、作成後のすべての種類のストレージリポジトリは、XenCenter および xe CLI で管理できます。

ホストで使用するストレージリポジトリを CLI で作成するには、以下の 2 つの基本手順があります:

1. 必要なパラメータの値を確認するためにストレージリポジトリをプローブする。
2. ストレージリポジトリを作成して SR オブジェクトとそれに関連付けられた PBD オブジェクトを初期化し、その PBD オブジェクトをプラグしてストレージリポジトリをアクティブ化する。

これらの手順の詳細は、作成されるストレージリポジトリのタイプによって異なります。いずれの場合でも、`sr-create` コマンドによる作成に成功すると、そのストレージリポジトリの UUID が返されます。

物理デバイスを解放するために不要なストレージリポジトリを破棄できます。また、Citrix Hypervisor サーバーからストレージリポジトリを消去して接続を解除したり、さらにそれを別のホストに接続したりできます。詳しくは、次のセクションの「ストレージリポジトリを削除する」を参照してください。

ストレージリポジトリをプローブする

次の目的で、`sr-probe` コマンドを実行できます:

- ストレージリポジトリ作成時に必要なパラメータを確認する
- 既存のストレージリポジトリの一覧を表示する

これらのいずれの場合でも、ストレージリポジトリの種類と、その種類に応じたいくつかの `device-config` パラメータを指定して `sr-probe` コマンドを実行します。必要なパラメータを指定せずに `sr-probe` コマンドを実行すると、必要なパラメータと指定可能なオプションを示すエラーメッセージが表示されます。必要なパラメータを正しく指定した場合は、既存のストレージリポジトリの一覧が表示されます。`sr-probe` コマンドによる出力は、すべて XML 形式で返されます。

たとえば、既知の iSCSI ターゲットがある場合は、その名前または IP アドレスを指定してプローブできます。これにより、そのターゲット上で使用可能なすべての IQN が以下のように返されます:

```
1      xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10
2
3      Error code: SR_BACKEND_FAILURE_96
4      Error parameters: , The request is missing or has an incorrect
      target IQN parameter, \
```

```
5    <?xml version="1.0" ?>
6    <iscsi-target-iqns>
7        <TGT>
8            <Index>
9                0
10           </Index>
11           <IPAddress>
12               192.168.1.10
13           </IPAddress>
14           <TargetIQN>
15               iqn.192.168.1.10:filer1
16           </TargetIQN>
17       </TGT>
18   </iscsi-target-iqns>
```

次に、このターゲットの名前または IP アドレスと、特定の IQN を指定してプローブを実行すると、その IQN 上で使用可能なすべての SCSIids (LUN) が以下のように返されます。

```
1    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
2    device-config:targetIQN=iqn.192.168.1.10:filer1
3
4    Error code: SR_BACKEND_FAILURE_107
5    Error parameters: , The SCSIid parameter is missing or incorrect, \
6    <?xml version="1.0" ?>
7    <iscsi-target>
8        <LUN>
9            <vendor>
10                IET
11            </vendor>
12            <LUNid>
13                0
14            </LUNid>
15            <size>
16                42949672960
17            </size>
18            <SCSIid>
19                149455400000000000000000000000002000000b70200000f000000
20            </SCSIid>
21        </LUN>
22    </iscsi-target>
```

最後に、これら 3 つのパラメーター (ターゲットの名前または IP アドレス、IQN、および SCSIid) を指定してプローブを実行すると、その LUN 上に存在するストレージリポジトリの一覧が以下のように返されます。

```
1    xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \
```

```

2 device-config:targetIQN=192.168.1.10:filer1 \
3 device-config:SCSIid=149455400000000000000000000000002000000
   b70200000f000000
4
5 <?xml version="1.0" ?>
6 <SRlist>
7   <SR>
8     <UUID>
9       3f6e1ebd-8687-0315-f9d3-b02ab3adc4a6
10    </UUID>
11    <Devlist>
12      /dev/disk/by-id/scsi-149455400000000000000000000000002000000
        b70200000f000000
13    </Devlist>
14  </SR>
15 </SRlist>

```

次の表は、ストレージリポジトリの各種類に対して、プローブ可能なパラメータの一覧です。

SRの種類	device-configパラ		
	メーター (依存順)	プローブの可否	sr-createで必須?
lvmoiscsi	target	いいえ	はい
	chapuser	いいえ	いいえ
	chappassword	いいえ	いいえ
	targetIQN	はい	はい
	SCSIid	はい	はい
lvmohba	SCSIid	はい	はい
NetApp	target	いいえ	はい
	username	いいえ	はい
	password	いいえ	はい
	chapuser	いいえ	いいえ
	chappassword	いいえ	いいえ
	aggregate	いいえ (注1参照)	はい
	FlexVols	いいえ	いいえ
nfs	allocation	いいえ	いいえ
	asis	いいえ	いいえ
	server	いいえ	はい

SRの種類	device-configパラ		
	メーター (依存順)	プローブの可否	sr-createで必須?
	serverpath	はい	はい
lvm	device	いいえ	はい
ext	device	いいえ	はい
EqualLogic	target	いいえ	はい
	username	いいえ	はい
	password	いいえ	はい
	chapuser	いいえ	いいえ
	chappassword	いいえ	いいえ
	storagepool	いいえ (注2 参照)	はい

注:

- アグリゲートのプローブは `sr-create`の実行時のみ可能です。
- ストレージプールのプローブは `sr-create`の実行時のみ可能です。

ストレージリポジトリを削除する

ストレージリポジトリ (SR) は、一時的または永続的に削除できます。

detach: ストレージデバイスとプールまたはホストの間の関連付けを削除します (`pbid-unplug`)。ストレージリポジトリ (およびその仮想ディスクイメージ) にはアクセスできなくなります。仮想ディスクイメージの内容と、仮想ディスクイメージにアクセスするために仮想マシンで使用されるメタ情報は保持されます。保守などのためにストレージリポジトリを一時的にオフラインにするときに、このコマンドを使用します。接続を解除したストレージリポジトリは後で再接続できます。

forget: 物理ディスク上のストレージリポジトリの内容は保持されますが、仮想マシンを仮想ディスクイメージに接続するのに使用した情報は永続的に削除されます。たとえば、ストレージリポジトリの内容を削除せずに、ストレージリポジトリを別の Citrix Hypervisor サーバーに再接続できます。

destroy: 物理ディスクからストレージリポジトリの内容を削除します。

`destroy` または `forget` の場合、ストレージリポジトリに接続されている PBD をホストからアンプラグする必要があります。

1. 次のコマンドを実行して、PBD をアンプラグします。これにより、Citrix Hypervisor サーバーからストレージリポジトリが接続解除されます:

```
1 xe pbd-unplug uuid=pbid_uuid
```

2. `sr-destroy` コマンドを使用してストレージリポジトリを削除します。このコマンドにより、ストレージリポジトリが破棄されます。これにより、Citrix Hypervisor サーバーのデータベースからストレージリポジトリおよびその PBD が削除され、そのストレージリポジトリの内容が物理ディスクから削除されます：

```
1 xe sr-destroy uuid=sr_uuid
```

3. `sr-forget` コマンドを使用してストレージリポジトリを消去します。このコマンドにより、Citrix Hypervisor サーバーのデータベースからストレージリポジトリおよびその PBD が削除されますが、ストレージリポジトリのコンテンツ自体は物理メディア上に残ります：

```
1 xe sr-forget uuid=sr_uuid
```

注：

対象のストレージリポジトリのソフトウェアオブジェクトでガベージコレクション処理が完了するまで、時間がかかる場合があります。

ストレージリポジトリをイントロデュースする

以前に接続を消去したストレージリポジトリを再度イントロデュースするには、PBD を作成します。この PBD を適切な Citrix Hypervisor サーバーに手でプラグし、ストレージリポジトリをアクティブ化します。

以下の例では、`lvmoiscsi` ストレージリポジトリを接続します。

1. 次のコマンドを実行して、既存のストレージリポジトリの UUID を確認します。

```
1 xe sr-probe type=lvmoiscsi device-config:target=192.168.1.10 \  
2 device-config:targetIQN=192.168.1.10:filer1 \  
3 device-config:SCSIid=1494554000000000000000000000000020000000  
b70200000f000000
```

2. 次のコマンドを実行して、`sr-probe` で返された既存のストレージリポジトリの UUID をイントロデュースします。これにより、新規 SR の UUID が返されます。

```
1 xe sr-introduce content-type=user name-label="Example Shared LVM  
over iSCSI SR" \  
2 shared=true uuid=valid_sr_uuid type=lvmoiscsi
```

3. 次のコマンドを実行して、ストレージリポジトリに添付する PBD を作成します。これにより、新規 PBD の UUID が返されます。

```
1 xe pbd-create type=lvmoiscsi host-uuid=valid_uuid sr-uuid=  
valid_sr_uuid \  
2 device-config:target=192.168.0.1 \  
3 device-config:targetIQN=192.168.1.10:filer1 \  

```

```
4 device-config:SCSIid=149455400000000000000000000002000000
b70200000f000000
```

4. 次のコマンドを実行して、PBD をプラグします。これにより、ストレージリポジトリが接続されます。

```
1 xe pbd-plug uuid=pbd_uuid
```

5. 次のコマンドを実行して、PBD プラグの状態を確認します。PBD が正しくプラグされている場合、`currently-attached`プロパティが `true` になります：

```
1 xe pbd-list sr-uuid=sr_uuid
```

注：

リソースプール内の各サーバーに対して、手順 3～手順 5 を実行します。これらの手順は、XenCenter の [ストレージ] > [修復] コマンドでも実行できます。

LUN のライブ拡張

ストレージの要件に応じてストレージアレイにキャパシティを追加して、Citrix Hypervisor サーバーにプロビジョニングされる LUN のサイズを増やすことができます。LUN のライブ拡張機能を使用すると、仮想マシンを停止せずに LUN のサイズを増やすことができます。

ストレージアレイの容量を増やしたら、次のように入力します。

```
1 xe sr-scan sr-uuid=sr_uuid
```

これにより、ストレージリポジトリが再スキャンされ、追加されたストレージ領域が使用可能になります。

この操作は XenCenter でも使用できます。ストレージリポジトリを選択してサイズを変更し、[再スキャン] をクリックします。

警告：

- 既存の LUN のサイズを小さくすることはできません。ストレージアレイ上の LUN のサイズを小さくすると、データが失われることがあります。

ライブ VDI マイグレーション

ストレージ XenMotion のライブ VDI マイグレーション機能を使用すると、仮想マシンの仮想ディスクイメージ (VDI) を仮想マシンを停止せずに再配置できます。これにより、管理者は以下のタスクを実行できます：

- 安価なローカルストレージに格納されている仮想マシンを、高速で耐障害性の高いストレージアレイに移動する。
- 仮想マシンを開発環境から実務環境に移動する。

- ストレージ容量による制限がある場合に、仮想マシンをストレージ階層間で移動する。
- ストレージアレイをアップグレードする。

制限事項

ライブ VDI マイグレーションには、以下の制限事項があります。

- 移動先のリポジトリ上に十分な空きディスク容量が必要です。

を使用して仮想ディスクを移動するには **XenCenter**

1. リソースペインで、仮想ディスクが格納されているストレージリポジトリを選択して [ストレージ] タブをクリックします。
2. [仮想ディスク] の一覧で、移動する仮想ディスクを選択して [移動] をクリックします。
3. [仮想ディスクの移動] ダイアログボックスで、移動先のストレージリポジトリを選択します。

注:

一覧には、各ストレージリポジトリの空き容量が表示されます。移動先のストレージリポジトリ上に十分なディスク容量があることを確認してください。

4. [移動] をクリックして仮想ディスクを移動します。

xe CLI リファレンスについては、「[vdi-pool-migrate](#)」 ([/ja-jp/citrix-hypervisor/command-line-interface.html#vdi-pool-migrate](#)) を参照してください。

停止した仮想マシンの **VDI** をほかのストレージリポジトリに移行する (オフラインマイグレーション)

メンテナンス時または階層ストレージを使用する場合は、仮想マシンに関連付けられた仮想ディスクイメージ (VDI) をほかのストレージリポジトリに移動することができます。XenCenter を使用すると、仮想マシンおよびその VDI を、同一または異なるストレージリポジトリにコピーできます。個々の VDI をコピーするには、XenCenter と xe CLI を使用します。

xe CLI リファレンスについては、「[vm-migrate](#)」 ([/ja-jp/citrix-hypervisor/command-line-interface.html#vm-migrate](#)) を参照してください。

仮想マシンのすべての仮想ディスクイメージをほかのストレージリポジトリにコピーする

XenCenter の [VM のコピー] コマンドでは、選択した仮想マシンのすべての VDI を同一または異なるストレージリポジトリ上にコピーできます。このとき、デフォルトでは、元の仮想マシンおよび VDI は変更されません。コピーを作成するのではなく、選択したストレージリポジトリに仮想マシンを移動するには、[VM のコピー] ダイアログボックスで [元の VM の削除] オプションを選択します。

1. 仮想マシンをシャットダウンします。
2. XenCenter で仮想マシンを選択し、**[VM] > [VM のコピー]** を選択します。
3. コピー先のストレージリポジトリを選択します。

個々の仮想ディスクイメージをほかのストレージリポジトリにコピーする

個々の VDI をストレージリポジトリ間でコピーするには、xe CLI と XenCenter を使用します。

1. 仮想マシンをシャットダウンします。
2. xe CLI を使用して、移動する VDI の UUID を識別します。仮想マシンに DVD ドライブがある場合、その `vdi-uuid` は `not in database` で示され、無視できます。

```
1 xe vbd-list vm-uuid=valid_vm_uuid
```

注:

`vbd-list` コマンドにより、VBD UUID および VDI UUID が表示されます。ここでは、VBD UUID ではなく VDI UUID を使用することに注意してください。

3. XenCenter で、仮想マシンの **[ストレージ]** タブを選択します。コピーする VDI を選択して、**[接続解除]** をクリックします。この操作は、`vbd-destroy` コマンドでも実行できます。

注:

`vbd-destroy` コマンドで VDI UUID を「接続解除」する場合は、その VBD の `other-config:owner` パラメーターが `true` に設定されていないことを確認してください。このパラメーターを `false` に設定します。VDI を「破棄」する場合は、`vbd-destroy` コマンドに `other-config:owner=true` を指定して実行することもできます。

4. 次の `vdi-copy` コマンドを実行して、仮想マシンの各 VDI を指定したストレージリポジトリにコピーします。

```
1 xe vdi-copy uuid=valid_vdi_uuid sr-uuid=valid_sr_uuid
```

5. XenCenter で、仮想マシンの **[ストレージ]** タブを選択します。**[接続]** をクリックして、新しいストレージリポジトリの VDI を選択します。この操作は、`vbd-create` コマンドでも実行できます。
6. 元の VDI を削除するには、XenCenter で元のストレージリポジトリの **[ストレージ]** タブを選択します。元の VDI は、一覧の **[仮想マシン]** 列が空白になっています。その VDI を選択して、**[削除]** をクリックすると VDI が削除されます。

ローカルのファイバチャネルストレージリポジトリを共有ストレージリポジトリに変換する

xe CLI および XenCenter の **[ストレージ] > [修復]** を使用して、ファイバチャネルストレージリポジトリを共有ストレージリポジトリに変換します。

1. リソースプール内のすべてのホストを、Citrix Hypervisor 8.1 にアップグレードします。
2. すべてのホストで、ストレージリポジトリの LUN が適切にゾーン設定されていることを確認します。各ホストで LUN が存在するかどうかを `sr-probe` コマンドで確認する方法については、「ストレージリポジトリをプローブする」を参照してください。
3. 次のコマンドを実行して、共有ストレージリポジトリに変換します。

```
1 xe sr-param-set shared=true uuid=local_fc_sr
```

4. 共有されたストレージリポジトリは、XenCenter のツリー表示でホストレベルからプールレベルに移動します。このリポジトリには赤い感嘆符「!」が付き、プール内のすべてのホストに接続されていないことを示します。
5. ストレージリポジトリを選択し、[ストレージ] > [ストレージリポジトリの修復] を選択します。
6. [修復] をクリックすると、プール内のホストごとに PBD が作成され、プラグされます。

バックアップレイ上で破棄操作によってブロックベースストレージの領域を解放する

領域の開放を使用すると、シンプロビジョニングされた LUN 上で、未使用のブロックを解放できます。解放された領域は、ストレージアレイでの再利用が可能になります。

注:

領域の開放は、一部のストレージアレイでのみ使用できます。現在のアレイがこの機能をサポートしているかどうか、および操作に特別な設定が必要かどうかを判断するには、「[ハードウェア互換性リスト \(英語\)](#)」およびストレージベンダー固有のドキュメントを参照してください。

XenCenter を使用して領域を解放するには:

1. [インフラストラクチャ] ビューで、ストレージリポジトリに接続されているサーバーまたはリソースプールを選択します。
2. [ストレージ] タブをクリックします。
3. 一覧でストレージリポジトリを選択して、[空き領域の解放] をクリックします。
4. [はい] をクリックして操作を確定します。
5. [通知]、[イベント] の順にクリックして、操作の状態を表示します。

詳しくは、XenCenter で F1 キーを押してオンラインヘルプを参照してください。

注:

- この操作は XenCenter でのみ有効です。
- この操作は、アレイ上でシンプロビジョニングされた LUN に基づいた、LVM ベースのストレージリポジトリでのみ使用できます。ローカル SSD の場合も、領域を解放できます。
- 領域の開放は、NFS や Ext3 などのファイルベースのストレージリポジトリでは必要ありません。これら

のストレージリポジトリでは、XenCenterで「空き領域の開放」は使用できません。

- 領域の解放は負荷の高い操作であり、ストレージアレイのパフォーマンスが低下する場合があります。このため、領域の解放はアレイで必要なときにのみ行うようにしてください。アレイ要求度の低いオフピーク時にこの操作を行うことをお勧めします。

スナップショット削除時にディスク領域を自動解放する

Citrix Hypervisor では、スナップショットを削除するときに、LVM ベースのストレージリポジトリに割り当てられていたディスク領域が自動的に解放されます。仮想マシンを再起動する必要はありません。この操作は「オンライン結合 (Online Coalescing)」と呼ばれます。

オンライン結合は、LVM ベースのストレージリポジトリ (LVM、LVMoISCSI、および LVMoHBA) のみに適用されます。EXT や NFS ストレージリポジトリには適用されません。オンライン結合が意図したとおりに実行されない場合があります。以下のシナリオでは、オフライン結合ツールを使用することをお勧めします：

- 仮想マシンによる入出力スループットが大きい場合
- いつまでも領域が解放されない場合

注：

- オフライン結合ツールを使用すると、仮想マシンのサスペンドおよび再開によるダウンタイムが発生します。
- オフライン結合ツールを使用する前に、不要なスナップショットや複製をすべて削除しておきます。これにより、より多くの領域が解放されます。すべての領域を解放するには、すべてのスナップショットおよび複製を削除しておきます。
- 仮想マシンのディスクが、共有ストレージ上か、単一ホストのローカルストレージ上に格納されている必要があります。共有ストレージとローカルストレージ上の複数のディスクを持つ仮想マシンでは、結合を実行できません。

オフライン結合ツールでディスク領域を解放する

注：

オンライン結合は、LVM ベースのストレージリポジトリ (LVM、LVMoISCSI、および LVMoHBA) のみに適用されます。EXT や NFS ストレージリポジトリには適用されません。

XenCenter で、隠しオブジェクトを表示します。[表示] > [隠しオブジェクト] をクリックします。[リソース] ペインで仮想マシンを選択します。[全般] タブに UUID が表示されます。

[リソース] ペインで、リソースプールのマスタ (一覧の最初のホスト) を選択します。[全般] タブに UUID が表示されます。スタンドアロンサーバー環境の場合は、仮想マシンのホストを選択します。

1. ホスト上でコンソールを開き、以下のコマンドを実行します。

```
1 xe host-call-plugin host-uuid=host-UUID \
```

```
2 plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=VM-UUID
```

たとえば、仮想マシンの UUID が 9bad4022-2c2d-dee6-abf5-1b6195b1dad5、ホストの UUID が b8722062-de95-4d95-9baa-a5fe343898ea の場合は、次のコマンドを実行します：

```
1 xe host-call-plugin host-uuid=b8722062-de95-4d95-9baa-a5fe343898ea  
  \  
2   plugin=coalesce-leaf fn=leaf-coalesce args:vm_uuid=9bad4022-2  
   c2d-dee6-abf5-1b6195b1dad5
```

2. このコマンドにより、仮想マシンが実行中の場合はサスペンドされ、ディスク領域が解放された後で仮想マシンが再開されます。

注：

オフライン結合ツールを実行する前に、仮想マシンを手動でシャットダウンまたは一時停止しておくことをお勧めします。仮想マシンをシャットダウンまたは一時停止するには、XenCenter または Citrix Hypervisor CLI コマンドを使用します。実行中の仮想マシンに対してこのツールを実行した場合、仮想マシンがサスペンドされ、VDI 結合が行われた後で仮想マシンが再開されます。

結合する仮想ディスクイメージ (VDI) が共有ストレージ上にある場合は、プールマスタ上でオフライン結合ツールを実行する必要があります。

VDI がローカルストレージ上にある場合は、そのストレージが接続されているサーバー上でオフライン結合ツールを実行します。

ディスク入出力スケジューラを変更する

通常、すべての種類の新規ストレージリポジトリに、デフォルトのディスクスケジューラ `noop` が適用されます。`noop` スケジューラでは、同一デバイスにアクセスする複数の仮想マシンによる競合に対して、適切なパフォーマンスが提供されます。ディスク QoS を適用するには、このデフォルト設定を変更して、`cfq` ディスクスケジューラをストレージリポジトリに割り当てる必要があります。スケジューラの変更を有効にするには、PBD をアンプラグして再プラグしてください。ディスクスケジューラは、次のコマンドを使用して調整できます：

```
1 xe sr-param-set other-config:scheduler=noop|cfq|anticipatory|deadline \  
2   uuid=valid_sr_uuid
```

注：

このコマンドは、EqualLogic、NetApp、および NFS ストレージには適用されません。

仮想ディスクの QoS 設定

仮想ディスクの入出力優先度に関する QoS (Quality of Service) オプションを設定できます。ここでは、xe CLI を使用して、既存の仮想ディスクに対してこの設定を行う方法について説明します。

複数のホストが同一 LUN にアクセスするような共有ストレージリポジトリの場合、各ホストから LUN にアクセスする VBD に QoS オプションが適用されます。リソースプール内のホスト全体には適用されません。

VBD に対する QoS パラメータを設定する前に、そのストレージリポジトリのディスクスケジューラが正しく設定されていることを確認してください。スケジューラの設定について詳しくは、前のセクションの「ディスク入出力スケジューラの変更」を参照してください。QoS を有効にするストレージリポジトリでは、スケジューラ用のパラメータを `cfq` に設定する必要があります。

注:

ストレージリポジトリのスケジューラを `cfq` に設定し、その変更を有効にするために PBD を再プラグすることを忘れないでください。

最初のパラメータは `qos_algorithm_type` です。このパラメータは、仮想ディスクの QoS アルゴリズムの種類を指定するもので、このバージョンで唯一サポートされる `ionice` を値として設定する必要があります。

QoS パラメータ自体は、`qos_algorithm_param` パラメータに割り当てられた「キー = 値」のペアを使用して設定されます。仮想ディスクの場合、`qos_algorithm_param` に `sched` キーを指定し、そのキーの値によっては `class` キーを指定します。

`qos_algorithm_param:sched` の設定可能な値:

`-sched=rt` または `sched=real-time` を設定すると、QoS スケジューリングの優先度が「リアルタイム」に設定されます。この場合は、`class` パラメータに値を設定する必要があります。

`-sched=idle` を設定すると、QoS スケジューリングの優先度が「アイドル」に設定されます。この場合は、`class` パラメータに値を設定する必要はありません。

`-sched=anything` を設定すると、QoS スケジューリングの優先度が「最大限の努力」に設定されます。この場合は、`class` パラメータに値を設定する必要があります。

`class` に使用できる値は以下のとおりです:

- キーワード `highest`、`high`、`normal`、`low`、または `lowest` のいずれか。
- 0 から 7 までの整数。7 が最高で 0 が最低の優先度を示します。たとえば、優先度 5 の I/O 要求は、優先度 2 の I/O 要求よりも優先されます。

これらのディスク QoS 設定を有効にするには、`other-config:scheduler` に `cfq` を設定し、そのストレージの PBD を再プラグします。

例えば、次のコマンドを実行すると、仮想ディスクの VBD が使用するリアルタイム優先度が 5 に設定されます:

```
1    xe vbd-param-set uuid=vbd_uuid qos_algorithm_type=ionice
2    xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:sched=rt
```

```

3    xe vbd-param-set uuid=vbd_uuid qos_algorithm_params:class=5
4    xe sr-param-set uuid=sr_uuid other-config:scheduler=cfq
5    xe pbd-plug uuid=pbd_uuid

```

ストレージのマルチパス

December 30, 2019

ファイバチャネルおよび iSCSI のストレージバックエンドでは、動的マルチパスがサポートされます。マルチパスを有効にするには、XenCenter または xe CLI を使用します。

重要:

マルチパスを有効にする前に、以下の事項を確認してください:

- ストレージサーバーで複数のターゲットが使用できる。

たとえば、iSCSI ストレージバックエンドの特定のポータルに対して「sendtargets」を照会した場合、以下のように複数のターゲットが返されます:

```

1    iscsiadm -m discovery --type sendtargets --portal
      192.168.0.161
2    192.168.0.161:3260,1 iqn.strawberry:litchie
3    192.168.0.204:3260,2 iqn.strawberry:litchie

```

- (iSCSI の場合のみ) コントロールドメイン (dom0) で、マルチパスのストレージにより使用されるサブネットごとに IP アドレスが構成されている。

ストレージへのパスごとに NIC があり、各 NIC に IP アドレスが構成されていることを確認してください。たとえば、ストレージにアクセスする 4 つのパスを作成する場合は、それぞれに IP アドレスが構成された 4 つの NIC が必要です。

- (HBA の場合のみ) 複数の HBA がスイッチファブリックに接続されている。

1. Citrix Hypervisor サーバーのコンソールを開きます。
2. 次のコマンドを使用して、サーバー上のすべての PBD をアンプラグします:

```
1 xe pbd-unplug uuid=<pbd_uuid>
```

3. 次のコマンドを使用して、`other-config:multipathing` パラメーターの値を **true** に設定します:

```
1 xe host-param-set other-config:multipathing=true uuid=<server_uuid>
```

4. 次のコマンドを使用して、`other-config:multipathhandle`パラメーターの値を`dmp`に設定します:

```
1 xe host-param-set other-config:multipathhandle=dmp uuid=<server_uuid>
```

5. サーバー上でシングルパスモードで動作しているストレージリポジトリのマルチパスを有効にするには、次の操作を行います:

- そのストレージリポジトリ上の仮想ディスクを使用している、実行中の仮想マシンを移行またはサスペンドします。
- そのストレージリポジトリの PBD をマルチパスで再接続するために、アンプラグして再プラグします:

```
1 xe pbd-unplug uuid=<pbid_uuid>
2 xe pbd-plug uuid=<pbid_uuid>
```

マルチパスを無効にする場合は、まず VBD をアンプラグし、ホストの`other-config:multipathing`パラメータを`false`に設定して、上記の手順で PBD を再プラグします。このとき、`other-config:multipathhandle`パラメータは変更しないでください。このパラメータは自動的に変更されます。

Citrix Hypervisor でのマルチパスのサポートは、デバイス Mapper `multipathd components`に基づいています。マルチパスノードの有効化および無効化は、ストレージマネージャ API により自動的に処理されます。Linux の標準ツール `dm-multipath`とは異なり、システム上のすべての LUN のデバイス Mapper ノードが自動的に作成されるわけではありません。ストレージ管理レイヤーにより LUN がアクティブに使用されるときにのみデバイス Mapper ノードがプロビジョニングされます。このため、`dm-multipath` CLI ツールを使って Citrix Hypervisor の DM テーブルノードを照会したり更新したりする必要はありません。システム上のアクティブなデバイス Mapper マルチパスノードを確認したり、デバイス Mapper テーブルの状態を手作業で照会したりするには、以下の `mpathutil` ユーティリティを使用します:

```
1 mpathutil list
```

```
1 mpathutil status
```

注:

- 組み込まれているマルチパス管理アーキテクチャとの互換性がないため、標準的な CLI ユーティリティ `dm-multipath` を Citrix Hypervisor で使用しないでください。ホスト上のノードの状態を照会するには、CLI ツール `mpathutil` を使用してください。
- EqualLogic アレイでは、従来の意味でのストレージ I/O のマルチパス化がサポートされず、ネットワーク/NIC ボンディングレベルでマルチパス化する必要があります。EqualLogic/LVMoISCSI ストレージリポジトリのネットワークフェイルオーバーの設定については、EqualLogic のドキュメントを参照してください。

IntelliCache

December 30, 2019

注:

この機能は、Citrix Virtual Desktops で Citrix Hypervisor を使用する場合にのみサポートされます。

GFS2 ストレージリポジトリを使用する仮想マシンでは、IntelliCache はサポートされていません。

Citrix Hypervisor の *IntelliCache* 機能により、共有ストレージとローカルストレージを組み合わせ使用して、仮想デスクトップインフラストラクチャをより効率的に展開できるようになりました。この機能は、多くの仮想マシンで同じオペレーティングシステムイメージを共有する場合に特に有効です。この機能を使用すると、ストレージレイへの負荷が軽減され、パフォーマンスが向上します。また、共有ストレージからマスターイメージがローカルストレージ上にキャッシュされるため、XenServer と共有ストレージ間のネットワークトラフィックが減少します。

IntelliCache により、仮想マシンの親 VDI のデータが、その仮想マシンホストのローカルストレージ上にキャッシュされます。このローカルキャッシュは、親 VDI からのデータ読み取りが必要になった時に使用されます。多数の仮想マシンで親 VDI を共有する場合、1つの仮想マシンでキャッシュに読み込まれたデータがほかの仮想マシンでも使用されるという状況が多く発生します。この場合、共有ストレージ上のマスターイメージにアクセスする代わりに、ローカルキャッシュが使用されます。

IntelliCache を使用するには、シンプロビジョニングで作成されたローカルストレージリポジトリが必要です。シンプロビジョニングという方法を使用すると、ストレージ領域を最大限に活用できます。これにより、ローカルストレージを効率的に使用できるようになります。シンプロビジョニングでは、オンデマンドでデータブロックが割り当てられます。一方、他の方法では、すべてのブロックが事前に割り当てられます。

重要:

シンプロビジョニングを有効にすると、ホストのデフォルトローカルストレージの種類が LVM から EXT3 に変更されます。Citrix Virtual Desktops を使用する場合は、ローカルキャッシュが正しく機能するように、シンプロビジョニングを有効にする必要があります。

シンプロビジョニングを使用すると、管理者はそのストレージリポジトリの実際の使用可能領域よりも大きなサイズを仮想マシンに提供できます。この場合、領域は予約されず、仮想マシンによりデータが書き込まれるまでは、LUN の割り当て処理でデータブロックが要求されることはありません。

警告:

仮想マシンでのディスク消費が増加すると、シンプロビジョニングのストレージリポジトリで物理領域が足りなくなることがあります。この問題を回避するため、IntelliCache が有効な仮想マシンでは、ローカルストレージリポジトリのキャッシュに空きがなくなると自動的に共有ストレージへのフォールバックが行われます。IntelliCache が有効な仮想マシンのサイズは急激に増加することがあるため、同じストレージリポジトリで通常の仮想マシンと IntelliCache 仮想マシンを共存させないでください。

IntelliCache の使用

IntelliCache は、XenServer をホストにインストールする時に有効にします。インストール済みの XenServer ホストでは、CLI を使用してこの機能を有効にすることもできます。

IntelliCache を使用する場合は、可能な限り高速にデータを転送できるように、高性能なローカルストレージデバイスを使用することをお勧めします。たとえば、SSD (Solid State Disk) や高性能な RAID などを使用します。ローカルディスクのデータスループットだけでなく、ストレージ容量についても考慮する必要があります。また、親 VDI をホストする共有ストレージの種類は、NFS または EXT である必要があります。

ホストのインストール時に有効にする

インストール時に IntelliCache を有効にするには、**[Virtual Machine Storage]** 画面で **[Enable thin provisioning]** を選択します。これにより、このローカルストレージリポジトリが仮想マシン VDI のローカルキャッシュとして使用されるようになります。



既存のホストでシンプロビジョニングに変換する

LVM ベースの既存のローカルストレージリポジトリを削除して EXT3 ベースのシンプロビジョニングストレージリポジトリに変換するには、次のコマンドを実行します。

警告:

これらのコマンドにより、既存のローカルストレージリポジトリが削除され、そのストレージリポジトリ上の仮想マシンがすべて消去されます。

```
1     localsr='xe sr-list type=lvm host=hostname params=uuid --minimal'
2     echo localsr=$localsr
3     pbd='xe pbd-list sr-uuid=$localsr params=uuid --minimal'
4     echo pbd=$pbd
```

```
5     xe pbd-unplug uuid=$pbd
6     xe pbd-destroy uuid=$pbd
7     xe sr-forget uuid=$localsr
8     sed -i "s/'lvm'/'ext'/" /etc/firstboot.d/data/default-storage.
      conf
9     rm -f /etc/firstboot.d/state/10-prepare-storage
10    rm -f /etc/firstboot.d/state/15-set-default-storage
11    service firstboot start
12    xe sr-list type=ext
```

ローカルキャッシュを有効にするには、次のコマンドを実行します：

```
1     xe host-disable host=hostname
2     localsr='xe sr-list type=ext host=hostname params=uuid --
      minimal'
3     xe host-enable-local-storage-caching host=hostname sr-uuid=
      $localsr
4     xe host-enable host=hostname
```

仮想マシンの起動設定

仮想マシン起動時の VDI の動作として、以下の 2 つのモードがあります：

1. 共有デスクトップモード

このモードで仮想マシンを起動すると、VDI が前回起動時の状態に復元されます。前回の仮想マシンセッション内での変更内容は、すべて削除されます。

仮想デスクトップに対する永続的な変更をユーザーに許可せず、常に標準的なデスクトップを提供する場合は、このオプションを選択します。

2. プライベートデスクトップモード

このモードの仮想マシンは、VDI が前回シャットダウン時の状態のまま起動します。

仮想デスクトップに対する永続的な変更をユーザーに許可する場合は、このオプションを選択します。

仮想マシンのキャッシュ設定

仮想マシンのキャッシュ設定は、VDI フラグ `allow-caching` により制御されます：

共有デスクトップモード

`on-boot` オプションを `reset` に設定して `allow-caching` フラグを `true` に設定した共有デスクトップの場合、仮想マシン上での新規データはローカルストレージにのみ書き込まれ、共有ストレージには書き込まれません。これ

により、共有ストレージへの負荷が軽減されます。ただし、仮想マシンをほかのホスト上に移行することはできません。

プライベートデスクトップモード

on-boot オプションを `persist` に設定して `allow-caching` フラグを `true` に設定したプライベートデスクトップの場合、仮想マシン上での新規データはローカルストレージおよび共通ストレージに書き込まれます。キャッシュされたデータの読み取り時には共有ストレージへの入出力が不要なため、共有ストレージへの負荷が軽減されます。仮想マシンをほかのホスト上に移行することも可能であり、移行先でのデータ読み取りに応じてそのホスト上にローカルキャッシュが生成されます。

実装の詳細とトラブルシューティング

Q: IntelliCache は、ライブマイグレーションや高可用性機能と互換性がありますか。

A: 仮想デスクトップがプライベートモード (`on-boot=persist`) の場合は、IntelliCache とライブマイグレーションや高可用性機能を併用できます。

警告:

VDI のキャッシュ動作として `on-boot=reset` および `allow-caching=true` が設定されている仮想マシンは、ほかのホスト上に移行することはできません。この場合、仮想マシンの移行に失敗します。

Q: ローカルキャッシュはローカルディスクのどこに生成されますか？

A: キャッシュはストレージリポジトリ内に生成されます。各ホストには、どの（ローカル）ストレージリポジトリがキャッシュファイルに使用されるかを示す構成パラメーター (`local-cache-sr`) があります。通常、これらのストレージリポジトリの種類は EXT です。IntelliCache を有効にして仮想マシンを実行すると、このストレージリポジトリ上に `uuid.vhdcache` という名前のファイルが作成されます。これが、UUID で示される VDI のキャッシュファイルです。これらのキャッシュファイルは、XenCenter には表示されません。キャッシュファイルを表示するには、`dom0` にログインし、`/var/run/sr-mount/sr-uuid` の内容を一覧します。

Q: キャッシュ用のストレージリポジトリを指定するには？

A: ローカルストレージリポジトリは、`host` オブジェクトの `local-cache-sr` フィールドで示されます。その値を表示するには、次のコマンドを実行します：

```
1 xe sr-list params=local-cache-sr,uuid,name-label
```

この値を設定するには、以下のいずれかを行います：

- XenServer をホストにインストールする時に、[Enable thin provisioning] オプションを選択する。または、
- `xe host-enable-local-storage-caching host=host sr-uuid=sr` を実行する。このコマンドを実行するには、指定されたホストが無効になっており、仮想マシンがシャットダウン状態である必要があります。

1 目目のオプションでは、ホストのインストール時に種類が EXT のローカルストレージリポジトリが作成されます。2 目目のオプションでは、コマンドラインで指定したストレージリポジトリが使用されます。

警告:

これらの手順が必要になるのは、複数のローカルストレージリポジトリを設定した場合のみです。

Q: ローカルキャッシュはいつ削除されますか？

A: VDI のキャッシュファイルが削除されるのは、その VDI 自体を削除した時のみです。VDI が仮想マシンに接続されると（仮想マシンの起動時など）、キャッシュがリセットされます。VDI を削除した時にホストがオフラインだった場合は、そのホストの起動時に実行されるストレージリポジトリ同期によりキャッシュファイルが削除されます。

注:

仮想マシンをほかのホストに移行した時、および仮想マシンをシャットダウンしたときは、ホスト上のキャッシュファイルは削除されません。

ストレージ読み取りキャッシュ

December 30, 2019

読み取りキャッシュでは、外部ディスクからの最初の読み取り後、データがホストの空きメモリにキャッシュされるので、仮想マシンのディスクパフォーマンスが向上します。単一のベース仮想マシンから多数の仮想マシンが複製されている状況では、ディスクからの読み取りブロック数が大幅に削減されるため、パフォーマンスが向上します。たとえば、Citrix Virtual Desktops の Machine Creation Service (MCS) 環境などです。

データがメモリにキャッシュされるため、ディスクから複数回読み取る場合には常にパフォーマンスが向上します。最も顕著な例は、負荷の高い I/O 処理によりサービス速度が低下している場合です。たとえば、次のような場合です:

- 多数のエンドユーザーが、非常に短時間の間に一斉に起動する場合（ブートストーム）
- 多数の仮想マシンが同時刻にマルウェアスキャンを実行するようにスケジュール指定されている場合（アンチウイルスストーム）。

適切なライセンスの種類がある場合は、読み取りキャッシュはデフォルトで有効です。

注:

ストレージ読み取りキャッシュ機能は、Citrix Hypervisor Premium Edition ユーザーが使用できます。

ストレージ読み取りキャッシュ機能は、Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーも使用できます。

読み取りキャッシュを有効または無効にする

NFS や EXT3 ストレージリポジトリなど、ファイルベースのストレージリポジトリの場合、読み取りキャッシュはデフォルトでオンになっています。ほかのストレージリポジトリの場合はすべてデフォルトでオフです。

特定のストレージリポジトリで読み取りキャッシュを無効にするには、次のコマンドを実行します：

```
1 xe sr-param-set uuid=sr-uuid other-config:o_direct=true
```

制限事項

- 読み取りキャッシュは、NFS および EXT3 ストレージリポジトリの場合にのみ使用できます。そのほかの種類
のストレージリポジトリでは使用できません。
- 読み取りキャッシュは、読み取り専用の VDI および親 VDI に対してのみ適用されます。これらの VDI は、「高
速複製」またはディスクスナップショットから作成された仮想マシン上に存在します。最もパフォーマンスが
向上するのは、多数の仮想マシンが単一の「ゴールドイメージ」から複製されている場合です。
- パフォーマンスが向上する度合いは、ホストのコントールドメイン (dom0) で使用可能な空きメモリ量に
応じて異なります。dom0 のメモリ量を増やすと、読み取りキャッシュに割り当てられるメモリ量も増加しま
す。dom0 のメモリ量の設定について詳しくは、[CTX134951](#)を参照してください。

IntelliCache との比較

IntelliCache およびメモリベースの読み取りキャッシュは、ある意味において相補的です。IntelliCache は、別の階層でキャッシュするだけでなく、読み取りおよび書き込みの両方をキャッシュします。IntelliCache は、ネットワークからの読み取りをローカルディスクにキャッシュします。インメモリ読み取りキャッシュは、ネットワークまたはディスクからの読み取りをホストメモリにキャッシュします。インメモリ読み取りキャッシュの利点は、メモリの方が Solid-State Disk (SSD) よりも速度が 10 倍速ということです。このため、ブートストームや負荷の高い I/O 処理の状況でも、パフォーマンスが向上します。

読み取りキャッシュと IntelliCache は、同時に有効にすることができます。この場合、ネットワークからの読み取りを IntelliCache がローカルディスクにキャッシュし、そのローカルディスクからの読み取りを、読み取りキャッシュがメモリにキャッシュします。

読み取りキャッシュサイズを設定する

読み取りキャッシュのパフォーマンスを最適化するには、Citrix Hypervisor のコントールドメイン (dom0) のメモリ量を増やします。

重要:

最適化のために、読み取りキャッシュサイズは、プール内のすべてのホストで個別に設定する必要があります。読み取りキャッシュサイズに変更を加える場合は、プール内のすべてのホストに対して設定する必要があります。

Citrix Hypervisor サーバーのローカルシェルを開き、root ユーザーでログインします。

読み取りキャッシュサイズを設定するには、次のコマンドを実行します:

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=nnM,max:nnM
```

初期値と最大値は、いずれも同じ値に設定する必要があります。たとえば、dom0 メモリを 2,048MiB に設定するには、次のように入力します:

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=20480M,max:20480M
```

重要:

読み取りキャッシュサイズを変更したら、すべてのホストを再起動します。

現在の **dom0** のメモリ割り当てを表示する

現在の dom0 のメモリ設定を表示するには、次のように入力します:

```
1 free -m
```

`free -m` の出力は、現在の dom0 のメモリ設定を示しています。この値は、さまざまなオーバーヘッドにより想定された値よりも小さくなっている場合があります。次の表は、dom0 を 2.6GiB に設定した場合のホストの出力例です。

	Available	Total	Used	Free	Shared	Buffer/cache
3	Mem:	2450	339	1556	9	554
4	Swap:	1023	0	1023		

使用可能な値の範囲

Citrix Hypervisor コントロールドメイン (dom0) は 64 ビットであるので、大きい値を使用できます (たとえば、32768MiB)。ただし、コントロールドメインに **1GiB** 未満のメモリを割り当てることはお勧めしません。

XenCenter の表示に関する注意事項

ホストの全メモリが Xen ハイパーバイザー、dom0、仮想マシン、および空きメモリから構成されていることを認識する必要があります。通常、dom0 と仮想マシンのメモリのサイズは固定されていますが、Xen ハイパーバイザーが使用するメモリ量は可変です。使用されるメモリの量は、さまざまな要素によって異なります。これらの要素には、常時ホストで実行中の仮想マシン数と、これらの仮想マシンの設定方法が含まれます。Xen が使用するメモリ量は制限できません。メモリ量を制限すると、Xen でメモリが不足し、ホストに空きメモリが存在する場合でも、別の仮想マシンが起動できなくなる可能性があります。

ホストに割り当てられているメモリ量を表示するには、XenCenter でホストを選択してから [メモリ] タブをクリックします。

Citrix Hypervisor フィールドに、dom0 に割り当てられているメモリおよび Xen メモリの合計容量が表示されます。このため、表示されるメモリ量は、管理者が指定した容量よりも大きくなる可能性があります。また、管理者が dom0 に固定サイズを設定した場合でも、仮想マシンの起動および停止時にメモリサイズが変動することがあります。

PVS アクセラレータ

March 12, 2020

Citrix Hypervisor の PVS アクセラレータ機能には、Citrix Hypervisor および Citrix Provisioning のユーザー向けの追加機能があります。Citrix Provisioning は、Citrix Virtual Apps and Desktops のイメージ管理とホスティングでよく使われます。PVS アクセラレータにより、既に申し分のない Citrix Hypervisor と Citrix Provisioning の組み合わせが大幅に改善されます。これにより、以下を含む機能が改善されます：

- **データの局所性：** メモリ、SSD、および NVM デバイスのパフォーマンスおよび局所性を読み取り要求に利用しながら、ネットワーク利用を大幅に削減します。
- **エンドユーザーエクスペリエンスの向上：** データの局所性により、キャッシュされたターゲットデバイス（仮想マシン）の読み取り I/O 遅延が短縮され、エンドユーザーアプリケーションの速度が向上します。
- **仮想マシンの起動およびブートストームの高速化：** 読み取り I/O 遅延の短縮および効率の改善により、仮想マシンの起動が高速化し、短時間のうちに多数のデバイスが起動する場合のパフォーマンスがより速くなります。
- **ハイパーバイザーホストの追加によるスケールアウトの簡素化：** Citrix Hypervisor サーバー全体でストレージの負荷が効率的に分散されることにより、必要な Citrix Provisioning サーバーの数が少なくなります。ピーク負荷は元のホストのキャッシュを使用して処理します。
- **TCO の削減およびインフラストラクチャ要件の簡素化：** Citrix Provisioning サーバーの数が減ることによってハードウェアおよびライセンス要件が緩和され、管理オーバーヘッドも低減されます。解放された容量はワークロードに使用できます。

注:

PVS アクセラレータは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。PVS アクセラレータ機能を使用するには、ライセンスサーバーを 11.14 にアップグレードする必要があります。

PVS アクセラレータの動作

PVS アクセラレータは、Citrix Hypervisor のコントロールドメイン (Dom0) に格納されているプロキシメカニズムを採用しています。この機能が有効化されると、Citrix Provisioning のターゲットデバイス (仮想マシン) の読み取り要求は Citrix Hypervisor サーバーマシン上で直接キャッシュされます。これらの要求は、物理メモリやストレージリポジトリでキャッシュされます。Citrix Hypervisor サーバー上の後続仮想マシンが同じ読み取り要求を行う場合、仮想ディスクは Citrix Provisioning サーバーではなくキャッシュから直接提供されます。Citrix Provisioning サーバーからのコンテンツ提供を削減することにより、ネットワークの使用およびサーバー上の処理が大幅に軽減され、仮想マシンのパフォーマンスが向上します。

PVS アクセラレータを有効にする

PVS アクセラレータ機能を有効にするには、Citrix Hypervisor と Citrix Provisioning で次の設定を完了する必要があります:

1. PVS アクセラレータサブメンタルパックをプール内の各 Citrix Hypervisor サーバーにインストールします。サブメンタルパックは[Citrix Hypervisor 製品ダウンロードページ](#)からダウンロードできます。サブメンタルパックは、XenCenter または xe CLI を使用してインストールできます。XenCenter を使用したサブメンタルパックのインストール方法について詳しくは、XenCenter ドキュメントの「[サブメンタルパックのインストール](#)」を参照してください。CLI の手順については、[Citrix Hypervisor Supplemental Packs and the DDK Guide \(英語\)](#) を参照してください。
2. XenCenter または xe CLI を使用した Citrix Hypervisor での PVS アクセラレータの構成この構成には、Citrix Provisioning サイトの追加および Citrix Provisioning キャッシュストレージの格納先の指定などがあります。
 - CLI の手順については、次のセクションの「[CLI を使用した Citrix Hypervisor での PVS アクセラレータの構成](#)」を参照してください。
 - XenCenter を使用した PVS アクセラレータの構成について詳しくは、XenCenter ドキュメントの「[PVS アクセラレータ](#)」を参照してください。
3. Citrix Hypervisor で PVS アクセラレータを構成した後は、PVS UI を使用して PVS サイトのキャッシュ構成を完了してください。詳しい手順については、Citrix Provisioning でのキャッシュ構成の完了を参照してください。

CLI を使用して **Citrix Hypervisor** で **PVS** アクセラレータを構成する

1. Citrix Hypervisor で Citrix Provisioning サイト構成を作成するには、次のコマンドを実行します:

```
1 PVS_SITE_UUID=$(xe pvs-site-introduce name=label=My PVS Site)
```

2. プールの各ホストに、どのキャッシュを使用するかを指定します。キャッシュをストレージリポジトリ (SR) に格納するか、コントロールドメインのメモリに格納するかを選択できます。

ストレージリポジトリでキャッシュストレージを構成する

キャッシュストレージとしてストレージリポジトリ (SR) を使用する場合は、次の特性を考慮する必要があります:

長所:

- 最新の読み取りデータがメモリにベストエフォートベースでキャッシュされるため、このデータには、コントロールドメインメモリを使用した場合と同様に迅速にアクセスできます。
- キャッシュは、SR に格納されている場合はより大きくなる可能性があります。SR の領域のコストは通常、メモリ領域のコストのほんの一部です。つまり、SR でのキャッシュは Citrix Provisioning サーバーの負荷をより軽減することができます。
- コントロールドメインのメモリ設定を変更する必要はありません。キャッシュによって、コントロールドメインで利用可能なメモリが自動的に使用されるため、コントロールドメインがメモリ不足になることはありません。
- キャッシュ VDI は共有ストレージに格納できます。ただし、この選択はほとんど意味がありません。この方法は、共有ストレージが Citrix Provisioning サーバーよりも大幅に速度で優れている場合にのみ意味があります。
- キャッシュストレージには、ファイルベースまたはブロックベースのストレージリポジトリのどちらでも使用できます。

短所:

- SR の動作が遅く、要求されたデータがメモリ層にない場合、キャッシュプロセスがリモートの Citrix Provisioning サーバーよりも遅くなる場合があります。
- 共有ストレージに格納されているキャッシュされた VDI は、ホスト間で共有できません。キャッシュされた VDI は 1 つのホストに固有のものです。

ストレージリポジトリでキャッシュストレージを構成するには、次の手順を実行します:

1. 次のコマンドを実行して、キャッシュに使用される SR の UUID を検索します:

```
1 xe sr-list name=label=Local storage host=host-name-label --minimal )
```

2. キャッシュストレージを作成します。

```
1 xe pvs-cache-storage-create host=host-name-label pvs-site-uuid=
  PVS_SITE_UUID \
2      sr-uuid=SR_UUID size=10GiB
```

注:

ストレージリポジトリ (SR) を選択していると、この機能は SR で指定されたキャッシュの最大サイズまで使用します。また、使用可能なコントロールドメインメモリを、ベストエフォートキャッシュ層として暗黙的に使用します。

コントロールドメインメモリでのキャッシュストレージの構成

キャッシュストレージとしてコントロールドメインメモリを使用する場合は、次の特性を考慮する必要があります。

長所:

メモリを使用すると、キャッシュへのアクセスまたはキャッシュの入力を行う際の読み取り/書き込みのパフォーマンスが常に高速になります。

短所:

- キャッシュストレージに使用される RAM が仮想マシンに使用できないため、ハードウェアのサイズを適切に設定する必要があります。
- キャッシュストレージを構成する前に、コントロールドメインのメモリを拡張する必要があります。

注:

キャッシュをコントロールドメインのメモリに格納する場合、この機能によってコントロールドメインのメモリが指定されたキャッシュサイズまで使用されます。このオプションは、追加のメモリがコントロールドメインに割り当てられた後でのみ使用できるようになります。コントロールドメインメモリの増加については、[コントロールドメインに割り当てられるメモリ量の変更](#)を参照してください。

ホストのコントロールドメインに割り当てられるメモリの量を増やすと、追加メモリを明示的に PVS アクセラレータに割り当てることができます。

コントロールドメインメモリでキャッシュストレージを構成するには、次の手順を実行します:

1. 次のコマンドを実行して、キャッシュに使用されるホストの UUID を検索します:

```
1 xe host-list name=label=host-name-label --minimal
```

2. 特別な種類 (tmpfs) の SR を作成します:

```
1 xe sr-create type=tmpfs name=label=MemorySR host-uuid=
  HOST_UUID device-config:uri=""
```

3. 次のコマンドを実行して、キャッシュストレージを作成します。

```
1 xe pvs-cache-storage-create host-uuid=HOST_UUID  
2 pvs-site-uuid=PVS_SITE_UUID sr-uuid=SR_UUID size=1GiB
```

SR_UUIDは、手順 b で作成された SR の UUID です。

Citrix Provisioning でキャッシュ構成を完了する

Citrix Hypervisor で PVS アクセラレータを構成した後、次の手順を実行して Citrix Provisioning サイトのキャッシュ構成を完了します。

Citrix Provisioning 管理コンソールで、(展開の種類に応じて) Citrix Virtual Desktops セットアップウィザードまたは仮想マシンのストリーミングウィザードを使用してプロキシ機能にアクセスします。この 2 つのウィザードは似たようなウィザードで、多くの画面を共有していますが、次の相違点があります。

- **Citrix Virtual Desktops** セットアップウィザードは、Citrix Virtual Desktops を使用して制御される Citrix Hypervisor ハイパーバイザーで実行される仮想マシンの構成に使用します。
- 仮想マシンのストリーミングウィザードは、ホストで仮想マシンを作成するために使用され、Citrix Virtual Desktops には使用されません。

Citrix Provisioning 管理コンソールを開始します：

1. Citrix Provisioning サイトに移動します。
2. Citrix Provisioning サイトを選択し、右クリックしてコンテキストメニューを表示します。
3. 環境に応じて適切なウィザードを選択します。オプション [すべての仮想マシンの **PVS** アクセラレータを有効にします] を選択して PVS アクセラレータ機能を有効化します。
4. 初めて仮想ディスクキャッシュを有効化する場合は、ストリーム配信仮想マシンのセットアップウィザードに **Citrix Hypervisor** の画面が表示されます。Citrix Provisioning サイトと関連付けられていない Citrix Hypervisor で構成されたすべての Citrix Provisioning サイトの一覧が表示されます。一覧を使用して、PVS アクセラレータを適用する Citrix Provisioning サイトを選択します。この画面は、同じ Citrix Hypervisor サーバーを使用して同じ Citrix Provisioning サイトのウィザードを実行する場合は表示されません。
5. [次へ] をクリックしてキャッシュ構成を完了します。
6. [完了] をクリックして Citrix Virtual Desktops またはストリーム配信された仮想マシンをプロビジョニングし、選択した Citrix Provisioning を Citrix Hypervisor の PVS アクセラレータに関連付けます。この手順が完了すると、**PVS** アクセラレータ構成ウィンドウの [PVS サーバー表示] ボタンが XenCenter で有効になります。[PVS サーバー表示] ボタンをクリックすると、Citrix Provisioning サイトに関連付けられたすべての PVS サーバーの IP アドレスが表示されます。

キャッシュ操作

PVS アクセラレータ機能を使用する場合は、次の点を考慮する必要があります：

- XenCenter および Citrix Provisioning の PVS アクセラレータユーザーインターフェイスは、PVS アクセラレータサプリメンタルパックがインストールされている場合にのみ表示されます。
- Citrix Provisioning のターゲットデバイスはプロキシのステータスを認識します。機能がインストールされたら、追加の構成は必要ありません。
- 同じ VHD で複数の Citrix Provisioning サーバーが展開されていて、ファイルシステムのタイムスタンプが異なる環境では、データが複数回キャッシュされる可能性があります。この制限により、仮想ディスク向けの VHD ではなく VHDX 形式を使用することをお勧めします。
- PVS サーバー通信に広いポート範囲を使用しないでください。20 を超える範囲のポートを設定する必要はほとんどありません。ポート範囲が広いと、PVS アクセラレータを使用する場合の Citrix Hypervisor コントロールドメインの起動時間が長くなることがあります。
- PVS アクセラレータが有効になった仮想マシンを起動した後、仮想マシンのキャッシュステータスは XenCenter に表示されます：
 - プールまたはホストの **[PVS]** タブ
 - 仮想マシンの **[一般]** タブ
- ユーザーは、XenCenter のホストの **[パフォーマンス]** タブで RRD 測定値を使用して、PVS アクセラレータの正しい操作を確認できます。詳しくは、「[環境の監視と管理](#)」を参照してください。

重要：

- PVS アクセラレータには、Citrix Provisioning 7.13 以降が必要です。
- PVS アクセラレータは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Desktops 権限および Citrix Virtual Apps 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。
- PVS アクセラレータにはライセンスサーバー 11.14 が必要です。
- PVS アクセラレータ機能では OVS の機能が使用されるため、ネットワークバックエンドとして Linux ブリッジを使用しているホストでは PVS アクセラレータ機能を利用できません。
- PVS アクセラレータと vSwitch Controller との併用はサポートされていません。
- PVS アクセラレータは、キャッシュされた仮想マシンの最初の仮想ネットワークインターフェイス (VIF) で機能します。そのため、キャッシュが機能するように、最初の VIF は Citrix Provisioning ストレージネットワークに接続する必要があります。
- 現時点で PVS アクセラレータは、IP を特定の MAC アドレスにバインドするネットワークポートでは使用できません。このスイッチの機能は「IP ソースガード」とも呼ばれます。このような環境で PVS アクセラレータを有効にすると、PVS ターゲットの起動に失敗し、「ログイン要求がタイムアウトしました」というエラーメッセージが表示されます。

PVS アクセラレータ機能では、以下がキャッシュされます。

- 仮想ディスクからの読み取り（書き込みキャッシュからの書き込みや読み取りはキャッシュされません）
- イメージのバージョンに基づくキャッシュ。複数の VM が同じイメージのバージョンを使用する場合、これらの VM はキャッシュされたブロックを共有します
- あらゆる非永続書き込みキャッシュの種類があるデバイス
- アクセスモードが「標準イメージ」の仮想ディスク。アクセスモードが「プライベートイメージ」の仮想ディスクには機能しません
- 種類が「実稼働」または「テスト」としてマークされているデバイス。種類が「保守」とマークされたデバイスはキャッシュされません

PVS アクセラレータの CLI 操作

次のセクションでは、CLI を使用して PVS アクセラレータを使用する際に実行できる操作について説明します。これらの操作は、XenCenter を使用しても実行できます。詳しくは、XenCenter ドキュメントの「[PVS アクセラレータ](#)」を参照してください。

Citrix Provisioning サーバーアドレス、および Citrix Provisioning で構成されたポートを表示する

PVS アクセラレータは、仮想マシンと Citrix Provisioning サーバー間のネットワークトラフィックを最適化することによって機能します。Citrix Provisioning サーバーの構成を完了すると、Citrix Provisioning サーバーによって Citrix Hypervisor に `pvs-server` オブジェクトが IP とポートとともに入力されます。PVS アクセラレータはその後、特に仮想マシンと Citrix Provisioning サーバー間のトラフィックを最適化するためにこの情報を使用します。次のコマンドを使用して、構成された Citrix Provisioning サーバーを一覧表示できます：

```
1 xe pvs-server-list pvs-site-uuid=PVS_SITE_UUID params=all
```

キャッシュ用に仮想マシンを構成する

次のいずれかのツールを使用して、仮想マシンに対する PVS アクセラレータを有効化できます：

- Citrix Provisioning CLI
- Citrix Virtual Desktops インストールウィザード
- ストリーム配信仮想マシンセットアップウィザード
- XenCenter
- xe CLI

xe CLI は、仮想マシンの VIF を使用して PVS アクセラレータを設定します。仮想マシンの VIF を Citrix Provisioning サイトとリンクする Citrix Provisioning プロキシを作成します。

仮想マシンを構成するには、次の手順を実行します：

1. キャッシュを有効にする仮想マシンの最初の VIF を見つけます。

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --minimal)
```

2. Citrix Provisioning プロキシを作成します。

```
1 xe pvs-proxy-create pvs-site-uuid=PVS_SITE_UUID vif-uuid=$VIF_UUID
```

仮想マシンのキャッシュを無効にする

仮想マシンの VIF と `pvs-site` をリンクする Citrix Provisioning プロキシを破棄することによって、仮想マシンに対して PVS アクセラレータを無効化することができます。

1. 仮想マシンの最初の VIF を見つけます：

```
1 VIF_UUID=$(xe vif-list vm-name=label=pvsdevice_1 device=0 --minimal)
```

2. 仮想マシンの Citrix Provisioning プロキシを見つけてます：

```
1 PVS_PROXY_UUID=$(xe pvs-proxy-list vif-uuid=$VIF_UUID --minimal)
```

3. Citrix Provisioning プロキシを破棄します：

```
1 xe pvs-proxy-destroy uuid=$PVS_PROXY_UUID
```

ホストまたはサイトの **PVS** アクセラレータストレージを削除する

ホストまたはサイトの PVS アクセラレータストレージを削除するには、次の手順を実行します：

1. ストレージを破棄するホストを見つけてます：

```
1 HOST_UUID=$(xe host-list name=label=HOST_NAME --minimal)
```

2. オブジェクトの UUID を見つけてます：

```
1 PVS_CACHE_STORAGE_UUID=$(xe pvs-cache-storage-list host-uuid=$HOST_UUID --minimal)
```

3. オブジェクトを破棄します：

```
1 xe pvs-cache-storage-destroy uuid=$PVS_CACHE_STORAGE_UUID
```

サイトの **PVS** アクセラレータ構成を破棄する

サイトの PVS アクセラレータ構成を破棄するには、次の手順を実行します：

1. Citrix Provisioning サイトを見つけます：

```
1 PVS_SITE_UUID=$(xe pvs-site-list name=label=My PVS Site)
```

2. 次のコマンドを実行して、Citrix Provisioning サイトを破棄します：

```
1 xe pvs-site-forget uuid=$PVS_SITE_UUID
```

グラフィックスの概要

December 30, 2019

このセクションでは、Citrix Hypervisor の 3D プロフェッショナルグラフィックアプリケーションおよびワークステーションの仮想配信の概要について説明します。オフリングには、GPU パススルー (NVIDIA、AMD、Intel GPU 用)、および NVIDIA GRID™ vGPU™、AMD MxGPU™、Intel GVT-g™ とのハードウェアベースの GPU (グラフィック処理装置) 共有などがあります。

グラフィック仮想化は、Citrix Hypervisor Premium Edition のユーザー、または Citrix Virtual Apps and Desktops 利用特典により Citrix Hypervisor にアクセスできるユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[ここから](#)シトリックスの Web サイトを参照してください。詳しくは、「[ライセンス](#)」を参照してください。

GPU パススルー

仮想化されたシステムでは、ほとんどの物理システムコンポーネントは共有されます。これらのコンポーネントは、ハイパーバイザーによって複数のクライアントに対する複数の仮想インスタンスとして表されます。パススルー GPU は抽象化されず、1つの物理デバイスのままとなります。ホストされた各仮想マシン (VM) に専用の GPU が割り当てられ、それによりソフトウェア抽象化とそれに伴うパフォーマンス低下がなくなります。

Citrix Hypervisor では、物理 GPU (Citrix Hypervisor サーバー内) を、同一ホスト上で実行する Windows または HVM Linux 仮想マシンに割り当てることができます。この機能は「GPU パススルー」と呼ばれ、CAD デザイナーなど、グラフィックパワーユーザー向けに用意されています。

共有 GPU

共有 GPU を使用すると、1つの物理 GPU を複数の仮想マシンで同時に使用できます。物理 GPU の一部が使用されるので、エミュレートされたグラフィックよりもパフォーマンスが高く、仮想マシンごとに1つのカードが必要にな

ることはありません。この機能により、リソースを最適化でき、仮想マシンのパフォーマンスが向上します。各仮想マシンのグラフィックコマンドは、ハイパーバイザーによる変換なしで、GPU に直接渡されます。

複数 vGPU

複数 vGPU により、単一の仮想マシンで複数の仮想 GPU を同時に使用できます。特定の vGPU プロファイルのみを使用でき、単一の仮想マシンに接続されているすべての vGPU が同じタイプである必要があります。これらの追加の vGPU を使用して、計算処理を実行できます。1 つの仮想マシンでサポートされる vGPU の数について詳しくは、「[構成の制限](#)」を参照してください。

この機能は、NVIDIA GPU でのみ使用可能です。複数 vGPU をサポートする物理 GPU について詳しくは、NVIDIA のドキュメントを参照してください。

ベンダーのサポート

次の表は、ゲスト用にサポートされている GPU、共有 GPU、複数 vGPU の一覧です：

	Windows 仮想マシンの GPU	HVM Linux 仮想マシンの GPU	Windows 仮想マシンの共有 GPU	Linux 仮想マシンの仮想 GPU	Windows 仮想マシンの複数 vGPU	Linux 仮想マシンの複数 vGPU
AMD	はい		はい			
Intel	はい		はい			
NVIDIA	はい	はい	はい	はい	はい（注を参照）	はい（注を参照）

注：

ゲストオペレーティングシステムのサブセットのみが複数 vGPU をサポートします。詳しくは、「[ゲストのサポートと制約](#)」を参照してください。

使用するグラフィックカードによっては、ベンダーのサブスクリプションまたはライセンスが必要な場合があります。

vGPU ライブマイグレーション

vGPU ライブマイグレーションでは、仮想 GPU を使用する仮想マシンで、ライブマイグレーション、ストレージライブマイグレーション、仮想マシンの一時停止を実行することができます。vGPU ライブマイグレーション機能を備えた仮想マシンは、ダウンタイムを避けるために移行できます。

vGPU ライブマイグレーションでは、vGPU 対応仮想マシンをホストしているプールでローリングプールアップグレードも実行できます。詳しくは、「[プールのローリングアップグレード](#)」を参照してください。

vGPU ライブマイグレーションを使用するには、仮想マシンが、この機能に対応するグラフィックカードで動作する必要があり、かつ、仮想マシンに、GPU ベンダーが提供するサポート対象ドライバーがインストールされている必要があります。

vGPU ライブマイグレーションを使用する場合は、次の制限事項が適用されます：

- vGPU を有効にした Windows 仮想マシンの XenServer 7.0 または 7.1 Cumulative Update 2 から Citrix Hypervisor 8.1 へのライブマイグレーションはサポートされていません。
- vGPU を有効にした旧バージョンの Citrix Hypervisor または XenServer から Citrix Hypervisor 8.1 への Linux 仮想マシンのライブマイグレーションはサポートされていません。
- ライブマイグレーションは GPU パススルーと互換性がありません。
- 仮想マシンには、どの vGPU ライブマイグレーション機能でもサポートされるように、適切な vGPU ドライバーがインストールされている必要があります。ゲスト内ドライバーは、vGPU を使用するすべてのゲストにインストールする必要があります。
- 移行の進行中は、仮想マシンの再起動操作とシャットダウン操作はサポートされません。これらの操作によって移行が失敗する可能性があります。
- Linux 仮想マシンは、vGPU ライブマイグレーション機能ではサポートされていません。
- vGPU を有効にした仮想マシンでは、ワークロードバランスアプライアンスを使用したライブマイグレーションはサポートされません。ワークロードバランスアプライアンスでは、vGPU が接続されている仮想マシンの容量を計画することはできません。
- vGPU ライブマイグレーションを使用して仮想マシンを移行すると、ゲストの VNC コンソールが破損する可能性があります。vGPU ライブマイグレーションの実行後に、ICA、RDP、または別のネットワークベースの方法で仮想マシンにアクセスしてください。
- VDI の移行ではライブマイグレーションが使用されるため、ホスト上に vGPU インスタンスのコピーを作成するのに十分な vGPU スペースが必要です。物理 GPU がすべて使用されている場合、VDI が移行できない可能性があります。

ベンダーのサポート

次の表は、vGPU ライブマイグレーションのサポートの一覧です：

	Windows 仮想マシンの GPRU	HVM Linux 仮想マシンの GPU	Windows 仮想マシンの共有 GPU	Linux 仮想マシンの仮想 GPU	Windows 仮想マシンの複数 GPU	Linux 仮想マシンの複数 GPU
NVIDIA			はい		はい	

この機能に対応するグラフィックカードについて詳しくは、このガイドのベンダー固有のセクションを参照してください

さい。使用するグラフィックカードによっては、ベンダーのサブスクリプションまたはライセンスが必要な場合があります。

ゲストのサポートと制約

Citrix Hypervisor 8.1 では、仮想 GPU 用に次のゲストオペレーティングシステムがサポートされています。

NVIDIA vGPU

アスタリスク (*) でマークされたオペレーティングシステムは、複数 vGPU もサポートします。

Windows ゲスト:

- Windows 7 (32 ビットまたは 64 ビット)
- Windows 8.1 (32 ビットまたは 64 ビット)
- Windows 10 (64 ビット) *
- Windows Server 2008 R2 Service Pack 1 (64 ビット)
- Windows Server 2012 (64 ビット) *
- Windows Server 2012 R2 (64 ビット) *
- Windows Server 2016 (64 ビット) *
- Windows Server 2019 (64 ビット) *

HVM Linux ゲスト:

- RHEL 7.x *
- CentOS 7.x
- Ubuntu 16.04 *
- Ubuntu 18.04 *

AMD MxGPU

Windows ゲスト:

- Windows 7 SP1 (64 ビット)
- Windows 10 (64 ビット)
- Windows Server 2016 (64 ビット)
- Windows Server 2019 (64 ビット)

Intel GVT-g

Windows ゲスト:

- Windows 7 (32 ビットまたは 64 ビット)
- Windows 8.1 (32 ビットまたは 64 ビット)
- Windows 10 (64 ビット)
- Windows Server 2008 R2 Service Pack 1 (64 ビット)
- Windows Server 2012 R2 (64 ビット)
- Windows Server 2016 (64 ビット)

制約

- 仮想 GPU を搭載した仮想マシンは、動的メモリ制御ではサポートされません。
- Citrix Hypervisor では、同一プール内の全ホストにわたり同一物理 GPU が自動的に検出され、グループ化されます。仮想マシンに GPU のグループの 1 つを割り当てると、そのグループ内の使用可能 GPU がある、プール内の任意のホスト上でその仮想マシンを起動できるようになります。
- すべてのグラフィックソリューション (Nvidia vGPU、Intel GVT-d、Intel GVT-G、AMD MxGPU、および vGPU パススルー) は、高可用性を利用する環境で使用できます。ただし、これらのグラフィックソリューションを使用する仮想マシンは、高可用性で保護できません。これらの仮想マシンは、適切な空きリソースを持つホストがある間は、ベストエフォート方式で再起動できます。

グラフィック処理のためのホストの準備

March 12, 2020

このセクションでは、サポートされているグラフィック仮想化技術を利用するために Citrix Hypervisor を準備する手順を説明します。これには、NVIDIA GRID vGPU、AMD MxGPU、Intel GVT-d、および GVT-g が含まれます。

NVIDIA GRID vGPU

NVIDIA GRID vGPU を使用すると、複数の仮想マシン (VM) で単一の物理 GPU に同時に直接アクセスできます。このとき、仮想化されていないオペレーティングシステムで動作するものと同じ NVIDIA グラフィックドライバーが使用されます。GRID 物理 GPU では、複数の仮想 GPU デバイス (vGPU) がサポートされます。このサポートを提供するには、物理 GPU が、Citrix Hypervisor コントロールドメイン (dom0) で実行される NVIDIA 社の GRID Virtual GPU マネージャーによって制御されている必要があります。vGPU は仮想マシンに直接割り当てることができます。

仮想マシンは、ハイパーバイザーがパススルーした物理 GPU と同じように、GRID 仮想 GPU を使用します。仮想マシンに NVIDIA ドライバーをインストールすると、GPU に直接アクセスして、パフォーマンス上重要な処理を高速化できるようになります。また、GRID Virtual GPU マネージャーに準仮想化インターフェイスが提供されます。

NVIDIA GRID は、Citrix Virtual Apps and Desktops の HDX 3D Pro 機能と互換性があります。詳しくは、「[HDX 3D Pro](#)」を参照してください。

ライセンスノート

NVIDIA vGPU は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[ここ](#)からシトリックスの Web サイトを参照してください。詳しくは、「[ライセンス](#)」を参照してください。

使用する NVIDIA グラフィックカードによっては、NVIDIA のサブスクリプションまたはライセンスが必要な場合があります。

NVIDIA カードのライセンスについては、[NVIDIA 社の Web サイト](#)を参照してください。

利用可能な **NVIDIA GRID vGPU** の種類

NVIDIA GRID カードには、複数のグラフィック処理装置 (GPU) が搭載されています。たとえば、Tesla M10 カードには GM107GL GPU が 4 つ、Tesla M60 カードには GM204GL GPU が 2 つ含まれています。各物理 GPU は、異なる種類の仮想 GPU (vGPU) をホストできます。vGPU の種類ごとに、特定の量のフレームバッファ、サポートされるディスプレイ数、および最大解像度が設定されており、さまざまなクラスのワークロードを対象としています。

サポートされる NVIDIA カードの最新リストについては、「[ハードウェア互換性リスト \(英語\)](#)」および[NVIDIA 製品情報](#)を参照してください。

注:

物理 GPU 上で同時にホストされる vGPU は、すべて同じ種類でなければなりません。同じカード上の物理 GPU については、このような制限は適用されません。この制限は自動的に適用されるため、容量の計画において予期せぬ問題が発生する可能性があります。

たとえば、Tesla M60 カードには 2 つの物理 GPU が搭載されており、次の 11 種類の vGPU をサポートします:

- GRID M60-1A
- GRID M60-2A
- GRID M60-4A
- GRID M60-8A
- GRID M60-0B
- GRID M60-1B
- GRID M60-0Q
- GRID M60-1Q
- GRID M60-2Q

- GRID M60-4Q
- GRID M60-8Q

M60-1A の vGPU が割り当てられた仮想マシンと、M60-2A の vGPU が割り当てられた仮想マシンを同時に起動する場合:

- 一方の物理 GPU では M60-1A のインスタンスのみがサポートされます。
- もう一方の物理 GPU では、M60-2A のインスタンスのみがサポートされます。

そのため、この単一のカードで M60-4A インスタンスは起動できません。

NVIDIA GRID のシステム要件

- NVIDIA GRID カード:
 - サポートされる NVIDIA カードの最新リストについては、「[ハードウェア互換性リスト \(英語\)](#)」および [NVIDIA 製品情報](#) を参照してください。
- 使用する NVIDIA グラフィックカードによっては、NVIDIA のサブスクリプションまたはライセンスが必要な場合があります。詳しくは、[NVIDIA 製品情報](#) を参照してください。
- Citrix Hypervisor Premium Edition (または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスできる)。
- Citrix Hypervisor のホストが可能で NVIDIA GRID カードが装着されたサーバー。
- Citrix Hypervisor 用 GRID Virtual GPU マネージャーおよび NVIDIA ドライバーで構成された、Citrix Hypervisor 用 NVIDIA GRID vGPU ソフトウェアパッケージ。
- また、NVIDIA vGPU が動作している仮想マシンで Citrix Virtual Desktops を実行するには、Citrix Virtual Desktops 7.6 以降をフルインストールする必要があります。

注:

[NVIDIA 社の Web サイト](#) から入手可能な『NVIDIA GRID Virtual GPU User Guide (Ref: DU-06920-001)』を参照してください。これらのコンポーネントにアクセスするには、NVIDIA に登録する必要があります。

vGPU ライブマイグレーション

Citrix Hypervisor では、ライブマイグレーションやストレージライブマイグレーションを使用したり、NVIDIA GRID vGPU 対応の仮想マシンを一時停止または再開したりすることができます。

vGPU ライブマイグレーション、ストレージライブマイグレーション、または一時停止機能を使用するには、次の要件を満たしている必要があります:

- NVIDIA GRID カード (Maxwell ファミリ以降)。

- ライブマイグレーションに対応した Citrix Hypervisor 用 NVIDIA GRID Virtual GPU マネージャー。詳しくは、NVIDIA のドキュメントを参照してください。
- ライブマイグレーションに対応した NVIDIA vGPU ドライバーがインストールされている Windows 仮想マシン。

vGPU ライブマイグレーションでは、プール内でのライブマイグレーション、プール間のライブマイグレーション、ストレージライブマイグレーション、および vGPU 対応仮想マシンの一時停止および再開を使用できます。

準備の概要

1. インストール Citrix Hypervisor
2. Citrix Hypervisor 用 NVIDIA GRID Virtual GPU マネージャーのインストール
3. Citrix Hypervisor サーバーの再起動

Citrix Hypervisor のインストール

Citrix Hypervisor は、[Citrix Hypervisor ダウンロード](#) ページからダウンロードできます。

以下をインストールします：

- **Citrix Hypervisor** 基本インストール ISO
- **XenCenter Windows** 管理コンソール

詳しくは、「[インストール](#)」を参照してください。

ライセンスノート

vGPU は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[ここ](#)からシトリックスの Web サイトを参照してください。詳しくは、「[ライセンス](#)」を参照してください。

使用する NVIDIA グラフィックカードによっては、NVIDIA のサブスクリプションまたはライセンスが必要な場合があります。詳しくは、「[NVIDIA 製品情報](#)」を参照してください。

NVIDIA カードのライセンスについては、[NVIDIA 社の Web サイト](#)を参照してください。

Citrix Hypervisor 用 NVIDIA GRID Virtual GPU マネージャーのインストール

[NVIDIA](#) から入手可能な NVIDIA GRID vGPU ソフトウェアをインストールします。NVIDIA GRID ソフトウェアは、以下によって構成されています：

- GRID vGPU マネージャー
(NVIDIA-vGPU-Citrix Hypervisor-7.2-367.64.x86_64.rpm など)
- Windows ディスプレイドライバー (Windows ディスプレイドライバーは、Windows のバージョンによって異なります)
(369.71_grid_win10_server2016_64bit_international.exe など)

GRID vGPU マネージャーは Citrix Hypervisor のコントロールドメイン (dom0) で動作し、サブリメンタルパックまたは RPM ファイルとして提供されます。インストールについて詳しくは、NVIDIA GRID vGPU ソフトウェアに含まれているユーザーガイドを参照してください。

注:

アップデート、RPM 名、およびバージョンは例であり、お客様の環境によって異なります。

アップデートは、次のいずれかの方法でインストールできます:

- XenCenter を使用します ([ツール] > [アップデートのインストール] > [ディスクからアップデートまたはサブリメンタルパックを選択])。
- xe CLI コマンド `xe-install-update` を使用します。

アップデートの名前は次のようになります: `NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.iso`

注:

RPM ファイルを使用して GRID vGPU マネージャーをインストールする場合は、この RPM ファイルを dom0 にコピーしてからインストールするようにしてください。

1. rpm コマンドを使用してパッケージをインストールします:

```
1 rpm -iv NVIDIA-vGPU-PRODUCT_BRAND-7.2-367.64.x86_64.rpm
```

2. Citrix Hypervisor サーバーを再起動します:

```
1 shutdown -r now
```

3. Citrix Hypervisor サーバーを再起動したら、NVIDIA カーネルドライバをチェックして、GRID パッケージが正常にインストールされているかどうか確認します:

```
1 [root@xenserver ~]# lsmod | grep nvidia
2     nvidia                8152994  0
3     i2c_core                20294  2 nvidia,i2c_i801
```

4. NVIDIA カーネルドライバがホスト内の GRID 物理 GPU と正常に通信できるかどうか確認します。プラットフォームの GPU 一覧を作成するには、次のような `nvidia-smi` コマンドを実行します:

```
1 [root@xenserver ~]# nvidia-smi
2
```

```

3 Thu Jan 26 13:48:50 2017
4 +-----+
5 NVIDIA-SMI 367.64 Driver Version: 367.64 |
6 -----+
7 GPU Name Persistence-M| Bus-Id Disp.A | Volatile Uncorr.
  ECC|
8 Fan Temp Perf Pwr:Usage/Cap| Memory-Usage | GPU-Util
  Compute M.|
9 =====+=====
10 |  0 Tesla M60      On | 0000:05:00.0  Off |  Off |
11 | N/A  33C  P8     24W / 150W |  7249MiB /  8191MiB |  0%
    Default |
12 +-----+
13 |  1 Tesla M60      On | 0000:09:00.0  Off |  Off |
14 | N/A  36C  P8     24W / 150W |  7249MiB /  8191MiB |  0%
    Default |
15 +-----+
16 |  2 Tesla M60      On | 0000:85:00.0  Off |  Off |
17 | N/A  36C  P8     23W / 150W |   19MiB /  8191MiB |  0%
    Default |
18 +-----+
19 |  3 Tesla M60      On | 0000:89:00.0  Off |  Off |
20 | N/A  37C  P8     23W / 150W |   14MiB /  8191MiB |  0%
    Default |
21 +-----+
22 +-----+
23 | Processes:           GPU Memory |
24 | GPU   PID Type  Process name  Usage  |
25 |=====+=====
26 | No running compute processes found |
27 +-----+

```

注:

768GB を超える RAM を搭載した Citrix Hypervisor サーバーで NVIDIA vGPU を使用する場合は、`iommu=dom0-passthrough` パラメーターを Xen コマンドラインに追加します:

a) コントロールドメイン (Dom0) で次のコマンドを実行します:

```
/opt/xensource/libexec/xen-cmdline --set-xen iommu=dom0-passthrough
```

b) ホストを再起動します。

AMD MxGPU

AMD MxGPU により、シングルルート I/O 仮想化を使用して、複数の仮想マシン (VM) で単一の物理 GPU の機能に直接アクセスし、仮想化されていないオペレーティングシステムで動作するものと同じ AMD グラフィックドライバーをゲスト内で使用できるようになります。

仮想マシンは、ハイパーバイザーがパススルーした物理 GPU と同じように、MxGPU の GPU を使用します。仮想マシンに AMD グラフィックドライバーをインストールすると、GPU に直接アクセスして、パフォーマンス上重要な処理を高速化できるようになります。

Citrix Hypervisor で AMD MxGPU を使用方法については、[AMD のドキュメント](#)を参照してください。

ライセンスノート

MxGPU は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor の各エディションおよびエディション間のアップグレードについては、[ここからシトリックスの Web サイト](#)を参照してください。ライセンスについて詳しくは、「[Citrix Hypervisor ライセンスに関するよくある質問](#)」を参照してください。

利用可能な AMD MxGPU vGPU の種類

AMD MxGPU カードには、複数の GPU を含めることができます。たとえば、S7150 カードには物理 GPU が 1 つ、S7150x2 カードには 2 つの GPU が含まれます。各物理 GPU は、異なる種類の仮想 GPU (vGPU) をホストできます。vGPU の種類ごとに、1 つの物理 GPU があらかじめ定義された数の vGPU に分割されます。これらの vGPU には、それぞれ、フレームバッファとグラフィック処理能力が均等に配分されます。異なる種類の vGPU は、さまざまなクラスのワークロードを対象とします。物理 GPU の分割数が少ない vGPU の種類は、負荷が高いワークロードに適しています。

注:

物理 GPU 上で同時にホストされる vGPU は、すべて同じ種類でなければなりません。同じカード上の物理 GPU については、このような制限は適用されません。この制限は自動的に適用されるため、容量の計画において予期せぬ問題が発生する可能性があります。

AMD MxGPU のシステム要件

- AMD FirePro S7100 シリーズ GPU。
- Citrix Hypervisor Premium Edition (または Citrix Virtual Desktops または Citrix Virtual Apps の権限により Citrix Hypervisor にアクセスできる)。
- Citrix Hypervisor のホストが可能で AMD MxGPU カードが装着されたサーバー。AMD による検証済みのサーバー一覧については、[AMD 社の Web サイト](#)を参照してください。
- Citrix Hypervisor 用の AMD MxGPU ホストドライバー。これらのドライバーは[AMD 社のダウンロードサイト](#)から入手可能です。
- Citrix Hypervisor 上の MxGPU に適した AMD FirePro ゲスト内ドライバー。これらのドライバーは[AMD 社のダウンロードサイト](#)から入手可能です。
- また、AMD MxGPU が動作している仮想マシンで Citrix Virtual Desktops を実行するには、Citrix Virtual Desktops 7.13 以降をフルインストールする必要があります。
- SR-IOV をサポートするように構成されたシステム BIOS と、セカンダリアダプターとして構成された MxGPU。

準備の概要

1. インストール Citrix Hypervisor
2. Citrix Hypervisor 用の AMD MxGPU ホストドライバーのインストール
3. Citrix Hypervisor サーバーの再起動

Citrix Hypervisor のインストール

Citrix Hypervisor は、[Citrix Hypervisor ダウンロードページ](#)からダウンロードできます。

以下をインストールします：

- **Citrix Hypervisor 8.1 基本インストール ISO**
- **XenCenter 8.1 Windows 管理コンソール**

インストールについて詳しくは、[Citrix Hypervisor インストールガイド](#)を参照してください。

Citrix Hypervisor 用の AMD MxGPU ホストドライバーのインストール

ホストドライバーをインストールするには、次の手順を実行します。

1. XenCenter または xe CLI を使用して、ドライバーを含むアップデートをインストールします。

- XenCenter を使用してインストールする場合は、 [ツール] > [アップデートのインストール] > [ディスクからアップデートまたはサブリメンタルパックを選択] の順に移動します。
- xe CLI を使用してインストールするには、更新をホストにコピーし、更新が存在するディレクトリで次のコマンドを実行します：

```
1 xe-install-supplemental-pack mxgpu-1.0.5.amd.iso
```

2. Citrix Hypervisor サーバーを再起動します。
3. Citrix Hypervisor サーバーを再起動したら、MxGPU パッケージが正常にインストールされているかどうかを確認します。Citrix Hypervisor サーバーコンソールで次のコマンドを実行して、gimカーネルドライバーがインストールされているかどうかを確認します：

```
1 modinfo gim
2 modprobe gim
```

4. gimカーネルドライバーによって、ゲストに提供する MxGPU 仮想機能が正常に作成されたかどうかを確認します。次のコマンドを実行します。

```
1 lspci | grep "FirePro S7150"
```

「S7150V」の識別子を持つ仮想機能が出力に表示されます。

5. XenCenter の [GPU] タブを使用して、MxGPU の仮想 GPU の種類がシステムで利用可能な種類として表示されていることを確認します。

AMD MxGPU ドライバーをインストールすると、GPU でパススルーオプションを使用できなくなります。代わりに、**MxGPU.1** オプションを使用してください。

MxGPU が有効な仮想マシンの作成

仮想マシンをインストールしてから、この仮想マシンで MxGPU を使用するように構成します。この仮想マシンのオペレーティングシステムが AMD MxGPU でサポートされていることを確認します。詳しくは、「[ゲストのサポートと制約](#)」を参照してください。

仮想マシンをインストールしたら、「[仮想 GPU が有効な仮想マシンの作成](#)」の手順に従って構成を完了します。

Intel GVT-d および **GVT-g**

Citrix Hypervisor では、追加のハードウェアを必要としないグラフィックアクセラレーションソリューションである Intel の仮想 GPU (GVT-g) がサポートされます。一部のプロセッサに埋め込まれた Intel Iris Pro 機能、および仮想マシン内にインストールされている標準の Intel GPU ドライバーが使用されます。

Intel GVT-d および GVT-g は、Citrix Virtual Apps and Desktops の HDX 3D Pro 機能と互換性があります。詳しくは、「[HDX 3D Pro](#)」を参照してください。

注:

Intel Iris Pro グラフィックスの機能はプロセッサに埋め込まれているため、CPU 負荷の高いアプリケーションでは GPU に十分なパワーが配分されず、GPU 集約型ワークロードで提供されるような優れたグラフィックアクセラレーションが提供されない場合があります。

Intel GVT-g のシステム要件と構成

Intel GVT-g を使用するには、Citrix Hypervisor サーバーに次のハードウェアが必要です:

- Iris Pro Graphics を搭載した CPU。この CPU は、Graphics でサポートされる CPU として「[ハードウェア互換性リスト \(英語\)](#)」に記載されている必要があります。
- Graphics 対応のチップセットが備わったマザーボード (Xeon E3 v4 CPU の場合は C226、Xeon E3 v5 CPU の場合は C236 など)。

注:

Intel GPU パススルー (GVT-d) と Intel 仮想 GPU (GVT-g) とを切り替えた場合、ホストを再起動してください。

Intel GVT-g を構成する場合、特定の Citrix Hypervisor サーバーでサポートされる Intel 仮想 GPU の数は、その GPU のバーサイズによって異なります。GPU のバーサイズは、BIOS では「Aperture size (アパーチャサイズ)」と表示されます。ホストあたり最大 7 つの仮想 GPU をサポートするために、アパーチャサイズを 1,024MB に設定することをお勧めします。

アパーチャサイズを 256MB に設定すると、ホストで起動できる仮想マシンは 1 つだけになり、512MB に設定しても、Citrix Hypervisor サーバーで 3 つの仮想マシンしか起動できません。1,024MB を超えるアパーチャサイズはサポートされていません。また、サイズが 1,024MB を超えても、ホストで起動できる仮想マシン数が増えることはありません。

Intel GPU パススルーの有効化

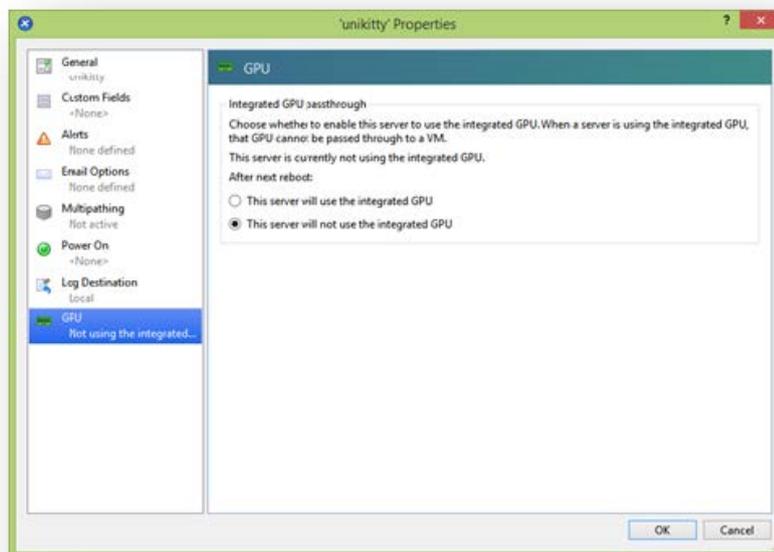
Citrix Hypervisor Intel 統合 GPU デバイスを使った Windows 7 および Windows 8.1 (32 ビットおよび 64 ビット) の仮想マシンに対する GPU パススルー機能をサポートします。サポートされるハードウェアについては、「[ハードウェア互換性リスト \(英語\)](#)」を参照してください。

Intel サーバー上の Intel GPU を使用する場合、Citrix Hypervisor サーバーのコントロールドメイン (dom0) が統合された GPU デバイスにアクセスします。このような場合、GPU ではパススルーが有効になります。Intel サーバーで Intel GPU パススルー機能を使用するには、GPU を仮想マシンにパススルーする前に dom0 および GPU 間の接続を無効にする必要があります。

この接続を無効にするには、次の手順を実行します:

1. [リソース] ペインで Citrix Hypervisor サーバーを選択します。

2. [全般] タブで [プロパティ] をクリックして、左ペインで [CPU] タブをクリックします。
3. [統合された GPU パススルー] で、 [このサーバーは統合された GPU を使用しません] をクリックします。



これにより、dom0 と Intel integrated GPU デバイス間の接続を無効にします。

4. [OK] をクリックします。
5. 変更を保存するには、Citrix Hypervisor サーバーを再起動します。

新しい仮想マシンを作成する間、GPU の種類の一覧に Intel GPU が表示されるようになりました。また、仮想マシンの [プロパティ] タブにも表示されます。

注:

dom0 と GPU との接続を無効にした後は Citrix Hypervisor サーバーの外部コンソール出力（たとえば、VGA、HDMI、DP）は利用できません。

仮想 GPU が有効な仮想マシンの作成

March 12, 2020

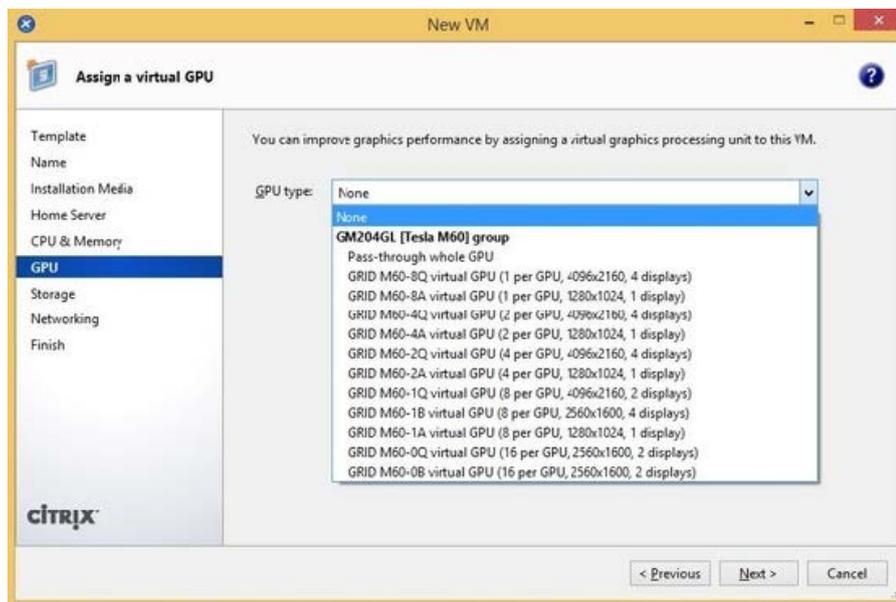
このセクションでは、仮想 GPU または GPU パススルーが有効な仮想マシンの作成手順を説明します。

注:

Intel GPU パススルー機能を使用する場合は、「Intel GPU パススルーの有効化」を参照して追加の構成を完了

してから、以下の手順を実行してください。

1. XenCenter を使用して仮想マシンを作成します。リソースペインでホストを選択し、[VM] メニューで [新規 VM] を選択します。
2. [新規 VM] の構成手順に従って、インストールメディア、ホームサーバー、**CPU**、およびメモリを選択します。
3. GPU が有効なサーバーに **GPU** 構成ページが表示されます：



4. [追加] をクリックします。[GPU の種類] 一覧で、[GPU 全体のパススルー] または仮想 GPU の種類を選択します。

使用できない仮想 GPU の種類は灰色で表示されます。

複数 vGPU を仮想マシンに割り当てる場合は、複数 vGPU をサポートする vGPU タイプを選択してください。同じタイプの vGPU をさらに追加するには、この手順を繰り返します。

5. [次へ] をクリックして、[ストレージ]、[ネットワーク] の順に構成します。
6. 構成を完了したら、[今すぐ作成] をクリックします。

Citrix VM Tools のインストール

1. Citrix VM Tools のインストール

Citrix VM Tools によって最適化されたネットワークおよびストレージドライバーが提供されないと、GRID vGPU で実行されるリモートグラフィックアプリケーションでは、パフォーマンスが最大化されません。

- a) [リソース] ペインで仮想マシンを右クリックし、ショートカットメニューの [インストール] **Citrix VM Tools** をクリックします。または、[VM] メニューの [インストール] **Citrix VM Tools** を選択します。

- b) 確認のメッセージが表示されるので、**[Citrix VM Tools のインストール]** をクリックします。これにより仮想マシンのコンソールが開き、インストールを開始できる状態になります。
- c) 仮想マシンの CD/DVD ドライブで自動実行が有効になっている場合は、しばらくすると自動的にインストールが開始されます。このプロセスによって I/O ドライバーと管理エージェントがインストールされます。要求された場合は仮想マシンを再起動し、仮想マシンが最適化された状態にします。自動実行が無効になっている場合は、Citrix VM Tools インストーラーによってインストールオプションが表示されます。**[インストール] Citrix VM Tools** をクリックして、インストールを続行します。これにより、仮想マシンの CD/DVD ドライブに Citrix VM Tools ISO (guest-tools.iso) がマウントされます。
- d) **[setup.exe の実行]** をクリックして Citrix VM Tools のインストールを開始し、要求された場合は仮想マシンを再起動して仮想マシンが最適化された状態にします。

ゲスト内ドライバーのインストール

XenCenter に仮想マシンコンソールを表示する場合、仮想マシンは通常、VGA モード (800 x 600 の解像度) でデスクトップに起動します。Windows の標準画面解像度の制御機能を使用して、解像度を他の標準解像度に上げることができます。([コントロールパネル] > [表示] > [画面の解像度])

注:

GPU パススルーまたは MxGPU を使用する場合は、RDP または VNC を使用してネットワーク経由でゲスト内ドライバーをインストールすることをお勧めします。つまり、XenCenter は使用しません。

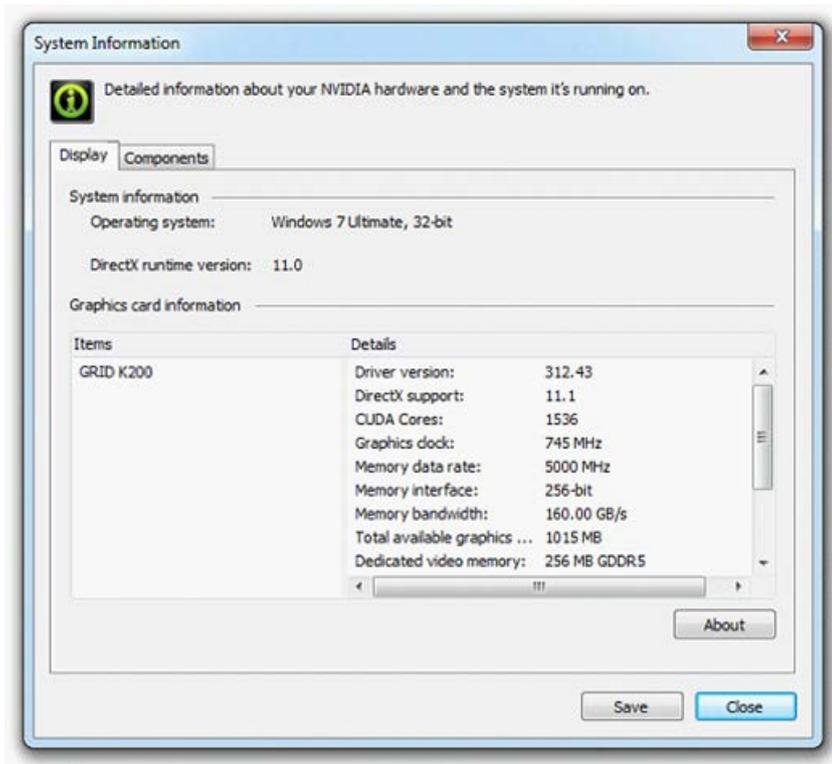
NVIDIA ドライバーのインストール

仮想 GPU の操作 (NVIDIA の物理 GPU に関して) を有効にするには、仮想マシンに NVIDIA ドライバーをインストールします。

次のセクションでは、手順の概要を示します。詳しい手順については、NVIDIA ユーザーガイドを参照してください。

1. 仮想マシンを起動します。リソースペインで仮想マシンを右クリックし、**[起動]** をクリックします。
この起動処理中に、Citrix Hypervisor は仮想マシンに仮想 GPU を動的に割り当てます。
2. Windows オペレーティングシステムのインストール画面の指示に従います。
3. オペレーティングシステムのインストールが完了したら、仮想マシンを再起動します。
4. GPU の適切なドライバーをゲスト内にインストールします。次の例は、NVIDIA GRID ドライバーをゲスト内にインストールする特定のケースを示しています。
5. Windows (32 ビットまたは 64 ビット) 用の NVIDIA ドライバーパッケージを仮想マシンにコピーし、ZIP ファイルを開いて setup.exe を実行します。
6. インストーラの手順に従ってドライバーをインストールします。

7. ドライバーのインストールが完了すると、仮想マシンを再起動するように求められる場合があります。[すぐに再起動] を選択して仮想マシンを直ちに再起動するか、インストーラパッケージを終了し、準備ができてから仮想マシンを再起動します。仮想マシンが起動すると、Windows デスクトップが起動します。
8. NVIDIA ドライバーが動作していることを確認するには、デスクトップを右クリックし、[NVIDIA コントロールパネル] を選択します。
9. NVIDIA コントロールパネルで、[システム情報] を選択します。このインターフェイスには、仮想マシンで使用される GPU の種類、その機能、および使用される NVIDIA ドライバーのバージョンが表示されます：



注：

使用する NVIDIA グラフィックカードによっては、NVIDIA のサブスクリプションまたはライセンスが必要な場合があります。詳しくは、[NVIDIA 製品情報](#)を参照してください。

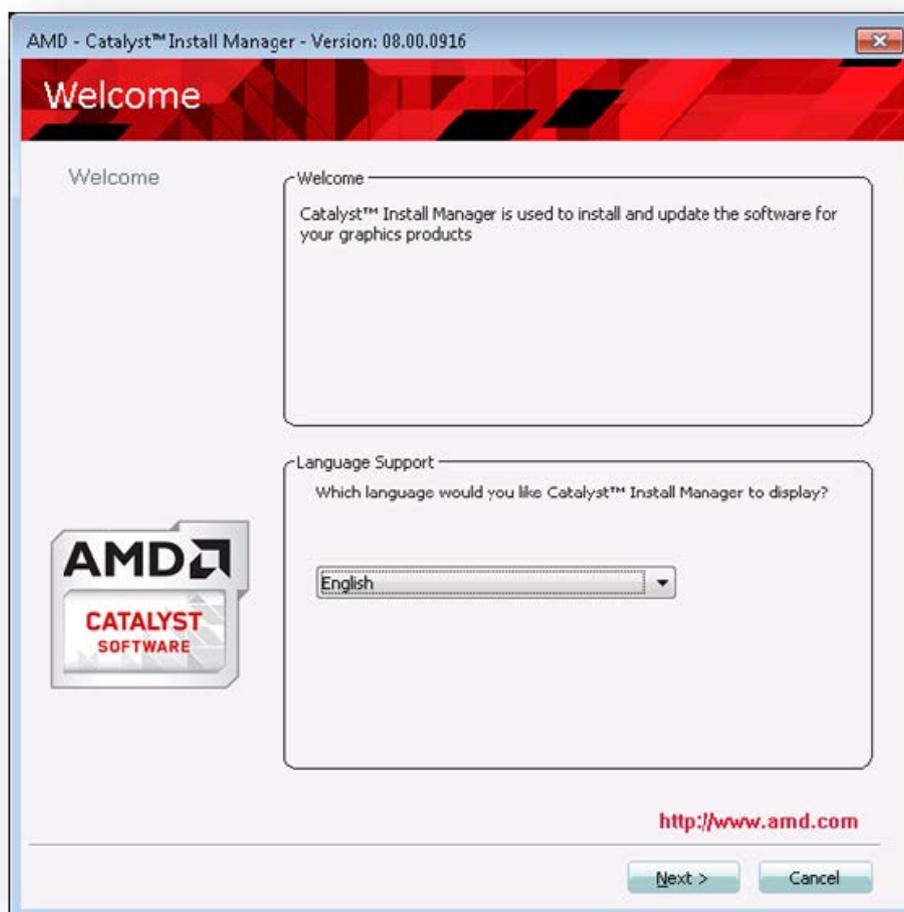
GPU でサポートされる、DirectX および OpenGL を使用したすべてのグラフィック処理アプリケーションを、仮想マシンで実行する準備が整いました。

AMD ドライバーのインストール

GPU の操作を有効にするには、仮想マシンに AMD ドライバーをインストールします。

1. 仮想マシンを起動します。リソースペインで仮想マシンを右クリックし、[起動] をクリックします。
この起動処理中に、Citrix Hypervisor は仮想マシンに GPU を動的に割り当てます。

2. Windows オペレーティングシステムのインストール画面の指示に従います。
3. オペレーティングシステムのインストールが完了したら、仮想マシンを再起動します。
4. Windows (32 ビットまたは 64 ビット) 用の AMD ドライバー (AMD Catalyst Install Manager) を仮想マシンにコピーします。
5. AMD Catalyst Install Manager を実行します。インストールフォルダーを選択して [インストール] をクリックします。

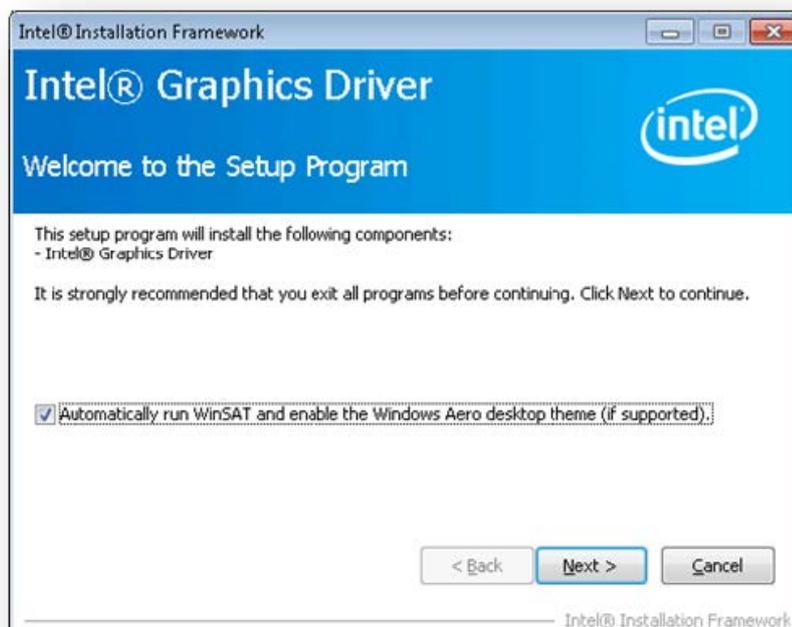


6. インストーラの手順に従ってドライバーをインストールします。
7. 仮想マシンを再起動してインストールを完了します。
8. 仮想マシンの再起動後、グラフィックが正常に機能していることを確認します。**Windows Device Manager** を開き、ディスプレイアダプターを展開して、AMD グラフィックアダプターに警告マークが付いていないかを確認します。

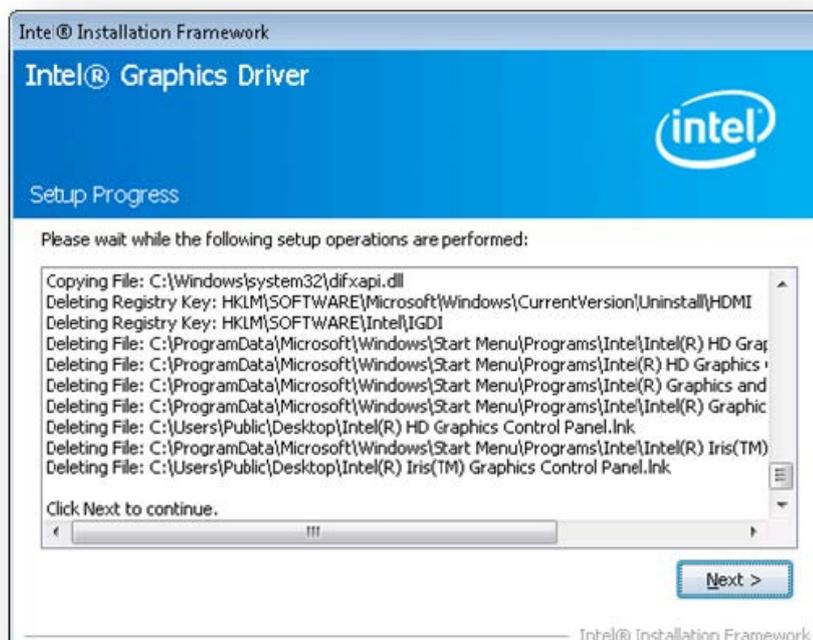
Intel ドライバーのインストール

GPU の操作を有効にするには、仮想マシンに Intel ドライバーをインストールします。

1. 仮想マシンを起動します。リソースペインで仮想マシンを右クリックし、[起動] をクリックします。
この起動処理中に、Citrix Hypervisor は仮想マシンに GPU を動的に割り当てます。
2. Windows オペレーティングシステムのインストール画面の指示に従います。
3. オペレーティングシステムのインストールが完了したら、仮想マシンを再起動します。
4. Windows (32 ビットまたは 64 ビット) 用の Intel ドライバー (Intel グラフィックドライバー) を仮想マシンにコピーします。
5. **Intel** グラフィックドライバーのセットアッププログラムの実行
6. [自動的に **WinSAT** を実行] チェックボックスをオンにし、[次へ] をクリックします。



7. 使用許諾契約書に同意する場合は [はい] をクリックし、Readme ファイル情報画面で [次へ] をクリックします。
8. セットアップが完了するまで待ちます。プロンプトが表示されたら、[次へ] をクリックします。



9. インストールを完了するには、仮想マシンを再起動するように求められます。[はい、コンピュータを今すぐ再起動します] を選択し、[完了] をクリックします。
10. 仮想マシンの再起動後、グラフィックが正常に機能していることを確認します。Windows Device Manager を開き、ディスプレイアダプターを展開して、Intel グラフィックアダプターに警告マークが付いていないかを確認します。

注:

[Intel 社の Web サイト](#)で最新のドライバーを入手できます。

メモリ使用率

December 30, 2019

Citrix Hypervisor サーバーでのメモリ占有量を計算する場合、考慮すべき2つのコンポーネントがあります。1つは Xen ハイパーバイザー自体が消費するメモリ、2つ目は、ホストのコントロールドメインが消費するメモリです。コントロールドメインは「Domain0」または「dom0」とも呼ばれ、Citrix Hypervisor の管理ツールスタックを実行するセキュアな特権 Linux 仮想マシンです。コントロールドメインは、Citrix Hypervisor の管理機能を提供するほか、ユーザーが作成した仮想マシンに物理デバイスへのアクセスを提供するドライバスタックも実行します。

コントロールドメインのメモリ

コントロールドメインに割り当てられるメモリの量は、物理ホストの物理メモリの量に基づいて自動的に調整されます。デフォルトでは、Citrix Hypervisor は **1GiB** に物理メモリの合計の **5%** を足した量のメモリをコントロールドメインに割り当てます (最大 8GiB)。

注:

XenCenter の Citrix Hypervisor セクションのレポートには、コントロールドメイン (dom0)、Xen ハイパーバイザー、クラッシュカーネルにより使用されているメモリ量が含まれます。XenCenter には、上記のメモリ量よりも大きな値が表示される場合があります。多くのメモリを搭載したホスト上では、ハイパーバイザーにより使用されるメモリ量も大きくなります。

コントロールドメインに割り当てられるメモリ量の変更

dom0 に割り当てるメモリの量は、XenCenter またはコマンドラインを使用して変更できます。コントロールドメインに割り当てるメモリ量をデフォルト設定よりも増やすと、仮想マシンで使用できるメモリが少なくなります。

XenCenter を使用した **dom0** メモリの変更

XenCenter を使用して dom0 用メモリを変更する方法については、XenCenter ドキュメントの「[コントロールドメインのメモリの変更](#)」を参照してください。

注:

XenCenter を使用して Citrix Hypervisor のインストール中に最初に設定された値よりコントロールドメインに割り当てるメモリを少なくすることはできません。設定を変更するにはコマンドラインを使用する必要があります。

コマンドラインを使用した **dom0** メモリの変更

注:

メモリの搭載量が少ないホスト (16GiB 未満) では、コントロールドメインに割り当てるメモリをインストール時のデフォルト値よりも少なくすることができます。設定を変更するにはコマンドラインを使用します。ただし、**dom0** メモリは **1GiB** 以下にしないことをお勧めします。また変更操作はサポートチームのガイダンスを受けながら行ってください。

1. Citrix Hypervisor サーバーのローカルシェルを開き、root ユーザーでログオンします。
2. 次のように入力します:

```
1 /opt/xensource/libexec/xen-cmdline --set-xen dom0_mem=<nn>M,max:<nn>M
```

<nn>に、コントロールドメインに割り当てるメモリ量を MiB 単位で指定します。

3. XenCenter を使用するか、Citrix Hypervisor コンソールで `reboot` コマンドを使用して、`{{ page.brand_server }}` サーバーを再起動します。

ホストが再起動したら、Citrix Hypervisor コンソールで `free` コマンドを実行してメモリ設定を確認します。

仮想マシンで使用できるメモリの確認

仮想マシンに割り当てることができるホストメモリの量を調べるには、`memory-free` を実行してホストの空きメモリの値を取得します。次に、コマンド `vm-compute-maximum-memory` を使用して、仮想マシンに割り当てることができる実際の空きメモリ量を取得します。次に例を示します：

```
1 xe host-list uuid=host_uuid params=memory-free
2 xe vm-compute-maximum-memory vm=vm_name total=host_memory_free_value
```

環境の監視と管理

March 12, 2020

Citrix Hypervisor では、パフォーマンスメトリックの詳細な監視ができます。監視対象のメトリックは、CPU、メモリ、ディスク、ネットワーク、C-状態/P-状態情報、ストレージなどです。これらの測定値は、必要に応じてホスト単位または仮想マシン単位で監視できます。これらの測定値は、直接アクセスして使用したり、XenCenter やそのほかのサードパーティ製アプリケーションで視覚的に表示したりできます。

また、Citrix Hypervisor ではシステムやパフォーマンスに関するアラートを生成できます。アラートは、特定のシステムイベントが発生した場合に通知を生成します。これらの通知は、ホスト、仮想マシン、またはストレージリポジトリで次の値が特定のしきい値を超過した場合に生成されます：CPU 使用率、ネットワーク使用量、メモリ使用量、コントロールドメインのメモリ使用率、ストレージスループット、または仮想マシンのディスク使用量。アラートは、xe CLI、または XenCenter を使用して構成できます。ホストまたは仮想マシンのパフォーマンスメトリックに基づいて通知を作成するには、「パフォーマンスアラート」を参照してください。

Citrix Hypervisor のパフォーマンスの監視

Citrix Hypervisor サーバーや仮想マシンのパフォーマンスは、ラウンドロビンデータベース (RRD) に格納される測定値を使って監視できます。これらの測定値は、HTTP または RRD2CSV ツールを使って照会できます。また、XenCenter では、これらのデータに基づいてシステムパフォーマンスグラフが作成されます。詳しくは、「メトリックの分析と視覚化」を参照してください。

以下の表は、ホストおよび仮想マシンで使用可能なパフォーマンス測定値の一覧です。

注:

- 一定期間における遅延は、その期間の遅延時間を平均化したものです。
- 一部の測定値は、ストレージリポジトリや CPU により使用できない場合があります。
- GFS2 ストレージリポジトリおよびこれらのストレージリポジトリ上のディスクでは、パフォーマンス測定値は利用できません。

ホストのパフォーマンス測定値

メトリック名	説明	条件	XenCenter 名前
avgqu_sz_<sr-uuid-short>	I/O キューのサイズの平均 (要求)。	ホストの SR<sr-uuid-short>で1つ以上の VBD がプラグされていること。	sr-uuid-short キューのサイズ
cpu<cpu>-C<cstate>	CPUcpuが C-状態cstateである時間 (ミリ秒)。	CPU に C-状態があること。	CPUcpuC-状態cstate
cpu<cpu>-P<pstate>	CPUcpuが P-状態pstateである時間 (ミリ秒)。	CPU に P-状態があること。	CPUcpuP-状態pstate
cpu<cpu>	物理 CPUcpuの使用率。デフォルトで有効。	CPUcpuがあること。	CPU cpu
cpu_avg	すべての物理 CPU の平均使用率。デフォルトで有効。	なし	平均 CPU
inflight_<sr-uuid-short>	インフライト状態の I/O 要求数。デフォルトで有効。	ホストの SRsrで1つ以上の VBD がプラグされていること。	srインフライト要求
io_throughput_read_<sr-uuidshort>	SR からの読み取りデータ (MiB/秒)。	ホストの SRsrで1つ以上の VBD がプラグされていること。	sr読み取りスループット
io_throughput_write_<sr-uuidshort>	SR への書き込みデータ (MiB/秒)。	ホストの SRsrで1つ以上の VBD がプラグされていること。	sr書き込みスループット
io_throughput_total_<sr-uuidshort>	すべての SR I/O (MiB/秒)。	ホストの SRsrで1つ以上の VBD がプラグされていること。	sr合計スループット

メトリック名	説明	条件	XenCenter 名前
<code>iops_read_<sr-uuid-short></code>	1 秒あたりの読み取り要求。	ホストの SRsr で 1 つ以上の VBD がプラグされていること。	sr 読み取り IOPS
<code>iops_write_<sr-uuid-short></code>	1 秒あたりの書き込み要求。	ホストの SRsr で 1 つ以上の VBD がプラグされていること。	sr 書き込み IOPS
<code>iops_total_<sr-uuid-short></code>	1 秒あたりの I/O 要求。	ホストの SRsr で 1 つ以上の VBD がプラグされていること。	sr 合計 IOPS
<code>iowait_<sr-uuid-short></code>	I/O 待機時間のパーセンテージ。	ホストの SRsr で 1 つ以上の VBD がプラグされていること。	srIO 待機
<code>latency_<sr-uuid-short></code>	平均 I/O 遅延 (ミリ秒)。	ホストの SRsr で 1 つ以上の VBD がプラグされていること。	sr 遅延
<code>loadavg</code>	ドメイン 0 の負荷平均。デフォルトで有効。	なし	コントロールドメインロード
<code>memory_free_kib</code>	合計空きメモリ量 (KiB)。デフォルトで有効。	なし	空きメモリ
<code>memory_reclaimed</code>	圧縮により解放されたホストメモリ (B)。	なし	解放されたメモリ
<code>memory_reclaimed_max</code>	圧縮 (B) により解放されるホストメモリ。	なし	解放されるメモリ (概算値)
<code>memory_total_kib</code>	ホストの合計メモリ量 (KiB)。デフォルトで有効。	なし	メモリ合計
<code>network/latency</code>	ローカルホストからすべてのオンラインホストに送信された最後の 2 回のハートビートの間隔 (秒)。デフォルトでは、無効になっています。	HA が有効であること。	ネットワーク遅延

メトリック名	説明	条件	XenCenter 名前
statefile/<t>/latency	ローカルホストからステートファイルへの前回アクセス時の応答時間(秒)。デフォルトでは、無効になっています。	HA が有効であること。	高可用性ステートファイル遅延
pif_<pif>_rx	物理インターフェイス pif での 1 秒あたりの受信バイト。デフォルトで有効。	PIF が存在すること	XenCenter-pifname 受信 (注参照)
pif_<pif>_tx	物理インターフェイス pif での 1 秒あたりの送信バイト。デフォルトで有効。	PIF が存在すること	XenCenter-pifname 送信 (注参照)
pif_<pif>_rx_errors	物理インターフェイス pif での 1 秒あたりの受信エラー数。デフォルトでは、無効になっています。	PIF が存在すること	XenCenter-pifname 受信エラー (注参照)
pif_<pif>_tx_errors	物理インターフェイス pif での 1 秒あたりの転送エラー数。デフォルトで無効。	PIF が存在すること	XenCenter-pifname 送信エラー (注参照)
pif_aggr_rx	すべての物理インターフェイスでの 1 秒あたりの受信バイト。デフォルトで有効。	なし	NIC 受信合計
pif_aggr_tx	すべての物理インターフェイスでの 1 秒あたりの送信バイト。デフォルトで有効。	なし	NIC 送信合計
pvsaccelerator_evicted	キャッシュから削除された 1 秒あたりのバイト数	PVS アクセラレータが有効	PVS アクセラレータの削除の割合
pvsaccelerator_read	キャッシュから供給された 1 秒あたりの読み取り数	PVS アクセラレータが有効	PVS アクセラレータでヒットした割合

メトリック名	説明	条件	XenCenter 名前
<code>pvsaccelerator_read_misses</code>	キャッシュから供給されない1秒あたりの読み取り数	PVS アクセラレータが有効	PVS アクセラレータでヒットしなかった割合
<code>pvsaccelerator_traffic</code>	キャッシュされた PVS クライアントから送信された1秒あたりのバイト数	PVS アクセラレータが有効	PVS アクセラレータはクライアントからのネットワークトラフィックを確認しました
<code>pvsaccelerator_traffic_server</code>	キャッシュされた PVS サーバーから送信された1秒あたりのバイト数	PVS アクセラレータが有効	PVS アクセラレータはサーバーからのネットワークトラフィックを確認しました
<code>pvsaccelerator_read_hits</code>	キャッシュによって観測された1秒あたりの読み取り数	PVS アクセラレータが有効	PVS アクセラレータで確認した読み取りの割合
<code>pvsaccelerator_traffic_server_proxy</code>	PVS サーバーの代わりに PVS Accelerator によって送信された1秒あたりのバイト数	PVS アクセラレータが有効	PVS アクセラレータはネットワークトラフィックを保存しました
<code>pvsaccelerator_space</code>	キャッシュストレージの合計サイズと比較した、このホスト上で PVS Accelerator によって使用された領域の割合	PVS アクセラレータが有効	PVS アクセラレータの容量使用率
<code>sr_<sr>_cache_size</code>	IntelliCache ストレージリポジトリのサイズ (B)。デフォルトで有効。	IntelliCache が有効であること。	IntelliCache キャッシュサイズ
<code>sr_<sr>_cache_hits</code>	1秒あたりの成功キャッシュ。デフォルトで有効。	IntelliCache が有効であること。	IntelliCache キャッシュ成功
<code>sr_<sr>_cache_misses</code>	1秒あたりの失敗キャッシュ。デフォルトで有効。	IntelliCache が有効であること。	IntelliCache キャッシュ失敗
<code>xapi_allocation_kib</code>	XAPI デモンによる割り当てメモリ量 (KiB)。デフォルトで有効。	なし	エージェントメモリ割り当て

メトリック名	説明	条件	XenCenter 名前
<code>xapi_free_memory_kib</code>	XAPI デーモンで使用可能な空きメモリ量 (KiB)。デフォルトで有効。	なし	空きエージェントメモリ
<code>xapi_healthcheck/latency_health</code>	ローカルホストでの前回 XAPI モニタリングコール時の応答時間 (秒)。デフォルトで無効。	高可用性が有効	Citrix Hypervisor ヘルスチェック遅延
<code>xapi_live_memory_kib</code>	XAPI デーモンで使用中のライブメモリ量 (KiB)。デフォルトで有効。	なし	エージェントメモリライブ
<code>xapi_memory_usage_kib</code>	XAPI デーモンで使用中の合計メモリ量 (KiB)。デフォルトで有効。	なし	エージェントメモリ使用

仮想マシンのパフォーマンス測定値

メトリック名	説明	条件	XenCenter 名前
<code>cpu<cpu></code>	仮想 CPU <code>cpu</code> の使用率。デフォルトで有効。	仮想 CPU <code>cpu</code> があること。	CPU
<code>memory</code>	仮想マシンに割り当てられているメモリ量 (B)。デフォルトで有効。	なし	メモリ合計
<code>memory_target</code>	仮想マシンバルーンドライバの目標メモリ量 (B)。デフォルトで有効。	なし	メモリ目標値
<code>memory_internal_free</code>	ゲストエージェントにより報告された使用メモリ量 (KiB)。デフォルトで有効。	なし	空きメモリ
<code>runstate_fullrun</code>	すべての仮想 CPU が実行されていた時間。	なし	vCPU 完全実行
<code>runstate_fullcontention</code>	すべての仮想 CPU が実行可能であった時間 (CPU の待機中など)。	なし	vCPU 完全競合

メトリック名	説明	条件	XenCenter 名前
<code>runstate_concurrer</code>	一部の仮想 CPU が実行されていて一部が実行可能であった時間。	なし	vCPU 並列性のハザード
<code>runstate_blocked</code>	すべての仮想 CPU がブロックされていたりオフラインであったりした時間。	なし	vCPU アイドル
<code>runstate_partial_r</code>	一部の仮想 CPU が実行されていて一部がブロックされていた時間。	なし	vCPU 部分実行
<code>runstate_partial_co</code>	一部の仮想 CPU が実行可能で一部がブロックされていた時間。	なし	vCPU 部分競合
<code>vbd_<vbd>_write</code>	デバイス <code>vbd</code> への 1 秒あたりの書き込みバイト。デフォルトで有効。	VBD <code>vbd</code> があること。	ディスク <code>vbd</code> 書き込み
<code>vbd_<vbd>_read</code>	デバイス <code>vbd</code> からの 1 秒あたりの読み取りバイト。デフォルトで有効。	VBD <code>vbd</code> があること。	ディスク <code>vbd</code> 読み取り
<code>vbd_<vbd>_write_latency</code>	デバイス <code>vbd</code> への書き込み (ミリ秒)。	VBD <code>vbd</code> があること。	ディスク <code>vbd</code> 書き込み遅延
<code>vbd_<vbd>_read_latency</code>	デバイス <code>vbd</code> からの読み取り (ミリ秒)。	VBD <code>vbd</code> があること。	ディスク <code>vbd</code> 読み取り遅延
<code>vbd <vbd>_iops_read</code>	1 秒あたりの読み取り要求。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> 読み取り IOPS
<code>vbd <vbd>_iops_write</code>	1 秒あたりの書き込み要求。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> 書き込み IOPS
<code>vbd <vbd>_iops_total</code>	1 秒あたりの I/O 要求。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> 合計 IOPS
<code>vbd <vbd>_iowait</code>	I/O 待機時間のパーセンテージ。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> IO 待機

メトリック名	説明	条件	XenCenter 名前
<code>vbd <vbd>_inflight</code>	インフライト状態の I/O 要求数。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> インフライト要求
<code>vbd <vbd>_avgqu_sz</code>	I/O キューのサイズの平均。	ホストの非 ISO VDI 用に 1 つ以上の VBD がプラグされていること。	ディスク <code>vbd</code> キューのサイズ
<code>vif_<vif>_rx</code>	仮想インターフェイス <code>vif</code> での 1 秒あたりの受信バイト。デフォルトで有効。	VIF <code>vif</code> があること。	<code>vif</code> 受信
<code>vif_<vif>_tx</code>	仮想インターフェイス <code>vif</code> での 1 秒あたりの転送バイト。デフォルトで有効。	VIF <code>vif</code> があること。	<code>vif</code> 送信
<code>vif_<vif>_rx_errors</code>	仮想インターフェイス <code>vif</code> での 1 秒あたりの受信エラー数。デフォルトで有効。	VIF <code>vif</code> があること。	<code>vif</code> 受信エラー
<code>vif_<vif>_tx_errors</code>	仮想インターフェイス <code>vif</code> での 1 秒あたりの転送エラー数。デフォルトで有効。	VIF <code>vif</code> があること。	<code>vif</code> 送信エラー

注:

<XenCenter-pif-name>の値は、以下のいずれかを示します:

```

|||
|-----|-----|
| NIC <pif> | <pif> が pif_eth# を含んでいる場合 (## は 0 ~ 9) |
| <pif> | <pif> が pif_eth### または pif_xenbr## または pif_bond## を含んでいる場合 |
| <内部> ネットワーク <pif> | <pif> が pif_xapi## を含んでいる場合 (<内部> の部分は変数ではありません) |
| TAP <tap> | <pif> が pif_tap## を含んでいる場合 |
| xapi ループバック | <pif> が pif_lo を含んでいる場合 |

```

メトリックの分析と視覚化

XenCenter の [パフォーマンス] タブでは、リソースプールの全体的なパフォーマンス測定値をリアルタイムで監視でき、仮想マシンおよび物理マシンのパフォーマンスの傾向を視覚的に確認することができます。デフォルトでは、CPU、メモリ、ネットワーク、ディスク入出力に関するデータが [パフォーマンス] タブに表示されます。パフォーマンス測定値を追加したり、既存のグラフの外観を変更したり、追加のグラフを作成したりすることができます。詳しくは、後のセクションで「パフォーマンス測定値の設定」を参照してください。

- 過去 12 か月までさかのぼってパフォーマンスデータを表示でき、測定値が急増している部分などをクローズアップして表示することもできます。
- XenCenter では、サーバー、仮想マシンまたはストレージリポジトリの CPU、メモリ、ネットワーク入出力、ストレージ入出力、またはディスク入出力の使用状況が特定のしきい値を超過した場合に、アラートが生成されるように設定できます。詳しくは、後述の「アラート」を参照してください。

注:

その仮想マシンに Citrix VM Tools (準仮想化ドライバ) をインストールして、仮想マシンのすべてのパフォーマンスデータを表示します。

パフォーマンスグラフを設定する

新しいグラフを追加するには:

1. [パフォーマンス] タブで、[操作]、[新規グラフ] の順にクリックします。[新規グラフ] ダイアログボックスが開きます。
2. [名前] ボックスにグラフの名前を入力します。
3. [データソース] の一覧で、グラフに追加するデータソースのチェックボックスをオンにします。
4. [保存] をクリックします。

既存のグラフを編集するには:

1. [パフォーマンス] タブで、編集するグラフをクリックします。
2. グラフを右クリックして [操作] を選択するか、[操作] ボタンをクリックします。[グラフの編集] を選択します。
3. グラフの [詳細] ダイアログボックスで、必要な変更を行って **[OK]** をクリックします。

グラフの種類の設定

パフォーマンスグラフ上のデータは線または面で表示できます。グラフの種類を変更するには、次の手順に従います。

1. [ツール] メニューの [オプション] を選択し、[グラフ] ページを開きます。
2. パフォーマンスデータを折れ線グラフで表示するには、[折れ線グラフ] オプションをクリックします。

3. パフォーマンスデータを面グラフで表示するには、[面グラフ] オプションをクリックします。
4. **[OK]** をクリックして変更を保存します。

XenCenter のパフォーマンスグラフの設定および表示については、XenCenter ドキュメントで「[システムパフォーマンスの監視](#)」のセクションを参照してください。

パフォーマンス測定値の設定

注:

C-状態および P-状態は、一部のプロセッサで提供される電源管理機能です。これらの状態の範囲は、ホストの物理的な能力と電源管理設定により異なります。

パフォーマンス測定値に関するコマンドでは、ホストおよび仮想マシンの両方で以下の情報が返されます。

- データソースの説明
- 測定値の単位
- 使用可能な値の範囲

次に例を示します:

```
1 name_label: cpu0-C1
2 name_description: Proportion of time CPU 0 spent in C-state 1
3 enabled: true
4 standard: true
5 min: 0.000
6 max: 1.000
7 units: Percent
```

特定の測定値を有効にする

デフォルトでは、多くの測定値が有効になっており、データが収集されます。無効な測定値を有効にするには、次のコマンドを実行します:

```
1 xe host-data-source-record data-source=metric name host=hostname
```

特定の測定値を無効にする

定期的なデータの収集が不要な測定値がある場合は、その測定値を無効にできます。測定値を無効にするには、次のコマンドを実行します。

```
1 xe host-data-source-forget data-source=metric name host=hostname
```

有効なホスト測定値を表示する

ホストに対して有効になっている測定値を表示するには、次のコマンドを実行します。

```
1 xe host-data-source-list host=hostname
```

有効な仮想マシン測定値を表示する

仮想マシンに対して有効になっている測定値を表示するには、次のコマンドを実行します。

```
1 xe vm-data-source-list vm=vm_name
```

RRD の使用

Citrix Hypervisor では、パフォーマンス測定値がラウンドロビンデータベース (RRD) に格納されます。これらの RRD は、固定サイズのデータベースに作成される複数のラウンドロビンアーカイブ (RRA) で構成されます。

各アーカイブでは、各測定値が以下の間隔でサンプリングされます。

- 10 分間は 5 秒間隔
- 過去 2 時間は 1 分間隔
- 過去 1 週間は 1 時間間隔
- 過去 1 年間は 1 日間隔

5 秒間隔で実行されるサンプリングでは実際の測定値が記録され、それ以降のラウンドロビンアーカイブでは集約関数が使用されます。以下は、Citrix Hypervisor でサポートされている集約関数です。

- AVERAGE (平均)
- MIN (最小)
- MAX (最大)

RRD は、個々の仮想マシン、dom0、および Citrix Hypervisor サーバー用に作成されます。仮想マシンの RRD は、実行ホスト (実行中の仮想マシンの場合)、またはプールマスタ (実行されていない仮想マシンの場合) 上に格納されます。このため、パフォーマンスデータを取得するには、仮想マシンがどこにあるかを知っている必要があります。

Citrix Hypervisor RRD の使用方法について詳しくは、『[Citrix Hypervisor ソフトウェア開発キットガイド](#)』を参照してください。

HTTP を使用した RRD の解析

RRD は、`/host_rrd`または`/vm_rrd`で登録された HTTP ハンドラーを使用して指定された Citrix Hypervisor サーバーから HTTP 経由でダウンロードできます。これらの両アドレスでは、HTTP 認証を使用するか、有効な管理 API セッション参照を照会引数として指定して認証を受ける必要があります。次に例を示します：

ホスト **RRD** のダウンロード。

```
1 wget http://server/host_rrd?session_id=OpaqueRef:SESSION HANDLE>
```

仮想マシン **RRD** のダウンロード。

```
1 wget http://server/vm_rrd?session_id=OpaqueRef:SESSION HANDLE>&uuid=VM
  UUID>
```

これらのコマンドでは、`rrdtool`にインポートしてそのまま解析可能な XML ファイルがダウンロードされます。

rrd2csv を使用した **RRD** の解析

パフォーマンス測定値は、XenCenter で表示するほかにも、`rrd2csv` ツールを使用して RRD をコンマ区切り (CSV) 形式のファイルとして書き出すことができます。このツールには、`man` ページおよびヘルプページが用意されています。`rrd2csv` ツールの `man` ページまたはヘルプページを表示するには、以下のコマンドを実行します：

```
1 man rrd2csv
```

または

```
1 rrd2csv --help
```

注：

複数のオプションを使用する場合は、個別に指定する必要があります。たとえば：仮想マシンまたはホストの UUID と名前ラベルを取得するには、次のように `rrd2csv` をコールします：

```
rrd2csv -u -n
```

取得した UUID は一意であるためプライマリーキーとして適していますが、名前ラベルは一意であるとは限りません。

このツールについて詳しくは、`man` ページ (`rrd2csv --help`) のヘルプテキストを参照してください。

アラート

Citrix Hypervisor では、ホストや仮想マシンのパフォーマンス測定値に応じてアラートが送信されるように設定できます。さらに、Citrix Hypervisor には、ホストが特定の状態になると生成される事前設定のアラートが用意されています。これらのアラートは、XenCenter または `xe CLI` で表示できます。

XenCenter を使用したアラートの表示

XenCenter には、さまざまなアラートが表示されます。アラートを表示するには、[通知]、[アラート] の順にクリックします。[アラート] ページには、パフォーマンスアラート、システムアラート、ソフトウェアアップデートア

ラートなどさまざまな種類のアラートが表示されます。

パフォーマンスアラート

パフォーマンスアラートは、ホスト、仮想マシン、またはストレージリポジトリで、次のうちいずれかの値が特定のしきい値を超過した場合に生成されるように設定できます：CPU 使用率、ネットワーク使用量、メモリ使用量、コントロールドメインのメモリ使用率、ストレージスループット、または仮想マシンのディスク使用量。

アラートのデフォルトの生成間隔は 60 分ですが、この間隔は必要に応じて変更できます。アラートは、XenCenter の [通知] 領域の [アラート] ページに表示されます。また、特定のパフォーマンスアラートをほかの重大なシステムアラートと同様にメールで送信するように XenCenter を設定することもできます。

XenCenter の [アラート] ページには、xe CLI で設定したカスタムのアラートも表示されます。

各アラートには、重要度が割り当てられます。これらのレベルを変更したり、アラート生成時にメールが送信されるように設定したりできます。アラートのデフォルトの重要度は、3 に設定されています。

優先度	名前	説明	デフォルトでのメール送信
1	重大	直ちに対処しないとデータが恒久的に失われたり破損したりする可能性があります。	はい
2	重要	直ちに対処しないと一部のサービスが停止する可能性があります。	はい
3	警告	直ちに対処しないとサービスが影響を受ける可能性があります。	はい
4	軽度	何らかの問題が改善されました。	いいえ
5	情報	一般的な情報（仮想マシンの起動、停止、再開など）です。	いいえ
?	不明	不明なエラー	いいえ

パフォーマンスアラートを設定する

1. リソースペインでホスト、仮想マシン、またはストレージリポジトリを選択して、[全般] タブの [プロパティ] をクリックします。

2. [アラート] をクリックします。次のアラートを構成できます。

- サーバーまたは仮想マシンの **CPU** 使用率パフォーマンスアラートが生成されるようにするには、[CPU 使用率アラートを有効にする] チェックボックスをオンにして、アラートを生成する CPU の使用率と許容時間のしきい値を設定します。
- サーバーまたは仮想マシンのネットワーク使用量パフォーマンスアラートが生成されるようにするには、[ネットワーク使用量アラートを有効にする] チェックボックスをオンにして、アラートを生成するネットワーク入出力の使用量と許容時間のしきい値を設定します。
- サーバーのメモリ使用量パフォーマンスアラートが生成されるようにするには、[メモリ使用量アラートを有効にする] チェックボックスをオンにして、アラートを生成する空きメモリと許容時間のしきい値を設定します。
- コントロールドメインのメモリ使用率パフォーマンスアラートが生成されるようにするには、[コントロールドメインのメモリ使用率アラートを有効にする] チェックボックスをオンにして、アラートを生成するコントロールドメインのメモリ使用量と許容時間のしきい値を設定します。
- 仮想マシンのディスク使用量パフォーマンスアラートが生成されるようにするには、[ディスク使用量アラートを有効にする] チェックボックスをオンにして、アラートを生成するディスク入出力の使用量と許容時間のしきい値を設定します。
- ストレージスループットパフォーマンスアラートが生成されるようにするには、[ストレージスループットアラートを有効にする] チェックボックスをオンにして、アラートを生成するストレージスループットと許容時間のしきい値を設定します。

注:

物理ブロックデバイス (PBD: Physical Block Device) は、Citrix Hypervisor サーバーとストレージリポジトリ間のインターフェイスです。PBD 上の読み取りおよび書き込み時の総スループット量が指定のしきい値を超えると、その PBD が接続されているホスト上でアラートが生成されます。ほかの Citrix Hypervisor サーバーアラートとは異なり、このアラートはストレージリポジトリに対して設定します。

3. アラートの送信間隔を変更するには、[アラートの送信間隔] ボックスに分単位で値を入力します。しきい値に達してアラートが生成されると、送信間隔が経過するまでそのアラートは生成されません。

4. [OK] をクリックして変更を保存します。

パフォーマンスアラートの表示、フィルタ、および重要度の設定方法については、XenCenter ドキュメントの「[パフォーマンスアラートの設定](#)」を参照してください。

システムアラート

次の表は、アラートが生成されるときのシステムのイベントまたは状態の一覧です。アラートは、XenCenter の [アラート] ページに表示されます。

名前	重要度	説明
license_expires_soon	2	Citrix Hypervisor のライセンスの有効期限が近づいています。
ha-statefile_lost	2	高可用性のストレージリポジトリとの接続が失われました。直ちに対処する必要があります。
ha-heartbeat_approaching_timeo	5	高可用性のタイムアウトが近づいています。直ちに対処しないとホストが再起動される可能性があります。
ha_statefile_approaching_timeo	5	高可用性のタイムアウトが近づいています。直ちに対処しないとホストが再起動される可能性があります。
haxapi_healthcheck_approachi	5	高可用性のタイムアウトが近づいています。直ちに対処しないとホストが再起動される可能性があります。
ha_network_bonding_error	3	サービスが失われる可能性があります。高可用性のハートビートを送信するためのネットワーク接続が失われました。
ha_pool_overcommitted	3	サービスが失われる可能性があります。高可用性で仮想マシンを保護できない可能性があります。
ha_poor_drop_in_plan_exists_fo	3	高可用性による保護が低下して失敗する可能性が高くなりましたが、まだ損失はありません。
ha_protected_vm_restart_faile	2	サービスが失われました。高可用性で保護されている仮想マシンを再起動できませんでした。
ha_host_failed	3	高可用性が、ホストが失敗したことを検出しました。
ha_host_was_fenced	4	仮想マシンの破損を防ぐため、高可用性によりホストが再起動されました。

名前	重要度	説明
redo_log_healthy	4	XAPI の redo ログがエラーから回復しました。
redo_log_broken	3	XAPI redo ログでエラーが発生しました。
ip_configured_pif_can_unplug	3	高可用性使用時に IP 設定済みの NIC が XAPI によりアンプラグされ、高可用性に問題が生じる可能性があります。
host_sync_data_failed	3	Citrix Hypervisor パフォーマンス測定値の同期に失敗しました。
host_clock_skew_detected	3	ホストの時計設定がプール内のほかのホストと同期していません。
host_clock_went_backwards	1	ホストの時計設定が破損しています。
pool_master_transition	4	新しいホストがプールマスターとして選出されました。
pbd_plug_failed_on_server_start	3	ホストの起動時にストレージとの接続に失敗しました。
auth_external_init_failed	2	ホストで Active Directory による外部認証に失敗しました。
auth_external_pool_non-homogeneous	2	プールのホスト間で Active Directory による外部認証設定が異なります。
multipath_period_alert	3	ストレージリポジトリへのいずれかのパスが切断または復元されました。
bond-status-changed	3	ボンディングを構成するいずれかのリンクが切断または再接続されました。

ソフトウェアアップデートアラート

- **XenCenter** の既存のバージョン: **XenCenter** の新しいバージョンが入手可能ですが、既存のバージョンでも新しいバージョンの Citrix Hypervisor に接続できます

- **XenCenter** の古いバージョン: XenCenter のバージョンが古いため新しいバージョンの Citrix Hypervisor に接続できません
- **Citrix Hypervisor** の古いバージョン: Citrix Hypervisor のバージョンが古いためこのバージョンの XenCenter で接続できません
- ライセンス期限切れ: Citrix Hypervisor のライセンスは有効期限切れです
- 不明な **IQN**: Citrix Hypervisor で iSCSI ストレージを使用していますがホストの IQN が空白です
- 重複した **IQN**: Citrix Hypervisor で iSCSI ストレージを使用していますがホストの IQN が重複しています

xe CLI を使用してパフォーマンスアラートを設定する

注:

アラートを生成するかどうかを 5 分未満の間隔でチェックすることはできません。これは、チェックによる過剰な負荷および障害の誤検出を防ぐためです。アラートのチェック間隔として 5 分よりも小さい値を指定しても、アラートの生成は 5 分おきに行われます。

パフォーマンスの監視機能である `perfmon` は 5 分おきに実行され、Citrix Hypervisor から 1 分間の平均パフォーマンスの情報を取得します。このデフォルト設定は、`/etc/sysconfig/perfmon` で変更できます。

`perfmon` ツールは、そのホスト上で実行されるパフォーマンス変数のアップデートを 5 分おきに読み取ります。これらの変数は、ホストおよびそのホスト上の仮想マシンごとにグループ化されます。`perfmon` は、ホストおよび仮想マシンごとに `other-config:perfmon` パラメータの内容を読み取り、そのパラメータの値により監視すべき変数およびメッセージを生成すべき状況を決定します。

以下の例では、`other-config:perfmon` パラメータの XML 文字列で仮想マシンの CPU 使用率アラートを設定しています:

```
1   xe vm-param-set uuid=vm_uuid other-config:perfmon=\
2
3   '<config>
4     <variable>
5       <name value="cpu_usage"/>
6       <alarm_trigger_level value="0.5"/>
7     </variable>
8   </config>'
```

注:

複数の変数ノードを使用できます。

新しい構成の設定後、次のコマンドを使用して各ホストの `perfmon` を更新します:

```
1   xe host-call-plugin host=host_uuid plugin=perfmon fn=refresh
```

更新しないと、新しい構成が有効になるまで時間がかかります。これは、デフォルトで 30 分ごとに `perfmon` が新しい構成を確認するためです。このデフォルト設定は、`/etc/sysconfig/perfmon` で変更できます。

有効な仮想マシンエレメント

- **name**: 変数の名前 (デフォルト値なし)。名前の値が `cpu_usage`、`network_usage`、または `disk_usage` のいずれかの場合、この値が使用されるため `rrd_regex` および `alarm_trigger_sense` パラメータはデフォルトとして必要ありません。
- **alarm_priority**: 生成するアラートの優先度 (デフォルト値は3)。
- **alarm_trigger_level**: アラートを生成する値レベル (デフォルト値なし)。
- **alarm_trigger_sense**: `alarm_trigger_level` が最大値の場合は `high`、`alarm_trigger_level` が最小値の場合は `low` (デフォルト値は `high`)。
- **alarm_trigger_period**: 値がしきい値に達した場合にアラートを送信するまでの秒数 (デフォルト値は60)。
- **alarm_auto_inhibit_period**: アラート送信後にそのアラートを無効にしておく秒数 (デフォルト値は3600)。
- **consolidation_fn**: `rrd_updates` からの変数の計算方法。 `cpu-usage` のデフォルトは `average`、`fs_usage` のデフォルトは `get_percent_fs_usage`、そのほかの変数では `sum` です。
- **rrd_regex**: パフォーマンス値の計算に使用される、`xe vm-data-sources-list uuid=vm_uuid` コマンドで返される変数名にマッチする正規表現。このパラメータは、以下の名前付き変数のデフォルト値を持ちます:
 - `cpu_usage`
 - `network_usage`
 - `disk_usage`

`xe vm-data-source-list` の正規表現にマッチするすべての値は、`consolidation_fn` で指定した方法で計算されます。

有効なホストエレメント

- **name**: 変数の名前 (デフォルト値なし)。
- **alarm_priority**: 生成するアラートの優先度 (デフォルト値は3)。
- **alarm_trigger_level**: アラートを生成する値レベル (デフォルト値なし)。
- **alarm_trigger_sense**: `alarm_trigger_level` が最大値の場合は `high`、`alarm_trigger_level` が最小値の場合は `low` (デフォルト値は `high`)。
- **alarm_trigger_period**: 値がしきい値に達した場合にアラートを送信するまでの秒数 (デフォルト値は60)。
- **alarm_auto_inhibit_period**: アラート送信後にそのアラートを無効にしておく秒数 (デフォルト値は3600)。
- **consolidation_fn**: `rrd_updates` からの変数の計算方法 (デフォルト値は `sum` または `average`)。

- `rrd_regex`: パフォーマンス値の計算に使用される、`xe vm-data-source-list uuid=vm_uuid` コマンドで返される変数名にマッチする正規表現。このパラメータは、以下の名前付き変数のデフォルト値を持ちます。
 - `cpu_usage`
 - `network_usage`
 - `memory_free_kib`
 - `sr_io_throughput_total_xxxxxxxx` (ここで`xxxxxxxx`はストレージリポジトリ UUID の最初の 8 文字)

ストレージリポジトリスループット: ストレージスループットアラートは、ホストではなくストレージリポジトリを対象にして設定します。次に例を示します:

```

1     xe sr-param-set uuid=sr_uuid other-config:perfmon=\
2     '<config>
3         <variable>
4             <name value="sr_io_throughput_total_per_host"/>
5             <alarm_trigger_level value="0.01"/>
6         </variable>
7     </config>'
```

一般的な設定例

以下は、一般的な設定の例です。

```

1     <config>
2     <variable>
3         <name value="NAME_CHOSEN_BY_USER"/>
4         <alarm_trigger_level value="THRESHOLD_LEVEL_FOR_ALARM"/>
5         <alarm_trigger_period value="
6             RAISE_ALARM_AFTER_THIS_MANY_SECONDS_OF_BAD_VALUES"/>
7         <alarm_priority value="PRIORITY_LEVEL"/>
8         <alarm_trigger_sense value="HIGH_OR_LOW"/>
9         <alarm_auto_inhibit_period value="
10            MINIMUM_TIME_BETWEEN_ALARMS_FROM_THIS_MONITOR"/>
11        <consolidation_fn value="FUNCTION_FOR_COMBINING_VALUES"/>
12        <rrd_regex value="
13            REGULAR_EXPRESSION_TO_CHOOSE_DATASOURCE_METRIC"/>
14    </variable>
15    <variable>
16        ...
17    </variable>
18    ...
```

メールアラートの設定

Citrix Hypervisor サーバーでアラートが生成されたときに、メールによる通知が送信されるように Citrix Hypervisor を設定できます。これを行うには、XenCenter または xe コマンドラインインターフェイス (CLI) を使用します。

XenCenter を使用したアラートメールの有効化

1. リソースペインでプールを右クリックして、[プロパティ] を選択します。
2. [プロパティ] ダイアログボックスで、[メールオプション] をクリックします。
3. [アラートをメールで送信する] チェックボックスをオンにして、メールアドレスと SMTP サーバーの詳細を入力します。

注:

ここで指定する SMTP サーバーは、認証が不要なものである必要があります。

4. パフォーマンスアラートメールを受信する場合、[Mail language] リストから表示言語を選択します。選択可能な言語は、日本語、英語、中国語です。

XenCenter のパフォーマンスアラートメールを構成するためのデフォルトの言語は英語です。

xe CLI を使用したアラートメールの有効化

重要:

XenCenter または xe CLI を使用してアラートメールを有効にする場合、認証が不要な SMTP サーバーの詳細を指定します。認証が必要な SMTP サーバーを指定すると、メールが送信されません。

アラートメールを構成するには、次のコマンドを実行して、メールアドレスと SMTP サーバーを指定します:

```
1   xe pool-param-set uuid=pool_uuid other-config:mail-destination=joe.
    bloggs@domain.tld
2   xe pool-param-set uuid=pool_uuid other-config:ssmtp-mailhub=smtp.
    domain.tld[:port]
```

また、次のように、メールで送信するアラートの最低優先度 (XenCenter では「重要度」と呼ばれます) を指定できます:

```
1   xe pool-param-set uuid=pool_uuid other-config:mail-max-priority=
    level
```

デフォルトの優先度は4です。

注:

一部の SMTP サーバーでは、完全修飾ドメイン名 (FQDN) が指定されたメールだけが転送されます。メールが転送されない場合は、これが原因になっている可能性があります。この場合、サーバーのホスト名を FQDN に設定し、メールサーバーでそれが使用されるように設定します。

パフォーマンスアラートメールの言語を構成するには:

```
1      xe pool-param-set uuid=pool_uuid other-config:mail-language=en-US |
      zh-CN | ja-JP
```

認証が必要な **SMTP** サーバーでアラートメールを送信する

Citrix Hypervisor の mail-alarm ユーティリティでは、sSMTP を使用してアラートメールを送信できます。mail-alarm ユーティリティは、アラートメールを送信する前に、設定ファイル `mail-alarm.conf` をチェックします。この設定ファイルが存在する場合は、その内容に基づいて sSMTP が構成されます。設定ファイルが存在しない場合は、XAPI データベースに格納されている情報 (XenCenter または xe CLI で設定された情報) に基づいてアラートメールが送信されます。認証が必要な SMTP サーバーでアラートメールを送信するには、以下の内容の `mail-alarm.conf` ファイルを `/etc/` に作成する必要があります。

```
1      root=postmaster
2      authUser=<username>
3      authPass=<password>
4      mailhub=<server address>:<port>
```

注:

この設定ファイルは、Citrix Hypervisor サーバーで生成されるすべてのアラートで使用されます。

その他の設定オプション

SMTP サーバーによっては、追加の設定が必要な場合があります。設定可能なオプションおよび構文については、`ssmtp.conf` の man ページを参照してください。主な内容は以下のとおりです:

```
1      NAME
2      ssmtp.conf - ssmtp configuration file
3
4      DESCRIPTION
5      ssmtp reads configuration data from /etc/ssmtp/ssmtp.conf The
6      file contains keyword-argument pairs, one per line. Lines starting with
7      '#' and empty lines are interpreted as comments.
```

```
8
9   The possible keywords and their meanings are as follows (both are
10  case-
11  insensitive):
12
13  Root
14  The user that gets all mail for userids less than 1000. If
15  blank,
16  address rewriting is disabled.
17
18  Mailhub
19  The host to send mail to, in the form host | IP_addr port
20  [:
21  port]. The default port is 25.
22
23  RewriteDomain
24  The domain from which mail seems to come. For user
25  authentication.
26
27  Hostname
28  The full qualified name of the host. If not specified, the
29  host
30  is queried for its hostname.
31
32  FromLineOverride
33  Specifies whether the From header of an email, if any, may
34  over-
35  ride the default domain. The default is "no".
36
37  UseTLS
38  Specifies whether smtp uses TLS to talk to the SMTP server.
39  The default is "no".
40
41  UseSTARTTLS
42  Specifies whether smtp does a EHLO/STARTTLS before
43  starting SSL
44  negotiation. See RFC 2487.
45
46  TLSCert
47  The file name of an RSA certificate to use for TLS, if
48  required.
49
50  AuthUser
51  The user name to use for SMTP AUTH. The default is blank,
52  in
```

```
44         which case SMTP AUTH is not used.
45
46     AuthPass
47         The password to use for SMTP AUTH.
48
49     AuthMethod
50         The authorization method to use. If unset, plain text is
           used.
51         May also be set to "cram-md5".
```

カスタムフィールドとタグ

XenCenter では、仮想マシンやストレージなどをわかりやすく分類するためのタグやカスタムフィールドを作成できます。詳しくは、「[システムパフォーマンスの監視](#)」を参照してください。

カスタム検索

XenCenter では、カスタムの検索条件を作成して保存できます。これらの検索条件をエクスポート/インポートしたり、検索結果をリソースペインに表示したりできます。詳しくは、「[システムパフォーマンスの監視](#)」を参照してください。

物理バスアダプタのスループットの確認

ファイバチャネル、SAS、および iSCSI のホストバスアダプタ (HBA) では、以下の手順で PBD のネットワークスループットを確認できます。

1. ホスト上の PBD のリストを出力します。
2. どの LUN がどの PBD 上にルーティングされているかを確認します。
3. 各 PBD およびストレージリポジトリで、そのストレージリポジトリ上の VDI を参照している VBD のリストを出力します。
4. ホスト上の仮想マシンに接続されているすべてのアクティブな VBD について、総スループットを算出します。

iSCSI および NFS ストレージでは、ネットワークの統計値を確認して、アレイでスループットのボトルネックが発生していないかどうか、PBD が飽和状態になっていないかを確認します。

仮想マシンの管理

December 30, 2019

このセクションでは、テンプレートを使用した仮想マシンの作成方法の概要について説明します。また、Physical-to-Virtual 変換 (P2V、物理マシンの仮想化)、テンプレートの複製、エクスポートされた仮想マシンのインポートについても説明します。

仮想マシンとは

仮想マシン (VM: Virtual Machine) とは、すべての要素がソフトウェアで構成されたコンピュータを指し、物理コンピュータと同様にオペレーティングシステムやアプリケーションを実行できます。仮想マシンには、その仮想マシンに関する一連の仕様と設定ファイルが含まれ、ホストの物理リソースにより機能します。すべての仮想マシンには、物理ハードウェアと同じ機能を提供する仮想デバイスがあります。仮想マシンには、移植性と安全性が高く管理しやすいという利点があります。さらに、必要に応じて各仮想マシンの起動設定を変更できます。詳しくは、「[仮想マシンの起動設定](#)」を参照してください。

Citrix Hypervisor は仮想マシンで、IPv4 および IPv6 の任意の組み合わせでアドレスを設定できます。

Citrix Hypervisor 仮想マシンは完全仮想化 (HVM) モードで動作できます。特定のプロセッサ機能を使用して、仮想マシンが実行する特権命令を「トラップ」します。この機能により、変更されていないオペレーティングシステムを使用することができます。ネットワークとストレージのアクセスのために、仮想マシンにはエミュレートされたデバイスが提示されます。また、パフォーマンスと信頼性の理由から、PV ドライバーを使用することもできます。

仮想マシンの作成

仮想マシンテンプレートの使用

仮想マシンはテンプレートから作成されます。テンプレートは、特定の仮想マシンのインスタンスを作成するためのさまざまな設定を含む「ゴールドイメージ」です。Citrix Hypervisor はテンプレートの基本セットとともに出荷されます。これは、オペレーティングシステムをインストールできる「未加工の」仮想マシンです。通常、オペレーティングシステムが最高のパフォーマンスで動作するためには、設定の最適化が必要です。Citrix Hypervisor テンプレートは、各オペレーティングシステムが最適なパフォーマンスで動作するように調整されています。

テンプレートを使用して仮想マシンを作成するには、以下の 2 つの方法があります。

- 設定済みの完全テンプレートを使用する (Demo Linux 仮想アプライアンスなど)。
- テンプレートに CD、ISO イメージ、またはネットワークリポジトリからオペレーティングシステムをインストールする。

仮想マシンに Windows オペレーティングシステムをインストールする方法については、[Windows 仮想マシン](#)を参照してください。

仮想マシンに Linux オペレーティングシステムをインストールする方法については、[Linux 仮想マシン](#)を参照してください。

注:

古いバージョンの Citrix Hypervisor で作成されたテンプレートは、新しいバージョンの Citrix Hypervisor で使用できます。一方、新しいバージョンの Citrix Hypervisor で作成されたテンプレートは、古いバージョンの Citrix Hypervisor では使用できません。既に Citrix Hypervisor 8.1 を使用して仮想マシンテンプレートを作成済みで、それを以前のバージョンで使用する場合、VDI を個別にエクスポートして仮想マシンを再度作成します。

そのほかの作成方法

テンプレートを使用する方法のほかに、以下の方法でも仮想マシンを作成できます。

Physical-to-Virtual 変換

Physical-to-Virtual 変換 (P2V) とは、物理サーバー上の既存の Windows オペレーティングシステムを、それ自体の仮想化されたインスタンスとして変換するプロセスを指します。変換にはファイルシステム、構成などが含まれます。この仮想化されたインスタンスは、その後、転送、インスタンス化され、Citrix Hypervisor サーバー上の仮想マシンとして起動します。

既存の仮想マシンの複製

テンプレートを複製することで、既存の仮想マシンのコピー (クローン) を作成できます。テンプレートは、仮想マシンインスタンスの作成元 (マスタコピー) としてのみ使用される通常の仮想マシンです。仮想マシンはカスタマイズ可能で、テンプレートに変換できます。仮想マシンの適切な準備手順に従ってください。詳しくは、「[sysprep を使用した Windows 仮想マシンの複製の準備](#)」および「[Linux 仮想マシンを複製する前に](#)」を参照してください。

注:

テンプレートを通常の仮想マシンとして使用することはできません。

Citrix Hypervisor には仮想マシンを複製する方式が 2 種類あります。

- 完全なコピー
- コピーオンライト

コピーオンライトモードでは、変更のあったブロックのみがディスクに書き込まれます。コピーオンライトモードはディスクのスペースを節約し、高速複製ができるように設計されていますが、通常のディスクパフォーマンスをわずかに低下させます。テンプレートは、パフォーマンスの低下なしに何度も高速複製できます。

注:

テンプレートを仮想マシンに複製してから、その複製をテンプレートに変換すると、ディスクのパフォーマンスが低下する場合があります。低下する量は、このプロセスが発生する回数に直接関係します。この場合、`vm-copy` CLI コマンドを使用して、ディスクの完全コピーを作成してディスクパフォーマンス

スを回復できます。

リソースプールでの注意事項

共有ストレージリポジトリで仮想マシンの仮想ディスクからテンプレートを作成すると、テンプレート複製処理は、共有ストレージリポジトリにアクセスできるプール内のサーバーに転送されます。これに対し、ローカルストレージリポジトリしかない仮想マシンの仮想ディスクからテンプレートを作成すると、テンプレート複製処理はそのストレージリポジトリにアクセスできるサーバーでのみ実行できます。

エクスポートされた仮想マシンのインポート

エクスポートされた仮想マシンをインポートすることで、新しい仮想マシンを作成できます。複製と同様に、特定の構成を持つ仮想マシンをさらに迅速に作成するには、仮想マシンのエクスポート/インポート機能を使用できます。この方法を使用すると、展開を迅速化できます。たとえば、特殊用途のサーバー構成があり、それを繰り返して使用する必要がある場合、必要に応じて仮想マシンを設定した後それをエクスポートし、後でインポートして、特別な構成の仮想マシンのコピーを作成できます。仮想マシンをほかのリソースプール内の Citrix Hypervisor サーバーに移動する場合にも、エクスポート/インポート機能を使用できます。

仮想マシンのインポートおよびエクスポート手順については、[仮想マシンのインポートとエクスポート](#)を参照してください。

Citrix VM Tools

Citrix VM Tools には従来型デバイスエミュレーションのようなオーバーヘッドがなく、高パフォーマンスの I/O サービスが提供されます。Citrix VM Tools は、I/O ドライバー（準仮想化ドライバーまたは PV ドライバーともいいます）と管理エージェントで構成されています。仮想マシンが完全にサポートされる構成となるように、また、xe CLI または XenCenter を使用できるように、各 Windows 仮想マシンに Citrix VM Tools をインストールします。仮想マシンにインストールされた Citrix VM Tools のバージョンは、Citrix Hypervisor サーバーにインストールされた最新バージョンと同じである必要があります。たとえば、一部の Hotfix には、ホストにインストールされているバージョンをアップデートするための最新の Citrix VM Tools ISO が含まれています。

I/O ドライバーにはストレージ、ネットワークドライバー、および低レベル管理インターフェイスが含まれています。準仮想化ドライバーは、エミュレートされたドライバーに置き換わり、Windows と Citrix Hypervisor ソフトウェア間的高速トランスポートを提供します。Windows オペレーティングシステムのインストール時、Citrix Hypervisor は従来型デバイスエミュレーションを使用して、標準 IDE コントローラーと標準ネットワークカードを仮想化マシンに提供します。このエミュレーションでは、組み込みドライバーを使って Windows のインストールを完了できますが、コントローラードライバーのエミュレーションに内在するオーバーヘッドによりパフォーマンスが低下します。

管理エージェント（ゲストエージェントともいいます）は、高レベルの仮想マシン管理機能を備えており、XenCenter にすべての機能を提供します。

仮想マシンが完全にサポートされる構成となるようにするには、各 Windows 仮想マシンに Citrix VM Tools をインストールする必要があります。仮想マシンにインストールされた Citrix VM Tools のバージョンは、Citrix Hypervisor サーバーにインストールされたバージョンと同じである必要があります。仮想マシンは、Citrix VM Tools がなくても機能しますが、I/O ドライバー（PV ドライバー）がインストールされていないと、パフォーマンスが大幅に低下します。次の操作を実行できるようにするには、Citrix VM Tools を Windows 仮想マシンにインストールする必要があります。

- 仮想マシンを正しくシャットダウン、再起動、または一時停止する
- XenCenter で仮想マシンのパフォーマンスデータを表示する
- 実行中の仮想マシンを移行する（ライブマイグレーションまたはストレージライブマイグレーションを使用）
- メモリを含んだスナップショット（チェックポイント）を作成したり、スナップショットを復元したりする
- 実行中の Linux 仮想マシンの仮想 CPU の数を変更する（Windows 仮想マシンの場合は再起動が必要）

仮想マシンの仮想化の状態を確認する

XenCenter では、仮想マシンの [全般] タブに仮想マシンの仮想化の状態が表示されます。Citrix VM Tools (I/O ドライバーと管理エージェント) がインストールされているかどうかを確認できます。また、このタブには、仮想マシンが Windows Update のアップデートをインストールおよび受信できるかどうか也表示されます。以下のセクションでは、XenCenter で表示されるメッセージを示します。

I/O が最適化されました (I/O は最適化されていません)： このフィールドには、I/O ドライバーが仮想マシンにインストールされているかどうかが表示されます。Citrix VM Tools ISO から I/O ドライバーをインストールするには、**[I/O ドライバーおよび管理エージェントをインストール]** リンクをクリックします。

注：

Windows Update からアップデートを受け取ることができる Windows 仮想マシンには、I/O ドライバーが自動的にインストールされます。詳しくは、「[Citrix VM Tools のアップデート](#)」を参照してください。

管理エージェントがインストールされました (管理エージェントはインストールされていません)： このフィールドには、管理エージェントが仮想マシンにインストールされているかどうかが表示されます。Citrix VM Tools ISO から管理エージェントをインストールするには、**[I/O ドライバーおよび管理エージェントをインストール]** リンクをクリックします。

Windows Update からのアップデート受信が可能 (Windows Update からのアップデート受信が不可能)： 仮想マシンが Windows Update から I/O ドライバーを受け取ることができるかどうかを示します。

注：

Windows Server Core 2016 では、I/O ドライバーのインストールまたはアップデートに Windows Update を使用できません。代わりに、Citrix VM Tools ISO のインストーラーを使用します。

I/O ドライバーおよび管理エージェントをインストール： このメッセージは、仮想マシンに I/O ドライバーと管理エージェントがインストールされていない場合に表示されます。Citrix VM Tools をインストールするには、リンクを

クリックします。Linux 仮想マシンの場合、状態リンクをクリックすると、仮想マシンのコンソールに切り替わり、Citrix VM Tools ISO がロードされます。ISO をマウントし、「[Citrix VM Tools のインストール](#)」で説明するように、手動でインストールを実行します。

サポートされるゲストオペレーティングシステムとリソースの割り当て

サポートされるゲストオペレーティングシステムの一覧については、「[サポートされるゲストオペレーティングシステム、仮想メモリ、および仮想ディスクのサイズ制限](#)」を参照してください。

このセクションでは、Citrix Hypervisor 製品ファミリーメンバーの仮想デバイスのサポートの違いについて説明します。

Citrix Hypervisor 製品ファミリーの仮想デバイスのサポート

このバージョンの Citrix Hypervisor 製品ファミリーには、仮想デバイスに関するいくつかの一般的な制限があります。一部のゲストオペレーティングシステムには、特定の機能に対する下限値があります。これらの制限については、各ゲストオペレーティングシステムのインストールのセクションで説明します。設定の制限値について詳しくは、「[構成の制限](#)」を参照してください。

ハードウェアや環境などの要因が、制限値に影響する場合があります。サポートされるハードウェアについて詳しくは、「[Citrix Hypervisor ハードウェア互換性リスト \(英語\)](#)」を参照してください。

仮想マシンブロックデバイス

Citrix Hypervisor は `hd*` デバイスの形式で IDE バスをエミュレートします。Windows の場合、Citrix VM Tools のインストールにより特別な I/O ドライバがインストールされ、完全に仮想化された環境であることを除き、Linux の場合と同様に動作します。

Windows 仮想マシン

March 12, 2020

Windows 仮想マシンを Citrix Hypervisor サーバーにインストールするには、ハードウェアの仮想化のサポート (Intel VT または AMD-V) が必要です。

Windows 仮想マシンの基本的な作成手順

Windows の仮想マシンへのインストールプロセスには、次の手順が含まれます:

1. 適切な Windows テンプレートを選択する。

2. 適切なブートモードを選択する
3. Windows オペレーティングシステムをインストールする。
4. Citrix VM Tools (I/O ドライバーおよび管理エージェント) をインストールする。

警告:

Windows 仮想マシンは、Citrix VM Tools がインストールされている場合にのみサポートされます。詳しくは、「Citrix VM Tools」を参照してください。

Windows VM テンプレート

Windows 仮想マシンは、XenCenter または CLI を使って、適切なテンプレートを複製して作成します。各ゲストのテンプレートには、仮想ハードウェアの構成を定義する、定義済みのプラットフォームフラグセットが含まれています。たとえば、すべての Windows 仮想マシンは ACPI Hardware Abstraction Layer (HAL) モードが有効な状態でインストールされます。後でこれらの仮想マシンのいずれかに複数の仮想 CPU を割り当てると、Windows で HAL がマルチプロセッサモードに自動的に切り替わります。

次の表に、利用可能な Windows テンプレートを示します:

テンプレート名	サポートされているブートモード	説明
Citrix XenApp on Windows Server 2008 (32 ビット)	BIOS	Windows Server 2008 SP2 (32 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。Citrix XenApp のパフォーマンスが最適化されるように特別に調整されたテンプレートです。
Citrix XenApp on Windows Server 2008 (64 ビット)	BIOS	Windows Server 2008 SP2 (64 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。Citrix XenApp のパフォーマンスが最適化されるように特別に調整されたテンプレートです。

テンプレート名	サポートされているブートモード	説明
Citrix XenApp on Windows Server 2008 R2 (64 ビット)	BIOS	Windows Server 2008 R2、または Windows Server 2008 R2 SP1 (64 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。Citrix XenApp のパフォーマンスが最適化されるように特別に調整されたテンプレートです。
Windows 7 (32 ビット)	BIOS	Windows 7 および Windows 7 SP1 (32 ビット) をインストールする場合に使用します。
Windows 7 (64 ビット)	BIOS	Windows 7 および Windows 7 SP1 (64 ビット) をインストールする場合に使用します。
Windows 8.1 (32 ビット)	BIOS	Windows 8.1 (32 ビット) をインストールする場合に使用します。(注を参照してください)
Windows 8.1 (64 ビット)	BIOS	Windows 8.1 (64 ビット) をインストールする場合に使用します。(注を参照してください)
Windows 10 (32 ビット)	BIOS	Windows 10 をインストールする場合に使用します。
Windows 10 (64 ビット)	BIOS、UEFI、UEFI セキュアブート	Windows 10 (64 ビット) をインストールする場合に使用します。
Windows Server 2008 (32 ビット)	BIOS	Windows Server 2008 SP2 (32 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。
Windows Server 2008 (64 ビット)	BIOS	Windows Server 2008 SP2 (64 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。

テンプレート名	サポートされているブートモード	説明
Windows Server 2008 R2 (64 ビット)	BIOS	Windows Server 2008 R2、または Windows Server 2008 R2 SP1 (64 ビット) をインストールする場合に使用します。すべてのエディションがサポートされています。
Windows Server 2012 (64 ビット)	BIOS	Windows Server 2012 (64 ビット) をインストールする場合に使用します。
Windows Server 2012 R2 (64 ビット)	BIOS	Windows Server 2012 R2 (64 ビット) をインストールする場合に使用します。
Windows Server 2016 (64 ビット)	BIOS、UEFI、UEFI セキュアブート	Windows Server 2016 または Windows Server Core 2016 (64 ビット) をインストールする場合に使用します。
Windows Server 2019 (64 ビット)	BIOS、UEFI、UEFI セキュアブート	Windows Server 2019 または Windows Server Core 2019 (64 ビット) をインストールする場合に使用します。

注:

Windows 8 はサポートされなくなりました。Windows 8 がインストールされている場合、Windows 8.1 にアップグレードしてください。

ISO イメージライブラリの接続

Windows オペレーティングシステムは、Citrix Hypervisor サーバーの物理 DVD/CD ドライブに挿入したインストールメディアや、その ISO イメージからインストールできます。Windows インストール CD から ISO イメージを作成し、インストールできるようにする方法については、[ISO イメージの作成](#)を参照してください。

ゲスト **UEFI** ブートとセキュアブート

Citrix Hypervisor では、最新バージョンの Windows ゲストオペレーティングシステムを UEFI モードで起動できます。UEFI ブートにより、ゲストオペレーティングシステムがハードウェアとやり取りするための、充実したインターフェイスが提供されるため、Windows 仮想マシンの起動時間を大幅に短縮できます。

これらの Windows オペレーティングシステムの場合、Citrix Hypervisor は Windows セキュアブートもサポートしています。セキュアブートは、未署名のバイナリ、正しく署名されていないバイナリ、または変更されたバイナリが起動中に実行されるのを防ぎます。セキュアブートを実施する UEFI 対応の仮想マシンでは、すべてのドライバーに署名する必要があります。この要件により、仮想マシンの使用範囲が制限される場合がありますが、未署名のドライバーや変更されたドライバーをブロックすることで安全を確保します。未署名のドライバーを使用するとセキュアブートが失敗し、XenCenter に通知が表示されます。

また、セキュアブートは、ゲスト内のマルウェアがブートファイルを操作したり、ブートプロセス中に実行されたりするリスクも減らします。

注:

ゲスト UEFI ブートは試験段階の機能として Citrix Hypervisor 8.0 で提供されました。Citrix Hypervisor 8.0 で作成された UEFI 対応の仮想マシンは、Citrix Hypervisor 8.1 でサポートされていません。これらの仮想マシンを削除して、Citrix Hypervisor 8.1 で新しい仮想マシンを作成してください。

Citrix Hypervisor は、新しく作成された Windows 10 (64 ビット)、Windows Server 2016 (64 ビット)、および Windows Server 2019 (64 ビット) の仮想マシンで UEFI ブートおよびセキュアブートをサポートします。仮想マシンの作成時に起動モードを指定する必要があります。仮想マシンを初めて起動した後で、BIOS と UEFI (または UEFI セキュアブート) の間で仮想マシンの起動モードを変更することはできません。ただし、UEFI と UEFI セキュアブートの間では起動モードはいつでも変更できます。

仮想マシンで UEFI ブートを有効にする場合は、次の点を考慮してください:

- UEFI 対応の仮想マシンに少なくとも 2 つの vCPU があることを確認します。
- Citrix Hypervisor で作成された UEFI 対応の仮想マシンを、OVA、OVF、または XVA ファイルとしてインポートまたはエクスポートできます。他のハイパーバイザーで作成された OVA または OVF パッケージからの、UEFI 対応仮想マシンのインポートはサポートされていません。
- Citrix Machine Creation Services では、UEFI 対応の仮想マシンはサポートされていません。
- UEFI 設定メニューを使用して、XenCenter コンソールの画面の解像度を変更します。詳しい手順については、画面の解像度の変更を参照してください。

仮想マシンで UEFI セキュアブートを有効にする場合は、次の点を考慮してください:

- Citrix Hypervisor サーバーは UEFI モードで起動する必要があります。詳しくは、「[ネットワークブートによるインストール](#)」を参照してください。
- リソースプールまたはスタンドアロンサーバーは、セキュアブート証明書にアクセスできる必要があります。証明書へのアクセス権が必要なプール内の Citrix Hypervisor サーバーは 1 つだけです。サーバーがプールに参加すると、そのサーバー上の証明書はプール内の他のサーバーで利用可能になります。

注

UEFI 対応の仮想マシンはエミュレートされたデバイスに NVME と E1000 を使用します。エミュレーション情報には、仮想マシン上の Citrix VM Tools をインストールするまでこれらの値は表示されません。

UEFI 対応の仮想マシンには、Citrix VM Tools をインストールするまで、2 つのネットワークインターフェイ

スカードしかないと表示されます。

UEFI ブートまたは UEFI セキュアブートを有効にする

XenCenter または xe CLI を使用することで、仮想マシンの UEFI ブートまたは UEFI セキュアブートを有効にできます。

XenCenter での UEFI 対応の仮想マシン作成については、「XenCenter を使用した仮想マシンの作成」を参照してください。

xe CLI を使用して UEFI ブートまたは UEFI セキュアブートを有効にする

仮想マシンを作成するときは、仮想マシンを初めて起動する前に次のコマンドを実行します：

```
1 xe vm-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
2 xe vm-param-set uuid=<UUID> platform:secureboot=<OPTION>
```

ここで、**UUID**は仮想マシンの UUID で、**MODE**は「BIOS」または「UEFI」のいずれかであり、**OPTION**は「true」または「false」のいずれかです。モードを指定しない場合、仮想マシンオペレーティングシステムで UEFI がサポートされていれば、デフォルトで「UEFI」になります。サポートされていない場合、モードはデフォルトで「BIOS」になります。**secureboot**オプションを指定しない場合は、デフォルトで「auto」になります。UEFI モードで起動され、セキュアブート証明書が利用可能な Citrix Hypervisor サーバーで作成された UEFI 対応の仮想マシンの場合、「auto」にすると仮想マシンのセキュアブートが有効になります。そうでない場合、セキュアブートは有効になりません。

Citrix Hypervisor が提供するテンプレートから UEFI 対応の仮想マシンを作成するには、次のコマンドを実行します：

```
1 UUID=$(xe vm-clone name-label='Windows 10 (64-bit)' new-name-label='Windows 10 (64-bit)(UEFI)')
2 xe template-param-set uuid=<UUID> HVM-boot-params:firmware=<MODE>
   platform:secureboot=<OPTION>
```

何かがインストールされているテンプレート、またはスナップショットから作成したテンプレートに対してはこのコマンドを実行しないでください。これらのスナップショットの起動モードは変更できません。また、起動モードを変更しようとする、仮想マシンは起動に失敗します。

セキュアブートを無効にする

場合によってはセキュアブートを無効にする必要が出てきます。たとえば、Windows デバッグは、セキュアブートユーザーモードの仮想マシンでは有効にできません。セキュアブートを無効にするには、仮想マシンをセキュアブートセットアップモードに変更します。Citrix Hypervisor サーバーで、次のコマンドを実行します：

```
1 varstore-sb-state <VM_UUID> setup
```

キー

UEFI 対応の仮想マシンは、一時的な秘密キー、Microsoft KEK、Microsoft Windows Production PCA、および Microsoft サードパーティキーからの PK でプロビジョニングされます。仮想マシンには、UEFI フォーラムの最新の失効リストが提供されます。この構成により、Windows 仮想マシンはセキュアブートをオンにして起動し、Microsoft からキーと失効リストの自動更新を受信できます。

UEFI および UEFI セキュアブート仮想マシンのトラブルシューティング

UEFI または UEFI セキュアブート仮想マシンのトラブルシューティングについては、「[Windows 仮想マシンの UEFI およびセキュアブートの問題のトラブルシューティング](#)」を参照してください。

XenCenter を使用した仮想マシンの作成

Windows 仮想マシンを作成するには：

1. XenCenter ツールバーで [新規 VM] をクリックします。[新規 VM] ウィザードが開きます。
[新規 VM] ウィザードでは、CPU、ストレージ、ネットワークなどの設定パラメータを選択しながら、目的に応じた仮想マシンを作成できます。
2. VM テンプレートを選擇して [次へ] をクリックします。

各テンプレートには、仮想マシンを特定のゲストオペレーティングシステム (OS) および適切なストレージ設定で作成するために必要な情報が含まれています。このテンプレート一覧には、現在 Citrix Hypervisor でサポートされているゲストオペレーティングシステムのテンプレートが表示されます。

注：

仮想マシンにインストールするオペレーティングシステムが特定のハードウェアでのみ動作する場合は、[ホストの BIOS 文字列を VM にコピーする] チェックボックスをオンにします。このオプションは、特定のコンピューターに同梱されていたオペレーティングシステムのインストール CD などに使用します。

CLI を使って BIOS 文字列をコピーする方法については、[BIOS でロックされた Reseller Option Kit メディアからの HVM 仮想マシンのインストール](#)を参照してください。ユーザー定義の BIOS 文字列を設定するオプションは、HVM 仮想マシンでは使用できません。

3. 新しい仮想マシンの名前と、必要に応じて説明を入力します。
4. 新しい仮想マシンにインストールするオペレーティングシステムのインストールメディアを選択します。
CD/DVD からのインストールが最も簡単な方法です。

- a) デフォルトのインストールソースオプション (DVD ドライブ) を選択します。
- b) Citrix Hypervisor サーバーの DVD ドライブにディスクを挿入します。

Citrix Hypervisor の既存の ISO ライブラリからインストールすることもできます。ISO ファイルには、光学ディスク (CD や DVD など) に収録されているすべての情報が含まれています。この場合、Windows のインストール CD の内容を含んでいる ISO ファイルを使用します。

既存の ISO ライブラリを接続するには、[新規 **ISO** ライブラリ] をクリックして ISO ライブラリの場所と種類を指定します。ISO ライブラリを指定すると、そのライブラリの ISO ファイルをリストで選択できるようになります。

5. 仮想マシンの起動モードを選択します。デフォルトでは、XenCenter は仮想マシンオペレーティングシステムのバージョンで利用可能な、最も安全な起動モードを選択します。

注:

- 1 - 選択した仮想マシンテンプレートがUEFIブートをサポートしていない場合、** [UEFIブート] ** オプションおよび ** [UEFIセキュアブート] ** オプションは灰色で表示されます。 - 仮想マシンを初めて起動した後で起動モードを変更することはできません。

6. 仮想マシンのホームサーバーを選択します。

ホームサーバーとは、プール内の仮想マシンにリソースを提供するサーバーを指します。仮想マシンのホームサーバーを指定すると、Citrix Hypervisor はそのサーバーで仮想マシンを起動しようとします。このアクションが不可能な場合、同じプール内の代替サーバーが自動的に選択されます。ホームサーバーを選択するには、[VMをこのサーバーに配置する] をクリックして、一覧からサーバーを選択します。

注:

- 1 - ワークロードバランス機能 (WLB) が有効なリソースプールでは、仮想マシンの起動、再起動、再開、および移行にホームサーバーは使用されません。代わりに、Citrix Hypervisor リソースプールの負荷測定基準と最適化の推奨項目に基づいて、最適なサーバー上で仮想マシンが起動、再起動、再開、および移行されます。 - 仮想マシンに1つ以上の仮想GPUが割り当てられている場合、ホームサーバーの指定は有効になりません。代わりに、サーバーはユーザーが設定した仮想GPU配置ポリシーに基づいて指定されます。

ホームサーバーを指定しない場合は、[ホームサーバーを割り当てない] を選択します。仮想マシンは、必要なリソースのあるすべてのサーバーで起動されます。

[次へ] をクリックして続行します。

7. 新しい仮想マシンに割り当てる仮想 CPU とメモリを指定します。Windows 10 の仮想マシンテンプレートでは、デフォルトで1つの仮想 CPU と 2048MB の RAM が割り当てられます。必要に応じて、これらの設定を

変更できます。 [次へ] をクリックして続行します。

8. 仮想 GPU を割り当てます。 [新規 VM] ウィザードにより、専用 GPU または仮想 GPU を仮想マシンに割り当てます。これにより、GPU の処理能力を仮想マシンで利用できるため、この機能を使用すると、CAD/CAM、GIS、および医療用画像処理アプリケーションなどの高度な 3D グラフィックアプリケーションのサポートが向上します。
9. 新しい仮想マシンに割り当てるストレージを指定します。

デフォルトの割り当てサイズ (24GB) と構成を選択する場合は [次へ] をクリックします。または、次のような追加の設定を行うこともできます：

- 仮想ディスクの名前、説明、またはサイズを変更する場合は、 [プロパティ] をクリックします。
- 新しい仮想ディスクを追加する場合は、 [追加] をクリックします。

10. 新しい仮想マシンのネットワークを設定します。

デフォルトの NIC と構成 (自動生成される各 NIC の MAC アドレスを含む) を選択する場合は、 [次へ] をクリックします。または、次のような追加の設定を行うこともできます：

- 物理ネットワーク、MAC アドレス、および仮想ディスクの QoS (Quality of Service: サービス品質) 制限を変更するには、 [プロパティ] をクリックします。
- 新しい仮想 NIC を追加する場合は、 [追加] をクリックします。

11. 設定内容を確認し、 [作成] をクリックして新しい仮想マシンを作成し、 [検索] タブに戻ります。

新しい仮想マシンのアイコンが、 [リソース] ペインのホストの下に表示されます。

リソースペインで仮想マシンを選択して、 [コンソール] タブをクリックします。仮想マシンのコンソール画面が表示されます。

12. オペレーティングシステムのインストール画面の指示に従って、インストールを完了します。
13. オペレーティングシステムがインストールされ、仮想マシンが再起動したら、Citrix VM Tools をインストールします。

インストール **Citrix VM Tools**

Citrix Hypervisor では、Windows 仮想マシンに Citrix VM Tools (I/O ドライバーおよび管理エージェント) をインストールおよびアップデートするためのよりシンプルなメカニズムが導入されています。

Citrix VM Tools には従来型デバイスエミュレーションのようなオーバーヘッドがなく、高パフォーマンスの I/O サービスが提供されます。Citrix VM Tools は、I/O ドライバー (準仮想化ドライバーまたは PV ドライバーともいいます) と管理エージェントで構成されています。Citrix VM Tools でサポートされるすべての機能を使用するには、各 Windows 仮想マシンにインストールする必要があります。仮想マシンはそれらがなくても動作しますが、パフォーマンスは大幅に低下します。

注:

Windows 仮想マシンに Citrix VM Tools をインストールするには、その仮想マシン上で Microsoft .NET Framework Version 4.0 またはそれ以降が実行されている必要があります。

Citrix VM Tools をインストールするには:

1. [リソース] ペインで仮想マシンを右クリックし、ショートカットメニューの [インストール] **Citrix VM Tools** をクリックします。または、[VM] メニューで [Citrix VM Tools のインストール] をクリックするか、仮想マシンの [全般] タブで [I/O ドライバーおよび管理エージェントをインストール] をクリックします。

注:

仮想マシンに Citrix VM Tools をインストールすると、I/O ドライバー (PV ドライバー) と管理エージェントの両方がインストールされます。

2. 仮想マシンの CD/DVD ドライブで自動実行が有効になっている場合は、しばらくすると自動的にインストールが開始されます。プロセスによって I/O ドライバーと管理エージェントがインストールされます。要求された場合は仮想マシンを再起動し、仮想マシンが最適化された状態にします。
3. AutoPlay が有効化されていない場合、[Citrix VM Tools のインストール] をクリックしてインストールを続行します。この操作により、仮想マシンの CD/DVD ドライブに Citrix VM Tools ISO (`guest-tools.iso`) がマウントされます。

メッセージが表示されたら、以下のオプションからいずれかを選択して Citrix VM Tools ISO で行う処理を指定します。

- [Setup.exe を実行] をクリックして Citrix VM Tools のインストールを開始します。この操作により、**Citrix Hypervisor [Windows Management Agent Setup]** ウィザードが開きます。ウィザードの指示に従って、仮想マシンを最適化された状態にし、インストールプロセスの完了に必要な操作を実行します。この方法で Citrix VM Tools をインストールすると、管理エージェントは自動的にアップデートを取得するよう構成されます。ただし、管理エージェントアップデートのメカニズムにより、I/O ドライバーが自動的にアップデートされることはありません。これはデフォルトの動作です。デフォルトの動作を変更する場合は、次の方法を使用して Citrix VM Tools をインストールします。
- [フォルダーを開いてファイルを表示] をクリックして、CD ドライブから `Setup.exe` を実行します。このオプションにより、**Citrix Hypervisor [Windows Management Agent Setup]** ウィザードが開き、Citrix VM Tools のインストールと管理エージェントのアップデート設定をカスタマイズできます。
- ウィザードの手順に従って、ライセンス契約書に同意し、保存先フォルダーを選択します。
- [Installation and Updates Settings] ページで設定をカスタマイズします。**Citrix Hypervisor [Windows Management Agent Setup]** ウィザードにデフォルト設定が表示されます。ウィザードは、デフォルトで以下の設定を表示します。
 - I/O ドライバーのインストール
 - 管理エージェントの自動アップデートの許可

- 管理エージェントが自動的に I/O ドライバーをアップデートすることを許可しない
- シトリックスに匿名の使用状況情報を送信する

管理エージェントの自動アップデートを許可しない場合は、[管理エージェントが自動的に I/O ドライバーをアップデートすることを許可しない] を選択します。

管理エージェントによる I/O ドライバーの自動アップデートを許可する場合は、[管理エージェントが自動的に I/O ドライバーをアップデートすることを許可する] を選択します。

注:

Windows Update メカニズムによる I/O ドライバーのアップデートを選択した場合は、管理エージェントによる I/O ドライバーの自動アップデートを許可しないでください。

匿名の使用状況情報をシトリックスと共有しない場合は、[匿名の使用状況情報をシトリックスに送信する] チェックボックスをオフにします。シトリックスに送信される情報には、アップデートを要求する仮想マシンの UUID が含まれます。それ以外の仮想マシンに関する情報は収集されず、シトリックスに送信されることもありません。

- [次へ]、[インストール] の順にクリックして Citrix VM Tools インストールプロセスを開始します。
- メッセージが表示されたら、インストールプロセスの完了に必要な操作を実行します。

注:

インストールの一環で仮想マシンが再起動された後に、Citrix VM Tools で、`/quiet /norestart`または`/quiet /forcerestart`を指定して再起動を要求できます。

- ウィザードを終了するには、[完了] をクリックします。

注:

Windows Update からアップデートを受け取ることができる Windows 仮想マシンには、I/O ドライバーが自動的にインストールされます。ただし、Citrix VM Tools パッケージをインストールして管理エージェントをインストールし、サポートされている構成を保持することをお勧めします。

I/O ドライバーと管理エージェントを多数の Windows 仮想マシンにインストールする場合、適切な MSI インストールツールを使用して、`managementagentx86.msi`または`managementagentx64.msi`をインストールします。これらのファイルは Citrix VM Tools ISO に収録されています。

RDP を介して Citrix VM Tools または管理エージェントをインストールすると、再起動のプロンプトが表示されない場合があります。これは、再起動のプロンプトが Windows コンソールセッションでのみ表示されるためです。仮想マシンを再起動し（必要な場合）、仮想マシンを最適化された状態にするために、RDP で強制再起動オプションを指定します。仮想マシンを最適化された状態にするために必要な場合のみ、強制再起動オプションによって仮想マシンが再起動されます。

サイレントインストール

Citrix VM Tools をサイレントインストールしてシステムが再起動されないようにするには、次のいずれかのコマンドを実行します：

```
1 Msiexec.exe /package managementagentx86.msi /quiet /norestart
2 Msiexec.exe /package managementagentx64.msi /quiet /norestart
```

または

```
1 Setup.exe /quiet /norestart
```

非インタラクティブで、サイレントインストールしない場合は、次を実行します。

```
1 Msiexec.exe managementagentx86.msi /passive
2 Msiexec.exe managementagentx64.msi /passive
```

または

```
1 Setup.exe /passive
```

インタラクティブで、サイレントおよびパッシブインストールを行う場合は、次のシステム再起動の後、Citrix VM Tools が完全にインストールされるまでに、何回か自動的に再起動される場合があります。/norestartフラグを指定してインストールした場合もこの動作になります。ただし、/norestartフラグを指定したインストールでは、最初の再起動は手動の場合があります。

Citrix VM Tools は、デフォルトで仮想マシンのC:\Program Files\Citrix\XenToolsにインストールされます。

注：

- Windows 仮想マシンに Citrix VM Tools をインストールするには、その仮想マシン上で Microsoft .NET Framework Version 4.0 またはそれ以降が実行されている必要があります。
- /quietパラメーターはインストールダイアログのみに適用され、デバイスドライバーのインストールには適用されません。/quietパラメーターが指定されている場合、デバイスドライバーのインストールで、必要に応じて再起動権限が要求されます。
 - /quiet /norestartが指定されている場合、すべてのツールのインストールが完了した後、システムは再起動されません。この動作は、再起動ダイアログボックスで指定した内容とは関係ありません。
 - /quiet /forcerestartが指定されている場合、すべてのツールのインストールが完了した後、システムは再起動されます。この動作は、再起動ダイアログボックスで指定した内容とは関係ありません。
 - デバイスドライバーのインストールで再起動権限が要求された場合は、quietパラメーターが指定されたツールのインストールがまだ進行中です。タスクマネージャーを使用して、インストーラー

が実行中かどうかを確認できます。

警告:

Citrix VM Tools をインストールまたはアップグレードすると、一部のネットワークアダプターのフレンドリ名と識別子が変更されてしまう場合があります。特定のアダプタを使用するように設定したソフトウェアは、Citrix VM Tools のインストールまたはアップグレードの後で再設定が必要になる場合があります。

CLI による **Windows** 仮想マシンの作成

xe CLI を使用して **ISO** リポジトリから **Windows** 仮想マシンを作成するには:

1. 次のコマンドを実行して、テンプレートから仮想マシンをインストールします。

```
1 xe vm-install new-name=label=vm_name template=template_name
```

これにより、新しい仮想マシンの UUID が返されます。

2. 次のコマンドを実行して、ISO ストレージリポジトリを作成します。

```
1 xe-mount-iso-sr path_to_iso_sr
```

3. 次のコマンドを実行して、使用可能な ISO のリストを出力します。

```
1 xe cd-list
```

4. 次のコマンドを実行して、仮想マシンの仮想 CD ドライブに ISO を挿入します。

```
1 xe vm-cd-add vm=vm_name cd-name=iso_name device=3
```

5. 次のコマンドを実行して、仮想マシンを起動してオペレーティングシステムをインストールします。

```
1 xe vm-start vm=vm_name
```

この時点で、XenCenter に仮想マシンのコンソール画面が表示されます。

CLI の使用について詳しくは、「[コマンドラインインターフェイス](#)」を参照してください。

Windows オペレーティングシステムの更新

このセクションでは、オペレーティングシステムが更新された Windows 仮想マシンの更新と Citrix VM Tools の再インストールについて説明します。

通常、Citrix Hypervisor の新しいバージョンに移行する場合、仮想マシンをアップグレードする必要があります。Citrix Hypervisor の新しいバージョンに仮想マシンをアップグレードする場合は、次の制限事項を確認してください。

- ライブマイグレーションを使用して Windows 仮想マシンを移行する前に、各仮想マシンで Citrix VM Tools をアップグレードする必要があります。
- Citrix VM Tools がアップグレードされるまで、Windows 仮想マシンでサスペンド/再開操作はサポートされません。
- Citrix VM Tools がアップグレードされていない Windows 仮想マシンで一部のアンチウイルスアプリケーションおよびファイアウォールアプリケーションを使用すると、仮想マシンがクラッシュすることがあります。

警告:

Windows オペレーティングシステムを更新する前に、Citrix VM Tools をアンインストールしてください。更新時に存在していると、更新は失敗します。

Windows の旧バージョンがインストールされている物理コンピュータを、新しいバージョンの Windows インストールディスクから起動すると、アップグレードのオプションが表示されます。

これと同じ方法で、Windows 仮想マシンのオペレーティングシステムをアップグレードできます。

Citrix VM Tools をアンインストールするには:

1. [スタート] ボタンをクリックし、[コントロールパネル] を選択します。
2. [プログラム] > [プログラムと機能] を選択します。
3. 次の項目を選択します:
 - Citrix Hypervisor Windows Management Agent
4. [アンインストール] を選択します。

この選択により Citrix VM Tools が削除されます。終了すると、メッセージが表示されます。[OK] をクリックしてメッセージボックスを閉じます。

オペレーティングシステムをアップグレードしたら、Windows 仮想マシンの新規インストール後と同じ要領で、Citrix VM Tools を再インストールします。

Citrix VM Tools の再インストール

Citrix VM Tools は、XenCenter から組み込みの `guest-tools.iso` を使用してインストールします。[VM] メニューの [インストール] **Citrix VM Tools** を選択します。このオプションにより、Citrix VM Tools を含む CD イメージが仮想マシンに接続されます。

仮想マシンの CD/DVD ドライブで自動実行が有効になっている場合は、しばらくすると自動的にインストールが開始されます。プロセスによって I/O ドライバーと管理エージェントがインストールされます。要求された場合は仮想マシンを再起動し、仮想マシンが最適化された状態にします。

自動実行が無効になっている場合は、Citrix VM Tools インストーラーによってインストールオプションが表示されます。[インストール] **Citrix VM Tools** をクリックして、インストールを続行します。このオプションにより、仮想マシンの CD/DVD ドライブに Citrix VM Tools ISO (`guest-tools.iso`) がマウントされます。[**setup.exe** の実

行] をクリックして Citrix VM Tools のインストールを開始し、要求された場合は仮想マシンを再起動して仮想マシンが最適化された状態にします。

更新 Citrix VM Tools

Citrix Hypervisor では、Windows 仮想マシンの I/O ドライバー (PV ドライバー) と管理エージェントを自動的にアップデートする、よりシンプルなメカニズムが搭載されています。このメカニズムにより、アップデートが利用可能になると、Hotfix を待たずにアップデートをインストールできます。

XenCenter の [全般] タブの [仮想化の状態] では、仮想マシンが Windows Update からアップデートを受け取ることができるかどうかを指定します。Windows Update から I/O ドライバーのアップデートを受け取るメカニズムは、デフォルトではオンになっています。Windows Update から I/O ドライバーのアップデートを受け取らない場合は、仮想マシンで Windows Update を無効にするか、グループポリシーを指定します。

以下のセクションで、I/O ドライバーおよび管理エージェントの自動アップデートについて説明します。

I/O ドライバーのアップデート

I/O ドライバーのアップデートは、次の場合、Microsoft Windows Update から自動的に入手できます：

- Citrix Hypervisor 8.1 Premium Edition を実行している、または Citrix Virtual Apps and Desktops 使用権により Citrix Hypervisor にアクセスできる。
- Citrix Hypervisor 8.1 と動作する XenCenter を使用して Windows 仮想マシンを作成している

重要：

以前のバージョンの Citrix Hypervisor からインポートされた仮想マシンは、Windows Update から I/O ドライバーを取得することができません。

- 仮想マシンで Windows Update が有効になっている
- 仮想マシンがインターネットにアクセスできる、または WSUS プロキシサーバーに接続できる

注：

Windows Server Core では、I/O ドライバーのインストールまたはアップデートに Windows Update を使用できません。代わりに、Citrix VM Tools ISO のインストーラーを使用します。

注：

ユーザーは、管理エージェントの自動アップデートメカニズムで I/O ドライバーのアップデートを自動的に受信することもできます。この設定は、Citrix VM Tools のインストール中に行うことができます。詳しくは、「インストール Citrix VM Tools」を参照してください。

I/O ドライバーバージョンを確認する

仮想マシンにインストールされている I/O ドライバーのバージョンを確認するには、次の手順に従います。

1. C:\Windows\System32\drivers にアクセスします。
2. 一覧からドライバーを見つけます。
3. ドライバーを右クリックして [プロパティ] を選択し、次に [詳細] を選択します。

[ファイルのバージョン] フィールドには、仮想マシンにインストールされているドライバーのバージョンが表示されます。

管理エージェントのアップデート

Citrix Hypervisor では、新しい Windows 仮想マシンおよび既存の Windows 仮想マシンの両方で、管理エージェントを自動的にアップデートできます。Citrix Hypervisor は、デフォルトで管理エージェントの自動アップデートを許可します。ただし、管理エージェントが自動的に I/O ドライバーをアップデートすることは許可しません。Citrix VM Tools のインストール中、管理エージェントのアップデート設定をカスタマイズできます。管理エージェントの自動アップデートはシームレスに行われ、仮想マシンを再起動しません。仮想マシンの再起動が必要なシナリオでは、必要なアクションをユーザーに通知するメッセージが仮想マシンの [コンソール] タブに表示されます。

次の場合、管理エージェントのアップデートを自動的に取得できます：

- Citrix Hypervisor 8.1 Premium Edition を実行している、または Citrix Virtual Apps and Desktops 使用権により Citrix Hypervisor にアクセスできる。
- Citrix Hypervisor 7.0 以上で発行された Citrix VM Tools がインストール済みである
- Windows 仮想マシンがインターネットにアクセスできる

重要：

Citrix VM Tools のアップデートは、標準の Citrix Hypervisor アップデート (Hotfix) メカニズムからも提供されます。Hotfix には、I/O ドライバーと管理エージェント両方のアップデートが含まれます。Hotfix として提供される Citrix VM Tools をアップデートするためのライセンス制限はありません。

管理エージェントバージョンの確認

仮想マシンにインストールされている管理エージェントのバージョンを確認するには、次の手順に従います。

1. C:\Program Files\Citrix\XenTools にアクセスします。
2. 一覧から XenGuestAgent を右クリックして [プロパティ] を選択し、次に [詳細] を選択します。

[ファイルのバージョン] フィールドには、仮想マシンにインストールされている管理エージェントのバージョンが表示されます。

CLI を使用した自動アップデートの管理

Citrix Hypervisor I/O ドライバーや管理エージェントの自動アップデートの管理にコマンドラインを使用できます。次の表の引数を指定して `setup.exe` または `msiexec.exe` を実行して、I/O ドライバーや管理エージェントを自動でアップデートするかどうかを指定できます。 `setup.exe` または `msiexec.exe` を使用した Citrix VM Tools のインストールの詳細については、「サイレントインストール」を参照してください。

注:

PVS または MCS を使用して管理される仮想マシンでは、Citrix Virtual Desktops VDA が存在し、マシンが非永続であることがレポートされている場合、自動アップデートは自動的にオフになります。

引数	値	説明
ALLOWAUTOUPDATE	YES/NO	管理エージェントの自動アップデートを許可/禁止
ALLOWDRIVERINSTALL	YES/NO	Citrix VM Tools インストーラーによる I/O ドライバーのインストールを許可/禁止
ALLOWDRIVERUPDATE	YES/NO	管理エージェントが自動的に I/O ドライバーをアップデートすることを許可/禁止
IDENTIFYAUTOUPDATE	YES/NO	匿名の使用状況情報を Citrix に送信する自動アップデートメカニズムを許可/禁止

次に例を示します:

```
1 setup.exe /passive /forcerestart ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
2   ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

または

```
1 msiexec.exe /i managementagentx64.msi ALLOWAUTOUPDATE=YES
   ALLOWDRIVERINSTALL=NO \
2   ALLOWDRIVERUPDATE=NO IDENTIFYAUTOUPDATE=YES
```

管理エージェントのアップデートのリダイレクト

Citrix Hypervisor ユーザーが管理エージェントのアップデートを、内部 Web サーバーにリダイレクトしてからインストールできます。このリダイレクトより、アップデートが仮想マシンに自動的にインストールされる前にレビューできます。

管理エージェントのアップデートをリダイレクトするには:

管理エージェントは、アップデートファイルを使用して利用可能な更新に関する情報を取得します。アップデートファイルの名前は、使用する管理エージェントのバージョンによって異なります:

- 管理エージェント 7.1.0.1396 以降の場合。 <https://pvupdates.vmd.citrix.com/updates.json>
- 管理エージェント 7.1.0.1354 以前の場合。 <https://pvupdates.vmd.citrix.com/updates.tsv>

管理エージェントの更新をリダイレクトするには、次の手順を実行します:

1. アップデートファイルをダウンロードします。
2. アップデートファイルで参照されている管理エージェントの MSI ファイルをダウンロードします。
3. MSI ファイルを仮想マシンがアクセスできる内部 Web サーバーにアップロードします。
4. アップデートファイルを更新して、内部 Web サーバーの MSI ファイルをポイントするようにします。
5. アップデートファイルを Web サーバーにアップロードします。

自動アップデートも、仮想マシンごとやプールごとにリダイレクトできます。仮想マシンごとにアップデートをリダイレクトする手順は、以下のとおりです。

1. 仮想マシンで、コマンドプロンプトを管理者として開きます。
2. エラーが発生したコンピューター上で

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_SZ /v update_url /  
d \  
2 url of the update file on the web server
```

プールごとに管理エージェントの自動アップデートをリダイレクトするには、以下のコマンドを実行します。

```
1 xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_url=url  
of the update file on the web server
```

管理エージェントのアップデートの無効化

仮想マシンごとに管理エージェントの自動アップデートを無効にするには:

1. 仮想マシンで、コマンドプロンプトを管理者として開きます。
2. 次のコマンドを実行します。

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools /t REG_DWORD /v  
   DisableAutoUpdate /d 1
```

プールごとに管理エージェントの自動アップデートを無効にするには、以下のコマンドを実行します。

```
1 xe pool-param-set uuid=pooluuid guest-agent-config:auto_update_enabled=  
   false
```

自動 I/O ドライバーのアップデート設定の変更

Citrix VM Tools のインストール中、管理エージェントが自動的に I/O ドライバーをアップデートするのを許可するかどうかを指定できます。Citrix VM Tools のインストールプロセスが完了してからこの設定をアップデートする場合は、次の手順を実行します。

1. 仮想マシンで、コマンドプロンプトを管理者として開きます。
2. 次のコマンドを実行します。

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate /t REG_SZ /v \  
2   InstallDrivers /d YES/NO
```

匿名の使用状況情報をシトリックスに送信するには:

Citrix VM Tools のインストール中、匿名の使用状況情報を Citrix に送信するかを指定できます。Citrix VM Tools のインストールプロセスが完了してからこの設定をアップデートする場合は、次の手順を実行します。

1. 仮想マシンで、コマンドプロンプトを管理者として開きます。
2. 次のコマンドを実行します。

```
1 reg.exe ADD HKLM\SOFTWARE\Citrix\XenTools\AutoUpdate REG_SZ /v \  
2   IDENTIFYAUTOUPDATE /d YES/NO
```

sysprep を使用した Windows 仮想マシンの複製の準備

Windows 仮想マシンを複製するには、Windows ユーティリティ `sysprep` を使用して仮想マシンを用意する必要があります。

`sysprep` ユーティリティはローカルコンピュータの SID を変更して、各コンピュータの一意性を確保します。`sysprep` バイナリは `C:\Windows\System32\Sysprep` フォルダにあります。

注:

Windows の以前のバージョンでは、`sysprep` バイナリは Windows 製品 CD の `\support\tools\`

`deploy.cab`ファイルに含まれています。これらのバイナリは、使用する前に Windows 仮想マシンにコピーする必要があります。

Windows 仮想マシンを複製するには:

1. 必要に応じて、Windows 仮想マシンの作成、インストール、設定を行います。
2. 適切なサービスパックをすべて適用し、アップデートします。
3. Citrix VM Tools をインストールします。
4. アプリケーションをインストールし、必要な設定を行います。
5. `sysprep`を実行します。処理が完了すると、仮想マシンがシャットダウンします。
6. XenCenter で、仮想マシンをテンプレートに変換します。
7. 作成したテンプレートを、新しい仮想マシンとして複製します。
8. 複製された仮想マシンを起動すると、使用可能になる前に、以下のアクションが実行されます:
 - 新しい SID と名前を取得する
 - 必要に応じて、ミニセットアップを実行して構成値を取得する
 - 最後に、再起動する

注:

この `sysprep` ステージの後に、元の `sysprep` された仮想マシン（「ソース」仮想マシン）を再起動しないでください。その後テンプレートに即時変換して、再起動しないようにしてください。ソース仮想マシンを再起動した場合は、その仮想マシンで再度 `sysprep` を実行してからテンプレートに変換し、その後で複製を行ってください。

`sysprep` の使用方法について詳しくは、Microsoft 社の以下の Web サイトを参照してください:

- [Windows 自動インストールキット \(AIK\)](#)

Windows 仮想マシンのリリースノート

Citrix Hypervisor が提供する機能に対するサポートが、Windows のバージョンやバリエーションにより異なる場合があります。ここでは、既知の差異に関する注記や不具合について説明します。

一般的な Windows の問題

- Windows 仮想マシンをインストールする場合、設定する仮想ドライブは 3 つ以下にしてください。4 つ目以降の仮想ドライブは、仮想マシンおよび Citrix VM Tools をインストールした後で追加できます。また、Citrix VM Tools がなくても仮想マシンが起動するように、最初の 3 つのディスクのいずれかを起動デバイスに設定します。

- Windows 仮想マシンのブートモードが BIOS ブートである場合、Windows はプライマリディスクをマスターブートレコード (MBR) でフォーマットします。MBR を使用すると、ディスクのアドレス指定可能な記憶域は最大 2TiB に制限されます。Windows 仮想マシンで 2TiB を超えるディスクを使用するには、次のいずれかの操作を行います：
 - Windows のバージョンで UEFI ブートがサポートされている場合は、Windows 仮想マシンのブートモードとして UEFI を使用してください。
 - 大容量ディスクは仮想マシンのセカンダリディスクとして作成し、GUID パーティションテーブル (GPT) 形式を選択します。
- 複数の仮想 CPU (vCPU) は、Windows 仮想マシンからは CPU ソケットとして表示され、ゲストのオペレーティングシステムのライセンスによる制限を受けます。ゲストの CPU の数は、デバイスマネージャで確認できます。実際に Windows によって使われている CPU の数は、タスクマネージャで確認できます。
- Windows ゲストのディスクは、最初に追加したときと異なる順序で列挙される場合があります。この動作は、I/O ドライバーと Windows プラグアンドプレイサブシステム間のやり取りにより発生します。たとえば、1 番目のディスクが「Disk 1」と表示され、後からホットプラグしたディスクが「Disk 0」、その後のディスクが「Disk 2」という順序で列挙される場合があります。それ以降は、正しい順序で列挙されます。
- VLC Media Player の DirectX バックエンドには、Windows の画面設定が 24 ビットカラーに設定された状態でビデオを再生すると、黄が青で表示される既知の問題があります。OpenGL をバックエンドに使用している VLC は正しく動作します。また、DirectX または OpenGL ベースのビデオプレーヤーも正常に動作します。ゲストが 24 ビットカラーではなく 16 ビットカラーに設定されている場合、この問題は発生しません。
- Windows 仮想マシンの PV Ethernet Adapter では、接続速度が 1Gbps として表示されます。この値はハードコードされており、仮想 NIC が仮想スイッチに接続される仮想環境での速度を適切に示すものではありません。データレートは、広告上でのネットワーク速度よりも高くなる場合があります。

Windows 7

Microsoft 社は、Service Pack 1 がインストールされている Windows 7 の使用のみをサポートします。Citrix Hypervisor でサポートされる Windows 7 の仮想マシンの場合、SP1 以降がインストールされているようにします。

Windows 8

Windows 8 ゲストは今後サポートされません。Windows 8 仮想マシンをインストールすると、Windows 8.1 にアップグレードされます。

Windows Server 2008 R2

Microsoft 社は、Service Pack 1 がインストールされている Windows Server 2008 R2 の使用のみをサポートします。Citrix Hypervisor でサポートされる Windows 2008 R2 の仮想マシンの場合、SP1 以降がインストールされているようにします。

Linux 仮想マシン

March 12, 2020

Linux 仮想マシンを作成するときは、その仮想マシン上で実行するオペレーティングシステムに応じて適切なテンプレートを使用します。オペレーティングシステムに提供される Citrix Hypervisor のテンプレートだけでなく、独自に作成したものも使用できます。仮想マシンを作成するには、XenCenter または CLI を使用します。ここでは、CLI の使用方法を中心に説明します。

注:

Citrix Hypervisor のインストールでサポートされているよりも新しいマイナーアップデートの RHEL リリースの仮想マシンを作成するには次の手順を実行します:

- サポートされている最新のメディアからインストールする
- `yum update` を使用して仮想マシンを最新状態にする

この作業は、CentOS や Oracle Linux などの RHEL 派生版にも適用されます。

仮想マシンにオペレーティングシステムをインストールしたら、すぐに Citrix VM Tools をインストールすることをお勧めします。詳しくは、「Linux ゲストエージェントのインストール」を参照してください。

Linux 仮想マシンを作成するには、以下の作業を行います。

1. XenCenter または CLI を使用して、適切なオペレーティングシステム用の仮想マシンを作成します。
2. ベンダのインストールメディアからオペレーティングシステムをインストールします。
3. Citrix VM Tools をインストールします (推奨)。
4. 通常の Linux のインストール時と同様に、仮想マシンと VNC で時間およびタイムゾーンを設定します。

Citrix Hypervisor は、多くの Linux ディストリビューションの仮想マシンへのインストールをサポートしています。

警告:

[他のインストールメディア] テンプレートは、サポートされていないオペレーティングシステムの仮想マシンをインストールする上級ユーザーのために用意されています。Citrix Hypervisor は、サポートしているディストリビューションと、付属している標準テンプレートが対応している特定のバージョンでのみその運用性がテストされており [他のインストールメディア] テンプレートでインストールした仮想マシンはサポートされません。

特定の Linux ディストリビューションでの手順については、Linux ディストリビューションのインストールに関する考慮事項を参照してください。

サポートされている Linux ディストリビューション

サポート対象 Linux ディストリビューションの一覧については、「[ゲストオペレーティングシステムのサポート](#)」を参照してください。

その他の Linux ディストリビューションはサポートされていません。ただし、Red Hat Enterprise Linux と同じインストールメカニズム（Fedora Core など）を使用するディストリビューションは、同じテンプレートを使用して正常にインストールされる場合があります。

Linux 仮想マシンの作成

ここでは、物理 CD/DVD またはネットワーク上の ISO イメージを使用した Linux 仮想マシンの作成方法について説明します。

1. 次のコマンドを実行して、適切なテンプレートから仮想マシンをインストールします。新しい仮想マシンの UUID が返されます。

```
1 xe vm-install template=template-name new-name-label=vm-name
```

2. 仮想 CD-ROM を新しい仮想マシンに追加します：

- CD または DVD からインストールする場合、次のコマンドで Citrix Hypervisor サーバーの物理 CD ドライブの名前を取得します：

```
1 xe cd-list
```

これにより、「SCSI 0:0:0:0」などのドライブ名が `name-label` フィールドに表示されます。

この値を `cd-name` パラメーターとして使用します：

```
1 xe vm-cd-add vm=vm_name cd-name="host_cd_drive_name_label" device=3
```

- ネットワーク上の ISO からインストールする場合、`cd-name` パラメーターの値として ISO ライブラリラベルの対象 ISO の名前を使用します：

```
1 xe vm-cd-add vm=vm_name cd-name="iso_name.iso" device=3
```

3. オペレーティングシステムのインストール CD を、Citrix Hypervisor サーバーの CD ドライブに挿入します。
4. XenCenter または SSH ターミナルで仮想マシンのコンソールを開き、オペレーティングシステムのインストール手順に従って操作します。
5. 次のコマンドを実行して、仮想マシンを起動します。次のコマンドを実行して、オペレーティングシステムインストーラーを起動します。

```
1 xe vm-start uuid=UUID
```

6. ゲストユーティリティをインストールし、グラフィカルコンソールを設定します。詳しくは、「Linux ゲストエージェントのインストール」を参照してください。

Linux ゲストエージェントのインストール

サポートされるすべての Linux ディストリビューションはネイティブに準仮想化されており、完全なパフォーマンスを得るために特別なドライバは不要です。ただし、Citrix Hypervisor にゲストエージェントが含まれ、インストールすると、仮想マシンに関する追加情報をホストに提供できるようになります。動的メモリ制御 (DMC: Dynamic Memory Control) を有効にするには、Linux 仮想マシンごとにゲストエージェントをインストールします。

Citrix Hypervisor サーバーをアップグレードする場合、Linux ゲストエージェントも最新状態にしてください。詳しくは、「Linux カーネルとゲストユーティリティのアップデート」を参照してください。

注:

SUSE Linux Enterprise Desktop 15 または SUSE Linux Enterprise Server 15 のゲストにゲストエージェントをインストールする前に、`insserv-compat-0.1-2.15.noarch.rpm` がゲストにインストールされていることを確認してください。

ゲストエージェントをインストールするには:

1. 必要なファイルは、組み込みの `guest-tools.iso` CD イメージ上にあります。また、XenCenter で [VM] > [インストール] **Citrix VM Tools** オプションを選択することもできます。
2. 次のコマンドを実行して、イメージをゲストにマウントします。

```
1 mount -o ro,exec /dev/disk/by-label/Citrix VM Tools /mnt
```

注:

イメージのマウントに失敗した場合は、次のコマンドでイメージを特定できます:

```
1 blkid -t LABEL="Citrix VM Tools"
```

3. ルートユーザーとして次のインストールスクリプトを実行します。

```
1 /mnt/Linux/install.sh
```

4. 次のコマンドを実行して、イメージをゲストからアンマウントします。

```
1 umount /mnt
```

5. カーネルがアップグレードされている場合、または仮想マシンが以前のバージョンからアップグレードされている場合は、ここで仮想マシンを再起動します。

注:

Linux 仮想マシンにマウントする CD-ROM ドライブや ISO イメージは、`/dev/cdrom`ではなく `/dev/xvdd`または `/dev/sdd`のようにデバイスとして表示されます。これは、真の CD-ROM デバイスではなく、通常のデバイスであるためです。XenCenter や CLI で CD を取り出すと、このデバイスは仮想マシンからホットアンプラグされ、表示されなくなります。一方、Windows 仮想マシンでは Linux の場合と異なり、CD は空の状態で仮想マシン内に残ります。

Linux ディストリビューションのインストールに関する考慮事項

以下は、指定した Linux 仮想マシンの作成時に考慮すべき、ベンダー特有の追加設定情報に関する説明です。

すべてのディストリビューションに関する詳細なリリースノートについては、「Linux 仮想マシンのリリースノート」を参照してください。

Red Hat Enterprise Linux* 7.x (32 ビット/64 ビット)

これらのゲスト用の新しいテンプレートは、2GB の RAM を指定します。このサイズは、バージョン 7.4 以降を正しくインストールするための要件です。バージョン 7.0 ~ 7.3 の場合、テンプレートは 2GB の RAM を指定しますが、以前のバージョンの Citrix Hypervisor では、1GB の RAM で十分です。

注:

この情報は、Red Hat と Red Hat 派生版の両方に適用されます。

Apt リポジトリ (Debian)

Linux のインストールが 1 回だけである場合は、Debian ミラーサイトから直接行うことも可能ですが、いくつかの仮想マシンをインストールする場合は、キャッシングプロキシやローカルミラーの使用をお勧めします。次のいずれかのツールを仮想マシン上にインストールできます。

- **Apt-cacher**: パッケージのローカルキャッシュを保持するプロキシサーバーの実装です
- **debmirror**: Debian リポジトリの一部ミラーまたは完全ミラーを作成するためのツールです

Linux 仮想マシンの複製の準備

通常、仮想マシンやコンピュータを複製すると、固有であるべき属性が環境内で重複してしまいます。重複する固有の属性には、IP アドレス、SID、MAC アドレスなどがあります。

Linux 仮想マシンの複製により属性の重複が発生する場合は、Citrix Hypervisor により一部の仮想ハードウェアパラメータが自動的に変更されます。XenCenter を使って仮想マシンを複製すると、XenCenter で MAC アドレスと IP アドレスが自動的に変更されます。これらのインターフェイスが動的に設定される環境では、複製後の仮想マシン

を変更する必要はありません。ただし、これらのインターフェイスが静的に設定されている環境では、重複が生じないようにネットワーク設定を変更する必要があります。

ここでは、カスタマイズすべき設定について説明します。特定の Linux ディストリビューションでの手順については、Linux 仮想マシンのリリースノートを参照してください。

マシン名

複製された仮想マシンは別のコンピュータであるため、ネットワークに新しいコンピュータを追加するときと同様に、そのネットワークドメイン内で固有の名前を持つ必要があります。

IP アドレス

複製された仮想マシンは、所属するネットワークドメイン内で固有の IP アドレスを持つ必要があります。通常、DHCP を使用してアドレスを割り当てる場合、この要件は必要ありません。仮想マシンの起動時に、DHCP サーバーが IP アドレスを割り当てます。複製した仮想マシンが静的な IP アドレスを持つ場合は、仮想マシンの起動前に、ネットワーク上で使用されていない IP アドレスを割り当てる必要があります。

MAC アドレス

以下の状況で、MAC アドレスルールを無効にしておくことをお勧めします：

1. Linux ディストリビューションによっては、複製した仮想マシンの仮想ネットワークインターフェイスの MAC アドレスが、ネットワーク設定ファイルに記録されている場合があります。このような場合でも、XenCenter で仮想マシンを複製すると、新しい仮想マシンに別の MAC アドレスが割り当てられます。このため、ネットワーク設定ファイルに記録されている MAC アドレスを更新しないと、この仮想マシンの初回起動時にネットワークに接続できません。
2. 一部の Linux ディストリビューションでは、各ネットワークインターフェイスの MAC アドレスが `udev` ルールで記憶され、インターフェイスの名前が保持されます。これは、同じ物理 NIC が常に同じ `ethn` インターフェイスにマップされるようにするためであり、リムーバブル NIC を使用する場合（ノートブックなど）に有用です。ただし、この動作は仮想マシンのコンテキストでは問題があります。

たとえば、次のような場合の動作を想定します。

- ```
1 1. Configure two virtual NICs when installing a VM
2 1. Shut down the VM
3 1. Remove the first NIC
```

仮想マシンが再起動すると、XenCenter は 1 つの NIC のみを表示しますが、`eth0` という名称にします。一方、仮想マシンではこの NIC が `udev` ルールにより `eth1` としてマップされます。この結果、仮想マシンがネットワークに接続できなくなります。

仮想マシンで永続的なインターフェイス名を使用する場合は、これらのルールを無効にしてから仮想マシンを複製します。永続的なインターフェイス名をオフにしない場合は、仮想マシン内で通常の手順に従ってネットワークを再設定する必要があります。この場合、XenCenter に表示される情報が実際のインターフェイス名と異なることに注意してください。

## Linux カーネルとゲストユーティリティのアップデート

Linux ゲストユーティリティをアップデートするには、組み込みの `guest-tools.iso` CD イメージから `Linux/install.sh` スクリプトを再実行します（「Linux ゲストエージェントのインストール」を参照）。

yum 対応のディストリビューション（CentOS および RHEL）の場合は、`xe-guest-utilities` により `yum` の設定ファイルがインストールされ、それ以降のアップデートは `yum` による標準的な方法で実行されるようになります。

Debian の場合、`/etc/apt/sources.list` のエントリにより、デフォルトで `apt` コマンドによるアップデートが可能になります。

アップグレード時に必ず `Linux/install.sh` を再実行することをお勧めします。このスクリプトでは、仮想マシンのバージョンが確認され、必要に応じてアップデートされます。

## PV から HVM ゲストへのアップグレード

サポートされていない既存の PV Linux ゲストを、**HVM** モードで動作しているサポート対象バージョンにアップグレードするには、ゲスト内アップグレードを実行します。この時点で、アップグレードされたゲストは PV モードでのみ動作します。ただし、これはサポートされている動作ではなく、既知の問題です。次のスクリプトを実行して、新規にアップグレードされたゲストを、サポートされている HVM モードに変換します。

Citrix Hypervisor サーバーで、ローカルシェルを開いてルートユーザーとしてログオンし、次のコマンドを実行します：

```
1 /opt/xensource/bin/pv2hvm vm_name
```

または

```
1 /opt/xensource/bin/pv2hvm vm_uuid
```

仮想マシンを再起動して処理を完了します。

## Linux 仮想マシンのリリースノート

最近のほとんどの Linux ディストリビューションは Xen 準仮想化を直接サポートしていますが、インストールメカニズムや一部のカーネルの制限が異なります。

## RHEL グラフィカルインストールのサポート

グラフィカルインストールを実行するには、XenCenter で、新規 **VM** ウィザードの指示に従います。[インストールメディア] ページの [高度な **OS** 起動パラメーター] セクションで、パラメーターの一覧に `vnc` を追加します:

```
1 graphical utf8 vnc
```

![新しい仮想マシンウィザードのスクリーンショット。[インストールメディア] ページで値 `graphical utf8 vnc` が [高度な OS 起動パラメーター] フィールドに入力されました。] (</ja-jp/citrix-hypervisor/media/rhel-graphical-network-install.png>)

ここで、新しい仮想マシン用のネットワーク構成を指定して、VNC 通信を有効にする必要があります。新規 VM ウィザードの残りのページの処理を進めます。ウィザードが完了したら、[インフラストラクチャ] ビューで、仮想マシンを選択して、[コンソール] をクリックして仮想マシンのコンソールセッションを表示します。この時点では標準のインストーラーが使用されます。仮想マシンのインストールは、最初はテキストモードで開始されます。また、ネットワーク構成が要求される場合があります。指定したら、[グラフィックコンソールに切り替える] が XenCenter ウィンドウの右上隅に表示されます。

## Red Hat Enterprise Linux 7

仮想マシンを移行または一時停止した後、RHEL 7.x ゲストは再開時にフリーズすることがあります。詳しくは、Red Hat の問題 [1141249](#) を参照してください。

## CentOS 7

CentOS 7.x リリースノートの一覧については、「Red Hat Enterprise Linux 7」を参照してください。

## Oracle Linux 7

Oracle Linux 7.x リリースノートの一覧については、「Red Hat Enterprise Linux 7」を参照してください。

## Scientific Linux 7

Scientific Linux 7.x リリースノートの一覧については、「Red Hat Enterprise Linux 7」を参照してください。

## Debian 10

PXE ネットワークブートを使用して Debian 10 (Buster) をインストールする場合、`console=tty0` をブートパラメーターに追加しないでください。このパラメーターは、インストールプロセスで問題を引き起こす可能性があります。ブートパラメーターでは `console=hvc0` のみを使用してください。

詳しくは、Debian の問題 [944106](#) および [944125](#) を参照してください。

## SUSE Linux Enterprise 12

### SLES ゲストの複製の準備

注:

SLES ゲストの複製を準備するには、次のようにネットワークデバイスのudev構成をクリアしてください:

```
1 cat< /dev/null > /etc/udev/rules.d/30-net_persistent_names.rules
```

SLES ゲストの複製を準備するには:

1. ファイル `/etc/sysconfig/network/config` を開きます。
2. 次の行を変更します:

```
1 FORCE_PERSISTENT_NAMES=yes
```

変更後は以下の通り

```
1 FORCE_PERSISTENT_NAMES=no
```

3. ファイルを保存して、仮想マシンを再起動します。

詳しくは、「Linux 仮想マシンの複製の準備」を参照してください。

## Ubuntu 18.04

Ubuntu 18.04 は、次のタイプのカーネルを提供します:

- 一般公開 (GA) カーネル。ポイントリリースでは更新されません。
- ハードウェアアクセラレーション (HWE) カーネル。ポイントリリースで更新されます。

Ubuntu 18.04 の一部のマイナーバージョン (18.04.2 および 18.04.3 など) は、グラフィカルコンソールの実行時に問題が発生する可能性のある HWE カーネルをデフォルトで使用します。そうした問題を回避するには、これらの Ubuntu 18.04 のマイナーバージョンを GA カーネルで実行するか、グラフィック設定の一部を変更するという選択肢があります。詳しくは、「[CTX265663 - Ubuntu 18.04.2 VMs can fail to boot on Citrix Hypervisor](#)」を参照してください。

## 仮想マシンのメモリ

January 20, 2020

VM を作成すると、一定量のメモリが VM に割り当てられます。Dynamic Memory Control (DMC) を使用して、Citrix Hypervisor 環境の物理メモリの使用率を向上させることができます。DMC は、VM 間のメモリの動的な再割り当てを可能にするメモリ管理機能です。

XenCenter の [メモリ] タブには、メモリの使用状況がグラフで示されます。詳しくは、[XenCenter ドキュメント](#) を参照してください。

動的メモリ制御機能には、以下の特長があります。

- VM を再起動せずにメモリを追加または削除して、ユーザーにシームレスなエクスペリエンスを提供できます。
- ホスト上で追加の仮想マシンを起動できない状況でも、実行中の仮想マシンのメモリ割り当て量が均等に削減されるため、仮想マシンを新たに起動できるようになります。

### 動的メモリ制御 (DMC) とは

Citrix Hypervisor の動的メモリ制御では、実行中の仮想マシンのメモリが自動的に調節されます。この機能では、各仮想マシンに割り当てられたメモリ量を特定の範囲内で増減して、パフォーマンスを維持しながらサーバーあたりの仮想マシン密度を向上させることができます。

DMC が無効な場合、サーバー上に使用可能なメモリがないときに追加の仮想マシンを起動しようとする、メモリ不足によるエラーが発生します。この問題を解決するには、既存の仮想マシンに割り当てたメモリ量を減らして、各仮想マシンを再起動しなければなりません。DMC を使用すると、Citrix Hypervisor で実行中の仮想マシンのメモリ割り当て量が (管理者が設定した範囲内で) 減らされ、メモリが解放されます。Citrix Hypervisor は、サーバー上に使用可能なメモリがない場合でもメモリを解放しようとします。

#### 注:

- 動的メモリ制御は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。
- 動的メモリ制御は、仮想 GPU を持つ仮想マシンではサポートされません。

### 動的メモリ範囲

仮想マシンごとに、管理者は動的メモリ範囲を設定できます。動的メモリ範囲は、仮想マシンを再起動せずに増減できるメモリ量の範囲を指します。管理者は、実行中の仮想マシンについてこのメモリ範囲を調節できます。Citrix Hypervisor では、仮想マシンに割り当てられるメモリ量がこの動的メモリ範囲内で維持されます。そのため、仮想マシンの実行中に調整すると、Citrix Hypervisor が仮想マシンに割り当てられるメモリの量を調整してしまう場合があります。たとえば、動的メモリ範囲の最小値と最大値に同じ値を設定すると、Citrix Hypervisor でその仮想マシンに割り当てられるメモリ量が強制的にその値に変更されます。使用可能なメモリがないサーバー上で追加の仮想マシンの起動が必要になると、実行中のほかの仮想マシンのメモリが解放されます。追加の仮想マシン用に必要なメモリは、実行中の各仮想マシンから、指定されたメモリ範囲内で均等に再割り当てされます。

動的メモリ制御機能では、動的最小メモリ量と動的最大メモリ量を設定して、その仮想マシンの動的メモリ範囲 (DMR: Dynamic Memory Range) を作成します。

- 動的最小メモリ量: その仮想マシンに割り当てるメモリ量の最小値。
- 動的最大メモリ量: その仮想マシンに割り当てるメモリ量の最大値。

たとえば、動的最小メモリ量を 512MB、動的最大メモリ量を 1024MB に設定した場合、この仮想マシンの動的メモリ範囲 (DMR) は 512 ~ 1024MB になり、この範囲内で仮想マシンが動作します。DMC を使用する場合は、Citrix Hypervisor 必ず指定された DMR の範囲内で各仮想マシンにメモリを割り当てるようにしてください。

### 静的メモリ範囲

Citrix Hypervisor でサポートされるオペレーティングシステムの中には、メモリの動的な追加や削除を正しく処理できないものがあります。そのため、Citrix Hypervisor が仮想マシンの再起動時に必要な最大メモリ量を宣言する必要があります。最大メモリ量を宣言することにより、ゲストオペレーティングシステムがページテーブルやほかのメモリ管理構造のサイズをそれに基づいて決めることができます。Citrix Hypervisor でこれを行うには、静的メモリ範囲という概念を使用します。静的メモリ範囲は、仮想マシンの実行中に増減できないメモリ範囲です。仮想マシンによっては、動的メモリ範囲が常に静的メモリ範囲内でなければならないなどの制約を受けます。静的最小メモリ量 (静的メモリ範囲の最小値) には、Citrix Hypervisor 上でそのオペレーティングシステムが動作するために必要な最低限のメモリ量が設定されています。

#### 注:

静的最小メモリ量にはそのオペレーティングシステムに必要な最低限のメモリ量が設定されているため、この値は変更しないことをお勧めします。詳しくは、メモリ制御の制限事項の表を参照してください。

静的最大メモリ量に動的最大メモリ量よりも大きな値を設定すると、仮想マシンを再起動せずに、仮想マシンにより多くのメモリを割り当てることができます。

### 動的メモリ制御の動作

#### 仮想マシンメモリの自動圧縮

- 動的メモリ制御が無効な場合、追加の仮想マシンを起動できない状態のホスト上で仮想マシンを新たに起動しようとする、メモリ不足エラーが発生し、起動に失敗します。
- 動的メモリ制御が有効な場合、Citrix Hypervisor は、実行中の仮想マシンに割り当てられているメモリを動的メモリ範囲内で削減することで、このような状態のホストでメモリを解放しようとしています。それにより、そのホストで実行中のすべての仮想マシンが、動的最小メモリ量と動的最大メモリ量の範囲内で均等に「圧縮」されます。

#### 動的メモリ制御が有効なとき

- ホストで使用可能なメモリ量が十分な場合、実行中のすべての仮想マシンに動的最大メモリ量が割り当てられます。
- ホストで使用可能なメモリ量が不十分な場合、実行中のすべての仮想マシンに動的最小メモリ量が割り当てられます。

動的メモリ制御を設定するときは、十分なメモリが仮想マシンに割り当てられるようにしてください。割り当てられたメモリが十分でないと、仮想マシンで以下の問題が発生する場合があります。

- 動的メモリ制御により割り当てられるメモリが十分でないと、仮想マシンの起動に時間がかかる場合があります。同様に、仮想マシンに割り当てるメモリ量が少なすぎると、起動に時間がかかる場合があります。
- 動的最小メモリ量の設定が低すぎると、仮想マシン起動時のパフォーマンスおよび安定性が低下する場合があります。

### 動的メモリ制御のしくみ

動的メモリ制御では、以下の2つのモードのいずれかで仮想マシンが動作します。

1. ターゲットモード：仮想マシンの動的メモリ範囲を指定します。Citrix Hypervisor は、このターゲットに合致するように仮想マシンのメモリ割り当てを調節します。メモリターゲットの設定は、特に仮想サーバー環境や、仮想マシンに必要なメモリが分かっている場合に使用します。Citrix Hypervisor は、指定されたターゲットに合致するように仮想マシンのメモリ割り当てを調節します。
2. 動的範囲モード：管理者は、仮想マシンの動的メモリ範囲を指定します。Citrix Hypervisor は、その範囲内でターゲットを選択し、そのターゲットに合致するように仮想マシンのメモリ割り当てを調節します。動的範囲の設定は、仮想デスクトップ環境や、実行する仮想マシンの数に応じて Citrix Hypervisor によって動的にメモリを再割り当てする場合に使用します。Citrix Hypervisor は、指定された範囲内でターゲットを選択し、そのターゲットに合致するように仮想マシンのメモリ割り当てを調節します。

#### 注：

これらの動作モードは、実行中の仮想マシンで必要に応じて切り替えることができます。Citrix Hypervisor では、仮想マシンは、特定のメモリサイズを指定するとターゲットモードになり、メモリ範囲を指定すると動的範囲モードになります。

### メモリの制約

Citrix Hypervisor 管理者は、すべてのゲストオペレーティングシステムに対してすべてのメモリ制御操作を使用できます。ただし、Citrix Hypervisor では常に以下の条件を満たしている必要があります。

0 `memory-static-min` `memory-dynamic-min` `memory-dynamic-max` `memory-static-max`

Citrix Hypervisor 仮想マシンのメモリプロパティを設定するときは、上記の条件を満たす任意の値を指定できますが、検証チェックが行われます。この条件に加えて、特定のオペレーティングシステムに適用される制限事項もあります。サポートされるメモリ範囲は、仮想マシン上で動作するオペレーティングシステムにより異なります。Citrix Hypervisor では、これらの制限を超えた値を設定しても、警告は表示されません。ただし、パフォーマンスおよび安定性の問題を避けるため、以下のメモリ制限を超えないように設定してください。サポートされるオペレーティングシステムごとの最小および最大メモリ制限の詳細なガイドラインについては、「[ゲストオペレーティングシステムのサポート](#)」を参照してください。

**警告:**

そのオペレーティングシステムで使用可能な物理メモリの上限を超えるメモリを仮想マシンに割り当てないことを推奨します。オペレーティングシステムがサポートするメモリ量の上限を超えると、その仮想マシンの動作が不安定になる場合があります。

サポートされるすべてのオペレーティングシステムにおいて、動的最小メモリ量は静的最大メモリ量の4分の1以上に設定する必要があります。動的最小メモリ量を下回るメモリを割り当てると、その仮想マシンの動作が不安定になる場合があります。仮想マシンのサイズを慎重に測定して、動的最小メモリ量でもアプリケーションが正しく動作することを確認してください。

**xe CLI コマンドを使用するには**

仮想マシンの静的メモリプロパティを表示する

1. 次のコマンドを実行して、仮想マシンの UUID を確認します。

```
1 xe vm-list
```

2. `uuid` を指定して、コマンド `param-name=memory-static` を実行します。

```
1 xe vm-param-get uuid=uuid param-name=memory-static-{
2 min,max }
```

たとえば、以下は、`ec77` で始まる UUID を持つ仮想マシンの静的最大メモリプロパティを示しています：

```
1 xe vm-param-get uuid= \
2 ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
3 param-name=memory-static-max;
4 268435456
```

この仮想マシンに設定されている静的最大メモリ量は、268,435,456 バイト (256MB) です。

仮想マシンの動的メモリプロパティを表示する

仮想マシンの動的メモリプロパティを表示するには、上記の手順で `param-name=memory-dynamic` コマンドを指定します：

1. 次のコマンドを実行して、仮想マシンの UUID を確認します。

```
1 xe vm-list
```

2. `uuid` を指定して、コマンド `param-name=memory-dynamic` を実行します：

```
1 xe vm-param-get uuid=uuid param-name=memory-dynamic-{
2 min,max }
```

たとえば、以下は、ec77 で始まる UUID を持つ仮想マシンの動的最大メモリプロパティを示しています

```
1 xe vm-param-get uuid= \
2 ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
3 param-name=memory-dynamic-max;
4 134217728
```

この仮想マシンに設定されている動的最大メモリ量は、134,217,728 バイト (128MB) です。

### メモリプロパティを更新する

#### 警告:

静的または動的メモリ量を設定する場合、各パラメータを正確な順序で指定してください。また、以下の条件を満たしている必要があります:

```
0 memory-static-min memory-dynamic-min memory-dynamic-max memory-static-
max
```

仮想マシンの静的メモリ範囲を変更するには、次のコマンドを実行します。

```
1 xe vm-memory-static-range-set uuid=uuid min=value max=value
```

仮想マシンの動的メモリ範囲を変更するには、次のコマンドを実行します。

```
1 xe vm-memory-dynamic-range-set \
2 uuid=uuid min=value \
3 max=value
```

メモリターゲットの設定は、特に仮想サーバー環境や、仮想マシンに必要なメモリが分かっている場合に使用します。Citrix Hypervisor は、指定されたターゲットに合致するように仮想マシンのメモリ割り当てを調節します。次に例を示します:

```
1 xe vm-target-set target=value vm=vm-name
```

仮想マシンのすべてのメモリ制限（静的および動的）を変更するには、次のコマンドを実行します。

```
1 xe vm-memory-limits-set \
2 uuid=uuid \
3 static-min=value \
4 dynamic-min=value \
5 dynamic-max=value static-max=value
```

注:

- 仮想マシンに特定サイズのメモリ量を割り当てるには、動的最大値と動的最小値に同じ値を指定します。
- static-max を超える値を動的メモリに指定することはできません。
- 仮想マシンの静的最大メモリ量を変更するには、仮想マシンをシャットダウンする必要があります。

### 個々のメモリプロパティを更新する

警告:

静的最小メモリ量にはそのオペレーティングシステムに必要な最低限のメモリ量が設定されているため、この値を変更しないことをお勧めします。詳しくは、「メモリの制約」を参照してください。

### 仮想マシンの動的メモリプロパティを変更する

1. 次のコマンドを実行して、仮想マシンの UUID を確認します。

```
1 xe vm-list
```

2. uuid を指定して、コマンド `memory-dynamic-{ min,max } =value` を実行します。

```
1 xe vm-param-set uuid=uuidmemory-dynamic-{
2 min,max }
3 =value
```

次の例では、動的最大値を 128MB に変更しています:

```
1 xe vm-param-set uuid=ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 memory-
 dynamic-max=128MiB
```

## 仮想マシンの移行

December 30, 2019

ライブマイグレーションやストレージライブマイグレーションを使用して仮想マシンを実行したまま移行したり、仮想マシンの仮想ディスクイメージ (VDI) を仮想マシンを停止せずに移動したりすることができます。

### ライブマイグレーションとストレージライブマイグレーション

ここでは、ライブマイグレーションとストレージライブマイグレーションの互換性に関する要件および制限事項について説明します。

### ライブマイグレーション

ライブマイグレーションは、Citrix Hypervisor のすべてのバージョンで使用できます。これは、共有ストレージ上の仮想マシンを、そのストレージを共有するほかのホストに実行したまま移行する機能です。高可用性やローリングプールアップグレード (RPU) などのプール保守機能では、ライブマイグレーションを使用することで、仮想マシンを自動で移動することができます。これらのプール保守機能は、ワークロードの分散、インフラストラクチャの耐障害性、およびサーバーソフトウェアのアップグレード機能を、仮想マシンを停止させることなく提供します。

#### 注:

ストレージを共有できるのは同一プールに属するホストのみです。このため、仮想マシンの移行も同一プール内に限られます。

仮想 GPU および Intel GVT-g は、ライブマイグレーション、ストレージライブマイグレーション、仮想マシンの一時停止には対応していません。ただし、GPU パススルー機能または仮想 GPU を使用した仮想マシンは、適切なリソースを備えたホストから起動できます。NVIDIA vGPU とこれらの機能の互換性について詳しくは、「[グラフィック](#)」を参照してください。

### ストレージライブマイグレーション

#### 注:

- Citrix Virtual Desktops の展開では、ストレージライブマイグレーションを使用しないでください。
- 変更ブロック追跡を有効にした仮想マシンで、ストレージライブマイグレーションを使用することはできません。ストレージライブマイグレーションを実行する前に、変更ブロック追跡を無効にします。
- VDI が GFS2 SR 上にある仮想マシンでは、ストレージライブマイグレーションは使用できません。

ストレージライブマイグレーションでは、ストレージを共有していないホスト間でも仮想マシンを移行できます。つまり、ローカルストレージ上で実行中の仮想マシンを、ほかのプール内のホストに移行することもできます。この機能により、以下のことが可能になります:

- 仮想マシンを Citrix Hypervisor プール間で再配置する (開発環境から実稼働環境に移行するなど)。
- スタンドアロンの Citrix Hypervisor サーバーを、仮想マシンのダウンタイムなしにアップグレードまたはアップデートする。
- Citrix Hypervisor サーバーのハードウェアをアップグレードする。

#### 注:

ホスト間で移行される仮想マシンの状態情報は保持されます。この情報には、仮想マシンを識別するための情報のほか、CPU やネットワークなどのパフォーマンス測定値の履歴が含まれます。

### 互換性に関する要件

ライブマイグレーションまたはストレージライブマイグレーションで仮想マシンを移行する場合、仮想マシンと移行するホストは、以下の互換性に関する要件を満たしている必要があります:

- 移行先のホストで、移行元ホストと同等またはそれ以降のバージョンの Citrix Hypervisor が動作している必要があります。
- 移行する Windows 仮想マシンごとに Citrix VM Tools がインストールされている必要があります。仮想マシンにインストールされた Citrix VM Tools のバージョンは、移行先 Citrix Hypervisor サーバーにインストールされたバージョンと同じである必要があります。
- ストレージライブマイグレーションのみ：移行元ホストと移行先ホストで CPU が異なる場合、移行元 CPU のすべての機能を移行先 CPU がサポートしている必要があります。そのため、たとえば AMD 社製プロセッサのホストから Intel 社製プロセッサのホストに仮想マシンを移行することはほぼ不可能です。
- チェックポイントがある仮想マシンは移行できません。
- ストレージライブマイグレーションのみ：7 つ以上の VDI を持つ仮想マシンは移行できません。
- 移行先のホストで、動的メモリ制御機能が有効な場合も含め、十分な空きメモリ領域が必要です。十分なメモリを割り当てられない場合、移行処理が完了しません。
- ストレージライブマイグレーションのみ：移行先のホストに十分な空きディスク領域が必要です。必要な空き領域は、VDI のサイズの 3 倍です（スナップショットなし）。十分な領域がない場合、移行処理は完了しません。

### 制限事項

ライブマイグレーションおよびストレージライブマイグレーションには、以下の制限事項があります：

- PCI バススルー機能を使用した仮想マシンは移行できません。
- 移行中は、仮想マシンのパフォーマンスは低下します。
- ストレージライブマイグレーションでは、リソースプールの高可用性を無効にしてから仮想マシンを移行する必要があります。
- 仮想マシン移行の完了までの時間は、仮想マシンのメモリフットプリントとそのアクティビティによって異なります。さらに、VDI のサイズとそのストレージアクティビティは、ストレージライブマイグレーションで移行される仮想マシンに影響します。
- IPv6 ベースの Linux 仮想マシンでは、Linux カーネル 3.0 以降が必要です。

### XenCenter を使用した仮想マシンの移行

1. リソースペインで仮想マシンを選択して、次のいずれかを行います。
  - ライブマイグレーションまたはストレージライブマイグレーションを使用して実行中または一時停止中の仮想マシンを移行するには、**[VM]** メニューから、**[移行先サーバー]**、**[VM の移行ウィザード]** の順に選択します。**[VM の移動]** ウィザードが開きます。
  - 停止した仮想マシンを移動するには：**[VM]** メニューで **[VM の移動]** を選択します。**[VM の移動]** ウィザードが開きます。

2. [移行先] 一覧から、スタンドアロンサーバーまたはプールを選択します。
3. [ホームサーバー] 一覧から仮想マシンのホームサーバーを選択して、[次へ] をクリックします。
4. [ストレージ] タブで仮想マシンの仮想ディスクを配置するストレージリポジトリを選択して、[次へ] をクリックします。
  - [すべての仮想ディスクを同一 **SR** 上に移行する] オプションがデフォルトで選択され、移行先プールのデフォルトの共有ストレージリポジトリが表示されます。
  - [仮想ディスクの移行先 **SR** を指定する] をクリックして、[ストレージリポジトリ] 一覧でストレージリポジトリを選択します。このオプションでは、移行する仮想マシンの仮想ディスクごとに異なるストレージリポジトリを選択できます。
5. [ストレージネットワーク] 一覧で、仮想マシンの仮想ディスクのライブマイグレーションで使用される移行先プールのネットワークを選択します。[次へ] をクリックします。

注：  
パフォーマンス上の理由から、管理ネットワークをライブマイグレーションで使用しないことをお勧めします。
6. 選択した内容を確認し、[完了] をクリックして移行を実行します。

## ライブ VDI マイグレーション

ストレージ XenMotion のライブ VDI マイグレーション機能を使用すると、仮想マシンの仮想ディスクイメージ (VDI) を仮想マシンを停止せずに再配置できます。これにより、管理者は以下のタスクを実行できます：

- 安価なローカルストレージに格納されている仮想マシンを、高速で耐障害性の高いストレージアレイに移動する。
- 仮想マシンを開発環境から実務環境に移動する。
- ストレージ容量による制限がある場合に、仮想マシンをストレージ階層間で移動する。
- ストレージアレイをアップグレードする。

## 制限事項

ライブ VDI マイグレーションには、以下の制限事項があります。

- Citrix Virtual Desktops の展開では、ストレージライブマイグレーションを使用しないでください。
- IPv6 ベースの Linux 仮想マシンでは、Linux カーネル 3.0 以降が必要です。
- vGPU を持つ仮想マシンでライブ VDI マイグレーションを実行すると、vGPU ライブマイグレーションが使用されます。仮想 GPU インスタンスのコピーを作成するには、ホストにそのための十分な領域が必要です。物理 GPU がすべて使用されている場合、VDI が移行できない場合があります。

仮想ディスクを移動するには

1. リソースペインで、仮想ディスクが格納されているストレージリポジトリを選択して [ストレージ] タブをクリックします。
2. [仮想ディスク] の一覧で、移動する仮想ディスクを選択して [移動] をクリックします。
3. [仮想ディスクの移動] ダイアログボックスで、移動先のストレージリポジトリを選択します。

注:

一覧には、各ストレージリポジトリの空き容量が表示されます。移動先のストレージリポジトリ上に十分なディスク容量があることを確認してください。

4. [移動] をクリックして仮想ディスクを移動します。

## 仮想マシンのインポートとエクスポート

March 12, 2020

Citrix Hypervisor では、さまざまな形式の仮想マシンをインポートおよびエクスポートできます。XenCenter のインポートウィザードでは、ディスクイメージ (VHD と VMDK)、Open Virtualization Format (OVF と OVA)、および Citrix Hypervisor XVA 形式の仮想マシンをインポートできます。また、VMware 社や Microsoft 社など、ほかの仮想化プラットフォーム上で作成された仮想マシンをインポートすることもできます。

注:

ほかの仮想化プラットフォーム上で作成された仮想マシンをインポートする場合、Citrix Hypervisor 上でゲストオペレーティングシステムが正しく起動するように、オペレーティングシステムを再構成 (修復) します。XenCenter には、仮想マシンの互換性の問題を解決するオペレーティングシステムの修復機能が用意されています。詳しくは、「オペレーティングシステムの修復」を参照してください。

XenCenter のエクスポートウィザードでは、仮想マシンを Open Virtualization Format (OVF と OVA)、および Citrix Hypervisor XVA 形式でエクスポートできます。

OVF/OVA パッケージやディスクイメージのインポートやエクスポートでは、「Transfer VM」という名前の一時的な仮想マシンが使用されます。このため、XenCenter の [インポート] ウィザードおよび [エクスポート] ウィザードでは、Transfer VM のネットワーク設定を行います。詳しくは、「Transfer VM」を参照してください。

xe CLI を使用して、Citrix Hypervisor XVA 形式の仮想マシンのインポートやエクスポートを行うこともできます。

サポートされる形式

| 形式                                     | 説明                                                                                                                                                               |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Open Virtualization Format (OVF と OVA) | OVF は、いくつかの仮想マシンで構成される仮想アプリケーションをパッケージ化および配布するためのオープンスタンダードです。                                                                                                   |
| ディスクイメージ形式 (VHD と VMDK)                | [インポート] ウィザードでは、VHD (Virtual Hard Disk: 仮想ハードディスク) および VMDK (Virtual Machine Disk: 仮想マシンディスク) 形式のディスクイメージファイルをインポートできます。この形式では、OVF メタデータがない仮想ディスクイメージをインポートできます。 |
| Citrix Hypervisor XVA 形式               | XVA は Xen ハイパーバイザー独自の形式で、個々の仮想マシンを記述子とディスクイメージを含んだ単一ファイルアーカイブとしてパッケージ化します。ファイル拡張子は <code>.xva</code> です。                                                         |

#### 各ファイル形式の用途

OVF/OVA 形式のファイルは、以下の用途に使用されます。

- Citrix Hypervisor の vApp および仮想マシンを、OVF をサポートするほかのハイパーバイザーと共有する。
- 複数の仮想マシンを保存する。
- vApp または仮想マシンを破損や改ざんから保護する。
- ライセンス契約書を追加する。
- OVF パッケージを OVA に格納して vApp を配布しやすくする。

XVA 形式のファイルは、以下の用途に使用されます。

- コマンドラインインターフェイスでスクリプトを実行して仮想マシンをインポートまたはエクスポートする。

#### Open Virtualization Format (OVF と OVA)

OVF は、Distributed Management Task Force (DMTF) により策定された、いくつかの仮想マシンで構成される仮想アプリケーションをパッケージ化および配布するためのオープンスタンダードです。OVF 形式および OVA 形式について詳しくは、以下のドキュメントを参照してください:

- Citrix Knowledge Center の CTX122244 [「OVF \(Open Virtualization Format\) の概要」](#)
- [オープン仮想化フォーマットの仕様](#)

注:

OVF/OVA パッケージをインポートまたはエクスポートするには、ルートアカウントまたはプール管理者の役割を持つアカウントでログインする必要があります。

**OVF** パッケージとは、仮想アプライアンスを構成する一連のファイルを指します。この形式のパッケージには、常に記述子ファイルが含まれます。そのほかにも、以下のパッケージ属性を示すファイルが含まれます。

属性

記述子 (**.ovf**): 記述子ファイルにより、その仮想マシンの仮想ハードウェアが定義されます。また、以下の情報が含まれる場合もあります。

- 仮想ディスク、そのパッケージ自体、およびゲストオペレーティングシステムに関する記述
- ライセンス契約書
- アプライアンス内の仮想マシンの起動および停止手順
- パッケージのインストール手順

署名 (**.cert**): X.509 形式の公開キー証明書で使用されるデジタル署名で、パッケージ作成者の同一性を保証します。

マニフェスト (**.mf**): パッケージに含まれているファイルの整合性を検証するために使用されます。パッケージに含まれる各ファイルの SHA-1 ダイジェスト値が含まれています。

仮想ディスク: OVF は、ディスクイメージの形式についての仕様ではありません。AOVF パッケージには仮想ディスクを構成するファイルが含まれますが、その形式は仮想ディスクをエクスポートした仮想化製品により異なります。Citrix Hypervisor で作成する OVF パッケージでは、Dynamic VHD 形式のディスクイメージが使用されます。VMware 製品や Virtual Box の OVF パッケージでは、ストリーム最適化の VMDK 形式が使用されます。

OVF パッケージは、圧縮、アーカイブ化、ライセンス契約書の添付、注釈などの機能に関するその他の非メタデータもサポートします。

注:

圧縮された OVF パッケージや圧縮ファイルを含む OVF パッケージをインポートする場合、Citrix Hypervisor サーバー上に圧縮ファイルを展開するためのディスク領域が必要です。

**OVA (Open Virtualization Appliance)** パッケージは、OVF パッケージを構成するファイルを含んだ単一の TAR (Tape Archive) 形式のアーカイブファイルです。

#### **OVF** 形式と **OVA** 形式の用途

OVF パッケージに含まれる一連のファイルは圧縮されていないため、ファイル内の個々のディスクイメージにアクセスするユーザーにとっては便利な形式です。一方、OVA パッケージは、サイズの大きな単体のファイルです。このファイルを圧縮することもできますが、OVF パッケージのように柔軟に個々のファイルにアクセスすることはできません。

このため、Web サイトからのダウンロードで配布する場合など、単一ファイルのパッケージを作成するには OVA 形式を使用します。OVA パッケージは、単一ファイルによる取り扱いの簡便さが重要な場合のみ使用します。この形式のパッケージは、エクスポートおよびインポートに時間がかかります。

### ディスクイメージ形式 (VHD と VMDK)

XenCenter では、VHD (Virtual Hard Disk) および VMDK (Virtual Machine Disk) 形式のディスクイメージファイルをインポートできます。ディスクイメージを単独でエクスポートすることはサポートされていません。

#### 注:

ディスクイメージをインポートするには、ルートアカウントで、またはプール管理者の RBAC の役割を持つアカウントでログインする必要があります。

ディスクイメージ形式では、OVF メタデータがない仮想ディスクイメージをインポートできます。このオプションは、以下の状況で使用することがあります。

- OVF メタデータが読み取り不能なディスクイメージをインポートする場合。
- OVF パッケージで定義されていない仮想ディスクをインポートする場合。
- OVF パッケージの作成をサポートしないプラットフォームから移行する場合 (古いプラットフォームやイメージなど)。
- OVF 情報を持たない VMware アプライアンスをインポートする場合。
- OVF 情報を持たない単独の仮想マシンをインポートする場合。

可能な場合は個々のディスクイメージではなく、OVF メタデータを含んでいるアプライアンスパッケージをインポートすることをお勧めします。OVF メタデータにより、ディスクイメージから仮想マシンを再構成するために必要な情報 (仮想マシンに関連付けられているディスクイメージ数、プロセッサ、ストレージ、ネットワーク、およびメモリ要件など) が提供されます。この情報がない場合、仮想マシンの再構成手順が複雑になるため、インポートエラーが発生しやすくなります。

### XVA 形式

XVA は Citrix Hypervisor 独自の形式で、単一の仮想マシンを記述子とディスクイメージを含んだファイルセットとしてパッケージ化します。ファイル拡張子は `.xva` です。

記述子 (ファイル拡張子 `ova.xml`) により、その仮想マシンの仮想ハードウェアが定義されます。

ディスクイメージ形式は、一連のファイルを含んだディレクトリによって表されます。このディレクトリの名前は、記述子に定義されている参照名に対応しており、ディスクイメージの 1MB ブロックにつき 2 ファイルが作成されます。このファイルの名前には 10 進数のブロック番号が使用され、最初のファイルにはディスクイメージの 1 ブロック分がローバイナリ形式で含まれ、拡張子はありません。2 番目のファイルは、最初のファイルのチェックサムです。仮想マシンが Citrix Hypervisor 8.0 以前からエクスポートされた場合、このファイルの拡張子は `.checksum` です。仮想マシンが Citrix Hypervisor 8.1 以降からエクスポートされた場合、このファイルの拡張子は `.xxhash` です。

### 重要:

Citrix Hypervisor サーバーからエクスポートした仮想マシンを、異なる種類の CPU が動作する Citrix Hypervisor サーバーにインポートすると、仮想マシンが正しく動作しなくなる場合があります。たとえば、インテル®VT 対応 CPU を搭載したホストからエクスポートされた Windows VM は、AMD-VTM CPU を搭載したホストにインポートすると動作しないことがあります。

### オペレーティングシステムの修復

Citrix Hypervisor 以外の仮想化プラットフォーム上で作成されエクスポートされた仮想アプライアンスやディスクイメージを Citrix Hypervisor サーバーにインポートするときに、仮想マシンの再構成が必要になる場合があります。

XenCenter のオペレーティングシステムの修復機能では、Citrix Hypervisor にインポートした仮想マシンの互換性の問題を解決することができます。XenServer 以外のハイパーバイザー上で作成した仮想マシンを OVF/OVA パッケージとディスクイメージからインポートする場合に、この機能を使用します。

オペレーティングシステムの修復処理により、ハイパーバイザー間の差異によるオペレーティングシステムデバイスおよびドライバの問題が解決されます。このプロセスでは、インポートされた仮想マシンによって Citrix Hypervisor 環境でオペレーティングシステムが起動できない可能性があるという起動デバイス関連の問題の修復を試みます。ただし、この機能は、プラットフォーム間の変換を行うものではありません。

### 注:

オペレーティングシステムの修復機能を使用するには、40MB の空き容量を持つ ISO ストレージリポジトリと、256MB の仮想メモリが必要です。

オペレーティングシステムの修復機能は、インポートした仮想マシンの DVD ドライブに挿入された自動起動 ISO イメージ (Fixup ISO) として提供されます。仮想マシンの初回起動時に、この自動起動イメージにより適切な修復が行われ、仮想マシンがシャットダウンされます。同時に起動デバイスの設定がリセットされるため、これ以降は設定されているデバイスの順序に従って仮想マシンが起動します。

インポートしたディスクイメージや OVF/OVA パッケージでオペレーティングシステムの修復機能を使用するには、XenCenter のインポートウィザードの [高度なオプション] ページでこの機能を有効にして、Citrix Hypervisor が使用できる Fixup ISO のコピー先を指定します。

### オペレーティングシステムの修復のしくみ

オペレーティングシステムの修復機能は、最小限の変更で仮想システムが起動可能になるように設計されています。ゲストオペレーティングシステムや移行元ホストのハイパーバイザーによっては、オペレーティングシステムの修復機能を使用した後に、構成の変更やドライバーのインストールなど、さらに操作が必要な場合があります。

オペレーティングシステムの修復処理では、ISO イメージが ISO ストレージリポジトリにコピーされます。この ISO イメージが仮想マシンの DVD ドライブにセットされ、起動デバイスの順序が変更されます。これにより、その仮想

DVD ドライブの ISO イメージから仮想マシンが起動します。仮想マシンが起動すると、ISO 内の環境により仮想マシンの各ディスクがチェックされ、Linux システムであるか Windows システムであるかが特定されます。

Linux システムの場合、GRUB 設定ファイルの場所が特定され、SCSI ディスク起動デバイスへのポインターが IDE ディスクに変更されます。たとえば、GRUB の `/dev/sda1`（最初の SCSI コントローラ上の最初のディスク）というエントリは、`/dev/hda1`（最初の IDE コントローラ上の最初のディスク）に変更されます。

Windows システムの場合は、インストールされている OS のドライバデータベースから汎用の起動デバイスドライバが抽出され、OS に登録されます。この処理は、古いバージョンの Windows オペレーティングシステムで起動デバイスが SCSI と IDE のインターフェイス間で変更される場合は特に重要です。

仮想マシン上に特定の仮想化ツールセットが検出された場合は、パフォーマンスの問題や不要なイベントメッセージを回避するために無効になります。

## Transfer VM

Transfer VM は、仮想ディスクイメージのインポートまたはエクスポート時にものみ実行される、組み込みの仮想マシンです。この仮想マシンにより、仮想ディスクイメージの内容がディスクイメージと Citrix Hypervisor ストレージリポジトリ間で転送されます。

ディスクイメージをインポートまたはエクスポートするたびに、1 つの Transfer VM が実行されます。複数のディスクイメージを持つ仮想アプライアンスをインポートまたはエクスポートする場合でも、同時に転送されるディスクイメージは 1 つのみです。

次の表は、1 つの Transfer VM を実行するための要件です。

|        |                                                                   |
|--------|-------------------------------------------------------------------|
| 仮想 CPU | 1                                                                 |
| 仮想メモリ  | 256MB                                                             |
| ストレージ  | 8MB                                                               |
| ネットワーク | Citrix Hypervisor サーバーから接続可能なネットワーク。静的または動的 IP アドレス（動的 IP アドレス推奨） |

デフォルトでは、転送プロトコルとして iSCSI が使用されます。このため、転送用の仮想マシンには Citrix Hypervisor サーバー上に iSCSI イニシエータが必要です。転送プロトコルとして RawVDI を使用することもできます。

**RawVDI 転送プロトコルを使用するには：**

1. インストール先フォルダーの `XenCenterMain.exe.config` ファイルのバックアップを作成します。
2. テキストエディタを使用して、`XenCenterMain.exe.config` ファイルを開きます。

3. configSectionエレメントに、以下の <sectionGroup> を追加します:

```
1 <sectionGroup name="applicationSettings"
2 type="System.Configuration.ApplicationSettingsGroup, System,
3 Version=2.0.0.0,
4 Culture=neutral, PublicKeyToken=b77a5c561934e089" >
5 <section name="XenOvfTransport.Properties.Settings"
6 type="System.Configuration.ClientSettingsSection, System,
7 Version=2.0.0.0,
8 Culture=neutral, PublicKeyToken=b77a5c561934e089"
9 requirePermission="false"/>
10 </sectionGroup>
```

4. ファイルの末尾に、以下のエレメントを追加します。

```
1 <applicationSettings>
2 <XenOvfTransport.Properties.Settings>
3 <setting name="TransferType" serializeAs="String"> <value>
4 UploadRawVDI</value>
5 </setting>
6 </XenOvfTransport.Properties.Settings>
7 </applicationSettings>
```

5. XenCenterMain.exe.configファイルを保存します。

注:

XenCenter が起動に失敗する場合は、追加した箇所を確認してください。

## 仮想マシンのインポート

仮想マシンのインポートでは、実質的に新しい仮想マシンを作成する場合と同じ手順が必要になります。これらの手順には、ホームサーバーの指定、ストレージやネットワークの設定が含まれます。

XenCenter のインポートウィザードでは OVF/OVA パッケージ、ディスクイメージ、XVA、および XVA Version 1 形式のファイルをインポートできます。また、xe CLI で XVA 形式のファイルもインポートできます。

### OVF/OVA からのインポート

注:

OVF/OVA パッケージをインポートするには、ルートアカウントまたはブール管理者の役割を持つアカウントでログインする必要があります。

XenCenter のインポートウィザードでは、OVF/OVA ファイルとして保存されている仮想マシンを XenServer 環境にインポートできます。XenCenter で仮想マシンを作成するときに必要な手順の多くが、このウィザードでも表示

されます。つまり、作成される仮想マシンのホームサーバー、ストレージ、およびネットワークを指定します。また、インポートに特有なものとして、以下の手順が必要です。

- ほかの仮想化プラットフォーム上で作成された仮想マシンをインポートする場合、その仮想マシンが正しく起動するように、オペレーティングシステムの修復機能を使用します。詳しくは、「オペレーティングシステムの修復」を参照してください。
- インポート処理で使用される一時的な仮想マシン（TransferVM）のネットワークオプションを設定する必要があります。詳しくは、「Transfer VM」を参照してください。

ヒント:

インポート先のホストに、インポートする仮想マシンの実行に必要な RAM が搭載されていることを確認してください。RAM の量が足りないと、インポートに失敗します。この問題の解決について詳しくは、[CTX125120 - Appliance Import Wizard Fails Because of Lack of Memory](#)を参照してください。

XenCenter でインポートした OVF パッケージは、vApp として表示されます。インポートが完了すると、XenCenter リソースペインに新しい仮想マシンが追加され、**[vApp の管理]** ダイアログボックスに vApp が追加されます。

を使用して **OVF/OVA** から仮想マシンをインポートするには:

1. 次のいずれかを実行して、**[インポート]** ウィザードを開きます:
  - リソースペインでプールまたはホストを右クリックして、**[インポート]** を選択します。
  - **[ファイル]** メニューの **[インポート]** を選択します。
2. ウィザードの最初のページで、インポートするファイルを選択して **[次へ]** をクリックします。
3. EULA の内容を確認して、同意します。

インポートするパッケージにライセンス契約書 (EULA) が含まれている場合は、内容を確認して同意し、**[次へ]** をクリックします。パッケージに EULA が含まれていない場合、この手順は不要です。
4. 仮想マシンのインポート先としてプールまたはホストを指定して、必要に応じてホーム Citrix Hypervisor サーバーを指定します。

**[VM のインポート先]** の一覧で、新しい仮想マシンのインポート先プールまたはホストを選択します。

各仮想マシンにホーム Citrix Hypervisor サーバーを指定するには、**[ホームサーバー]** 列でホストを選択します。ホームサーバーを指定しない場合は、**[ホームサーバーを割り当てない]** を選択します。

**[次へ]** をクリックして続行します。

5. インポートする仮想マシンのストレージを設定します。インポートする仮想マシンのディスクイメージの格納先となるストレージリポジトリを選択して、**[次へ]** をクリックします。

インポートするすべての仮想ディスクを同じストレージリポジトリ上に配置する場合は、**[インポートするすべての仮想ディスクをこの SR に配置する]** を選択します。一覧からストレージリポジトリを選択します。

インポートする仮想ディスクをいくつかのストレージリポジトリ上に分けて配置する場合は、**[インポートする各仮想ディスクを以下の SR に配置する]** をクリックして、一覧の **[SR]** 列で配置するストレージリポジトリを選択します。

6. インポートする仮想マシンのネットワークを設定します。インポートする仮想マシンの仮想ネットワークインターフェイスを、インポート先プールのネットワークに割り当てます。ウィザードの一覧に表示されるネットワークおよび MAC アドレスは、エクスポートされた元の仮想マシンのファイル内に定義されています。仮想ネットワークインターフェイスをターゲットネットワークに割り当てるには、[マップするネットワーク] 列のドロップダウンリストでネットワークを選択します。[次へ] をクリックして続行します。
7. セキュリティ設定を指定します。インポートする OVF/OVA パッケージに証明書やマニフェストなどのセキュリティが設定されている場合は、必要な情報を指定して [次へ] をクリックします。

[セキュリティ] ページに表示されるオプションは、インポートする OVF アプライアンスに設定されているセキュリティ機能によって異なります。

- 署名されたアプライアンスでは、[デジタル署名の検証] チェックボックスが表示され、デフォルトでオンになっています。[証明書の表示] をクリックすると、パッケージの署名に使用された証明書が表示されます。証明書を信頼できない場合、ルート証明書または証明書の発行機関がローカルコンピューターで信頼されていないことを示します。署名を検証しない場合は、[デジタル署名の検証] チェックボックスをオフにします。
- マニフェストを含んでいるアプライアンスでは、[マニフェストの検証] チェックボックスが表示されます。パッケージに含まれているファイルの一覧を検証するには、このチェックボックスをオンにします。

デジタル署名が追加されたパッケージで署名を検証すると、マニフェストも自動的に検証されます。このため、[セキュリティ] ページに [マニフェストの検証] チェックボックスは表示されません。

注:

VMware Workstation 7.1.x で作成する OVF ファイルは、マニフェストの検証を行うと、インポートに失敗します。これは、VMware Workstation 7.1 で作成する OVF ファイルに、無効な SHA-1 ハッシュを含んだマニフェストが追加されるためです。この問題を回避するには、マニフェストの検証を行わずにインポートしてください。

8. オペレーティングシステムの修復機能を有効にします。Citrix Hypervisor 以外のハイパーバイザーで作成された仮想マシンを含んでいるパッケージをインポートする場合は、[オペレーティングシステムの修復 (Fixup) を使用する] チェックボックスをオンにして、Citrix Hypervisor からアクセスできるように Fixup ISO のコピー先となる ISO ストレージリポジトリを指定します。この機能について詳しくは、「オペレーティングシステムの修復」を参照してください。

[次へ] をクリックして続行します。

9. Transfer VM のネットワークを構成します。

インポート先のプールまたはホストのネットワークインターフェイスの一覧で、使用するネットワークを選択します。自動または手動でネットワーク設定を構成することを選択します。

- ネットワーク設定 (IP アドレス、サブネットマスク、ゲートウェイなど) を DHCP (Dynamic Host Configuration Protocol) で割り当てる場合は、[ネットワーク設定を DHCP で自動取得する] をクリックします。

- ネットワーク設定を手作業で割り当てる場合は、[以下のネットワーク設定を使用する] を選択してから必要な値を入力します。IP アドレスを入力してください。必要に応じて、サブネットマスクとゲートウェイの設定を行います。

[次へ] をクリックして続行します。

10. 選択した設定内容を確認し、[完了] をクリックしてインポートを実行し、ウィザードを閉じます。

注:

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、インポート処理に時間がかかる場合があります。

処理の進行状況は [XenCenter] ウィンドウの下部のステータスバーおよび [ログ] タブに表示されます。新しくインポートした仮想マシンが利用できるようになると、リソースペインに表示されます。新しい vApp は、[vApp の管理] ダイアログボックスに追加されます。

注:

XenCenter を使って Windows オペレーティングシステムがインストールされた OVF パッケージをインポートした後で、platform パラメータを設定する必要があります。

1. platform パラメータを device\_id=0002 に設定します。次に例を示します:

```
xe vm-param-set uuid=VM uuid platform:device_id=0002
```

2. platform パラメータを viridian=true に設定します。次に例を示します:

```
xe vm-param-set uuid=VM uuid platform:viridian=true
```

## ディスクイメージのインポート

XenCenter のインポートウィザードを使用すると、ディスクイメージをリソースプールや特定のホスト上に仮想マシンとしてインポートできます。XenCenter で仮想マシンを作成するときに必要な手順の多くが、このウィザードでも表示されます。つまり、作成される仮想マシンのホームサーバー、ストレージ、およびネットワークを指定します。

### 要件

- ルートアカウントまたはプール管理者の役割を持つアカウントでログインする必要があります。
- DHCP が Citrix Hypervisor の使用する管理ネットワーク上で動作することを確認します。
- インポートウィザードを実行するサーバー上にローカルストレージが必要です。

**XenCenter** を使用してディスクイメージから仮想マシンをインポートするには:

1. 次のいずれかを実行して、[インポート] ウィザードを開きます:
  - リソースペインでプールまたはホストを右クリックして、[インポート] を選択します。
  - [ファイル] メニューの [インポート] を選択します。

2. ウィザードの最初のページで、インポートするファイルを選択して [次へ] をクリックします。

3. 仮想マシン名を指定し、CPU およびメモリリソースを割り当てます。

インポートするディスクイメージから作成される新しい仮想マシンの名前と、割り当てる CPU の数とメモリの量を指定します。 [次へ] をクリックして続行します。

4. 仮想マシンのインポート先としてプールまたはホストを指定して、必要に応じてホーム Citrix Hypervisor サーバーを指定します。

[VM のインポート先] の一覧で、新しい仮想マシンのインポート先プールまたはホストを選択します。

各仮想マシンにホーム Citrix Hypervisor サーバーを指定するには、[ホームサーバー] 列でホストを選択します。ホームサーバーを指定しない場合は、[ホームサーバーを割り当てない] を選択します。

[次へ] をクリックして続行します。

5. インポートする仮想マシンのストレージを設定します。インポートする仮想マシンのディスクイメージの格納先となるストレージリポジトリを選択して、[次へ] をクリックします。

インポートするすべての仮想ディスクを同じストレージリポジトリ上に配置する場合は、[インポートするすべての仮想ディスクをこの **SR** に配置する] を選択します。一覧からストレージリポジトリを選択します。

インポートする仮想ディスクをいくつかのストレージリポジトリ上に分けて配置する場合は、[インポートする各仮想ディスクを以下の **SR** に配置する] をクリックして、一覧の [SR] 列で配置するストレージリポジトリを選択します。

6. インポートする仮想マシンのネットワークを設定します。インポートする仮想マシンの仮想ネットワークインターフェイスを、インポート先プールのネットワークに割り当てます。ウィザードの一覧に表示されるネットワークおよび MAC アドレスは、エクスポートされた元の仮想マシンのファイル内に定義されています。仮想ネットワークインターフェイスをターゲットネットワークに割り当てるには、[マップするネットワーク] 列のドロップダウンリストでネットワークを選択します。 [次へ] をクリックして続行します。

7. オペレーティングシステムの修復機能を有効にします。Citrix Hypervisor 以外のハイパーバイザーで作成されたディスクイメージをインポートする場合は、[オペレーティングシステムの修復 (Fixup) を使用する] チェックボックスをオンにして、Citrix Hypervisor からアクセスできるように Fixup ISO のコピー先となる ISO ストレージリポジトリを指定します。この機能について詳しくは、「オペレーティングシステムの修復」を参照してください。

[次へ] をクリックして続行します。

8. Transfer VM のネットワークを構成します。

インポート先のプールまたはホストのネットワークインターフェイスの一覧で、使用するネットワークを選択します。自動または手動でネットワーク設定を構成することを選択します。

- ネットワーク設定 (IP アドレス、サブネットマスク、ゲートウェイなど) を DHCP (Dynamic Host Configuration Protocol) で割り当てる場合は、[ネットワーク設定を **DHCP** で自動取得する] をクリックします。

- ネットワーク設定を手作業で割り当てる場合は、[以下のネットワーク設定を使用する] を選択してから必要な値を入力します。IP アドレスを入力してください。必要に応じて、サブネットマスクとゲートウェイの設定を行います。

[次へ] をクリックして続行します。

9. 選択した設定内容を確認し、[完了] をクリックしてインポートを実行し、ウィザードを閉じます。

注:

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、インポート処理に時間がかかる場合があります。

処理の進行状況は [XenCenter] ウィンドウの下部のステータスバーおよび [ログ] タブに表示されます。新しくインポートした仮想マシンが利用できるようになると、リソースペインに表示されます。

注:

XenCenter を使って Windows オペレーティングシステムがインストールされたディスクイメージをインポートした後で、`platform` パラメータを設定する必要があります。設定する値は、ディスクイメージに含まれる Windows のバージョンによって異なります:

- Windows Server 2008 以降のバージョンでは、`platform` パラメータに `device_id=0002` を設定します。次に例を示します:

```
1 xe vm-param-set uuid=VM uuid platform:device_id=0002
```

- それ以外のすべてのバージョンの Windows で、`platform` パラメータに `viridian=true` を設定します。次に例を示します:

```
1 xe vm-param-set uuid=VM uuid platform:viridian=true
```

## XVA からのインポート

ローカルマシン上に XVA 形式 (.xva) としてエクスポート済みの仮想マシン、テンプレート、およびスナップショットをインポートできます。これを行うには、仮想マシンを作成するときの通常の手順に従います: つまり、作成される仮想マシンのホームサーバー、ストレージ、およびネットワークを指定します。

警告:

CPU の種類が異なる別のホストからエクスポートした仮想マシンをインポートしても、正しく実行できない場合があります。たとえば、インテル VT 対応 CPU を搭載したサーバーからエクスポートされた Windows VM は、AMD-VTM CPU を搭載したサーバーにインポートすると動作しないことがあります。

**XenCenter** を使用して **XVA** から仮想マシンをインポートするには:

1. 次のいずれかを実行して、[インポート] ウィザードを開きます:

- リソースペインでプールまたはホストを右クリックして、[インポート] を選択します。
  - [ファイル] メニューの [インポート] を選択します。
2. ウィザードの最初のページで、インポートするファイル (.xvaまたはova.xml) を選択して [次へ] をクリックします。  
[ファイル名] ボックスに URL (http、https、file、またはftp) を入力した場合は、[次へ] をクリックすると、[パッケージのダウンロード] ダイアログボックスが開きます。ここでは、ファイルのダウンロード先となる XenCenter ホスト上のフォルダーを指定します。
  3. インポートした仮想マシンが起動するプールまたはホストを選択し、[次へ] を選択して続行します。
  4. インポートする仮想マシンのディスクイメージの格納先となるストレージリポジトリを選択して、[次へ] をクリックします。
  5. インポートする仮想マシンのネットワークを設定します。インポートする仮想マシンの仮想ネットワークインターフェイスを、インポート先プールのネットワークに割り当てます。ウィザードの一覧に表示されるネットワークおよび MAC アドレスは、エクスポートされた元の仮想マシンのファイル内に定義されています。仮想ネットワークインターフェイスをターゲットネットワークに割り当てるには、[マップするネットワーク] 列のドロップダウンリストでネットワークを選択します。[次へ] をクリックして続行します。
  6. 選択した設定内容を確認し、[完了] をクリックしてインポートを実行し、ウィザードを閉じます。

## 注:

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、インポート処理に時間がかかる場合があります。

処理の進行状況は [XenCenter] ウィンドウの下部のステータスバーおよび [ログ] タブに表示されます。新しくインポートした仮想マシンが利用できるようになると、リソースペインに表示されます。

**xe CLI** を使用して **XVA** ファイルから仮想マシンをインポートするには:

仮想マシンを Citrix Hypervisor サーバーのデフォルトのストレージリポジトリにインポートするには、次のコマンドを実行します:

```
1 xe vm-import -h hostname -u root -pw password \
2 filename=pathname_of_export_file
```

仮想マシンを Citrix Hypervisor サーバーの別のストレージリポジトリにインポートするには、次のようにオプションの `sr-uuid` パラメーターを追加します:

```
1 xe vm-import -h hostname -u root -pw password \
2 filename=pathname_of_export_file sr-uuid=uuid_of_target_sr
```

元の仮想マシンの MAC アドレスを保持するには、次のようにオプションの `preserve` パラメータを `true` に設定します:

```
1 xe vm-import -h hostname -u root -pw password \
2 filename=pathname_of_export_file preserve=true
```

注:

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、インポート処理に時間がかかる場合があります。

処理が完了すると、新規にインポートした仮想マシンの UUID がコマンドプロンプトに表示されます。

## 仮想マシンのエクスポート

XenCenter のエクスポートウィザードでは OVF/OVA パッケージ、および XVA 形式のファイルのエクスポートでき、xe CLI では XVA 形式のファイルのエクスポートできます。

### OVF/OVA としてのエクスポート

XenCenter のエクスポートウィザードでは、いくつかの仮想マシンを OVF または OVA パッケージとしてエクスポートできます。仮想マシンを OVF/OVA パッケージとしてエクスポートすると、各仮想マシンの仮想ハードディスクおよび構成データがエクスポートされます。

注:

OVF/OVA パッケージをエクスポートするには、ルートアカウントまたはプール管理者の役割を持つアカウントでログインする必要があります。

**XenCenter** を使用して仮想マシンを **OVF/OVA** としてエクスポートするには:

1. エクスポートする仮想マシンをシャットダウンまたはサスペンドします。
2. [エクスポート] ウィザードを開きます。これを行うには、リソースペインでエクスポートする仮想マシンを含んでいるプールまたはホストを右クリックし、[エクスポート] を選択します。
3. ウィザードの最初のページ:
  - エクスポートファイルの名前を入力します
  - ファイルを保存するフォルダーを指定します
  - **OVF/OVA** パッケージ (**\*.ovf**、**\*.ova**) を [形式] ボックスの一覧から選択します
  - [次へ] をクリックして続行します。
4. OVF/OVA パッケージに含める仮想マシンを選択して、[次へ] をクリックします。
5. 必要に応じて、既存のライセンス契約書 (EULA: End User Licensing Agreement) ドキュメント (RTF または TXT ファイル) を追加できます。

EULA を追加するには、[追加] をクリックしてファイルを指定します。追加したファイルの内容を確認するには、[EULA ファイル] の一覧でそのファイルを選択して [表示] をクリックします。

EULA では、そのアプライアンスやそれに含まれるアプリケーションの使用許諾項目や条件が提供されます。

複数の EULA を追加できるため、アプライアンスにインストールされているソフトウェアも法的に保護できます。たとえば、アプライアンスに所有権が保護されたオペレーティングシステムをインストールした仮想マシンを含める場合は、そのオペレーティングシステム用の EULA を追加します。追加した EULA はアプライアンスのインポート時に表示され、ユーザーはそれに同意する必要があります。

注:

サポートされていない形式の EULA ファイル (XML やバイナリファイルなど) を追加しようとすると、処理に失敗します。

[次へ] をクリックします。

6. [高度なオプション] ページでは、必要に応じてマニフェストや署名、および出力ファイルに関するオプションを選択し、[次へ] をクリックします。

- a) パッケージのマニフェストを作成するには、[マニフェストの作成] チェックボックスをオンにします。

マニフェストとは、パッケージに含まれるすべてのファイルの一覧 (インベントリ) を提供するファイルです。マニフェストを使用すると、配布するパッケージに含まれているファイルが、そのパッケージの作成時に含まれていたものと同じであることを証明できます。ファイルのインポート時に、チェックサムを使用してパッケージの作成時から変更されていないことを検証します。

- b) デジタル署名をパッケージに追加するには、[OVF パッケージに署名する] チェックボックスをオンにして、証明書に関連付けられた秘密キーのパスワードを指定します。

デジタル署名されたパッケージをインポートするユーザーは、公開キーを使って署名を検証し、そのパッケージ作成者の同一性を確認できます。信頼された機関から取得して、`.pem` ファイルまたは `.pfx` ファイルとしてエクスポートした X.509 証明書を使用します。このファイルには、マニフェストファイルのデジタル署名と、その署名を作成するときに使用した証明書が含まれています。

- c) 選択した仮想マシンを OVA 形式の単一 TAR ファイルとして出力するには、[OVA パッケージ (単一 OVA エクスポートファイル) を作成する] チェックボックスをオンにします。ファイルの形式について詳しくは、Open Virtualization Format を参照してください。

- d) パッケージに含める仮想ハードディスクイメージ (VHD ファイル) を圧縮するには、[OVF ファイルを圧縮する] チェックボックスをオンにします。

OVF パッケージを作成すると、デフォルトでは、エクスポートされた仮想マシンと同じ量のスペースが仮想ハードディスクイメージに割り当てられます。たとえば、26GB が割り当てられた仮想マシンの場合、ハードディスクイメージも 26GB になります。ハードディスクイメージは、実際に必要なディスク領域に関係なくこの領域を使用します。

注:

VHD ファイルを圧縮すると、エクスポート処理にかかる時間が長くなります。また、圧縮された VHD ファイルを含んでいるパッケージをインポートする場合も、インポートウィザードですべて

の VHD イメージを抽出する必要があるため、時間がかかります。

[**OVA** パッケージ (単一 **OVA** エクスポートファイル) を作成する] と [**OVF** ファイルを圧縮する] チェックボックスの両方をオンにすると、圧縮された OVA ファイル (拡張子 **.ova.gz**) としてエクスポートされます。

#### 7. Transfer VM のネットワークを構成します。

インポート先のプールまたはホストのネットワークインターフェイスの一覧で、使用するネットワークを選択します。自動または手動でネットワーク設定を構成することを選択します。

- ネットワーク設定 (IP アドレス、サブネットマスク、ゲートウェイなど) を DHCP (Dynamic Host Configuration Protocol) で割り当てる場合は、[ネットワーク設定を **DHCP** で自動取得する] をクリックします。
- ネットワーク設定を手作業で割り当てる場合は、[以下のネットワーク設定を使用する] を選択してから必要な値を入力します。IP アドレスを入力してください。必要に応じて、サブネットマスクとゲートウェイの設定を行います。

[次へ] をクリックして続行します。

#### 8. エクスポート設定を確認します。

エクスポートしたパッケージを検証するには、[完了時にエクスポートを検証する] チェックボックスをオンにします。[完了] をクリックしてエクスポートを実行し、ウィザードを閉じます。

注:

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、エクスポート処理に時間がかかる場合があります。

処理の進行状況は [XenCenter] ウィンドウの下部のステータスバーおよび [ログ] タブに表示されます。進行中のエクスポートをキャンセルするには、[ログ] タブをクリックしてイベントの一覧からエクスポート処理を選択し、[キャンセル] をクリックします。

#### **XVA** としてのエクスポート

XenCenter のエクスポートウィザードおよび xe CLI では、単一の仮想マシンを XVA ファイルとしてエクスポートできます。仮想マシンのエクスポート先として、すべてのエクスポートファイルを保持するために十分なディスク領域を持つ、Citrix Hypervisor サーバー以外のマシンを使用することをお勧めします。たとえば、XenCenter を実行中のマシンに仮想マシンをエクスポートできます。

警告:

CPU の種類が異なる別のホストからエクスポートした仮想マシンをインポートしても、正しく実行できない場合があります。たとえば、インテル VT 対応 CPU を搭載したサーバーからエクスポートされた Windows VM は、AMD-VTM CPU を搭載したサーバーにインポートすると動作しないことがあります。

**XenCenter** を使用して仮想マシンを **XVA** ファイルとしてエクスポートするには:

1. エクスポートする仮想マシンをシャットダウンまたはサスペンドします。

2. エクスポートウィザードを開きます：これを行うには、リソースペインでエクスポートする仮想マシンを含んでいるプールまたはホストを右クリックし、[エクスポート] を選択します。
3. ウィザードの最初のページ：
  - エクスポートファイルの名前を入力します
  - ファイルを保存するフォルダーを指定します
  - **XVA** ファイル (\*.xva) を [形式] ボックスの一覧から選択します
  - [次へ] をクリックして続行します。
4. エクスポートする仮想マシンが選択されていることを確認して、[次へ] をクリックします。
5. エクスポート設定を確認します。

エクスポートしたパッケージを検証するには、[完了時にエクスポートを検証する] チェックボックスをオンにします。[完了] をクリックしてエクスポートを実行し、ウィザードを閉じます。

注：

仮想マシンのサイズ、およびネットワーク接続の速度と帯域幅によっては、エクスポート処理に時間がかかる場合があります。

処理の進行状況は [XenCenter] ウィンドウの下部のステータスバーおよび [ログ] タブに表示されます。進行中のエクスポートをキャンセルするには、[ログ] タブをクリックしてイベントの一覧からエクスポート処理を選択し、[キャンセル] をクリックします。

**xe CLI** を使用して仮想マシンを **XVA** ファイルとしてエクスポートするには：

1. エクスポートする仮想マシンをシャットダウンします。
2. 次のコマンドを実行して、仮想マシンをエクスポートします。

```
1 xe vm-export -h hostname -u root -pw password vm=vm_name \
2 filename=pathname_of_file
```

注：

仮想マシンのエクスポート先のファイル名には、必ず拡張子 **.xva** を使用してください。この拡張子を付けずにエクスポートしたファイルは、XenCenter でのインポート時に有効な XVA ファイルとして認識されません。

## Bromium Secure Platform

December 30, 2019

Citrix Hypervisor は、Windows 仮想マシン上で Bromium Secure Platform をサポートします。この機能によって、企業が不法侵入から保護され、ユーザーはセキュリティを侵害することなく必要な操作を行うことができます。

注:

サポートされる Bromium の最小バージョンは 4.0.4 です。

この機能を使用することで、以下のことを実行できます:

- 既知および未知の脅威から企業を保護する。
- 脅威の活動をリアルタイムで検出し、監視する。
- 表示される攻撃に反応し、修復方法を確認する。

### 互換性に関する要件と制限事項

Citrix Hypervisor が Bromium をサポートする環境:

- **CPU:** Intel Core i3、i5、i7 v3 (Haswell) 以降 (Intel Virtualization Technology (Intel VT) および Extended Page Tables (EPT) がシステム BIOS で有効になっている)。  
AMD CPU はサポートされません。
- 仮想マシン: Windows 7 SP1 (32 ビットおよび 64 ビット)、Windows 8.1 (64 ビット)、Windows 10 (64 ビット)。
- 仮想マシンリソース: 最低 2 基の仮想 CPU、4GB RAM、32GB の空きディスク容量。

Bromium を実行している仮想マシンの場合、Citrix Hypervisor は以下の機能をサポートせず、使用を妨げます。

- あらゆる形式の VM モーション (ライブマイグレーション、ストレージライブマイグレーションなど)。
- 動的メモリ制御 (DMC: Dynamic Memory Control) の使用。

注:

PCI パススルーおよび仮想 GPU は、入れ子構造の仮想化を有効にした仮想マシンで使用できます。ただし、Citrix ではこのような構成はサポートされていません。

重要:

Bromium Secure Platform は入れ子構造の仮想化のサポートを利用します。この機能は、Bromium Secure Platform でのみ使用できます。入れ子構造の仮想化は、他の使用例ではサポートされません。この機能を使用するには、Citrix Hypervisor Premium Edition を実行するか、Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスする必要があります。

### 構成

Bromium Secure Platform で使用するための Citrix Hypervisor システムを準備するには、次のいずれかを実行します。

1. 各ホストで、次のコマンドをコマンドプロンプトで実行し、ソフトウェア VMCS シャドウを強制的に使用します:

```
1 /opt/xensource/libexec/xen-cmdline --set-xen
 force_software_vmcs_shadow
```

2. ホストを再起動します。
3. 各仮想マシンで、入れ子構造の仮想化のサポートを有効にするには、以下のコマンドを使用します。

```
1 xe vm-list name-label='vm_name' --minimal
2
3 xe vm-param-set uuid=$VM platform:nested-virt=1
```

注:

Citrix Virtual Desktops の場合、入れ子構造の仮想化のゴールドイメージを使用します。

4. 仮想マシンで Bromium Secure Platform をインストールするには、以下のインストール手順に従います。

## コンテナ管理

January 20, 2020

Citrix Hypervisor には、Citrix Hypervisor 上での Docker コンテナの展開を拡張する 2 つの新機能があります。

- CoreOS Linux 仮想マシンのサポートとクラウド構成ドライブの構成
- CoreOS、Debian 8、Ubuntu 14.04、RHEL/CentOS/OEL 7 のコンテナ管理
- Windows Server 2016 Technology Preview 上の Windows Server コンテナのコンテナ管理のプレビュー

CoreOS はミニマリズム Linux ディストリビューションで、Docker アプリケーションをホストするため人気となりました。CoreOS のクラウド構成ドライブにより、さまざまなオペレーティングシステム構成オプションのカスタマイズが可能となります。仮想マシンでコンテナ管理が有効な場合、Citrix Hypervisor は仮想マシンで実行されている任意の Docker コンテナを認識します。

注:

CoreOS ゲストのインストール方法、クラウド構成パラメーターの構成方法、および Docker コンテナの管理方法について詳しくは、[XenCenter ドキュメント](#)を参照してください。

Container Management Supplemental Pack によって、Citrix Hypervisor は次の操作を実行できます:

- 仮想マシンへのクエリ
- クラウド構成ドライブとの相互通信

- アプリケーションコンテナの検出
- XenCenter のインフラストラクチャビューでアプリケーションのコンテナの表示

また XenCenter はコンテナとの相互通信を有効にして、開始、停止、および一時停止操作と、そのほかの監視機能を許可します。詳しくは、「Container Management Supplemental Pack」を参照してください。

## Docker について

Docker は、開発者およびシステム管理者が配布アプリケーションを構築、出荷、および実行するためのオープンプラットフォームです。Docker コンテナは、アプリケーションとその依存関係のみで構成されます。これは、ホストオペレーティングシステムのユーザースペースで分離されたプロセスとして実行され、ほかのコンテナとカーネルおよび基本ファイルシステムを共有します。詳しくは、「<https://www.docker.com/whatisdocker>」を参照してください。

注:

Citrix Hypervisor コンテナ管理機能は Docker 環境を補足しますが、代わりになるものではありません。仮想マシンの個々の Docker Engine インスタンスは、利用可能な多くの Docker 管理ツールの 1 つによって管理できます。

## Container Management Supplemental Pack

Container Management Supplemental Pack では、次のものが提供されます。

監視および可視性: Docker のホスティングに使用されている仮想マシンと、仮想マシン上の実行中のコンテナを確認できるようになります。

診断: 転送されるネットワークポートや発信元の Docker イメージ名などの基本的なコンテナ情報にアクセスできます。この機能は、インフラストラクチャおよびアプリケーションレイヤーに影響を与える可能性がある場所の問題を迅速に調査するのに役立ちます。

パフォーマンス: その仮想マシンで実行されているコンテナの詳細情報を確認できます。オペレーティングシステムから提供される情報に応じて、コンテナで実行されているプロセスおよびアプリケーションと、消費された CPU リソースに関する情報が提供されます。

アプリケーションの制御: XenCenter を使用して、アプリケーションコンテナを開始、停止、および一時停止（オペレーティングシステムでサポートされている場合）して、問題のあるアプリケーションを迅速に終了できます。

注:

Citrix Hypervisor では、XenCenter を使用したサブリメンタルパックのインストールがサポートされています。XenCenter を使用したサブリメンタルパックのインストール方法について詳しくは、[XenCenter ドキュメント](#)を参照してください。xe CLI を使用してインストールする場合は、『[Citrix Hypervisor Supplemental Packs and the DDK Guide](#)』を参照してください。

## XenCenter を使用した Docker コンテナの管理

このセクションでは、XenCenter を使用した CoreOS 仮想マシンの管理について説明します。CoreOS 仮想マシンを管理するには、次の手順を完了します：

1. Citrix Hypervisor 8.1 をホストにインストールまたはアップグレードします。
2. Citrix Hypervisor 8.1 と共に出荷された XenCenter をインストールします。
3. [シトリックス Web サイト](#) から取得できる Container Management Supplemental Pack をインストールします。
4. CoreOS 仮想マシンを作成し、仮想マシンの構成ドライブを含めます。

XenCenter で CoreOS 仮想マシンを作成している場合、新規 **VM** ウィザードにより仮想マシンのクラウド構成パラメーターを指定するよう求められます。構成ドライブは仮想マシンインスタンスにユーザーデータを提供します。Citrix Hypervisor を使って仮想マシン内で実行中のコンテナを管理しようとする場合は、構成ドライブを作成します。

デフォルトでは、XenCenter の [クラウド構成パラメーター] ページにはパラメーターの事前定義セットが含まれています。必要に応じてこれらのパラメーターを変更できます。サポートされている構成パラメーターについては詳しくは、CoreOS のドキュメントを参照してください。

### 警告：

仮想マシンの構成ドライブを作成しないと、コンテナ管理が機能しない場合があります。

5. 仮想マシンに対するコンテナ管理を有効にします。この設定は XenCenter の仮想マシンの [プロパティ] タブでアップデートできます。

### 注：

プール間でコンテナ管理された仮想マシンを移行すると、コンテナ管理は仮想マシンに対する動作を停止します。これは、コンテナ管理がプール固有のキーを使用して実装されているため起こります。コンテナ管理機能を再度有効にするには、仮想マシンの設定でクラウド構成ドライブをアップデートします。

## その他の Linux ゲストでのコンテナの管理

クラウド構成ドライブのデフォルト構成で作成された CoreOS 仮想マシンは、コンテナ管理用に自動的に準備され、機能を有効にするだけで済みます。その他の Linux ゲストは手動で準備できます。この機能は、Debian 8、Ubuntu 14.04、RHEL/CentOS/OEL 7.x の仮想マシンでのみサポートされます。

Linux ゲストを手動で準備するには、次の手順に従います：

1. 仮想マシンに Citrix VM Tools がインストールされ、ネットワークの要件とセキュリティの説明どおりに仮想マシンネットワークが構成されていることを確認します。
2. 仮想マシン内に Docker、Ncat、SSHD をインストールします。

Ubuntu 14.04 の場合：

```
1 apt-get install docker.io nmap openssh-server
```

RHEL/CentOS/OEL 7.x の場合:

```
1 yum install docker nmap openssh-server
```

3. `docker.service` の自動起動を有効にします。

```
1 systemctl enable docker.service
```

4. `docker.service` を起動します。

```
1 systemctl start docker.service
```

コンテナ管理には非ルートユーザーを使用します。Docker へのアクセスを提供するために、ユーザーを「docker」グループに追加します。

5. コンテナ管理用に仮想マシンを準備します。プール内のいずれかのホストのコントロールドメイン (dom0) で次のコマンドを実行します:

```
1 xscontainer-prepare-vm -v vm_uuid -u username
```

ここで、`vm_uuid`は準備する仮想マシンで、`username`はコンテナ管理で管理アクセスに使用する仮想マシンのユーザー名です。

準備スクリプトにより、プロセスがガイドされ、この仮想マシンのコンテナ管理が自動的に有効になります。

注:

プール間でコンテナ管理された仮想マシンを移行すると、コンテナ管理は仮想マシンに対する動作を停止します。これは、コンテナ管理がプール固有のキーを使用して実装されているため起こります。コンテナ管理機能を再度有効にするには、`xscontainer-prepare-vm`コマンドを再実行します。このコマンドの実行後でも、移行前の Citrix Hypervisor プールが仮想マシンにアクセスし続けることがあります。

## Docker コンテナコンソールおよびログへのアクセス

Linux 仮想マシンの場合、XenCenter ではユーザーが Docker コンテナで実行されているアプリケーションを管理し、監視するためにコンテナコンソールにアクセスし、ログを表示することができます。XenCenter を使用してコンテナコンソールとログにアクセスするには、以下の手順に従います。

1. [リソース] ペインでコンテナを選択します。
2. [コンテナの全般プロパティ] で [コンソールの表示] をクリックし、コンテナコンソールを開きます。コンソールログを表示するには、[ログを表示] をクリックします。これにより、XenCenter を実行しているマシンで SSH クライアントが開きます。

3. 確認メッセージが表示されたら、仮想マシンのユーザー名とパスワードを使用して SSH クライアントにログインします。

注:

公開/秘密 SSH キーを構成することで、認証プロセスを自動化できます。詳しくは、以降のセクションを参照してください。

#### 認証プロセスの自動化（オプション）

コンテナコンソールとログにアクセスする場合、仮想マシンのログイン資格情報を入力して SSH 接続を認証する必要があります。ただし、この認証プロセスを自動化して、手動による資格情報の入力を省略できます。自動認証プロセスを構成するには、以下の手順に従います。

1. 公開/秘密キーのペアを生成します。
2. コンテナを実行している仮想マシンのユーザーディレクトリに公開 SSH キーを追加します。
  - CoreOS 仮想マシンで実行されているコンテナの場合、XenCenter の仮想マシンの [全般] タブの [クラウド構成パラメーター] に公開キーを追加します。
  - Ubuntu 14.04、RHEL/CentOS/Oracle Linux 7、Debian 8 で実行されているコンテナの場合、`~/.ssh/authorized_keys` に公開キーを追加します。
3. XenCenter を実行しているマシンの `%userprofile%` ディレクトリに秘密 SSH キーを追加し、キーの名前を `ContainerManagement.ppk` に変更します。

#### Windows Server コンテナの管理

Windows Server コンテナは、Windows Server 2016 ゲストオペレーティングシステムの一部です。これらにより、プロセスが独自の名前空間に分離されて、Windows アプリケーションをカプセル化できます。Citrix Hypervisor コンテナ管理は、Windows Server 2016 ゲストオペレーティングシステムで Windows Server コンテナの監視と管理をサポートします。

注:

TLS サーバー証明書は特定の IP アドレスにバインドされるため、TLS 通信の 1 つまたは複数の静的 IP アドレスを使用して Windows Server 2016 仮想マシンを構成する必要があります。

コンテナ管理用に Windows Server コンテナを準備するには、次の手順に従います。

1. 仮想マシンに Citrix VM Tools がインストールされ、ネットワークの要件とセキュリティの説明どおりに仮想マシンネットワークが構成されていることを確認します。
2. [Microsoft 社のドキュメント](#) の説明に従って、仮想マシン内に Windows Server コンテナのサポートをインストールします。Windows Server コンテナは Hyper-V コンテナではありません。

3. 以下の内容の「daemon.json」という名称のファイルをフォルダー「C:\ProgramData\docker\config」に作成します:

```

1 {
2
3 "hosts": ["tcp://0.0.0.0:2376", "npipe://"],
4 "tlsverify": true,
5 "tlscacert": "C:\ProgramData\docker\certs.d\ca.pem",
6 "tlscert": "C:\ProgramData\docker\certs.d\server-cert.pem",
7 "tlskey": "C:\ProgramData\docker\certs.d\server-key.pem"
8 }
```

4. コンテナ管理用に仮想マシンを準備します。プール内のいずれかのホストのコントロールドメイン (dom0) で次のいずれかのコマンドを実行します:

オプション **1** (単一ユーザー仮想マシンの場合): Citrix Hypervisor を使用して、この仮想マシンの TLS 証明書を作成します。

**重要:**

このオプションは、単一ユーザーのみが仮想マシンにアクセスできる場合にのみ安全です。TLS サーバーとクライアントキーは、仮想 CD を使用して仮想マシンに挿入されます。この情報は、準備中に悪意のあるユーザーによってコピーされる危険があります。

```

1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls --generate-
 certs
```

ここで、*vm-uuid* は準備する仮想マシンです。画面の指示に従って、Windows Server コンテナの準備プロセスを完了します。これには、dom0 および仮想マシンとの相互通信が含まれます。

オプション **2**: 外部で生成された TLS 証明書を使用して Citrix Hypervisor を構成します。

```

1 xscontainer-prepare-vm -v vm_uuid -u root --mode tls \
2 --client-cert client_cert --client-key client_key --ca-cert
 ca_cert
```

ここで、*vm\_uuid* は準備する仮想マシンで、*client\_cert* は TLS クライアント証明書で、*client\_key* は TLS クライアントキーで、*ca\_cert* は CA 証明書です。このオプションは、Docker が仮想マシン内で TLS 用に既に構成されていることを前提としています。

## ネットワークの要件とセキュリティ

**重要:**

コンテナ管理を機能させるために、ネットワークの分離に関するセキュリティ要件を緩和する必要がある場合があります。

仮想化環境の最大限のセキュリティを実現するために、仮想マシンから Citrix Hypervisor の管理ネットワーク (Citrix Hypervisor コントロールドメインを使用) を分離して、管理者がネットワークをパーティション化することをお勧めします。

コンテナ管理を有効にするには、これらの 2 つのネットワーク間のルートが必要ですが、これにより、管理ネットワーク (つまり、dom0) を攻撃する不正な仮想マシンのリスクが増大します。仮想マシンと管理ネットワークの間のトラフィックを許可するリスクを軽減するために、信頼できるソースのみが 2 つのネットワーク間の接続を開始できるようにファイアウォールルールを構成することをお勧めします。

次の場合、この機能を実稼働環境で使用しないでください。

- ここで推奨されるネットワーク構成がリスクプロファイルと一致しない場合
- 特定の使用シナリオで十分にこのルートを確保するために必要なネットワークまたはファイアウォールの専門知識が不足している場合

### ネットワークのパーティション化とファイアウォール

そのほかの仮想マシンと同様に、必要な分離を実現するため、コンテナ管理仮想マシンを Citrix Hypervisor の管理ネットワークに直接接続しないでください。

コンテナ管理を機能させるには、Citrix Hypervisor のコントロールドメイン (dom0) から管理されている仮想マシンに到達する必要があります。Linux ベースのオペレーティングシステムのコンテナを監視するには、ネットワークトポロジおよびファイアウォールが、dom0 からコンテナ管理仮想マシンへのアウトバウンド SSH 接続を許可する必要があります。Windows Server コンテナを監視するには、ネットワークトポロジおよびファイアウォールが、dom0 からコンテナ管理仮想マシンへのアウトバウンド Docker TLS (宛先 TCP ポート 2376) 接続を許可する必要があります。

仮想マシンと管理ネットワークの間のトラフィックを許可するリスクを軽減するために、すべてのトラフィックが外部のステートフルなファイアウォールを通過する必要があります。このファイアウォールは、特定のビジネスおよびセキュリティの要件に従って、専門家が手動で設定および構成する必要があります。

次のセクションで構成例を示します。

ネットワーク間の接続を保護するため、次のようにします。

- Citrix Hypervisor 管理ネットワーク (dom0 など) と仮想マシンネットワーク (コンテナ管理仮想マシンなど) の間のすべての接続を無効化します。

次のように、コンテナ管理を有効化するための例外を追加します。

- Linux ベースのオペレーティングシステムを監視するには、dom0 でコンテナ管理仮想マシンへのアウトバウンド SSH (TCP ポート 22) 接続 (NEW と ESTABLISHED の両方) を許可します。
- Windows Server コンテナを監視するには、dom0 でコンテナ管理仮想マシンへのアウトバウンド Docker TLS (TCP ポート 2376) 接続 (NEW と ESTABLISHED の両方) を許可します。

- dom0 によって開始された (ESTABLISHED) SSH および Docker TLS の接続に対するコンテナ管理仮想マシンの応答を許可します。

### Linux ベースのオペレーティングシステムでの認証

Citrix Hypervisor のコンテナ管理では、コンテナ管理仮想マシンでの認証のために、プール固有の 4096 ビットの秘密/公開 RSA キーペアが使用されます。秘密キーは、Citrix Hypervisor コントロールドメイン (dom0) に格納されます。各公開キーは、クラウド構成ドライブまたは `~user/.ssh/authorized_keys` ファイルを使用して、準備中にコンテナ管理仮想マシンに登録されます。すべての秘密/公開キーペアと同様に、公開キーによってすべてのコンテナ管理仮想マシンにパスワードなしでアクセスできるため、公開キーを安全に保持する必要があります。これには、現在管理されている仮想マシンと過去に管理されていた仮想マシンの両方が含まれます。

Citrix Hypervisor のコンテナ管理では、仮想マシン内で実行されている Citrix VM Tools によって提案された IP アドレスを使用して、コンテナ管理仮想マシンへのアクセスが試行されます。最初の接続後に、Citrix Hypervisor によってコンテナ管理仮想マシンの公開キーが格納され、以降の接続時にキーが一致するかどうかを検証されます。提案された IP を使用してコンテナ管理仮想マシンのみアクセスできることを確認します (IP ソースガードなどの手段を使用)。ネットワークポロジがこれを保証できない場合、管理者が、仮想マシンへの最初の接続時にコンテナ管理で取得した SSH ホストキーを確認することをお勧めします。

このキーには、次のコマンドを使用してアクセスできます:

```
1 xe vm-param-get-uuid=vm_uuid param-name=other-config /
2 param-key=xscntainer-sshhostkey
```

ここで、`vm_uuid` は仮想マシンの UUID です。

### Windows Server コンテナの認証

Citrix Hypervisor では、Windows Server コンテナの監視および制御に SSL または TLS が使用されます。このインスタンスでは、Citrix Hypervisor は SSL/TLS クライアントとして動作し、Windows Server 仮想マシンは SSL/TLS サーバーとして動作します。キーは Dom0 と仮想マシンの両方に格納されます。

#### 重要:

- クライアントキーを使用するとパスワードなしで仮想マシン上の Docker にアクセスできるため、クライアントキーは安全に保管する必要があります。
- サーバーキーによって仮想マシンへの監視接続が認証されるため、サーバーキーを安全に保持する必要があります。

Citrix Hypervisor のコンテナ管理で `-generate-certs` オプションを使用して TLS 証明書とキーが生成されると、特定のプールおよび仮想マシン用に一時的な CA、サーバー、クライアントの証明書が生成されます。証明書では sha256 ハッシュが使用されます。また、証明書は最大で 2×365 日間有効で、その日数が過ぎると準備を繰り返す必要があります。TLS 接続は常に AES128-SHA 暗号を使用して確立されます。

## 注

Citrix Hypervisor コンテナ管理と Docker を使用する場合は、次の点に注意してください。

- コンテナの名前を変更しても、コンテナ管理ビューのアップデートはトリガーされません。また、Ubuntu 14.04 では、XenCenter 外部からコンテナを一時停止または一時停止解除しても、ビューがアップデートされることはありません。つまり、Citrix Hypervisor では、現在の（名前変更/一時停止/一時停止解除された）コンテナの状態が表示されない場合があります。根本的な原因は、ビューが Docker イベント通知によってのみ更新されることです。回避策として、同じ仮想マシン上の無関係なコンテナで操作（開始や停止など）を実行することで、更新をトリガーできます。

## vApp

January 20, 2020

vApp は、関連する複数の仮想マシンを単一の管理対象として論理的にグループ化したものです。vApp が起動されると、vApp に含まれる仮想マシンが、ユーザーが事前定義した順序で起動されます。この機能により、お互いに依存する仮想マシンを自動的に順序付けすることができます。ソフトウェアのアップデート時など、システム全体の再起動が必要な場合に、管理者が依存関係を考慮しながら順番に仮想マシンを起動する必要はありません。vApp に含まれる仮想マシンは同一ホスト上で動作する必要はなく、通常の規則に従ってリソースプール内で移行されます。

vApp 機能は、障害回復の状況で役立ちます。同一のストレージリポジトリにあるすべての仮想マシン、または同じ SLA (Service Level Agreement) に関連するすべての仮想マシンをグループ化できます。

注:

vApp の作成および変更は、XenCenter または xe CLI を使用して行えます。CLI を使用して vApp を操作する方法については、「[コマンドラインインターフェイス](#)」を参照してください。

## XenCenter での vApp の管理

[vApp の管理] ダイアログボックスでは、vApp を作成、削除、変更、起動、シャットダウンしたり、選択したプールで vApp をインポートおよびエクスポートしたりできます。一覧で vApp を選択すると、その vApp に含まれているすべての仮想マシンが詳細ペイン右側に表示されます。

[vApp の管理] を使用して、次の操作を実行できます:

- vApp の名前または説明を変更する
- vApp に仮想マシンを追加する、または vApp から仮想マシンを削除する
- vApp 内の仮想マシンの起動順序を変更する

**vApp** を変更するには:

1. プールを選択して、[プール] メニューの **[vApp の管理]** を選択します。  
また、[リソース] ペインで右クリックして、**[vApp の管理]** を選択することもできます。
2. 一覧で vApp を選択し、[プロパティ] を選択して [プロパティ] ダイアログボックスを開きます。
3. [全般] タブを選択して、vApp の名前または説明を変更します。
4. [仮想マシン] タブを選択して、vApp の仮想マシンを追加または削除します。
5. **[VM 起動シーケンス]** タブを選択して、vApp の各仮想マシンに設定されている起動順序および起動間隔を変更します。
6. **[OK]** をクリックして変更を保存し、[プロパティ] を閉じます。

## vApp の作成

**vApp** で仮想マシンをグループ化するには、次の手順に従います：

1. プールを選択して、[プール] メニューの **[vApp の管理]** を選択します。
2. vApp の名前と、オプションで説明を入力します。[次へ] をクリックします。  
  
どんな名前でも選択できますが、vApp の内容を示す名前を指定すると便利です。XenCenter では複数の vApp に同じ名前を使用することも可能ですが、重複しないわかりやすい名前を指定することをお勧めします。また、スペースを含む名前を引用符で囲む必要はありません。
3. 新しい vApp に追加する仮想マシンを選択します。[次へ] をクリックします。  
  
[検索] フィールドを使用して、名前に特定の文字列が含まれる仮想マシンだけを一覧に表示することもできます。
4. vApp に追加した仮想マシンの起動順序を指定します。[次へ] をクリックします。

| 値             | 説明                                                                                                                       |
|---------------|--------------------------------------------------------------------------------------------------------------------------|
| 起動順序          | vApp に追加した仮想マシンの起動順序を指定します。起動順序の値が 0 (ゼロ) の仮想マシンが最初に起動されます。起動順序の値が 1 の仮想マシンが次に起動されます。その後、起動順序の値が 2 の仮想マシンが起動されるといった具合です。 |
| 次の VM 起動までの間隔 | 仮想マシンを起動した後、仮想マシンの次のグループを起動するまでの起動間隔を起動順序で指定します。次のグループとは、起動順序が後の仮想マシンセットです。                                              |

1. **[vApp の管理]** の最後のページで、vApp 構成オプションを確認できます。[前へ] をクリックして前のペー

ジに戻って設定を変更するか、[完了] をクリックして vApp を作成し、[vApp の管理] を閉じます。

注:

同一リソースプール内の異なるホスト上の仮想マシンをグループ化して vApp を作成することはできませんが、異なるプールの仮想マシンで vApp を作成することはできません。

## vApp の削除

vApp を削除するには、以下の手順に従います:

1. プールを選択して、[プール] メニューの [vApp の管理] を選択します。
2. 削除する vApp を一覧から選択します。[削除] をクリックします。

注:

vApp を削除しても、その vApp に追加されている仮想マシンは削除されません。

## XenCenter を使用した vApp の起動とシャットダウン

vApp を起動またはシャットダウンするには、[プール] メニューから開く [vApp の管理] を使用します。vApp を起動すると、その vApp に含まれているすべての仮想マシンが特定の順番で起動します。仮想マシンごとに指定した起動順序と遅延時間の値により、起動順序が制御されます。これらの値は、vApp の初回作成時に設定できます。これらの値は、[vApp のプロパティ] ダイアログボックスまたは個別の仮想マシンの [プロパティ] ダイアログボックスからいつでも変更できます。

vApp を起動するには:

1. [vApp の管理] を開きます: vApp で仮想マシンが存在するプールを選択して、[プール] メニューの [vApp の管理] を選択します。また、[リソース] ペインで右クリックして、[vApp の管理] を選択することもできます。
2. 一覧で vApp を選択し、[起動] をクリックします。これにより、その vApp に含まれているすべての仮想マシンが起動します。

vApp をシャットダウンするには:

1. [vApp の管理] を開きます: vApp で仮想マシンが存在するプールを選択して、[プール] メニューの [vApp の管理] を選択します。また、[リソース] ペインで右クリックして、[vApp の管理] を選択することもできます。
2. 一覧で vApp を選択し、[シャットダウン] をクリックします。これにより、その vApp に含まれているすべての仮想マシンがシャットダウンします。

すべての仮想マシンでソフトシャットダウンが試行されます。ソフトシャットダウンが不可能な場合、強制シャットダウンが実行されます。

注:

ソフトシャットダウンでは、仮想マシンを通常の方法でシャットダウンします。実行中のプロセスは個別に停止されます。

強制シャットダウンでは、仮想マシンを強制的にシャットダウンします。物理サーバーの電源プラグを抜くのと同等です。実行中のすべてのプロセスが必ずシャットダウンされるとは限りません。この方法で仮想マシンをシャットダウンすると、データを損失する危険があります。ソフトシャットダウンが不可能な場合にのみ、強制シャットダウンを使用してください。

## vApp のインポートとエクスポート

XenCenter では、vApp を OVF/OVA パッケージとしてエクスポートおよびインポートできます。詳しくは、「[仮想マシンのインポートとエクスポート](#)」を参照してください。

vApp をエクスポートするには:

1. **[vApp の管理]** を開きます: [プール] メニューの **[vApp の管理]** を選択します。
2. 一覧から、エクスポートする vApp を選択します。[エクスポート] をクリックします。
3. 「[OVF/OVA としてのエクスポート](#)」の手順に従って操作します。

vApp のエクスポート処理には時間がかかる場合があります。

vApp をインポートするには:

1. **[vApp の管理]** を開きます: [プール] メニューの **[vApp の管理]** を選択します。
2. [インポート] をクリックして、[インポート] ダイアログボックスを開きます。
3. 「[OVF/OVA としてのインポート](#)」の手順に従って操作します。

インポートが完了すると、**[vApp の管理]** の一覧に新しい vApp が表示されます。

## Demo Linux Virtual Appliance

January 20, 2020

Citrix では、CentOS 7.5 ディストリビューションに基づいたデモ用の仮想アプライアンス「Demo Linux Virtual Appliance」を提供しています。

アプライアンスは、単一の xva ファイルとして [Citrix Hypervisor ダウンロード](#) ページからダウンロードできます。

xva ファイルは、XenCenter で簡単にインポートして、完全な機能持つ Linux 仮想マシンを作成できます。追加の設定手順は必要ありません。

Demo Linux Virtual Appliance を使用すると、仮想マシンを迅速かつ簡単に展開できます。このアプライアンスを使用して、ライブマイグレーションのような Citrix Hypervisor の製品機能、動的メモリ制御、高可用性をテストします。Demo Linux Virtual Appliance には Citrix VM Tools がインストールされており、構成済みのネットワークおよびテスト用の Web サーバー機能も含まれています。

**警告:**

Demo Linux Virtual Appliance を業務用途で使用することはできません。

## Demo Linux Virtual Appliance のインポート

1. Demo Linux Virtual Appliance を [Citrix Hypervisor ダウンロード](#) ページからダウンロードします。  
このページにアクセスするには、マイアカウントにアクセスする必要があります。Citrix アカウントは、Citrix ホームページで取得できます。
2. リソースペインでホストまたはプールを右クリックして、[インポート] を選択します。 \*\* インポートウィザードが開きます。
3. [参照] をクリックして、ダウンロードした Demo Linux Virtual Appliance の `xva` ファイルを指定します。
4. [次へ] をクリックします。
5. インポート先の Citrix Hypervisor サーバーまたはプールを選択して、[次へ] をクリックします。
6. 仮想アプライアンスのディスクを作成するストレージリポジトリを選択して、[次へ] をクリックします。
7. [完了] をクリックすると仮想アプライアンスのインポート処理が開始されます。

**注:**

インポートした仮想アプライアンスの初回起動時に、ルートパスワードを設定するための画面が表示されます。次に、仮想マシンの IP アドレスが表示されます。テスト目的には便利なので、IP アドレスを記録してください。

## テストについて

ここでは、Demo Linux Virtual Appliance が正しく設定されているかどうかを確認するためのいくつかのテストについて説明します。

1. 外部ネットワークへの接続についてテストします。

XenCenter のコンソールから、仮想マシンにログインします。次のコマンドを実行して、Google への ping パケットを送信して応答を確認します。

```
1 ping -c 10 google.com
```

インストールされているその他のネットワークツールには、`ifconfig`、`netstat`、`tracert` があります。

2. 仮想アプライアンスの初回起動時に表示された IP アドレスを使用して、ほかのコンピュータからこの仮想マシンに ping パケットを送信できることを確認します。

3. Web サーバーの設定についてテストします。

Web ブラウザーで、仮想マシンの IP アドレスを入力します。「デモンストレーション Linux 仮想マシン」ページが開きます。このページには、仮想マシンにマウントされたディスクのサイズ、場所、および使用状況についての簡単な情報が表示されます。

この Web ページでは、ほかのディスクをマウントすることもできます。

### 「**Demonstration Linux Virtual Machine**」ページでディスクをマウントする

1. XenCenter で、仮想マシンに仮想ディスクを追加します。これを行うには、リソースペインで仮想マシンを選択して、[ストレージ] タブの [追加] をクリックします。

2. 新しい仮想ディスクの名前と、任意で説明を入力します。

3. 新しい仮想ディスクのサイズを入力します。

仮想ディスクを格納するストレージリポジトリに、そのディスクに十分な容量があることを確認する必要があります。

4. 新しい仮想ディスクを格納するストレージリポジトリを選択します。

5. [作成] をクリックします。新しい仮想ディスクが作成され、ダイアログボックスが閉じます。

6. [コンソール] タブをクリックして、通常の方法で仮想ディスクのパーティション作成およびフォーマットを行います。

7. Web ブラウザーで「Demonstration Linux Virtual Machine」ページの表示を更新します。

8. [マウント] をクリックします。これによりディスクがマウントされ、ファイルシステムの情報が表示されます。

仮想ディスクの追加について詳しくは、[XenCenter ドキュメント](#)を参照してください。

## 仮想マシンに関する注意事項

December 30, 2019

ここでは、仮想マシンに関するいくつかの注意事項について説明します。

### 仮想マシンの起動設定

仮想マシン起動時の VDI の動作として、以下の 2 つのモードがあります。

**注:**

仮想マシンの起動設定を変更する場合は、その仮想マシンをシャットダウンしておく必要があります。

**Persist (Citrix Virtual Desktops - プライベートデスクトップモード)**

仮想マシンのデフォルトの起動モードです。このモードの仮想マシンは、VDI が前回シャットダウン時の状態のまま起動します。

仮想デスクトップに対する永続的な変更をユーザーに許可する場合は、このオプションを選択します。このモードを指定するには、仮想マシンをシャットダウンしてから次のコマンドを実行します。

```
1 xe vdi-param-set uuid=vdi_uuid on-boot=persist
```

**Reset (Citrix Virtual Desktops - 共有デスクトップモード)**

このモードで仮想マシンを起動すると、VDI が前回起動時の状態に復元されます。前回の仮想マシンセッション内での変更内容は、すべて削除されます。

仮想デスクトップに対する永続的な変更をユーザーに許可せず、常に標準的なデスクトップを提供する場合は、このオプションを選択します。このモードを指定するには、仮想マシンをシャットダウンしてから次のコマンドを実行します。

```
1 xe vdi-param-set uuid=vdi_uuid on-boot=reset
```

**警告:**

`on-boot=reset`を変更すると、仮想マシンの次回シャットダウン時、起動時、または再起動時に VDI 上の変更内容がすべて破棄されます。

**Citrix Hypervisor サーバーで ISO ライブラリを使用できるようにする**

Citrix Hypervisor サーバーで ISO ライブラリを使用できるようにするには、外部 NFS または SMB/CIFS 共有ディレクトリを作成します。NFS サーバーまたは SMB/CIFS サーバーは、共有ディレクトリへのルートアクセスができるように設定する必要があります。NFS 共有の場合は、NFS サーバーの `/etc/exports` に共有エントリを作成するときに、`no_root_squash` フラグを設定します。

次に、XenCenter を使用して ISO ライブラリに接続するか、ホストコンソールに接続して次のコマンドを実行します。

```
1 xe-mount-iso-sr host:/volume
```

このマウントコマンドには、必要に応じて追加引数を指定することができます。

Windows SMB/CIFS 共有をホストで利用できるようにするには、XenCenter を使用して接続するか、ホストコンソールに接続して次のコマンドを実行します：

```
1 xe-mount-iso-sr unc_path -t cifs -o username=myname/myworkgroup
```

unc\_path 引数のバックスラッシュをスラッシュに置き換えます。次に例を示します：

```
1 xe-mount-iso-sr //server1/myisos -t cifs -o username=johndoe/mydomain
```

共有をマウントすると、その中にある ISO を XenCenter の [インストール元 **ISO** ライブラリまたは **DVD** ドライブ] の一覧から選択できるようになります。CLI コマンドから CD イメージとして指定することもできます。

適切な Windows テンプレートに ISO を添付します。

## Windows 仮想マシンへのリモートデスクトップ接続

次のいずれかの方法で Windows 仮想マシンコンソールを表示できます。どちらもキーボードとマウスを完全にサポートしています。

- XenCenter による表示。XenCenter で表示する標準のグラフィックコンソールでは、Citrix Hypervisor に組み込まれている VNC 技術により仮想マシンコンソールへのリモートアクセスが提供されます。
- Windows リモートデスクトップによる表示。この方法では、RDP (Remote Desktop Protocol) 技術が使用されます。

XenCenter の [コンソール] タブには、[リモートデスクトップに切り替える] ボタンが表示されます。このボタンをクリックすると、XenCenter の標準グラフィックコンソールが無効になり、リモートデスクトップに切り替わります。

仮想マシンのリモートデスクトップ機能が有効になっていない場合、このボタンは使用できません。有効にするには、Citrix VM Tools をインストールします。リモートデスクトップ機能を使用して接続する各仮想マシンで有効にするには、以下の手順を実行する必要があります。

**Windows** 仮想マシンのリモートデスクトップを有効にするには：

1. [スタート] ボタンをクリックし、[コンピューター] を右クリックして [プロパティ] を選択します。[システム] コントロールパネルが開きます。
2. [リモートの設定] をクリックします。管理者のパスワードを入力する画面が開いたら、仮想マシンのセットアップ時に指定したパスワードを入力します。
3. [リモートデスクトップ] の [リモートデスクトップを実行しているコンピューターからの接続を許可する] (Windows 7) をクリックします。

4. この Windows 仮想マシンへの接続を許可する、管理者以外のユーザーを選択するには、[リモートユーザーの選択] ボタンをクリックしてユーザー名を入力します。デフォルトでは、Windows ドメイン上で管理者権限を持つユーザーがリモートデスクトップに接続できます。

これにより、仮想マシンのコンソールにリモートデスクトップで接続できるようになります。詳しくは、Microsoft 社のナレッジベースの「[リモートデスクトップ接続を使用して別のコンピューターに接続する](#)」を参照してください。

注:

スリープ状態または休止状態の仮想マシンには接続できません。リモートのコンピュータでこれらの機能が無効になっていることを確認してください。

## Windows 仮想マシン内での時間の処理

Windows ゲストマシンの場合、当初はコントロールドメインの時計に基づいて初期設定されます。時間は、仮想マシンのライフサイクル操作（サスペンド、再起動など）に応じてアップデートされます。このため、コントロールドメインおよびすべての Windows 仮想マシンで、信頼性の高い NTP サービスを実行することをお勧めします。

手動で仮想マシンの時計をコントロールドメインの時計よりも 2 時間進めて設定すると、その設定は保持されます。仮想マシン内でタイムゾーンのオフセットを使用して、時計を進めて設定できます。この場合、コントロールドメインの時計を（手作業または NTP サービスを使用して）変更すると、仮想マシンの時計も調整されますが、2 時間のオフセットは保持されます。コントロールドメインのタイムゾーンの変更によって、仮想マシンのタイムゾーンやオフセットが影響を受けることはありません。Citrix Hypervisor は仮想マシンのハードウェアクロック設定を使用して、仮想マシンと同期します。Citrix Hypervisor は仮想マシンのシステムクロック設定を使用しません。

仮想マシンのサスペンドや再開操作、ライブマイグレーションを使用する場合、最新の Citrix VM Tools がインストールされていることが重要です。これにより、サスペンド後の再開や異なる物理ホスト上への移行の後で、Citrix VM Tools が時計の同期が必要であることを Windows カーネルに通知します。

注:

Citrix Virtual Desktops 環境で Windows 仮想マシンを実行する場合は、ホストの時計設定のソースが Active Directory (AD) ドメインと同じであることを確認してください。時計の同期に失敗すると、仮想マシンに誤った時間が表示され、Windows PV ドライバーがクラッシュする可能性があります。

## Linux 仮想マシン内での時間の処理

Citrix Hypervisor で定義される動作に加えて、オペレーティングシステムの設定および動作が Linux 仮想マシンの時間の処理動作に影響を与える可能性があります。Linux オペレーティングシステムは定期的にシステムクロックとハードウェアクロックを同期することがあります。または、自身の NTP サービスをデフォルトで使用することがあります。詳しくは、Linux 仮想マシンのオペレーティングシステムのドキュメントを参照してください。

注:

新しい Linux 仮想マシンをインストールしたら、必ずタイムゾーンをデフォルトの UTC からローカルの値に変更してください。各ディストリビューションでの手順については、「[Linux リリースノート](#)」を参照してください。

Linux 仮想マシン内のハードウェアクロックがコントロールドメイン上の時計に同期せず、個別に変更できます。コントロールドメイン上の時計は、仮想マシンの起動後にハードウェアクロックおよびシステムクロックの初期の時間設定で使用されます。

ハードウェアクロックの時間を変更すると、仮想マシンが再起動されても変更は保持されます。

システムクロックの動作は、仮想マシンのオペレーティングシステムに依存します。詳しくは、お使いの仮想マシンのオペレーティングシステムのドキュメントを参照してください。

Citrix Hypervisor で時間処理の動作を変更することはできません。

## BIOS でロックされた **Reseller Option Kit** メディアからの仮想マシンのインストール

次の 2 種類の仮想マシンがあります: BIOS 汎用および BIOS カスタマイズ済み。ホスト上の仮想マシンに、BIOS でロックされた Reseller Option Kit OEM バージョンの Windows をインストールする場合は、その Reseller Option Kit メディアが添付されていたホストから BIOS 文字列をコピーする必要があります。また、上級ユーザーは BIOS 文字列にユーザー定義の値を設定できます。

### BIOS 汎用

汎用の Citrix Hypervisor BIOS 文字列を持つ仮想マシンです。

注:

BIOS 文字列が設定されていない仮想マシンを起動すると、標準的な Citrix Hypervisor BIOS 文字列がコピーされ、BIOS 汎用の仮想マシンになります。

### BIOS カスタマイズ済み

HVM 仮想マシンの場合、BIOS のカスタマイズは次の 2 つの方法を使用できます: コピーホスト BIOS 文字列およびユーザー定義 BIOS 文字列。

#### コピーホスト **BIOS** 文字列

プール内の特定サーバーの BIOS 文字列がコピーされた仮想マシンです。BIOS で特定ホスト用にロックされたメディアをインストールするには、以下の手順に従います。

**XenCenter** での手順:

1. 新規 VM ウィザードで [ホストの **BIOS** 文字列を **VM** にコピーする] チェックボックスをオンにします。

**CLI** での手順:

1. `vm-install copy-bios-strings-from` コマンドを実行します。BIOS 文字列のコピー元ホスト (つまり Reseller Option Kit メディアが添付されていたホスト) の `host-uuid` を指定します。host uuid はホスト UUID、template name はテンプレート名、name of sr はストレージリポジトリ名、name for new VM は新しい仮想マシンの名前です:

```
1 xe vm-install copy-bios-strings-from=host uuid \
2 template=template name sr-name-label=name of sr \
3 new-name-label=name for new VM
```

これにより、新しい仮想マシンの UUID が返されます。

次に例を示します:

```
1 xe vm-install copy-bios-strings-from=46dd2d13-5aee-40b8-ae2c-95786
 ef4 \
2 template="win7sp1" sr-name-label=Local\ storage \
3 new-name-label=newcentos
4 7cd98710-bf56-2045-48b7-e4ae219799db
```

2. BIOS 文字列が仮想マシンに正しくコピーされたかどうかを確認するには、次の `vm-is-bios-customized` コマンドを実行します。

```
1 xe vm-is-bios-customized uuid=VM uuid
```

次に例を示します:

```
1 xe vm-is-bios-customized uuid=7cd98710-bf56-2045-48b7-e4ae219799db
2 This VM is BIOS-customized.
```

注:

この仮想マシンは、BIOS 文字列のコピー元の物理ホスト上で起動されます。

警告:

BIOS でロックされたオペレーティングシステムを使用するには、専用のライセンス契約書に同意する必要があります。

**ユーザー定義 BIOS** 文字列

CLI/API を使用して選択した BIOS 文字列で、カスタム値を設定するオプションがあります。カスタマイズされた BIOS で HVM 仮想マシンにメディアをインストールするには、以下の手順に従います。

**CLI** での手順:

1. `vm-install` コマンド (`copy-bios-strings-from` を除く) を実行します:

```
1 xe vm-install template=template name sr-name-label=name of sr \
2 new-name-label=name for new VM
```

これにより、新しい仮想マシンの UUID が返されます。

次に例を示します:

```
1 xe vm-install template="win7spl" sr-name-label=Local\ storage \
2 new-name-label=newcentos \
3 7cd98710-bf56-2045-48b7-e4ae219799db
```

2. ユーザー定義 BIOS 文字列を設定するには、仮想マシンを初めて起動する前に次のコマンドを実行します:

```
1 xe vm-param-set uuid=VM_UUID bios-strings:bios-vendor=VALUE \
2 bios-strings:bios-version=VALUE bios-strings:system- \
3 manufacturer=VALUE \
4 bios-strings:system-product-name=VALUE bios-strings:system- \
5 version=VALUE \
6 bios-strings:system-serial-number=VALUE bios-strings:enclosure \
7 -asset-tag=VALUE
```

次に例を示します:

```
1 xe vm-param-set uuid=7cd98710-bf56-2045-48b7-e4ae219799db \
2 bios-strings:bios-vendor="vendor name" \
3 bios-strings:bios-version=2.4 \
4 bios-strings:system-manufacturer="manufacturer name" \
5 bios-strings:system-product-name=guest1 \
6 bios-strings:system-version=1.0 \
7 bios-strings:system-serial-number="serial number" \
8 bios-strings:enclosure-asset-tag=abk58hr
```

注:

- 1 - 一度ユーザー定義 BIOS 文字列を単一の CLI/API 呼び出しで設定すると、変更することはできません。 - ユーザー定義 BIOS 文字列を設定するために使用するパラメーターの数を指定できます。

警告:

以下は、お客様の責任の下で行う必要があります:

- 仮想マシンの BIOS で設定される値は必要な EULA および標準を遵守する。
- パラメーターで指定する値がパラメーターが機能していることを確認する。誤ったパラメーターを指定す

ると、起動エラーやメディアのインストールエラーが発生することがあります。

## Windows 仮想マシンへの GPU の割り当て (Citrix Virtual Desktops 用)

Citrix Hypervisor では、Citrix Hypervisor サーバーの物理 GPU を、そのホスト上で実行する Windows 仮想マシンに割り当てることができます。この機能は「GPU パススルー」と呼ばれ、CAD デザイナーなど、高度なグラフィックパフォーマンスを要求するユーザー向けに用意されています。この機能は、Citrix Virtual Desktops でのみ使用できます。

Citrix Hypervisor でサポートされる仮想マシンごとの GPU 数は 1 つのみですが、リソースプール内の全ホストの物理 GPU が自動的に検出され、GPU ごとにグループ化されます。仮想マシンに GPU のグループの 1 つを割り当てると、そのグループの GPU を持つ任意のホスト上でその仮想マシンを起動できるようになります。GPU が割り当てられた仮想マシンでは、のライブマイグレーション、メモリを含んだスナップショット作成、サスペンド/再開などの一部の機能を使用できなくなります。

仮想マシンに GPU を割り当てても、プール内のほかの仮想マシンには影響しません。ただし、GPU が割り当てられた仮想マシンは、「非アジャイル」になります。高可用性が有効なプールで仮想マシンに GPU を割り当てると、この仮想マシンは高可用性の対象外になります。仮想マシンは自動的に移行されなくなります。

GPU パススルー機能は、Windows 仮想マシンでのみ使用できます。この機能を有効にするには、XenCenter または xe CLI を使用します。

### 要件

GPU パススルー機能は、特定のマシンおよび GPU でのみサポートされます。この機能を使用するには、Citrix Hypervisor サーバーで IOMMU チップセット機能 (Intel の VT-d など) が使用可能であり、有効になっている必要があります。GPU パススルー機能を有効にする前に、[ハードウェア互換性リスト \(英語\)](#) を確認してください。

### GPU を仮想マシンに割り当てる前に

GPU を仮想マシンに割り当てる前に、Citrix Hypervisor サーバーに十分な物理 GPU を追加して、そのマシンを再起動する必要があります。ホストが再起動すると、Citrix Hypervisor により自動的に物理 GPU が検出されます。プール内のホストで使用可能なすべての物理 GPU を確認するには、`xe pgpu-list` コマンドを使用します。

各ホストで IOMMU チップセット機能が有効になっていることを確認してください。これを行うには、以下のコマンドを実行します。

```
1 xe host-param-get uuid=uuid_of_host param-name=chipset-info param-key=iommu
```

IOMMU が無効なホストは、**false** で示されます。この場合、その Citrix Hypervisor サーバーでは GPU パススルー機能を使用できません。

**XenCenter** を使用して **Windows** 仮想マシンに **GPU** を割り当てるには:

1. GPU を割り当てる仮想マシンをシャットダウンします。
2. 仮想マシンの [プロパティ] ダイアログボックスを開きます。これを行うには、仮想マシンを右クリックして [プロパティ] を選択します。
3. 仮想マシンに GPU を割り当てます。これを行うには、[GPU] ページで GPU の種類を選択し、[OK] をクリックします。
4. 仮想マシンを起動します。

**xe CLI** を使用して **Windows** 仮想マシンに **GPU** を割り当てるには:

1. `xe vm-shutdown` コマンドを使用して、GPU を割り当てる仮想マシンをシャットダウンします。
2. 次のコマンドを実行して、GPU グループの UUID を確認します。

```
1 xe gpu-group-list
```

このコマンドを実行すると、プール内のすべての GPU グループが表示されます。割り当てる GPU グループの UUID を控えておきます。

3. 次のコマンドを実行して、GPU グループを仮想マシンに割り当てます。

```
1 xe vgpu-create gpu-group-uuid=uuid_of_gpu_group vm-uuid=uuid_of_vm
```

GPU グループが正しく割り当てられたことを確認するには、`xe vgpu-list` コマンドを実行します。

4. `xe vm-start` コマンドを使用して、仮想マシンを起動します。
5. 仮想マシンが起動したら、その仮想マシンにグラフィックカードドライバーをインストールします。

仮想マシンはホスト上のハードウェアに直接アクセスするため、グラフィックカードドライバーをインストールすることは重要です。ドライバの入手については、ハードウェアベンダにお問い合わせください。

注:

GPU パススルー機能を有効にした仮想マシンを、適切な GPU グループの GPU が搭載されていないホスト上で起動しようとすると、Citrix Hypervisor にエラーが表示されます。

**XenCenter** を使用して **Windows** 仮想マシンの **GPU** 割り当てを解除するには:

1. 仮想マシンをシャットダウンします。
2. 仮想マシンの [プロパティ] ダイアログボックスを開きます。これを行うには、仮想マシンを右クリックして [プロパティ] を選択します。
3. 仮想マシンの GPU 割り当てを解除します。これを行うには、[GPU] ページで GPU の種類として [なし] を選択し、[OK] をクリックします。
4. 仮想マシンを起動します。

**xe CLI** を使用して **Windows** 仮想マシンの **GPU** 割り当てを解除するには:

1. `xe vm-shutdown` コマンドを実行して、仮想マシンをシャットダウンします。
2. 次のコマンドを実行して、割り当てられている仮想 GPU の UUID を確認します。

```
1 xe vgpu-list vm-uuid=uuid_of_vm
```

3. 次のコマンドを実行して、仮想マシンの GPU 割り当てを解除します。

```
1 xe vgpu-destroy uuid=uuid_of_vgpu
```

4. `xe vm-start` コマンドを使用して、仮想マシンを起動します。

## ISO イメージの作成

Citrix Hypervisor では、ISO イメージを、Windows 仮想マシンまたは Linux 仮想マシンのインストールメディアおよびデータソースとして使用できます。ここでは、CD/DVD メディアから ISO イメージを作成する方法について説明します。

**Linux** システムで **ISO** を作成するには:

1. CD-ROM または DVD-ROM をドライブに挿入します。ディスクがマウントされていないことを確認します。これを確認するには、次のコマンドを実行します。

```
1 mount
```

ディスクがマウントされている場合は、アンマウントします。手順については、使用するオペレーティングシステムのドキュメントを参照してください。

2. ルートユーザーとして、次のコマンドを実行します。

```
1 dd if=/dev/cdrom of=/path/cdimg_filename.iso
```

このコマンドには時間がかかります。処理が完了すると、次のようなメッセージが表示されます:

```
1 1187972+0 records in
2 1187972+0 records out
```

これで、ISO ファイルが作成されました。

**Windows** システムで **ISO** を作成するには:

Windows には、Linux の `dd` コマンドのような、ISO を作成するためのコマンドがありません。その代わりに、ほとんどの CD 作成ツールには、CD を ISO ファイルとして保存するための機能が用意されています。

## Linux 仮想マシンの VNC 設定

December 30, 2019

Citrix Hypervisor では、リモートから Linux 仮想マシンを制御するためにデフォルトで VNC (Virtual Network Computing) が使用されます。ただし、仮想マシンに Linux オペレーティングシステムをインストールした段階では、VNC のサポートが設定されていない場合があります。XenCenter から接続できるようにするには、VNC サーバーと X ディスプレイマネージャを仮想マシンにインストールして、適切に設定する必要があります。ここでは、サポートされている各 Linux ディストリビューション上で VNC を設定し、XenCenter と適切に対話できるようにする方法を説明します。

CentOS ベースの仮想マシンには、下記の Red Hat ベースの仮想マシンの手順を適用できます。これは、同じベースコードでグラフィカル VNC アクセスが提供されているためです。CentOS X は Red Hat Enterprise Linux X をベースにしています。

### Debian 仮想マシンのグラフィックコンソールを有効にする

注:

Debian 仮想マシンのグラフィックコンソールを有効にする前に、Linux ゲストエージェントがインストール済みであることを確認してください。詳しくは、「[Linux ゲストエージェントのインストール](#)」を参照してください。

Debian 仮想マシンのグラフィックコンソールは、その仮想マシン内で動作する VNC サーバーにより提供されます。推奨される設定では、標準ディスプレイマネージャによりコンソールが制御され、ログインダイアログボックスが表示されます。

1. Debian をデスクトップシステムパッケージでインストールするか、標準的な apt コマンドを使って GDM (ディスプレイマネージャー) をインストールします。
2. 次のような apt-get コマンドを実行して、Xvnc サーバーをインストールします:

```
1 apt-get install vnc4server
```

注:

Gnome ディスプレイマネージャー version 3 デーモンを使用する Debian デスクトップ環境では、多くの CPU 負荷がかかることがあります。以下のコマンドを実行して、Gnome ディスプレイマネージャー-gdm3 パッケージをアンインストールし、gdm パッケージをインストールしてください:

```
1 apt-get install gdm
2 apt-get purge gdm3
```

3. vncpasswd コマンドを使用して VNC パスワードを設定します (設定しないと深刻なセキュリティ上のリスクの可能性があります)。パスワード情報を書き込むファイル名を渡します。次に例を示します:

```
1 vncpasswd /etc/vncpass
```

4. `gdm.conf`ファイル (`/etc/gdm/gdm.conf`) の`[servers]`および`[daemon]`セクションを次のように編集して、VNC サーバーがディスプレイ番号0を管理するように設定します。

```
1 [servers]
2 0=VNC
3 [daemon]
4 VTAllocation=false
5 [server-VNC]
6 name=VNC
7 command=/usr/bin/Xvnc -geometry 800x600 -PasswordFile /etc/
 vncpass BlacklistTimeout=0
8 flexible=true
```

5. GDM を再起動し、XenCenter によりグラフィックコンソールが検出されるのを待ちます：

```
1 /etc/init.d/gdm restart
```

注：

`ps ax | grep vnc`などのコマンドを使用して、VNC サーバーが動作しているかどうかを確認できます。

## Red Hat、CentOS、または Oracle Linux 仮想マシンのグラフィックコンソールを有効にする

注：

Red Hat 仮想マシンの VNC を設定する前に、Linux ゲストエージェントがインストール済みであることを確認してください。詳しくは、「[Linux ゲストエージェントのインストール](#)」を参照してください。

VNC を Red Hat 仮想マシン上で設定するには、GDM 設定を変更します。GDM 設定はファイルに保持されていますが、そのファイルの場所は Red Hat Linux のバージョンによって異なります。変更前に、最初にこの設定ファイルの場所を決定します。このファイルは、以降のいくつかの手順で変更されます。

### VNC 設定ファイルの場所の確認

Red Hat Linux を使用している場合、GDM 設定ファイルは`/etc/gdm/custom.conf`です。このファイルは、デフォルト設定を上書きするユーザー指定の値のみを含む分割設定ファイルです。このタイプのファイルは、GDM の新しいバージョンではデフォルトで使用され、Red Hat Linux の前述のバージョンに含まれています。

## VNC を使用するための GDM の設定

1. 仮想マシンのテキストコンソールのプロンプトで、ルートユーザーとして `rpm -q vnc-server gdm` を実行します。パッケージ名 `vnc-server` と `gdm` およびそれらのバージョン番号が表示されます。

これらのパッケージ名が表示された場合は、既に適切なパッケージがインストール済みです。パッケージがインストールされていないという内容のメッセージが表示された場合は、インストール時にグラフィカルデスクトップオプションを選択しなかった可能性があります。以降の手順に進むには、これらのパッケージをインストールする必要があります。仮想マシンへの追加ソフトウェアのインストールについて詳しくは、適切なバージョンの『Red Hat Linux x86 インストールガイド』を参照してください。

2. 任意のテキストエディターを使って GDM 設定ファイルを開き、次の行をファイルに追加します：

```
1 [server-VNC]
2 name=VNC Server
3 command=/usr/bin/Xvnc -SecurityTypes None -geometry 1024x768 -
 depth 16 \
4 -BlacklistTimeout 0
5 flexible=true
```

Red Hat Linux の設定ファイルでは、空の `[servers]` セクション内にこれらの行を追加します。

3. 標準の X サーバーの代わりに `Xvnc` サーバーが使用されるように設定を変更します。

- `0=Standard`

これを次のように変更します。

`0=VNC`

- Red Hat Linux を使用している場合、この行 (`0=VNC`) を `[servers]` セクションのすぐ下、`[server-VNC]` セクションの上に追加する必要があります。

4. ファイルを保存して閉じます。

設定の変更を有効にするために、`/usr/sbin/gdm-restart` を実行して GDM を再起動します。

### 注：

Red Hat Linux では、ランレベル 5 でグラフィカルユーザーインターフェイスが起動します。インストールがランレベル 3 で起動する場合は、ディスプレイマネージャが起動されるように（そしてグラフィックコンソールにアクセスできるように）設定を変更する必要があります。詳しくは、「ランレベルの確認」を参照してください。

## ファイアウォールの設定

デフォルトのファイアウォール設定では、VNC の通信がブロックされます。仮想マシンと XenCenter 間にファイアウォールを設定している場合は、VNC 接続が使用するポートを開放して、このポートでの通信を許可します。デフォ

ルトでは、VNC サーバーは TCP ポート 5900 + n で VNC ビューアからの接続を待機します。ここで、n はディスプレイ番号です（通常は 0）。つまり、VNC サーバーのディスプレイ番号が 0 の場合は TCP ポート 5900 で、ディスプレイ番号が 1 の場合は TCP-5901 で通信します。使用するファイアウォールのドキュメントを参照して、これらのポートが開放されていることを確認してください。

IP 接続を追跡したり、一方向からのみの接続を許可したりするには、ファイアウォール設定を設定します。

**Red Hat** ベースの仮想マシンのファイアウォールを設定して **VNC** ポートを開放するには：

1. Red Hat Linux の場合、`system-config-securitylevel-tui` を実行します。
2. [カスタマイズ] を選択して、その他のポートの一覧に 5900 を追加します。

または、`service iptables stop` を実行して、次回起動時までファイアウォールを無効にしたり、`chkconfig iptables off` を使用してファイアウォールを恒久的に無効にしたりできます。ただし、これにより、ほかのサービスが外部にさらされ、仮想マシン全体のセキュリティのレベルが下がることに注意してください。

### VNC 画面の解像度

グラフィックコンソールで仮想マシンに接続した後、画面解像度が一致しないことがあります。たとえば、仮想マシンの表示が大きすぎるため、グラフィックコンソールペイン内に収まらないことがあります。この挙動を制御するには、VNC サーバー `geometry` パラメーターを次のように設定します。

1. 任意のテキストエディタを使って GDM 設定ファイルを開きます。詳しくは、「VNC 設定ファイルの場所の確認」を参照してください。
2. [server-VNC] セクションを探します。
3. 次の行を編集します。

```
1 command=/usr/bin/Xvnc -SecurityTypes None -geometry 800x600
```

ここで、`geometry` パラメーターに、有効な画面の幅と高さを指定できます。

4. ファイルを保存して閉じます。

### RHEL、CentOS、または OEL の仮想マシンで VNC を有効にする

Red Hat Linux を使用している場合、GDM 設定ファイルは `/etc/gdm/custom.conf` です。このファイルは、デフォルト設定を上書きするユーザー指定の値のみを含む分割設定ファイルです。このタイプのファイルは、上記バージョンの Red Hat Linux などに含まれている、新しいバージョンの GDM でデフォルトで使用されます。

オペレーティングシステムのインストール時に、デスクトップモードを選択します。これを行うには、RHEL のインストール画面で、[Desktop]、[Customize now] の順に選択して、[Next] をクリックします。

The default installation of Red Hat Enterprise Linux is a basic server install. You can optionally select a different set of software now.

- Basic Server
- Database Server
- Web Server
- Identity Management Server
- Virtualization Host
- Desktop
- Software Development Workstation
- Minimal

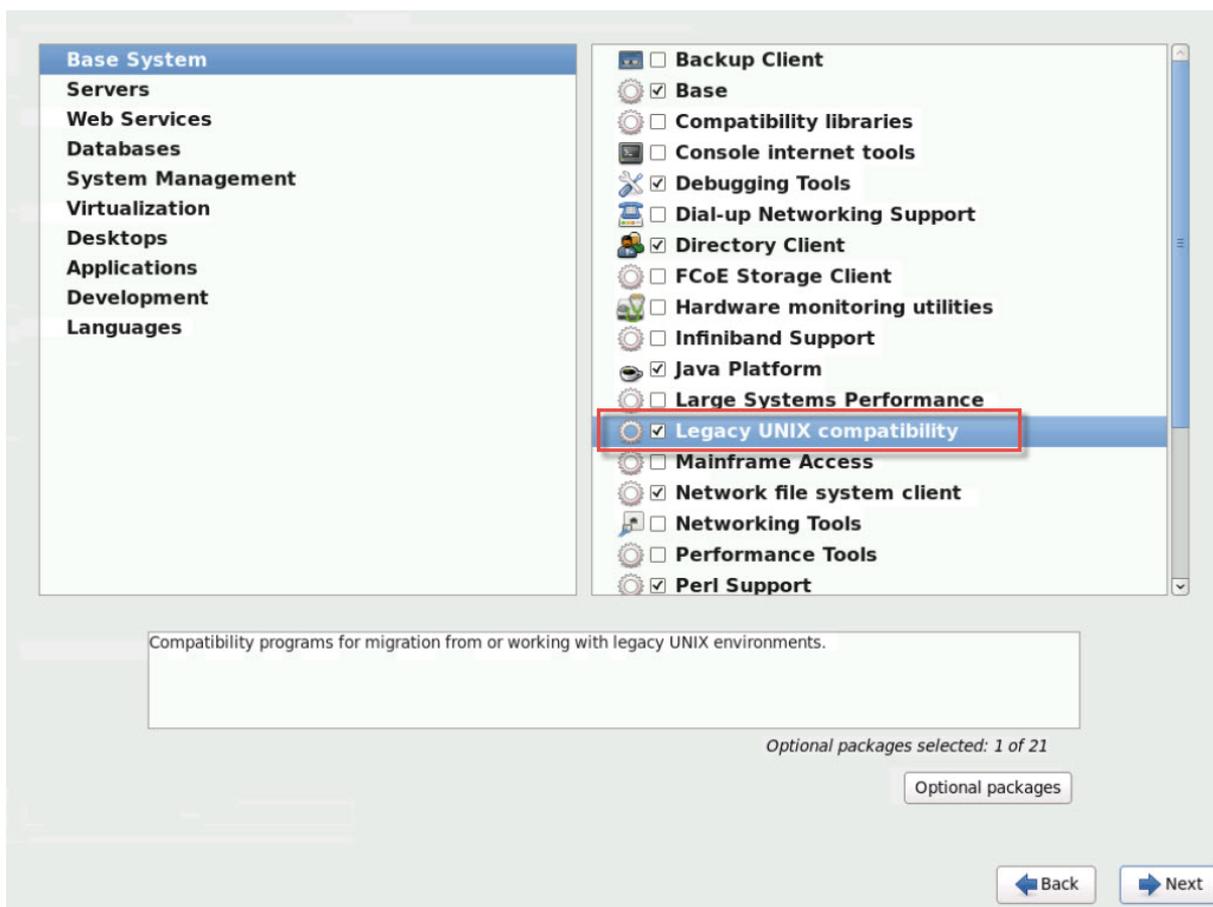
Please select any additional repositories that you want to use for software installation.

- High Availability
- Load Balancer
- Red Hat Enterprise Linux
- Resilient Storage

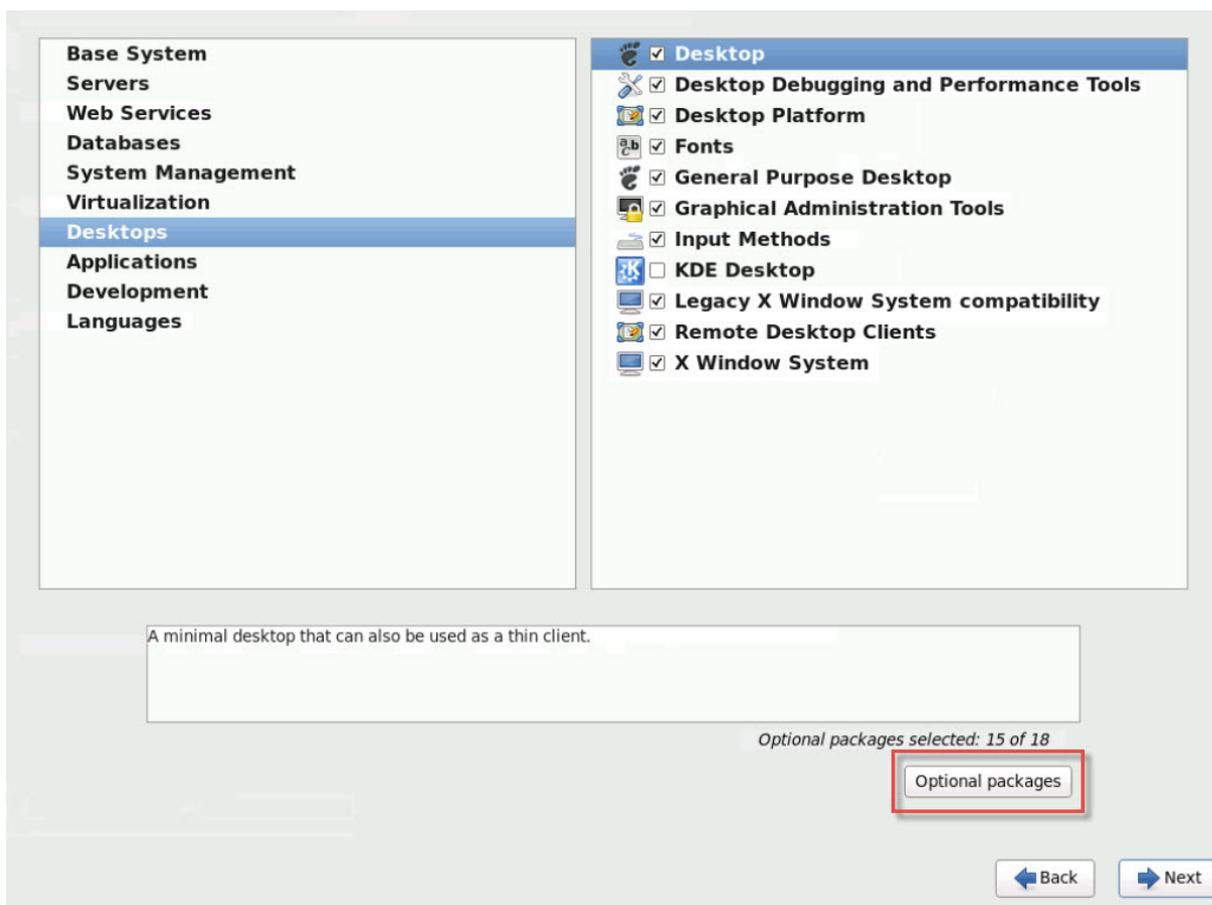
You can further customize the software selection now, or after install via the software management application.

- Customize later
- Customize now

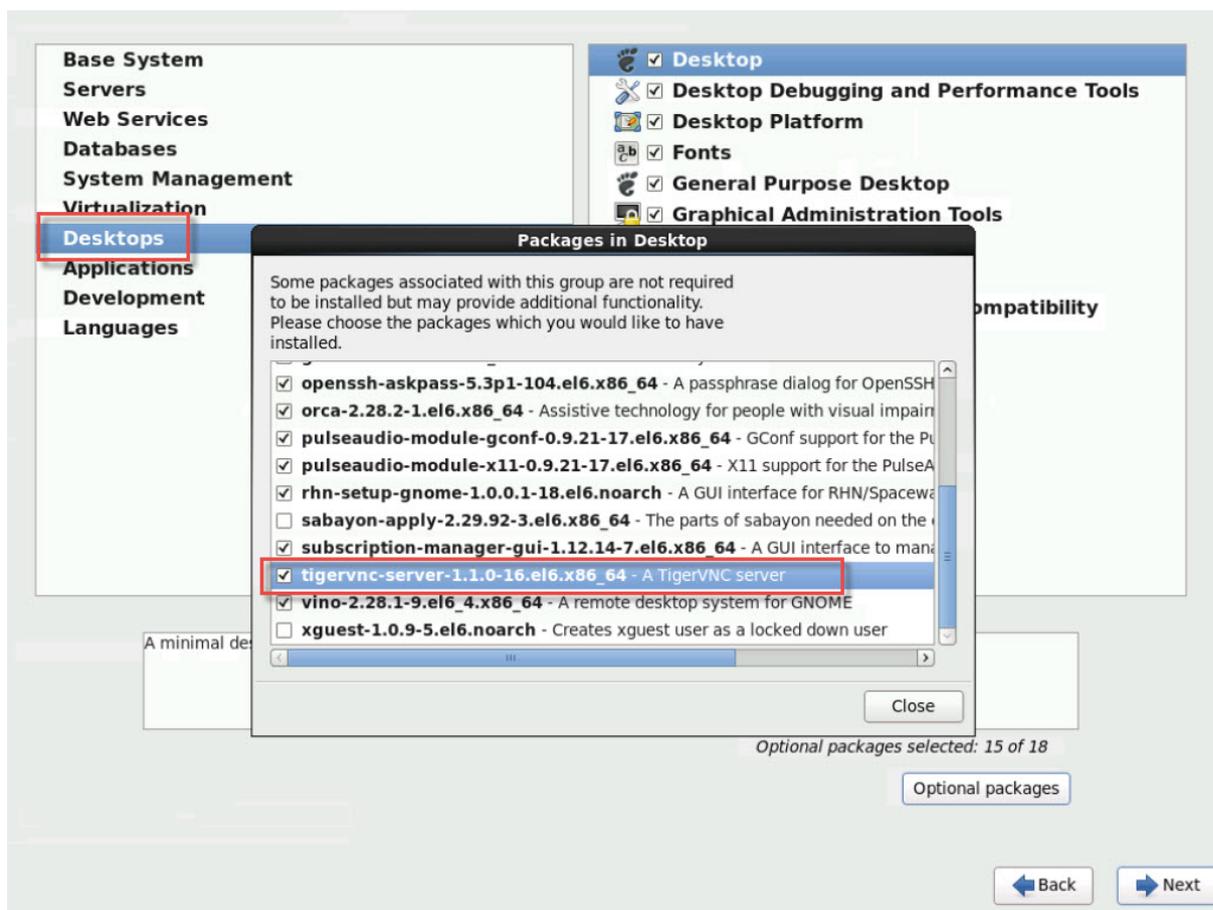
これにより、ベースシステム画面が開きます。【Legacy UNIX compatibility】が選択された状態にします。



[Desktops]、[Optional packages] の順に選択して、[Next] をクリックします。



これにより、**[Packages in Desktop]** ウィンドウが開きます。**tigervnc-server-<version\_number>** を選択して **[Next]** をクリックします：



次の手順の処理を進めて、RHEL 仮想マシンの設定を続けます：

1. 任意のテキストエディターを使って GDM 設定ファイルを開き、次の行を適切なセクションに追加します：

```

1 [security]
2 DisallowTCP=false
3
4 [xdmcp]
5 Enable=true

```

2. ファイル `/etc/xinetd.d/vnc-server-stream` を作成します：

```

1 service vnc-server
2 {
3
4 id = vnc-server
5 disable = no
6 type = UNLISTED
7 port = 5900
8 socket_type = stream
9 wait = no

```

```
10 user = nobody
11 group = tty
12 server = /usr/bin/Xvnc
13 server_args = -inetd -once -query localhost -
14 SecurityTypes None \
15 -geometry 800x600 -depth 16
16 }
```

3. 次のコマンドを実行して、`xinetd`サービスを起動します。

```
1 # service xinetd start
```

4. ファイル`/etc/sysconfig/iptables`を開きます。`-A INPUT -j REJECT --reject-with icmp-host-prohibited`の上に次の行を追加します:

```
1 -A INPUT -m state --state NEW -m tcp -p tcp --dport 5900 -j ACCEPT
```

5. 次のコマンドを実行して、`iptables`を再起動します:

```
1 # service iptables restart
```

6. 次のコマンドを実行して、`gdm`を再起動します:

```
1 # telinit 3
2 # telinit 5
```

注:

Red Hat Linux では、ランレベル 5 でグラフィカルユーザーインターフェイスが起動します。インストールがランレベル 3 で起動する場合は、ディスプレイマネージャが起動されるように（そしてグラフィックコンソールにアクセスできるように）設定を変更する必要があります。詳しくは、「ランレベルの確認」を参照してください。

## VNC 用 SLES ベース仮想マシンの設定

注:

SUSE Linux Enterprise Server 仮想マシンの VNC を設定する前に、Linux ゲストエージェントがインストール済みであることを確認してください。詳しくは、[Linux ゲストエージェントのインストール](#)を参照してください。

SLES では、YaSTの設定オプションで「Remote Administration」を有効にできます。SLES インストーラの [Network Services] 画面で利用可能な Remote Administration を、インストール時に有効にできます。この機能を使用すると、外部の VNC ビューアをゲストに接続して、グラフィックコンソールを表示できます。SLES リモ

ート管理機能を使用する方法は、XenCenter の方法と多少異なります。ただし、グラフィックコンソール機能と統合されるように SUSE Linux 仮想マシンの設定ファイルを変更することは可能です。

### VNC サーバーの確認

設定を変更する前に、VNC サーバーがインストール済みであることを確認する必要があります。SUSE には、デフォルトで `tightvnc` サーバーが付属しています。このサーバーは適した VNC サーバーですが、標準的な RealVNC デイストリビューションを使用することもできます。

次のコマンドを実行して、`tightvnc` ソフトウェアがインストール済みかどうかを確認できます。

```
1 rpm -q tightvnc
```

### リモート管理を有効にする

SLES ソフトウェアのインストール時にリモート管理を有効にしなかった場合は、次のようにして有効にすることができます。

1. 仮想マシン上でテキストコンソールを開き、`YaST` ユーティリティを実行します：

```
1 yast
```

2. 矢印キーを使用して、左のメニューで **[Network Services]** を選択します。**Tab** キーで右のメニューに移動し、矢印キーで **[Remote Administration]** を選択します。**Enter** キーを押します。
3. **[Remote Administration]** 画面で **Tab** キーを押して **[Remote Administration Settings]** セクションに移動します。矢印キーを使って **[Allow Remote Administration]** を選択し、**Enter** キーを押してこのオプションを有効にします。
4. **Tab** キーを押して **[Firewall Settings]** セクションに移動します。矢印キーを使って **[Open Port in Firewall]** を選択し、**Enter** キーを押してこのオプションを有効にします。
5. **Tab** キーを押して **[Finish]** ボタンに移動し、**Enter** キーを押します。
6. 設定を有効にするためにディスプレイマネージャの再起動が必要があるという内容のメッセージボックスが表示されます。メッセージを確認するには、**Enter** キーを押します。
7. `YaST` のトップレベルの画面に戻ります。**Tab** キーを押して **[Quit]** ボタンに移動し、**Enter** キーを押します。

### xinetd 設定の変更

リモート管理を有効にした後で、XenCenter を接続できるようにするには、設定ファイルを変更します。または、サードパーティの VNC クライアントを使用します。

1. 任意のエディタで `/etc/xinetd.d/vnc` ファイルを開きます。
2. このファイルには、以下に示すセクションが含まれています。

```
1 service vnc1
2 {
3
4 socket_type = stream
5 protocol = tcp
6 wait = no
7 user = nobody
8 server = /usr/X11R6/bin/Xvnc
9 server_args = :42 -inetd -once -query localhost -geometry 1024
 x768 -depth 16
10 type = UNLISTED
11 port = 5901
12 }
```

3. `port` 行を次のように変更します。

```
1 port = 5900
```

4. ファイルを保存して閉じます。
5. 次のコマンドを実行して、ディスプレイマネージャと `xinetd` サービスを再起動します:

```
1 /etc/init.d/xinetd restart
2 rcxdm restart
```

SUSE Linux では、ランレベル 5 でグラフィカルユーザーインターフェイスが起動します。リモートデスクトップが表示されない場合は、仮想マシンがランレベル 5 で起動するように設定されているかどうかを確認します。詳しくは、「ランレベルの確認」を参照してください。

#### ファイアウォールの設定

デフォルトのファイアウォール設定では、VNC の通信がブロックされます。仮想マシンと XenCenter 間にファイアウォールを設定している場合は、VNC 接続が使用するポートを開放して、このポートでの通信を許可します。デフォルトでは、VNC サーバーは TCP ポート `5900 + n` で VNC ビューアからの接続を待機します。ここで、`n` はディスプレイ番号です (通常は 0)。つまり、VNC サーバーのディスプレイ番号が 0 の場合は TCP ポート 5900 で、ディスプレイ番号が 1 の場合は TCP 5901 で通信します。使用するファイアウォールのドキュメントを参照して、これらのポートが開放されていることを確認してください。

IP 接続を追跡したり、一方向からのみの接続を許可したりするには、ファイアウォール設定を設定します。

**SLES 11.x** の仮想マシンのファイアウォールで **VNC** ポートを開放するには:

1. 仮想マシン上でテキストコンソールを開き、YaSTユーティリティを実行します:

```
1 yast
```

2. 矢印キーを使用して、左のメニューで **[Security and Users]** を選択します。 **Tab** キーで右のメニューに移動し、矢印キーで **[Firewall]** を選択します。 **Enter** キーを押します。
3. **[Firewall]** 画面の左のメニューで、矢印キーを使って **[Custom Rules]** を選択して **Enter** キーを押します。
4. **Tab** キーを押して **[Custom Allowed Rules]** の **[Add]** ボタンに移動し、 **Enter** キーを押します。
5. **[Source Network]** フィールドに「0/0」と入力します。 **Tab** キーを押して **[Destination Port]** フィールドに移動し、「5900」と入力します。
6. **Tab** キーを押して **[Add]** ボタンに移動し、 **Enter** キーを押します。
7. **Tab** キーを押して **[Next]** に移動し、 **Enter** キーを押します。
8. **[Summary]** 画面で、 **Tab** キーを押して **[Finish]** に移動し、 **Enter** キーを押します。
9. 最上位階層のYaST画面で、 **Tab** キーを押して **[Quit]** に移動し、 **Enter** キーを押します。
10. 次のコマンドを実行して、ディスプレイマネージャとxinetdサービスを再起動します:

```
1 /etc/init.d/xinetd restart
2 rcxadm restart
```

または、**rcSuSEfirewall2 stop** を実行して、次回起動時までファイアウォールを無効にしたり、YaSTを使用してファイアウォールを恒久的に無効にしたりできます。ただし、これにより、ほかのサービスが外部にさらされ、仮想マシン全体のセキュリティのレベルが下がることに注意してください。

## VNC 画面の解像度

グラフィックコンソールで仮想マシンに接続した後、画面解像度が一致しないことがあります。たとえば、仮想マシンの表示が大きすぎるため、グラフィックコンソールペイン内に収まらないことがあります。この挙動を制御するには、VNC サーバー **geometry** パラメーターを次のように設定します。

1. 任意のテキストエディタを使って **/etc/xinetd.d/vnc** ファイルを開き、**service\_vnc1** セクション (**displayID 1** に対応する) を探します。
2. **server-args** 行の **geometry** 引数を、目的のディスプレイ解像度に変更します。例:

```
1 server_args = :42 -inetd -once -query localhost -geometry 800x600
 -depth 16
```

ここで、**geometry** パラメーターに、有効な画面の幅と高さを指定できます。

3. ファイルを保存して閉じます。
4. 次のコマンドを実行して、VNC サーバーを再起動します。

```
1 /etc/init.d/xinetd restart
2 rcxdrm restart
```

### ランレベルの確認

Red Hat および SUSE Linux の仮想マシンでは、ランレベル 5 でグラフィカルユーザーインターフェイスが起動します。ここでは、仮想マシンがランレベル 5 で起動するように設定されていることを確認する方法と、この設定を変更する方法を説明します。

1. `/etc/inittab`を開き、デフォルトのランレベルを確認します。次の行を探します。

```
1 id:n:initdefault:
```

`n` が 5 でない場合は、5 に変更してファイルを保存します。

2. このように変更した後でコマンド `telinit q ; telinit 5` を実行すると、仮想マシンを再起動しなくてもランレベルの変更が適用されます。

## 仮想マシンの問題のトラブルシューティング

December 30, 2019

Citrix は、以下の 2 つの形式のサポートを提供します：

- [シトリックス Web サイト](#)での無料セルフヘルプサポート
- サポートサイトから購入可能な有料のサポートサービス

Citrix のテクニカルサポートを受けるには、オンラインでサポートケースを登録したり、サポート担当者に電話したりできます。

[シトリックスサポート](#)サイトでは、Citrix Hypervisor の問題解決に有用な情報が提供されています。ここでは、製品のドキュメント、ナレッジベース、ディスカッションフォーラムなどのリソースにアクセスできます。

このセクションは、仮想マシンの動作が異常な場合に問題の解決を支援することを目的としています。このセクションでは、問題について Citrix Hypervisor ソリューションプロバイダーに問い合わせる場合に必要な、アプリケーションログの場所やその他の情報についても説明します。

#### 重要：

ここで説明するトラブルシューティングを実行する場合には、Citrix Hypervisor ソリューションプロバイダ

—またはサポートチームの指示に従うことをお勧めします。

ベンダーによるアップデート：オペレーティングシステムのベンダーが提供するアップデートを使用して、仮想マシンを最新の状態にしておきます。ベンダーから、仮想マシンのクラッシュやその他の障害に対する修正プログラムが提供されている場合があります。

## 仮想マシンのクラッシュ

仮想マシンのクラッシュの問題を解決するには、カーネルのクラッシュダンプ情報を参照します。可能であれば、クラッシュを再現し、この手順に従ってください。この問題の詳細な調査については、ゲスト OS ベンダーにお問い合わせください。

### Linux 仮想マシンのクラッシュダンプ動作の制御

Linux 仮想マシンでのクラッシュダンプの動作は、`actions-after-crash`パラメーターで制御できます。使用可能な値は次のとおりです：

| 値                     | 説明                                    |
|-----------------------|---------------------------------------|
| <code>preserve</code> | 仮想マシンを一時停止状態にします。(分析用)                |
| <code>restart</code>  | コアダンプを記録せずに、仮想マシンの再起動のみを実行します。(デフォルト) |
| <code>destroy</code>  | コアダンプを記録せずに、仮想マシンを停止状態のままにします。        |

Linux 仮想マシンのクラッシュダンプの保存を有効にするには：

1. Citrix Hypervisor サーバー上で、次のコマンドを実行して、対象の仮想マシンの UUID を確認します：

```
1 xe vm-list name=label=name params=uuid --minimal
```

2. `xe vm-param-set`を使用して、`actions-after-crash`の値を変更します。たとえば、`dom0` で次のコマンドを実行します：

```
1 xe vm-param-set uuid=vm_uuid actions-after-crash=preserve
```

3. 仮想マシンをクラッシュします。

- PV ゲストの場合は、仮想マシンで次のコマンドを実行します。

```
1 echo c | sudo tee /proc/sysrq-trigger
```

4. dom0 でダンプコアコマンドを実行します。たとえば、次のコマンドを実行します。

```
1 xl dump-core domid filename
```

### Windows 仮想マシンのクラッシュダンプ動作の制御

Windows 仮想マシンでのコアダンプの動作は、`actions-after-crash`パラメーターで制御できません。デフォルトでは、Windows のクラッシュダンプは、Windows 仮想マシン自体の`%SystemRoot%\Minidump`に保存されます。

仮想マシンでのダンプレベルは、[マイコンピュータ] > [プロパティ] > [詳細設定] > [起動と回復] で設定できます。

### Linux 仮想マシンの起動の問題のトラブルシューティング

Citrix Hypervisor サーバーコントロールドメインに、`xe-edit-bootloader`という名前のユーティリティスクリプトがあります。このスクリプトを使用して、シャットダウンされた Linux 仮想マシンのブートローダー構成を編集し、仮想マシンが起動できない問題を修正できます。

このスクリプトを使用するには：

1. 次のコマンドを実行します。

```
1 xe vm-list
```

このコマンドにより、対象の仮想マシンがシャットダウンされているかどうかを確認できます (`power-state`の値は `halted` になります)。

2. 仮想マシンの UUID を指定して編集対象のブートローダーを開くには、次のコマンドを実行します。

```
1 xe-edit-bootloader -u linux_vm_uuid -p partition_number
```

または、名前ラベルを次のように使用できます：

```
1 xe-edit-bootloader -n linux_vm_name_label -p partition_number
```

パーティション番号には、ファイルシステムが設定されているディスクのスライスを指定します。デフォルトの Debian テンプレートの場合、最初のパーティションになるため、パーティション番号は `1` です。

3. 指定した仮想マシンの `grub.conf`ファイルがエディタで表示されます。問題を解決するためファイルに変更を行い、ファイルを保存してエディターを終了し、仮想マシンを起動します。

## Windows 仮想マシンの UEFI およびセキュアブートの問題のトラブルシューティング

UEFI 対応の仮想マシンで **XenCenter** コンソールの画面の解像度を変更するにはどうすればよいですか

UEFI 対応の仮想マシンで XenCenter コンソールの画面の解像度を変更するには、次の手順を実行します：

1. [**Windows** の設定] を開きます。
2. [更新とセキュリティ] をクリックします。
3. [回復] タブの [今すぐ再起動] をクリックします。
4. [トラブルシューティング] > [詳細オプション] > [**UEFI** ファームウェアの設定] の順に移動します。
5. [再起動] をクリックします。再起動中に、UEFI 設定メニューがロードされます。
6. [**Device Manager**] > [**OVMF** プラットフォームの設定] に移動します。現在の画面の解像度が表示されます。
7. 画面の解像度オプションを表示するには、**Enter** キーを押します。
8. 矢印キーを使用して希望する画面解像度を選択し、**Enter** キーを押します。
9. **F10** キーを押して変更を保存し、選択内容を確定します。
10. 仮想マシンを再起動して、更新された画面の解像度で XenCenter コンソールを表示します。

**UEFI** セキュアブート仮想マシンを作成できないのはなぜですか

仮想マシンのオペレーティングシステムが UEFI セキュアブートモードをサポートしていることを確認します。Citrix Hypervisor 8.1 では、次のオペレーティングシステムのみがセキュアブートをサポートしています：Windows 10 (64 ビット)、Windows Server 2016 (64 ビット)、Windows Server 2019 (64 ビット)

Citrix Hypervisor サーバーが UEFI モードで起動されることを確認します。UEFI セキュアブート仮想マシンを作成できるのは、セキュアブート証明書が存在する Citrix Hypervisor サーバーのみです。セキュアブート証明書は、UEFI モードで起動されたサーバー、または UEFI モードで起動されたサーバーと同じプール内のサーバーにのみ存在します。詳しくは、「[ネットワークブート](#)」を参照してください。

UEFI モードで起動された Citrix Hypervisor サーバーが [ハードウェア互換性リスト \(英語\)](#) に含まれていることを確認します。古いサーバーは、UEFI モードで起動した場合にセキュアブート証明書を含まない可能性があります。

セキュアブート **VM** を作成する **Citrix Hypervisor** サーバーにセキュアブート証明書があることをどのようにして確認できますか

Citrix Hypervisor サーバーが UEFI モードで起動すると、サーバー上でセキュアブート証明書が利用可能になります。Citrix Hypervisor サーバーは、同じリソースプール内の他のサーバーと証明書を共有します。リソースプールに UEFI モードで起動するサーバーがある場合、そのプール内のすべてのサーバーにセキュアブート証明書があります。

Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe pool-param-get param-name=uefi-certificates uuid=<pool-uuid> | wc -c
```

ゼロより大きい値が返される場合、セキュアブート証明書が存在します。

証明書が有効であることを確認するには、Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 xe pool-param-get uuid=$(xe pool-list --minimal) param-name=uefi-
 certificates|base64 -d|tar tv
2 -rw-r--r-- root/root 1600 2019-11-11 17:09 KEK.auth
3 -rw-r--r-- root/root 3212 2019-11-11 17:09 db.auth
```

セキュアブート証明書が存在しない場合は、Citrix Hypervisor サーバーで次のコマンドを実行します：

```
1 ls /sys/firmware/efi/efivars | grep KEK
```

このコマンドが値を返さない場合、必要な証明書が UEFI ファームウェアにないため、そのサーバー上にセキュアブート仮想マシンを作成できません。

#### UEFI セキュアブート仮想マシンの起動に失敗するのはなぜですか

UEFI セキュアブート仮想マシンのコンソールに次のメッセージが表示され、XenCenter にアラートが表示される場合、セキュアブートプロセスが失敗したため、仮想マシンが起動しません。

```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.70 (EDK II, 0x00010000)
Mapping table
FS0: Alias(s) :F1:;BLK3:
 PciRoot (0x0) /Pci (0x3,0x0) /VenHw (3D3CA290-B9A5-11E3-B75D-B8AC6F7D65E6,0
1004016) /VenMedia (C5BD4D42-1A76-4996-8956-73CDA326CD0A)
BLK0: Alias(s) :
 PciRoot (0x0) /Pci (0x3,0x0) /VenHw (3D3CA290-B9A5-11E3-B75D-B8AC6F7D65E6,0
1000003)
BLK1: Alias(s) :
 PciRoot (0x0) /Pci (0x3,0x0) /VenHw (3D3CA290-B9A5-11E3-B75D-B8AC6F7D65E6,0
1004016)
BLK2: Alias(s) :
 PciRoot (0x0) /Pci (0x3,0x0) /VenHw (3D3CA290-B9A5-11E3-B75D-B8AC6F7D65E6,0
1004016) /CDROM (0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> _
```

これは通常、署名されていないドライバーを仮想マシンにインストールしたことが原因です。前回の正常なセキュアブート以降に更新またはインストールされたドライバーを調査します。

セキュアブートを無効にし、セットアップモードで仮想マシンを起動して、署名されていないドライバーを削除できます。

**重要:**

この処理を行う前に、スナップショットを作成して仮想マシンをバックアップします。

UEFI セキュアブート仮想マシンを UEFI ブート仮想マシンに変更するには、仮想マシンをホストする Citrix Hypervisor サーバーで次のコマンドを実行します:

```
1 varstore-sb-state <VM_UUID> setup
```

仮想マシンを修正したら、次のコマンドを実行してセキュアブートを再び有効にします:

```
1 varstore-sb-state <VM_UUID> user
```

セキュアブートは **Windows** 仮想マシンで問題を引き起こしていますか

Windows 仮想マシンの問題の原因が、仮想マシンに対して有効なセキュアブートであるかどうかを診断するには、セキュアブートを無効にして、問題の再現を試みます。

セキュアブートを無効にするには、仮想マシンをホストする Citrix Hypervisor サーバーで次のコマンドを実行します:

```
1 varstore-sb-state <VM_UUID> setup
```

問題をデバッグしたら、次のコマンドを実行してセキュアブートを再び有効にします:

```
1 varstore-sb-state <VM_UUID> user
```

セキュアブート仮想マシンで **Windows** デバッグを実行するにはどうすればよいですか

セキュアブート仮想マシンで Windows デバッグを実行することはできません。仮想マシンで Windows デバッグを実行するには、次のいずれかを実行できます:

- 次のコマンドを実行して、仮想マシンを UEFI ブートモードに切り替えます:

```
1 xe vm-param-set uuid=<UUID> platform:secureboot=false
```

仮想マシンを再起動します。

問題をデバッグしたら、次のコマンドを実行してセキュアブートを再び有効にします:

```
1 xe vm-param-set uuid=<UUID> platform:secureboot=auto
```

仮想マシンを再起動します。

- 仮想マシンをホストする Citrix Hypervisor サーバーで次のコマンドを実行し、セキュアブートを無効にします:

```
1 varstore-sb-state <VM_UUID> setup
```

問題をデバッグしたら、次のコマンドを実行してセキュアブートを再び有効にします:

```
1 varstore-sb-state <VM_UUID> user
```

### UEFI 仮想マシンに 2 つの NIC しか表示されないのはなぜですか

UEFI 対応の仮想マシンの作成時に 3 つ以上の NIC をセットアップした場合でも、仮想マシンの初回起動時には、2 つの NIC しか表示されません。この情報は、Citrix VM Tools が仮想マシンにインストールされた後に正しく表示されます。

### エミュレートされたデバイスが予想と異なるタイプとして表示されるのはなぜですか

UEFI セキュアブート仮想マシンはエミュレートされたデバイスに NVME と E1000 を使用します。ただし、仮想の初回起動時には、エミュレートされたデバイスが異なるタイプとして表示されます。この情報は、Citrix VM Tools が仮想マシンにインストールされた後に正しく表示されます。

### テンプレートを BIOS モードから UEFI または UEFI セキュアブートモードに変換できないのはなぜですか

UEFI 対応の仮想マシンテンプレートは、Citrix Hypervisor が提供するテンプレートのみから作成できます。

何かインストールされているテンプレート、またはスナップショットから作成したテンプレートに対しては `xe template-param-set` コマンドを実行しないでください。これらのスナップショットの起動モードは変更できません。また、起動モードを変更しようとすると、仮想マシンは起動に失敗します。

### UEFI および UEFI セキュアブート設定を確認するにはどうすればよいですか

UEFI または UEFI セキュアブート仮想マシンがホストされている Citrix Hypervisor サーバーで、次のコマンドを実行します:

```
1 varstore-ls
```

このコマンドでは、使用可能な設定の ID が一覧にされます。設定 ID を次のコマンドで使用します:

```
1 varstore-get <setting_ID> <VM_ID> | hexdump -C
```

設定の値は、無効の場合は 0、有効の場合は 1 です。

セキュアブート仮想マシンで「テスト」ドライバーを使用できないのはなぜですか

お客様が UEFI セキュアブート仮想マシンの問題をデバッグおよび修正するためにサードパーティと協力している場合、サードパーティはテストまたは検証の目的で署名されていないドライバーを提供する場合があります。これらのドライバーは、UEFI セキュアブート仮想マシンでは機能しません。

サードパーティに署名済みのドライバーをリクエストするようにお客様に伝えます。また、お客様は UEFI セキュアブート仮想マシンをセットアップモードに切り替えて、署名されていないドライバーで実行することもできます。

## 高可用性

March 12, 2020

Citrix Hypervisor サーバーは障害により接続不能になったり停止したりすることがあります。Citrix Hypervisor の高可用性機能には、これらの障害に備え、安全に回復するための一連の自動化オプションが用意されています。たとえば、ネットワークの物理的な切断やホストのハードウェア障害が考えられます。

### 概要

高可用性により、ホストが接続不能になったり不安定になったりしたときに、そのホストで実行されている仮想マシンが確実にシャットダウンされて別のホストで再起動されます。仮想マシンをシャットダウンして別のホストで再起動することで、その仮想マシンが（手作業または自動的に）新しいホストで起動されないようにします。その後いずれかの時点で、元のホストが回復されます。このシナリオでは、同じ仮想マシンの 2 つのインスタンスが異なるホスト上で動作する可能性があり、それに伴い仮想マシンディスクが破損してデータが失われる可能性が高くなります。

プールマスタが接続不能になったり不安定になったりしたときに、高可用性により、プールの管理機能を回復することもできます。高可用性によりプールの管理機能が自動的に復元されます。手動での介入は必要ありません。

オプションで、高可用性により、状態が良いと認識されているホストで手動での介入なしで仮想マシンを再起動するプロセスを自動化することもできます。複数の仮想マシンが特定の順番で起動して、特定の仮想マシン上のサービスが起動してからほかの仮想マシンが起動するようにスケジュールを設定することもできます。これにより、依存仮想マシン（依存 SQL サーバーなど）よりもインフラストラクチャ仮想マシン（DHCP サーバーなど）が先に起動するように設定できます。

#### 警告:

高可用性は、マルチパス化したストレージとボンディングしたネットワークと合わせて使用します。マルチパス化したストレージとボンディングしたネットワークは、高可用性を設定する前に構成してください。マルチパス化したストレージとネットワークボンディングを使用しない場合、インフラストラクチャでの問題発生時にホストが予期せず再起動されることがあります（自己隔離）。

すべてのグラフィックソリューション（NVIDIA vGPU、Intel GVT-d、Intel GVT-G、AMD MxGPU、および

vGPU パススルー) は、高可用性を利用する環境で使用できます。ただし、これらのグラフィックソリューションを使用する仮想マシンは、高可用性で保護できません。これらの仮想マシンは、適切な空きリソースを持つホストがある間は、ベストエフォート方式で再起動できます。

### オーバーコミット

ユーザー定義のホスト障害数の後に、いずれかの場所で現在実行中の仮想マシンを再起動できない場合、プールはオーバーコミットされます。

オーバーコミットは、プール全体に障害後の仮想マシンの実行に必要な十分な空きメモリがない場合に発生する可能性があります。また、軽微な設定変更により、意図したとおりに仮想マシンが保護されなくなる場合もあります：たとえば、仮想ブロックデバイス (VBD) とネットワークの設定を変更すると、どのホストでどの仮想マシンを再起動できるかが変更される可能性があります。Citrix Hypervisor ですべての要因を予測して、高可用性機能による保護が正しく反映されるかどうかをチェックすることはできません。ただし、高可用性を維持できなくなった場合は、非同期的なアラートが送信されます。

Citrix Hypervisor では、プール内の複数のホストに障害が発生した場合にどのような対処を行うかというフェイルオーバープランが動的に保持されます。理解すべき重要な概念は許容されるホスト障害数の値です。この値は高可用性構成の一部として定義されます。許容されるホスト障害数の値で、サービスを中断せずに許容される障害の回数が決まります。たとえば、64 のホストで構成されるリソースプールで、許容される障害数が 3 に設定されているとします。この場合、プールでは、3 台のホストの障害は許容し、他のホストで仮想マシンを再起動するフェイルオーバープランを計算します。フェイルオーバープランが見つからない場合は、プールがオーバーコミットしたとみなされます。フェイルオーバープランは、仮想マシンの追加や起動などのライフサイクル操作や移行に応じて動的に再計算されます。プールへの新しい仮想マシンの追加など、プールがオーバーコミット状態になるような変更を加えると、アラートが送信されます (XenCenter 経由またはメールで)。

### オーバーコミットの警告

仮想マシンを起動または一時停止しようとしてプールがオーバーコミット状態になった場合は、警告アラートが表示されます。この警告は XenCenter に表示されるほか、管理 API ではメッセージインスタンスとしても使用できます。メールアドレスを構成してある場合は、そのメールアドレスにメッセージが送信されるように設定することもできます。その後、操作をキャンセルするか、そのまま続行することができます。処理を続行すると、リソースプールがオーバーコミット状態になります。さまざまな再起動優先度の仮想マシンで消費されているメモリ量が、プール全体およびホストごとに表示されます。

### ホストを隔離する

サーバーの障害は、ネットワーク接続の損失により、または管理スタックの問題が発生したときに発生する可能性があります。このような場合、Citrix Hypervisor サーバーは自己隔離を行って、仮想マシンが 2 台のサーバーで同時に実行されないようにします。隔離されたホストは直ちに再起動され、そのホスト上で実行中のすべての仮想マシン

が停止します。リソースプール内のほかのホストは、これらの仮想マシンの停止を検出し、設定されている再起動優先度に従って仮想マシンを再起動します。隔離されたホストが再起動すると、リソースプールへの復帰を試行します。

注:

クラスター化プール内のホストは、リソースプール内の半分以上のほかのホストと通信できないときに、自己隔離を行うこともできます詳しくは、「[クラスター化プール](#)」を参照してください。

### 設定要件

高可用性機能を使用するために必要な条件:

- Citrix Hypervisor のリソースプール。高可用性機能では、単一リソースプール内のホストレベルの障害に対する高可用性が提供されます。

注:

高可用性は、3 台以上の Citrix Hypervisor サーバーが動作するプールでを使用することをお勧めします。詳しくは、「[CTX129721 - High Availability Behavior When the Heartbeat is Lost in a Pool](#)」を参照してください。

- ハートビートストレージリポジトリとして、356MB 以上の iSCSI、NFS、またはファイバチャネル LUN を少なくとも 1 つ含む共有ストレージ。高可用性メカニズムによりハートビートストレージリポジトリに次の 2 つのボリュームが作成されます:

4MB ハートビートボリューム: ハートビートに使用されます。

256MB メタデータボリューム: マスタがフェールオーバーした場合にプールマスタメタデータの格納に使用されます。

注:

- 信頼性を向上させるため、高可用性ハートビートディスクとして専用の NFS または iSCSI ストレージリポジトリを使用することをお勧めします。このストレージリポジトリは、ほかの目的で使用しないでください。
- プールがクラスター化されている場合、ハートビートストレージリポジトリは GFS2 ストレージリポジトリでなければなりません。
- CHAP で認証した場合、SMB または iSCSI を使用して接続されたストレージはハートビートストレージリポジトリとして使用できません。
- NetApp または EqualLogic のストレージリポジトリを使用する場合は、ハートビートストレージリポジトリに使用するアレイに NFS または iSCSI の論理ユニット番号を手作業で準備する必要があります。

- すべてのホストの静的 IP アドレス。

**警告:**

高可用性を有効にしているときにサーバーの IP アドレスを変更すると、高可用性によりホストのネットワークに障害が発生したとみなされます。IP アドレスを変更したことでホストが隔離されて、起動できない状態になることがあります。この状況を改善するには、`host-emergency-ha-disable` コマンドを使用して高可用性を無効にし、`pool-emergency-reset-master` を使用してプールマスタをリセットしてから、高可用性を再度有効にします。

- 信頼性を最大限に高めるために、専用のボンディングされたインターフェイスを高可用性管理ネットワークとして使用することをお勧めします。

高可用性で仮想マシンを保護するには、その仮想マシンがアジャイルである必要があります。仮想マシンの条件:

- 仮想ディスクが共有ストレージ上にある。共有ストレージは種類を問いません。iSCSI、NFS、またはファイバチャネルの論理ユニット番号のみがストレージハートビートの必須条件ですが、仮想ディスクストレージとしても使用できます。
- ライブマイグレーションを使用可能。
- ローカル DVD ドライブへの接続が設定されていない。
- 仮想ネットワークインターフェイスがプール全体にわたるネットワーク上にある。

**注:**

高可用性を有効にする場合はプール内のサーバーで管理インターフェイスをボンディングし、ハートビートストレージリポジトリにはマルチパスストレージを使用することを強くお勧めします。

コマンドラインインターフェイスから仮想 LAN およびボンディングされたインターフェイスを作成する場合、作成されても接続されず、アクティブにならない場合があります。この場合、仮想マシンがアジャイルでないため、高可用性機能で保護されません。CLI の `pif-plug` コマンドを使用して、仮想 LAN とボンディング PIF をアクティブにすると仮想マシンがアジャイルになります。 `xe diagnostic-vm-status` CLI コマンドを使用して、仮想マシンがアジャイルではない正確な理由を判定することもできます。このコマンドは配置制約を分析し、必要に応じて是正措置を取ることができます。

**構成設定を再起動する**

仮想マシンは、高可用性機能によって「保護する」、「ベストエフォート」、または「保護しない」と分類されます。`ha-restart-priority` の値は、仮想マシンを保護する、ベストエフォート、または保護しないのうちのいずれに分類するかを定義します。これらの各カテゴリにおいて、仮想マシンの再起動の動作はそれぞれ異なります。

**保護する**

高可用性機能によって、オフラインになった保護する仮想マシン、またはオフラインになっているそのホストを確実に再起動できます。これは、プールがオーバーコミット状態ではなく、仮想マシンがアジャイルであることが前提です。

サーバー障害時に保護されている仮想マシンを再起動できない場合、高可用性機能は、プールに余分な容量があるときは仮想マシンの起動を試行します。余分な容量があるときは、仮想マシン起動の試行が成功する可能性があります。

`ha-restart-priority`値: `restart`

#### ベストエフォート

ベストエフォート仮想マシンのホストがオフラインになった場合、高可用性は、別のホストでベストエフォート仮想マシンの再起動を試行します。この試行は、保護されているすべての仮想マシンが正常に再起動された後にのみ行われます。高可用性は、ベストエフォート仮想マシンの再起動を1回のみ試行します。この試行が失敗すると、高可用性は仮想マシンの再起動をそれ以上試行しません。

`ha-restart-priority`値: `best-effort`

#### 保護しない

保護しない仮想マシン、またはそれが実行されているホストが停止しても、高可用性は仮想マシンの再起動を試行しません。

`ha-restart-priority`値: 値は空文字です

#### 注:

高可用性は、保護する仮想マシン、またはベストエフォート仮想マシンの再起動に使用するリソースを解放するために、実行中の仮想マシンを停止したり、移行したりすることはありません。

リソースプールで複数回のサーバー障害が発生し、許容障害数がゼロになった場合、保護されている仮想マシンの再起動は保証されません。そのような場合、システムアラートが生成されます。これ以降のサーバー障害では、再起動優先度が設定されたすべての仮想マシンは、`best-effort` が設定されているものとして処理されます。

#### 起動順序

起動順序は、障害が発生した場合、Citrix Hypervisor の高可用性機能が保護する仮想マシンを再起動しようとする順序です。各保護する仮想マシンの`order`プロパティの値によって、起動順序が決定されます。

仮想マシンの`order`プロパティは、高可用性、および仮想マシンを起動およびシャットダウンするほかの機能でも使用されます。保護する仮想マシンとして高可用性でマークされた仮想マシンだけでなく、すべての仮想マシンで`order`プロパティを設定できます。ただし、高可用性が`order`プロパティを使用するのは、保護する仮想マシンに対してのみです。

`order`プロパティは整数値です。デフォルトの値は0（最優先）です。`order`の値が0の保護する仮想マシンが、最初に高可用性によって再起動されます。`order`プロパティの値が大きくなるほど、仮想マシンの再起動の順番は後になります。

仮想マシンの`order`プロパティの値は、次のコマンドラインインターフェイスで設定できます:

```
1 xe vm-param-set uuid=VM_UUID order=int
```

XenCenter では、仮想マシンの [高可用性オプション] パネルで [起動順序] を必要な値に設定することもできます。

## Citrix Hypervisor プールの高可用性を有効にする

プールの高可用性を有効にするには、XenCenter または CLI を使用します。いずれの方法でも、仮想マシンに再起動優先度を設定して、プールがオーバーコミット状態になったときに優先的に再起動する仮想マシンを指定します。

### 警告:

- 高可用性を有効にすると、プールからサーバーを削除するなど、仮想マシンのフェイルオーバープランを変更するような操作が無効になる場合があります。このような操作を行うために、一時的に高可用性を無効にするか、高可用性によって保護されている仮想マシンを保護しない状態にすることができます。
- 高可用性が有効になっている場合、プールのクラスタリングは有効にできません。クラスタリングを有効にするには、一時的に高可用性を無効にします。クラスタ化されたプールで高可用性を有効にすることができます。クラスタ化されたプールでは、自己隔離などの一部の高可用性の動作が異なります。詳しくは、「[クラスタ化プール](#)」を参照してください。

## CLI を使用して高可用性を有効にする

- リソースプールに、高可用性機能をサポートするストレージリポジトリが接続されていることを確認します。この機能をサポートするストレージリポジトリは、iSCSI、NFS、およびファイバチャネルです。これらのストレージリポジトリを CLI を使用して構成する方法について詳しくは、「[ストレージリポジトリ \(SR\) の管理](#)」を参照してください。
- 保護する各仮想マシンに再起動優先度を設定します。再起動優先度は次のコマンドで設定できます:

```
1 xe vm-param-set uuid=vm_uuid ha-restart-priority=restart order=1
```

- 次のコマンドを実行して、プールの高可用性を有効にし、オプションでタイムアウトを指定します:

```
1 xe pool-ha-enable heartbeat-sr-uuids=sr_uuid ha-config:timeout=
 timeout in seconds
```

タイムアウトは、プール内のホストがネットワークまたはストレージにアクセスできない期間です。高可用性を有効にするときにタイムアウトを指定しない場合、Citrix Hypervisor ではデフォルトの 30 秒のタイムアウトが使用されます。タイムアウト期間内にすべての Citrix Hypervisor サーバーがネットワークまたはストレージにアクセスできない場合は、自己隔離されて再起動されることがあります。

- `pool-ha-compute-max-host-failures-to-tolerate` コマンドを実行します。このコマンドは、プールにあるすべての保護された仮想マシンを実行するためのリソースが不足する前に、失敗する可能性のあるホストの最大数を返します。

```
1 xe pool-ha-compute-max-host-failures-to-tolerate
```

許容される失敗の数によって、通知が送信されるタイミングが決まります。プールの状態が変化したときに、フェイルオーバープランが再計算されます。この計算を使用して、プールの容量と、保護されている仮想マシンの稼働を保証しながら許容できる障害の回数が特定されます。この計算値が`ha-host-failures-to-tolerate`の指定値を下回ると、システムアラートが生成されます。

5. `ha-host-failures-to-tolerate`パラメーターを指定します。値は計算された値以下でなければなりません:

```
1 xe pool-param-set ha-host-failures-to-tolerate=2 uuid=pool-uuid
```

#### CLI を使用して仮想マシンから高可用性保護を削除する

特定の仮想マシンに対する高可用性機能を無効にするには、`xe vm-param-set`コマンドで`ha-restart-priority`パラメータに空文字列を指定します。`ha-restart-priority`パラメータを設定しても、その仮想マシンに設定されている起動順序が変更されることはありません。`ha-restart-priority`パラメータを適宜`restart`または`best-effort`に設定することで、仮想マシンの高可用性を再度有効にすることができます。

#### 到達不能なホストを復元する

何らかの理由でホストが高可用性ステートファイルにアクセスできない場合、そのホストは到達不可として認識されます。Citrix Hypervisor インストールを復元するには、`host-emergency-ha-disable`コマンドを使用して高可用性を無効にする必要があります:

```
1 xe host-emergency-ha-disable --force
```

プールマスタとして動作していたホストの場合、高可用性が無効になって起動します。プールメンバーが再接続すると、高可用性が自動的に無効になります。プールメンバーとして動作していたホストがマスタに接続できない場合、次のいずれかの操作を行う必要があります:

- ホストをプールマスタとして強制的にリポートする (`xe pool-emergency-transition-to-master`)

```
1 xe pool-emergency-transition-to-master uuid=host_uuid
```

- ホストに新しいマスタの位置を教える (`xe pool-emergency-reset-master`):

```
1 xe pool-emergency-reset-master master-address=new_master_hostname
```

すべてのホストが正常に再起動したら、高可用性を再度有効にします:

```
1 xe pool-ha-enable heartbeat-sr-uuid=sr_uuid
```

高可用性が有効なときにホストをシャットダウンする

ホストをシャットダウンまたは再起動するときは、ホストに障害が発生したと高可用性メカニズムに見なされないように特に注意してください。高可用性が有効なときにホストを完全にシャットダウンするには、XenCenter または CLI を使用して、ホストの `disable`、ホストの `evacuate`、ホストの `shutdown` の順に実行する必要があります。高可用性が有効になっている環境でホストをシャットダウンするには、次のコマンドを実行します：

```
1 xe host-disable host=host_name
2 xe host-evacuate uuid=host_uuid
3 xe host-shutdown host=host_name
```

高可用性により保護されている仮想マシンをシャットダウンする

高可用性機能により保護されている仮想マシンが自動的に再起動するように設定されている場合、その設定を有効にしたまま仮想マシンをシャットダウンすることはできません。このような仮想マシンをシャットダウンするには、仮想マシンの高可用性を無効にしてからシャットダウン用の CLI コマンドを実行します。XenCenter を使用する場合は、保護されている仮想マシンの [シャットダウン] ボタンをクリックしたときに、高可用性による保護を無効にするためのダイアログボックスが開きます。

注：

ただし、保護されている仮想マシン上で実行されているオペレーティングシステム内でシャットダウンを実行すると、ホスト障害が発生したときと同じように、自動的に再起動されます。この自動再起動により、オペレーターが間違えても、保護されている仮想マシンがシャットダウンされない事態を防ぐことができます。この仮想マシンをシャットダウンする場合は、その仮想マシンに設定されている高可用性機能による保護を最初に無効にします。

## 障害回復とバックアップ

December 30, 2019

Citrix Hypervisor の障害回復 (DR: Disaster Recovery) 機能により、ハードウェア障害などによりそのプールやサイト全体が使用不能になった場合に、仮想マシンや vApp を回復させることができます。単一サーバーの障害からの回復については、「[高可用性](#)」を参照してください。

注:

DR 機能を使用するには、ルートユーザーまたはプールオペレータ以上の権限が必要です。

## Citrix Hypervisor の障害回復のしくみ

Citrix Hypervisor の障害回復では、仮想マシンや vApp を回復するために必要なすべての情報がストレージリポジトリ (SR) 上に格納されます。その後、SR が実稼働環境 (プライマリサイト) からバックアップ環境 (セカンダリサイト) に複製されます。プライマリサイトのリソースプールが停止した場合、セカンダリサイト (障害回復サイト) 上に再作成された複製ストレージから仮想マシンや vApp を復元し、アプリケーションおよびユーザーのダウンタイムを最小限に抑えることができます。

XenCenter の [障害回復] 設定により、障害発生中に実行する複製ストレージへのクエリを生成し、インポートする仮想マシンや vApp を選択します。障害回復サイトのプールで仮想マシンが起動すると、そのプールのメタデータも複製されストレージ上に格納されます。プライマリサイトがオンライン状態に復帰するときに、セカンダリサイトで再作成された仮想マシンや vApp が、このメタデータに基づいてプライマリサイトに復元されます。同一仮想マシンの情報が複数の場所に存在する場合があります。(プライマリサイトのストレージ、障害回復サイトのストレージ、およびインポート先のプールに同一仮想マシンのメタデータが見つかった場合など。) もし XenCenter により同一仮想マシンの情報が複数の場所で検出された場合は、最新の情報のみが使用されます。

障害回復機能は、XenCenter および xe CLI で使用できます。CLI コマンドについては、「[障害回復コマンド](#)」を参照してください。

ヒント:

[障害回復] 設定を使って、障害回復システムの設定を確認するために、フェイルオーバーテストを実行することもできます。このテストでは、通常フェイルオーバーと同じ処理が実行されます。ただし、障害回復サイトにエクスポートされた仮想マシンや vAPP は起動しません。テストが完了したら、クリーンアップが実行され、障害回復サイトに再作成されたすべての仮想マシン、vAPP、およびストレージが削除されます。

Citrix Hypervisor の仮想マシンは、以下の 2 つのコンポーネントで構成されています:

- 仮想マシンにより使用される仮想ディスク。その仮想マシンのリソースプールで構成されているストレージリポジトリ上に格納されます。
- 仮想マシン環境の内容が記述されたメタデータ。このメタデータは、使用不能になったり破損したりした仮想マシンを再作成するために必要です。通常、仮想マシンの作成時にメタデータ設定データが書き込まれ、仮想マシン構成を変更すると更新されます。プール内の仮想マシンでは、メタデータのコピーがそのプール内のすべてのサーバー上に格納されます。

障害回復機能が有効な場合、プールメタデータおよびプール内のすべての仮想マシンや vApp についての設定情報を使って、仮想マシンがセカンダリサイト上に再作成されます。各仮想マシンのメタデータには、仮想マシンの名前と説明、固有の識別子である UUID (Universally Unique Identifier)、メモリと仮想 CPU の構成、およびネットワークとストレージの情報が記録されます。また、仮想マシンの起動オプション (起動順序、起動間隔、および再起動優先度) も仮想マシンのメタデータに記録されます。これらのオプションは、高可用性または障害回復環境で仮想マ

シンを起動するときに使用されます。たとえば、障害発生時に仮想マシンを DR サイトのプールに再作成する場合、vApp に含まれる各仮想マシンはメタデータに記録されている順序および間隔で起動します。

## 障害回復のインフラストラクチャ要件

Citrix Hypervisor の障害回復機能を使用するには、プライマリサイトおよびセカンダリサイトで適切なインフラストラクチャをセットアップします。

- プールメタデータおよび仮想マシンの仮想ディスクで使用されるストレージが、実稼働環境（プライマリサイト）からバックアップ環境（セカンダリサイト）に複製されている必要があります。ストレージの複製方法（ミラー化など）はデバイスによって異なります。ストレージの複製については、使用するストレージソリューションのベンダーにお問い合わせください。
- 障害回復サイトのプールに再作成された仮想マシンおよび vApp が起動した後で、障害回復プールのメタデータと仮想ディスクを格納するストレージリポジトリが複製されている必要があります。これにより、プライマリサイトがオンライン状態になったときに、これらの仮想マシンおよび vApp がプライマリサイトに復元（フェイルバック）されます。
- DR サイトのハードウェアインフラストラクチャは、プライマリサイトと一致する必要はありません。ただし、Citrix Hypervisor のバージョンおよびパッチレベルが一致している必要があります。さらに、プライマリサイトすべての仮想マシンの再作成および実行に必要なリソースが障害回復プールに設定されている必要があります。

### 警告:

[障害回復] 設定では、ストレージレイの機能を制御することはできません。

障害回復機能を使用する場合は、メタデータのストレージが 2 つのサイト間で複製されるように設定しておく必要があります。一部のストレージレイには、ストレージを自動的に複製するためのミラー化機能が用意されています。このような機能を使用する場合は、仮想マシンが障害回復サイト上で再起動する前に、ミラー化機能を無効にしておく必要があります。

## 展開に関する考慮事項

障害回復機能を有効にする前に、以下の点について確認します。

### 障害発生前の手順

障害が発生する前に、以下の手順を行います。

- 仮想マシンおよび vApp を設定します。
- 仮想マシンおよび vApp とストレージリポジトリとの対応、ストレージリポジトリと LUN との対応を確認します。特に、`name_label`パラメーターと`name_description`パラメーターにこれらの対応を示す内容

を使用すると便利です。仮想マシンや vApp とストレージリポジトリの対応、およびストレージリポジトリと LUN の対応を表すストレージリポジトリ名を使用すると、複製ストレージからの仮想マシンや vApp の回復がわかりやすくなります。

- LUN の複製を設定します。
- これらの LUN 上の 1 つまたは複数のストレージリポジトリへのプールメタデータの複製を有効にします。
- プライマリプールメタデータを複製するストレージリポジトリが 1 つのプールにのみ接続されているようにします。

#### 障害発生後の手順

障害が発生した後では、以下の手順を行います。

- 障害回復サイトから共有ストレージへの読み取り/書き込みアクセスが正しく行われるように、既存のミラー化機能を無効にします。
- 仮想マシンデータの回復元の LUN がほかのプールに接続されていないことを確認します。ほかのプールに接続されていると、データが破損することがあります。
- 障害回復サイトを障害から保護する場合は、障害回復サイトの 1 つまたは複数のストレージリポジトリにプールメタデータを複製します。

#### 回復後の手順

仮想マシンが正しく回復された後では、以下の手順を行います。

- ミラー化されたストレージを再同期します。
- 障害回復サイトで、プライマリサイトにフェイルバックする仮想マシンや vApp を完全にシャットダウンします。
- プライマリサイトで、フェイルオーバー時と同じ手順に従って、選択した仮想マシンや vApp をプライマリサイトにフェイルバックします（前のセクションを参照）。
- プライマリサイトを再び保護する場合は、複製 LUN 上の 1 つまたは複数のストレージリポジトリへのプールメタデータの複製を有効にする。

#### 障害回復を有効にする

December 30, 2019

ここでは、XenCenter を使用して障害回復を有効にする方法について説明します。[障害回復の設定] オプションを使用して、プール内のすべての仮想マシンや vApp についての設定情報であるプールメタデータの格納先ストレージ

ジリポジトリを指定します。このメタデータは、管理者がプールの仮想マシンや vApp の設定を変更するたびにアップデートされます。

注:

障害回復を有効にできるのは、ストレージとして HBA 上の LVM または iSCSI 上の LVM を使用する場合があります。プールリカバリ情報を含む新しい LUN のために、このストレージに少量のスペースが必要です。

最初に、障害回復に使用しているストレージリポジトリがプライマリサイトで1つのプールにのみ接続され、セカンダリサイトのプールに接続されていないことを確認します。

障害回復を構成するには、次の手順を実行します。

1. プライマリサイトでフェイルオーバー対象のリソースプールを選択します。[プール] メニューから [障害回復]、[設定] の順に選択します。
2. プールメタデータの格納先として、最大で 8 つのストレージリポジトリを選択できます。プールリカバリ情報を含む新しい LUN のために、このストレージに少量のスペースが必要です。

注:

プール内のすべての仮想マシンの上方が格納されます。仮想マシンを個別に選択する必要はありません。

3. **[OK]** を選択します。これでプールの障害回復が有効になりました。

### 障害発生時の仮想マシンと vApp の回復（フェイルオーバー）

ここでは、障害発生時に仮想マシンや vApp をセカンダリ（障害回復）サイトにフェイルオーバーする方法について説明します。

1. XenCenter で、セカンダリサイトのリソースプールを選択し、[プール] メニューから [障害回復]、[障害回復ウィザード] の順に選択します。

この障害回復ウィザードでは、実行する操作として [フェイルオーバー]、[フェイルバック]、または [フェイルオーバーテスト] を選択できます。仮想マシンや vApp をセカンダリサイトにフェイルオーバーするには、[フェイルオーバー] をクリックして [次へ] を選択します。

警告:

ファイバチャネル共有ストレージで LUN ミラー化によるセカンダリサイトへのデータ複製を行っている場合は、回復を実行する前にミラー化を無効にする必要があります。これにより、セカンダリサイトからの読み取りおよび書き込みアクセスが可能になります。

2. 回復対象の仮想マシンや vApp のプールメタデータを格納しているストレージリポジトリを選択します。

デフォルトでは、このウィザードの一覧にプール内で接続されているすべてのストレージリポジトリが表示されます。ほかのストレージリポジトリを検出するには、[ストレージリポジトリの検出] をクリックして、目的のストレージの種類を選択します。

- ハードウェア HBA ストレージリポジトリを検出するには、[ハードウェア **HBA SR** の検出] を選択します。
- ソフトウェア iSCSI ストレージリポジトリを検出するには、[ソフトウェア **iSCSI SR** の検出] を選択して、ターゲットホスト、IQN、および LUN の情報を指定します。

ストレージリポジトリを選択したら、[次へ] をクリックして次のページに進みます。

3. 回復する仮想マシンと vApp を選択します。適切な [回復後の電源状態] オプションを選択して、回復後にウィザードがこれらを自動的に起動するかを指定します。または、フェイルオーバーの完了後に手動で起動することもできます。

[次へ] を選択して次のページに進み、事前チェックを開始します。

4. このウィザードでは、対象の仮想マシンや vApp が正しくセカンダリサイトにフェイルオーバーされるように、事前にいくつかのチェックが実行されます。たとえば、選択した仮想マシンや vApp に必要なストレージが使用可能かどうかチェックされます。この時点でストレージが見つからない場合は、このページの [**SR** の接続] を選択して適切なストレージリポジトリを接続できます。

事前チェックで見つかったすべての問題を解決したら、[フェイルオーバー] を選択します。回復処理が開始されます。

5. 進行状況のページに、各仮想マシンや vApp の回復処理が成功したかが表示されます。フェールオーバー処理は、複製されたストレージから仮想マシンおよび vApp のメタデータをエクスポートします。したがって、フェールオーバーに要する時間は、回復する仮想マシンおよび vApp によって異なります。それらの仮想マシンや vApp がプライマリサイトのプールで再作成された後、仮想ディスクを格納しているストレージリポジトリが仮想マシンに接続され、指定されている場合、仮想マシンが起動します。
6. フェールオーバーが完了したら、[次へ] を選択して結果レポートを表示します。結果レポートのページで [完了] をクリックして、ウィザードを終了します。

プライマリサイトが障害から復帰した後、仮想マシンをプライマリサイトに復元するには、再度障害回復ウィザードを使用して [フェイルバック] オプションを選択します。

#### 障害発生後の仮想マシンと vApp のプライマリサイトへの復元（フェイルバック）

このセクションでは、複製ストレージから仮想マシンおよび vApp を復元する方法について説明します。プライマリサイト（実務環境）が障害から復帰した後で、仮想マシンや vApp を複製ストレージからプライマリサイトに復元（フェイルバック）できます。仮想マシンや vApp をプライマリサイトにフェイルバックするには、障害回復ウィザードを使用します。

1. XenCenter で、プライマリサイトのリソースプールを選択し、[プール] メニューから [障害回復]、[障害回復ウィザード] の順に選択します。

この障害回復ウィザードでは、実行する操作として [フェイルオーバー]、[フェイルバック]、または [フェイルオーバーテスト] を選択できます。仮想マシンや vApp をプライマリサイトにフェイルバックするには、[フェイルバック] をクリックして [次へ] を選択します。

**警告:**

ファイバチャネル共有ストレージで LUN ミラー化によってプライマリサイトにデータを複製する場合は、復元を実行する前にミラー化を無効にする必要があります。プライマリサイトに読み取り/書き込みアクセス権があることを確認するには、ミラーリングを解除する必要があります。

2. 回復対象の仮想マシンや vApp のプールメタデータを格納しているストレージリポジトリを選択します。

デフォルトでは、このウィザードの一覧にプール内で接続されているすべてのストレージリポジトリが表示されます。ほかのストレージリポジトリを検出するには、[ストレージリポジトリの検出] をクリックして、目的のストレージの種類を選択します。

- ハードウェア HBA ストレージリポジトリを検出するには、[ハードウェア **HBA SR** の検出] を選択します。
- ソフトウェア iSCSI ストレージリポジトリを検出するには、[ソフトウェア **iSCSI SR** の検出] を選択して、ターゲットホスト、IQN、および LUN の情報を指定します。

ストレージリポジトリを選択したら、[次へ] をクリックして次のページに進みます。

3. 復元する仮想マシンと vApp を選択します。適切な [回復後の電源状態] オプションを選択して、回復後にウィザードがこれらを自動的に起動するかを指定します。または、フェイルバックの完了後に手動で起動することもできます。

[次へ] を選択して次のページに進み、事前チェックを開始します。

4. このウィザードでは、正しくフェイルバックされるように、事前にいくつかのチェックが実行されます。たとえば、選択した仮想マシンや vApp に必要なストレージが使用可能かどうかチェックされます。この時点でストレージが見つからない場合は、このページの [**SR** の接続] を選択して適切なストレージリポジトリを接続できます。

事前チェックで見つかったすべての問題を解決したら、[フェイルバック] を選択します。回復処理が開始されます。

5. 進行状況のページに、各仮想マシンや vApp の回復処理が成功したかが表示されます。フェイルバック処理は、複製されたストレージから仮想マシンおよび vApp のメタデータをエクスポートします。そのため、選択した仮想マシンや vApp の数によっては、フェイルバック処理に時間がかかることがあります。それらの仮想マシンや vApp がプライマリサイトのプールで再作成された後、仮想ディスクを格納しているストレージリポジトリが仮想マシンに接続され、指定されている場合、仮想マシンが起動します。

6. フェールオーバーが完了したら、[次へ] を選択して結果レポートを表示します。結果レポートのページで [完了] をクリックして、ウィザードを終了します。

## フェイルオーバーテスト

フェイルオーバーテストは、障害回復を計画するときに重要な機能です。[障害回復] ウィザードを使って、障害回復システムの設定を確認するために、フェイルオーバーテストを実行することもできます。このテストでは、通常のフ

フェイルオーバーと同じ処理が実行されますが、障害回復サイトにエクスポートされた仮想マシンや vApp は一時停止状態で起動します。テストが完了すると、これらの仮想マシンや vApp、および再作成されたストレージが障害回復サイトから自動的に削除されます。障害回復の初回設定時、および障害回復が有効なプールの構成を大幅に変更したときに、フェイルオーバーテストを実行して障害回復が正しく機能することを確認します。

1. XenCenter で、セカンダリサイトのリソースプールを選択し、[プール] メニューから [障害回復]、[障害回復ウィザード] の順に選択します。
2. 実行する操作として [フェイルオーバーテスト] をクリックし、[次へ] を選択します。

注:

ファイバチャネル共有ストレージで LUN ミラー化によるセカンダリサイトへのデータ複製を行っている場合は、回復を実行する前にミラー化を無効にする必要があります。これにより、セカンダリサイトからの読み取りおよび書き込みアクセスが可能になります。

3. 回復対象の仮想マシンや vApp のプールメタデータを格納しているストレージリポジトリを選択します。

デフォルトでは、このウィザードの一覧にプール内で接続されているすべてのストレージリポジトリが表示されます。ほかのストレージリポジトリを検出するには、[ストレージリポジトリの検出] をクリックして、目的のストレージの種類を選択します:

- ハードウェア HBA ストレージリポジトリを検出するには、[ハードウェア **HBA SR** の検出] を選択します。
- ソフトウェア iSCSI ストレージリポジトリを検出するには、[ソフトウェア **iSCSI SR** の検出] を選択して、ターゲットホスト、IQN、および LUN の情報を指定します。

ストレージリポジトリを選択したら、[次へ] をクリックして次のページに進みます。

4. フェイルオーバーする仮想マシンや vApp を選択し、[次へ] を選択して次のページに進み、事前チェックを開始します。
5. フェイルオーバーテストを開始する前に、ウィザードはいくつかの事前チェックを実行します。たとえば、選択した仮想マシンや vApp に必要なストレージが使用可能かどうかチェックされます。

- ストレージが使用可能かどうかのチェック。必要なストレージが見つからない場合は、このページの [SR の接続] をクリックして適切なストレージリポジトリを接続できます。
- 障害回復サイトのプールで高可用性が無効になっているかどうかのチェック。プライマリプールと DR プールの両方で同じ仮想マシンを実行しないようにするには、セカンダリプールで高可用性を無効にする必要があります。回復後に回復された仮想マシンおよび vApp が自動的に起動しないようにするには、高可用性を無効にする必要があります。セカンダリサイトのプールの高可用性を無効にするには、[高可用性の無効化] をクリックしますここで無効にした高可用性機能は、フェイルオーバーテストの完了時に自動的に有効になります。

事前チェックで見つかったすべての問題を解決したら、[フェイルオーバー] を選択します。フェイルオーバーテストが開始されます。

6. 進行状況のページに、各仮想マシンや vApp の回復処理が成功したかが表示されます。フェイルオーバー処理は、複製されたストレージから仮想マシンおよび vApp のメタデータを回復します。そのため、選択した仮想マシンや vApp の数によっては、フェイルオーバー処理に時間がかかることがあります。それらの仮想マシンや vApp がセカンダリサイトのプールで再作成された後、仮想ディスクを格納しているストレージリポジトリが仮想マシンに接続されます。

フェイルオーバーテストでは、セカンダリサイトにフェイルオーバーされた仮想マシンは実行されず、一時停止状態になります。

7. フェイルオーバーテストに成功したら、[次へ] を選択します。これにより、障害回復サイトがクリーンアップされます：

- フェイルオーバーにより再作成された仮想マシンや vApp が、ここで削除されます。
- これにより、障害回復サイトがクリーンアップされます。
- フェイルオーバーテストの事前チェック時にセカンダリサイトのプールの高可用性を無効にした場合は、ここで自動的に有効になります。

障害回復サイトのクリーンアップ処理の進行状況がウィザードに表示されます。

8. [完了] を選択してウィザードを終了します。

## vApp

December 30, 2019

vApp は、関連する複数の仮想マシンを単一の管理対象として論理的にグループ化したものです。vApp が起動されると、vApp に含まれる仮想マシンが、ユーザーが事前定義した順序で起動されます。この起動順序により、お互いに依存する仮想マシンを自動的に順序付けすることができます。システム全体の再起動が必要な場合に、管理者が依存関係を考慮しながら順番に仮想マシンを起動する必要はありません。たとえば、ソフトウェアのアップデート時などです。vApp に含まれる仮想マシンは同一ホスト上で動作する必要はなく、通常の規則に従ってリソースプール内で移行されます。vApp 機能は、障害回復 (DR) の状況で役立ちます。DR シナリオでは、管理者はすべての仮想マシンを同じストレージリポジトリにグループ化するか、同じ SLA (Service Level Agreement: サービスレベルアグリーメント) に関連付けることができます。

vApp で仮想マシンをグループ化するには、次の手順に従います：

1. プールを選択して、[プール] メニューの [vApp の管理] を選択します。
2. 新しい vApp の名前と、任意で説明を入力し、[次へ] をクリックします。

vApp の内容を示す名前を指定すると便利です。XenCenter では複数の vApp に同じ名前を使用することも可能ですが、重複しないわかりやすい名前を指定することをお勧めします。また、スペースを含む名前を引用符で囲む必要はありません。

3. 新しい vApp に追加する仮想マシンを選択して、[次へ] をクリックします。

[検索] オプションを使用して、名前に特定のテキスト文字列が含まれる仮想マシンだけを一覧に表示することもできます。

4. vApp に追加した仮想マシンの起動順序を指定し、[次へ] をクリックします。

起動順序: vApp に追加した仮想マシンの起動順序を指定します。起動順序の値が 0 (ゼロ) の仮想マシンが最初に起動されます。次に値が 1 の仮想マシン、そして値が 2 の仮想マシンという順序で起動されます。

次の VM 起動までの間隔: 起動シーケンスの値でグループ化される仮想マシンの起動間隔を指定します。

5. 最後のページで、vApp 構成オプションを確認できます。[前へ] をクリックして前のページに戻って設定を変更するか、[完了] をクリックして vApp を作成します。

注:

同一リソースプール内の異なるホスト上の仮想マシンをグループ化して vApp を作成することもできますが、異なるプールの仮想マシンで vApp を作成することはできません。

## XenCenter での vApp の管理

XenCenter の [vApp の管理] 設定によって、vApp を作成、削除、変更できます。vApp を起動やシャットダウンしたり、選択したプールで vApp をインポートおよびエクスポートしたりできます。一覧で vApp を選択すると、その vApp に含まれているすべての仮想マシンがダイアログボックスに表示されます。詳しくは、XenCenter ドキュメントの「[vApp](#)」を参照してください。

## ホストと仮想マシンのバックアップと復元

December 30, 2019

可能な限り、Citrix Hypervisor サーバーのインストール後の状態を変更しないでください。Citrix Hypervisor サーバーは通常のサーバーとは異なるため、追加のパッケージをインストールしたり、追加のサービスを起動したりしないでください。Citrix Hypervisor サーバーの状態を元に戻すには、インストールメディアからサーバーを再インストールします。複数の Citrix Hypervisor サーバーがある場合は、TFTP サーバーと、適切な回答ファイルを設定することが最善の方法です。詳しくは、「[ネットワークブートによるインストール](#)」を参照してください。

認定パートナーが提供するバックアップソリューションの使用をお勧めします。詳しくは、「[Citrix Ready Marketplace](#)」を参照してください。

Citrix Hypervisor 7.3 以降のバージョンを実行中の Citrix Hypervisor Premium Edition ユーザーは、変更ブロックのみの、より高速なバックアップを利用できます。詳しくは、Citrix ブログの[変更ブロック追跡のバックアップ API](#)に関するエントリを参照してください。

潜在的なハードウェアやソフトウェアの障害に備えて、ここで説明する複数のバックアップ手順を頻繁に行うことをお勧めします。

プールメタデータをバックアップするには:

1. 次のコマンドを実行します:

```
1 xe pool-dump-database file-name=backup
```

2. データベースを復元するには、次のコマンドを実行します:

```
1 xe pool-restore-database file-name=backup dry-run=true
```

このコマンドでは、バックアップに必要な、適切な名前を持つ NIC が適切な数だけホストにインストールされているかどうかチェックされます。

ホスト構成およびソフトウェアをバックアップするには:

1. 次のコマンドを実行します:

```
1 xe host-backup host=host file-name=hostbackup
```

注:

- コントロールドメイン (Dom0) にバックアップを作成しないでください。
- バックアップ手順で大きなバックアップファイルを作成できます。
- 復元処理を完了するために、元のインストール CD から起動する必要があります。
- この手順で作成したバックアップファイルは、作成元のホストの復元にものみ使用できます。

仮想マシンをバックアップするには:

1. バックアップ対象の仮想マシンがオフラインであることを確認します。
2. 次のコマンドを実行します:

```
1 xe vm-export vm=vm_uuid filename=backup
```

注:

この手順により、仮想マシン上のすべてのデータも一緒にバックアップされます。仮想マシンをインポートするときは、バックアップデータ用に使用するストレージメカニズムを指定できます。

警告:

バックアップ処理は、すべての仮想マシンデータをバックアップするため、完了まで時間がかかります。

仮想マシンメタデータのみをバックアップするには:

次のコマンドを実行します:

```
1 xe vm-export vm=vm_uuid filename=backup metadata=true
```

## 仮想マシンのメタデータのバックアップ

ストレージやネットワークなどの関連リソースや仮想マシンに関するメタデータは、各 Citrix Hypervisor サーバー上のデータベースに格納されます。ストレージリポジトリとこのデータベースにより、プール内で使用可能なすべての仮想マシンの完全な情報が提供されます。このため、物理ハードウェアの障害やそのほかの災害シナリオから復旧できるように、このデータベースのバックアップ方法を理解しておくことは重要です。

ここでは、最初に単一ホスト環境のメタデータのバックアップ方法を説明し、次に複雑なプール構成のバックアップ方法を説明します。

### 単一ホスト環境でのバックアップ

プールデータベースをバックアップするには、CLI を使用します。一貫したプールメタデータバックアップファイルを取得するには、Citrix Hypervisor サーバー上で `pool-dump-database` を実行し、その結果ファイルをアーカイブします。バックアップファイルには、プールに関する機密性の高い認証情報が含まれます。このため、安全な方法で保管してください。

プールメタデータを復元するには、最新のダンプファイルに対して `xe pool-restore-database` コマンドを実行します。Citrix Hypervisor サーバーが完全に動作不能になった場合は、再度新規インストールを行い、その後でその Citrix Hypervisor サーバーに対して `pool-restore-database` コマンドを実行します。

プールデータベースの復元後、一部の仮想マシンは引き続き `Suspended` 状態として認識される場合があります。そのサスペンド状態のメモリが格納されている場所 (`suspend-VDI-uuid` フィールドで定義される) がローカルのストレージリポジトリである場合、ホストの再インストールにより仮想マシンが使用不可になります。このような仮想マシンを起動できるように `Halted` 状態にリセットするには、`xe vm-shutdown vm=vm_name -force` コマンドまたは `xe vm-reset-powerstate vm=vm_name -force` コマンドを使用します。

#### 警告:

この方法で復元された Citrix Hypervisor ホストでは、元の UUID が保持されます。このため、元の Citrix Hypervisor サーバーが動作しているときに、別の物理マシンにそのホストを復元すると、UUID の競合が発生します。結果として、XenCenter は 2 番目の Citrix Hypervisor サーバーへの接続を拒否します。物理ホストを複製する目的でプールデータベースのバックアップを使用することは推奨されません。物理ホストを複製するには、自動インストールの機能を使用してください。詳しくは、「[インストール](#)」を参照してください。

### プール環境でのバックアップ

リソースプール環境では、プールマスタがプライマリのデータベースを提供し、このデータベースがプールメンバホストによって同期され、ミラー化されます。これにより、プールに冗長性が提供されます。プール内のすべてのホス

トがプールデータベースの正確なコピーを保持しているため、任意のメンバがプールマスターとして動作することができます。メンバーホストをプールマスターとして動作させる方法については、「[ホストとリソースプール](#)」を参照してください。

このレベルの冗長性では不十分なことがあります。たとえば、仮想マシンデータを格納する共有ストレージを複数サイトにバックアップし、プールメタデータを格納するローカルサーバストレージをバックアップしない場合などです。共有ストレージを持つプールを作成し直すには、最初にプールマスター上の `pool-dump-database` ファイルのバックアップを行い、このファイルをアーカイブしておきます。このバックアップを新しいホストセットで後で復元するには：

1. インストールメディアを使用して Citrix Hypervisor サーバーの新規インストールを行うか、TFTP サーバーからネットワークブートを実行します。
2. 新しいプールマスターとして動作するホストで、`xe pool-restore-database` を実行します。
3. 新しいプールマスターで、`xe host-forget` コマンドを実行し、古いメンバホストを消去します。
4. メンバーホストで `xe pool-join` コマンドを実行し、それらのホストを新しいプールに追加します。

## Citrix Hypervisor サーバーのバックアップ

ここでは、Citrix Hypervisor サーバーのコントロールドメインのバックアップおよび復元の手順について説明します。以下の手順では、仮想マシンを格納するストレージリポジトリはバックアップしません。Xen および Citrix Hypervisor エージェントを実行するコントロールドメイン (Dom0) のみをバックアップします。

### 注：

特権コントロールドメインは、ほかのパッケージでカスタマイズしないで、インストール後の状態で運用するのが最善です。このため復旧方法として、Citrix Hypervisor メディアから Citrix Hypervisor のインストールを正常に行えるよう、ネットワークブート環境を設定しておくことをお勧めします。通常、コントロールドメインをバックアップする必要はありませんが、プールのメタデータを保存することをお勧めします（「仮想マシンのメタデータのバックアップ」参照）。このバックアップ方法は、プールメタデータのバックアップを補完するものです。

さらに、`xe` コマンドの `host-backup` と `host-restore` を使用することもできます。`xe host-backup` コマンドでは、アクティブなパーティションを指定したファイルにアーカイブします。`xe host-restore` コマンドは、`xe host-backup` コマンドで作成したアーカイブを、ホストの非アクティブなパーティションに抽出します。このパーティションをアクティブにするには、インストール CD から起動して、バックアップを復元するオプションを選択します。

上記の手順を実行してホストを再起動したら、仮想マシンメタデータが一貫した状態に復元されていることを確認します。`/var/backup/pool-database- $\{$ DATE $\}$`  で `xe pool-restore-database` を実行して、仮想マシンメタデータを復元します。このファイルは、`xe pool-dump-database` コマンドにより作成されたものです。このコマンドでは、実行中のファイルシステムをアーカイブする前に仮想マシンメタデータの一貫した状態のスナップショットを作成する `xe host-backup` が実行されます。

**Citrix Hypervisor** サーバーをバックアップするには:

十分な空きディスク容量があるリモートホスト上で、次のコマンドを実行します。

```
1 xe host-backup file-name=filename -h hostname -u root -pw password
```

これにより、コントロールドメインのファイルシステムの圧縮イメージが作成され、`file-name` 引数で指定したファイルに保存されます。

実行中の **Citrix Hypervisor** サーバーを復元するには:

1. 特定のバックアップから実行中の Citrix Hypervisor サーバーを復元するには、その Citrix Hypervisor サーバーが稼働していて到達可能な状態で次のコマンドを実行します:

```
1 xe host-restore file-name=filename -h hostname -u root -pw password
```

これにより、(`filename` で指定するファイルを格納するホストではなく) コマンドを実行した Citrix Hypervisor サーバーのハードディスクに、圧縮イメージが復元されます。この意味では、「復元」という言葉は紛らわしいかもしれません。通常、復元とはバックアップした状態に完全に戻すことを指します。この復元コマンドは、圧縮されたバックアップファイルを展開するだけですが、別のパーティション (`/dev/sda2`) に書き込んでおり、現在のバージョンのファイルシステムを上書きしません。

2. ルートファイルシステムの復元されたバージョンを使用するには、Citrix Hypervisor のインストール CD を使用して Citrix Hypervisor サーバーを再起動し、[バックアップから復元] オプションを選択する必要があります。

バックアップからの復元後、Citrix Hypervisor サーバーを再起動すると、復元されたイメージから起動します。

3. 最後に、次のコマンドを実行して、仮想マシンメタデータを復元します:

```
1 xe pool-restore-database file-name=/var/backup/pool-database-* -h hostname -u root -pw password
```

注:

ここで説明したバックアップからの復元を行っても、バックアップパーティションは破棄されません。

クラッシュした **Citrix Hypervisor** サーバーを再起動するには:

Citrix Hypervisor サーバーがクラッシュして到達不能になった場合は、Citrix Hypervisor のインストール CD を使用してアップグレードインストールを実行します。アップグレードインストールが完了したら、マシンを再起動し、XenCenter またはリモート CLI からホストに到達可能であることを確認します。

その後、このセクションでの説明どおりに Citrix Hypervisor サーバーのバックアップを続行します

### 仮想マシンのバックアップ

認定パートナーが提供するバックアップソリューションの使用をお勧めします。詳しくは、「[Citrix Ready Marketplace](#)」を参照してください。

Citrix Hypervisor 7.3 以降のバージョンを実行中の Citrix Hypervisor Premium Edition ユーザーは、変更ブロックのみの、より高速なバックアップを利用できます。詳しくは、Citrix ブログの[変更ブロック追跡のバックアップ API](#)に関するエントリを参照してください。

### 仮想マシンスナップショット

December 30, 2019

Citrix Hypervisor には、便利なスナップショット機能が用意されています。この機能では、仮想マシンのストレージとメタデータのスナップショットを作成して、その時点の仮想マシンの状態を保存しておくことができます。スナップショットを作成するときは、自己矛盾のないディスクイメージが保存されるように、必要に応じて一時的にデータ入出力が停止します。

スナップショットにより、仮想マシンのテンプレート化と類似の機能が提供されます。仮想マシンのスナップショットには、すべてのストレージ情報と、接続している仮想インターフェイス (VIF) などの仮想マシン設定が含まれ、バックアップ用にエクスポートしたり復元したりできます。スナップショットはすべての種類のストレージでサポートされています。ただし、ストレージが LVM ベースである場合、次の要件を満たす必要があります：

- 以前のバージョンの Citrix Hypervisor でストレージリポジトリが作成された場合、アップグレードされる必要があります
- ボリュームはデフォルトの形式にする必要があります (`type=raw` ボリュームのスナップショットは作成できません)

スナップショット処理では、次の 2 段階のプロセスが実行されます。

- メタデータをテンプレートとして取り込む。
- ディスクの VDI スナップショットを作成する。

次のタイプの仮想マシンスナップショットがサポートされています：標準スナップショット、およびメモリを含んだスナップショット。

#### 標準スナップショット

標準スナップショットはクラッシュ整合状態であり、Linux 仮想マシンを含むすべての種類の仮想マシンで作成できます。

## メモリを含んだスナップショット

仮想マシンのディスク（ストレージ）およびメタデータに加えて、仮想マシンのメモリ（RAM）をスナップショットに含めることができます。この機能は、ソフトウェアをアップグレードする場合、またはパッチを適用する場合に役立ち、変更前の仮想マシンのメモリ（RAM）に戻すこともできます。この種類のスナップショットへの復元時に仮想マシンを再起動する必要はありません。

メモリを含んだスナップショットは、管理 API、xe CLI、または XenCenter を使って、実行中またはサスペンド状態の仮想マシンで作成できます。

## 仮想マシンスナップショットの作成

スナップショットを作成する前に、オペレーティングシステム固有の設定と考慮事項について、次の情報を参照してください。

- [sysprep を使用した Windows 仮想マシンの複製の準備](#)
- [Linux 仮想マシンの複製の準備](#)

まず、メモリステータスを取得できるように、仮想マシンが実行または一時停止されていることを確認します。対象の仮想マシンを指定するには、`vm=name` または `vm=vm uuid` 引数を使用します。

仮想マシンのスナップショットを作成するには、`vm-snapshot` コマンドを実行します。

```
1 xe vm-snapshot vm=vm uuid new-name-label=vm_snapshot_name
```

## メモリを含んだスナップショットの作成

次の `vm-checkpoint` コマンドを実行します。このとき、メモリを含んだスナップショットであることを示す名前を指定すると便利です：

```
1 xe vm-checkpoint vm=vm uuid new-name-label=name of the checkpoint
```

Citrix Hypervisor でスナップショットが作成されると、その UUID が表示されます。

次に例を示します：

```
1 xe vm-checkpoint vm=2d1d9a08-e479-2f0a-69e7-24a0e062dd35 \
2 new-name-label=example_checkpoint_1
3 b3c0f369-59a1-dd16-ecd4-a1211df29886
```

メモリを含んだスナップショットを作成するには、各ディスクに 4MB 以上の空き領域と、RAM と同等のサイズ、および 20% 程度のオーバーヘッドが必要です。つまり、RAM のサイズが 256MB である場合は、約 300MB のストレージが必要です。

注:

メモリを含んだスナップショットの作成中に、仮想マシンが一時的に停止し、使用できない状態になります。

**Citrix Hypervisor** プールのすべてのスナップショットの一覧を表示するには

`snapshot-list` コマンドを実行します:

```
1 xe snapshot-list
```

これにより、Citrix Hypervisor プール内のすべてのスナップショットの一覧が表示されます。

特定の仮想マシンのスナップショットを一覧表示するには

`vm-list` コマンドを実行して、特定の仮想マシンの UUID を取得します。

```
1 xe vm-list
```

これにより、すべての仮想マシンとその UUID が表示されます。次に例を示します:

```
1 xe vm-list
2 uuid (RO): 116dd310-a0ef-a830-37c8-df41521ff72d
3 name-label (RW): Windows Server 2012 (1)
4 power-state (RO): halted
5
6 uuid (RO): 96fde888-2a18-c042-491a-014e22b07839
7 name-label (RW): Windows 2008 R2 (1)
8 power-state (RO): running
9
10 uuid (RO): dff45c56-426a-4450-a094-d3bba0a2ba3f
11 name-label (RW): Control domain on host
12 power-state (RO): running
```

また、仮想マシンのリストをフィールドの値でフィルタして、対象の仮想マシンを指定することもできます。

たとえば、`power-state=halted` を指定すると、`power-state` フィールドの値が `halted` である仮想マシンだけが対象になります。複数の仮想マシンがフィルタ条件に一致し、そのすべてのオブジェクトに対してコマンドを実行する場合は、オプション `--multiple` を指定する必要があります。`xe vm-list params=all` コマンドを使用して、一致するフィールドの完全なリストを取得します。

目的の仮想マシンの UUID を指定して、次のコマンドを実行します。

```
1 xe snapshot-list snapshot-of=vm uuid
```

次に例を示します：

```
1 xe snapshot-list snapshot-of=2d1d9a08-e479-2f0a-69e7-24a0e062dd35
```

これにより、この仮想マシンのスナップショットの一覧が表示されます。

```
1 uuid (RO): d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
2 name-label (RW): Regular
3 name-description (RW):
4 snapshot_of (RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
5 snapshot_time (RO): 20090914T15:37:00Z
6
7 uuid (RO): 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef
8 name-label (RW): Snapshot with memory
9 name-description (RW):
10 snapshot_of (RO): 2d1d9a08-e479-2f0a-69e7-24a0e062dd35
11 snapshot_time (RO): 20090914T15:39:45Z
```

仮想マシンをスナップショット作成時の状態に戻す

仮想マシンを特定のスナップショット作成時の状態に復元するには、そのスナップショットの UUID を指定して、`snapshot-revert` コマンドを実行します：

1. 次の `snapshot-list` コマンドを実行して、復元先のスナップショットの UUID を取得します：

```
1 xe snapshot-list
```

2. 取得した UUID を指定して、次のコマンドを実行します。

```
1 xe snapshot-revert snapshot-uuid=snapshot uuid
```

次に例を示します：

```
1 xe snapshot-revert snapshot-uuid=b3c0f369-59a1-dd16-ecd4-
 a1211df29886
```

仮想マシンがスナップショット作成時の状態に戻り、サスペンド状態になります。

注：

- スナップショットのシックプロビジョニングのためのディスク容量が足りない場合は、ディスク領域が解放されるまでスナップショットを復元できません。この場合は、操作を再試行してください。
- その仮想マシンの任意のスナップショットを復元先として指定できます。また、この復元処理により既存のスナップショットが削除されることはありません。

## スナップショットの削除

スナップショットを削除するには、以下の手順に従います：

1. 次の`snapshot-list`コマンドを実行して、復元先のスナップショットの UUID を取得します：

```
1 xe snapshot-list
```

2. 取得した UUID を指定して、次の`snapshot-uninstall`コマンドを実行します：

```
1 xe snapshot-uninstall snapshot-uuid=snapshot-uuid
```

3. これにより、仮想マシンおよび VDI が削除されることを警告するメッセージが表示されます。処理を続行するには、`yes`と入力します。

次に例を示します：

```
1 xe snapshot-uninstall snapshot-uuid=1760561d-a5d1-5d5e-2be5-
 d0dd99a3b1ef
2 The following items are about to be destroyed
3 VM : 1760561d-a5d1-5d5e-2be5-d0dd99a3b1ef (Snapshot with memory)
4 VDI: 11a4aa81-3c6b-4f7d-805a-b6ea02947582 (0)
5 VDI: 43c33fe7-a768-4612-bf8c-c385e2c657ed (1)
6 VDI: 4c33c84a-a874-42db-85b5-5e29174fa9b2 (Suspend image)
7 Type 'yes' to continue
8 yes
9 All objects destroyed
```

スナップショットのメタデータのみを削除する場合は、次のコマンドを実行します。

```
1 xe snapshot-destroy snapshot-uuid=snapshot-uuid
```

次に例を示します：

```
1 xe snapshot-destroy snapshot-uuid=d7eefb03-39bc-80f8-8d73-2ca1bab7dcff
```

## スナップショットテンプレート

スナップショットから新しいテンプレートを作成する

スナップショットから仮想マシンテンプレートを作成できます。ただし、メモリの状態は削除されます。

1. 次の`snapshot-copy`コマンドを実行します。ここで、`new-name-label`でテンプレートの名前を指定します：

```
1 xe snapshot-copy new-name-label=vm-template-name \
2 snapshot-uuid=uuid of the snapshot
```

次に例を示します:

```
1 xe snapshot-copy new-name-label=example_template_1 \
2 snapshot-uuid=b3c0f369-59a1-dd16-ecd4-a1211df29886
```

注:

これにより作成されるテンプレートは、スナップショットと同じリソースプールに属します。つまり、そのプールの Citrix Hypervisor データベース内にもみ格納されます。

2. テンプレートが作成されたことを確認するには、次の `template-list` を実行します:

```
1 xe template-list
```

これにより、その Citrix Hypervisor サーバー上のすべてのテンプレートが一覧表示されます。

スナップショットをテンプレートとしてエクスポートする

仮想マシンのスナップショットをエクスポートすると、ディスクイメージを含む仮想マシンの完全な複製が、ローカルコンピュータ上に格納されます。このファイルのファイル拡張子は `.xva` です。

1. `snapshot-export-to-template` コマンドを使用してテンプレートファイルを作成します:

```
1 xe snapshot-export-to template snapshot-uuid=snapshot-uuid \
2 filename=template- filename
```

次に例を示します:

```
1 xe snapshot-export-to-template snapshot-uuid=b3c0f369-59a1-dd16- \
 ecd4-a1211df29886 \
2 filename=example_template_export
```

仮想マシンのエクスポート/インポート機能は、さまざまな方法で使用できます:

- 仮想マシンのバックアップのための便利な機能として。障害発生時には、エクスポートした仮想マシンファイルを使用して仮想マシン全体を復元できます。
- 仮想マシンを簡単に複製する方法として。たとえば、よく使用する特別な目的のサーバー設定の仮想マシンなどです。思いどおりに仮想マシンを設定、エクスポート、およびインポートして、元の仮想マシンの複製を作成できます。
- 仮想マシンを簡単にほかのサーバーに移動する方法として。

テンプレートの使用について詳しくは、「[仮想マシンの作成](#)」および XenCenter ドキュメントの「[仮想マシンの管理](#)」を参照してください。

## スケジュールされたスナップショット

スケジュールされたスナップショットについてスケジュールされたスナップショットについてスナップショットスケジュール機能では、重要なサービスを提供する仮想マシンを保護するためのシンプルな手段が提供されます。この機能では、定期的にスナップショットが自動作成されるように設定できます。スケジュールされたスナップショットは、リソースプールレベルで特定の仮想マシンのスナップショットスケジュールを作成します。スケジュールされたスナップショットを有効にすると、指定した時刻、曜日、または週に仮想マシンのスナップショットが作成されます。仮想マシンの用途に応じていくつかのスケジュールされたスナップショットを作成して、異なるスケジュールを定義できます。仮想マシンの用途に応じていくつかのスケジュールされたスナップショットを作成して、異なるスケジュールを定義できます。

XenCenter のこの機能を使用するためのいくつかのツールが用意されています。

- スケジュールされたスナップショットを定義するには、新規スナップショットスケジュールウィザードを使用します。
- リソースプールのスケジュールされたスナップショットを有効/無効化、変更、削除するには、**[VM スナップショットスケジュール]** ダイアログボックスを使用します。
- スナップショットスケジュールを編集するには、**[VM スナップショットスケジュール]** ダイアログボックスから **[プロパティ]** ダイアログボックスを開きます。
- スケジュールされたスナップショットから仮想マシンを復元するには、**[スナップショット]** タブでそのスナップショットを選択し、スナップショットへの復元を行います。

詳しくは、XenCenter ドキュメントの「[スケジュールされたスナップショット](#)」を参照してください。

## マシン障害への対処

March 12, 2020

ここでは、さまざまな障害からの回復方法について詳しく説明します。ここで説明するすべての障害回復シナリオでは、[バックアップ](#)で説明されているいずれかの方法でバックアップされていることを前提としています。

### メンバーの障害

高可用性機能が無効なリソースプールでは、プールマスタがメンバホストからの定期的なハートビートメッセージを監視して、メンバホストに発生する障害を検出します。ハートビートが 600 秒受信されない場合、プールマスタはメンバホストに障害が発生していると認識します。この状態から回復させる方法には、2 つあります。

- 動作していないメンバーホストの問題を解決して起動します（物理的に再起動するなど）。メンバーホストとプールマスターとの接続が復元されると、そのメンバーホストが動作中であることがプールマスターにより再度マーク付けされます。
- メンバーホストをシャットダウンし、`xe host-forget` CLI コマンドを使用してそのメンバーの情報をプールマスターから消去します。メンバーホストの情報をプールマスターから消去すると、そのメンバーホスト上で実行されていたすべての仮想マシンは「オフライン」としてマーク付けされ、ほかの Citrix Hypervisor サーバー上で再起動可能になります。

障害が発生した Citrix Hypervisor サーバーが正しくオフラインとして認識されないと、仮想マシンデータが破損することがあるため注意してください。

`xe host-forget`でプールを単一ホストの複数のプールに分割しないでください。この処理を行うと、分割したプールがすべて同じ共有ストレージを使用するために、仮想マシンデータが破損することがあります。

**警告:**

- プールから消去したホストをアクティブなホストとして再度使用する場合は、Citrix Hypervisor ソフトウェアを新規にインストールしてください。
- リソースプールの高可用性を有効にしたまま、`xe host-forget`コマンドを使用しないでください。最初に高可用性を無効にしてからそのホストの接続を消去し、高可用性を再度有効にします。

メンバー Citrix Hypervisor サーバーに障害が発生した後で、そのホスト上の仮想マシンの状態が「実行中」として認識されることがあります。そのメンバー Citrix Hypervisor サーバーが停止していることが確実である場合は、`xe vm-reset-powerstate`コマンドを使用して、仮想マシンの電源状態を強制的に「停止」(`halted`) に設定してください。詳しくは、「[vm-reset-powerstate](#)」を参照してください。

**警告:**

このコマンドの使用を誤ると、データが破損することがあります。このコマンドは必要な場合にのみ使用してください。

ほかの Citrix Hypervisor サーバー上で仮想マシンを起動できるようにするには、仮想マシンストレージのロックを解除する必要があります。ストレージリポジトリ上の各ディスクは、同時に複数のホストで使用することはできません。停止したホストにより使用されていたディスクをほかの Citrix Hypervisor サーバーで使用できるようにするには、ストレージのロックを解除します。これを行うには、プールマスター上で、仮想マシンのディスクを格納している各ストレージリポジトリに対して次のスクリプトを実行します：`/opt/xenource/sm/resetvdis.py host_UUID SR_UUID master`

`master` を指定するのは、そのホストが障害発生時にストレージリポジトリマスターであった場合のみです。（ストレージリポジトリマスターはプールマスター、またはローカルストレージを使用する Citrix Hypervisor サーバー）

**警告:**

このコマンドを実行する前に、そのホストが停止していることを確認してください。このコマンドの使用を誤ると、データが破損することがあります。

`resetvdis.py`スクリプトを実行する前にほかの Citrix Hypervisor サーバー上で仮想マシンを起動しようとすると、次のエラーメッセージが表示されます: `VDI <UUID> already attached RW`。

## マスターの障害

リソースプールの各メンバーには、必要に応じてプールマスターの役割を引き継ぐための情報がすべて格納されています。プールマスターに障害が発生した場合、以下の処理が行われます。

1. 高可用性が有効なリソースプールでは、ほかのホストがプールマスターとして自動的に選出されます。
2. 高可用性が無効な場合、各メンバーはマスターが回復するのを待機します。

この時点でプールマスターが回復した場合、プール内のメンバーとの通信が再確立され、通常の状態に戻ります。

プールマスターが機能を停止している場合は、任意のメンバーホスト上で `xe pool-emergency-transition-to-master` コマンドを実行します。選択したメンバーホストがプールマスターとしての動作を開始したら、`xe pool-recover-slaves` コマンドを実行します。これにより、ほかのすべてのメンバーホストが新しいプールマスターとの通信を開始します。

停止したプールマスターのハードウェアの問題が解決した場合、または新しいサーバーに交換した場合は、Citrix Hypervisor ソフトウェアをインストールして、プールに追加できます。通常、リソースプール内の Citrix Hypervisor サーバーは同種であるため、新しいサーバーをプールマスターとして指定し直す必要はありません。

プールマスターとして動作する Citrix Hypervisor サーバーが変更された場合、デフォルトのプールストレージリポジトリに適切な値が設定されていることを確認します。このチェックを行うには、`xe pool-param-list` コマンドを使用して、`default-SR` パラメータに正しいストレージリポジトリが指定されていることを確認します。

## リソースプールの障害

リソースプール全体に障害が発生した場合は、プールデータベースを最初から作成し直さなければなりません。このような事態を避けるためにも、`xe pool-dump-database` コマンド (`pool-dump-database` を参照) を使用して、プールメタデータを定期的にバックアップしておく必要があります。

リソースプール全体の障害から回復するには:

1. ホストに XenServer ソフトウェアを新規にインストールします。この時点では、リソースプールを作成しません。
2. プールマスターとして動作するホストに対して `xe pool-restore-database` コマンド (`pool-restore-database` を参照) を使用し、バックアップからプールデータベースを復元します。
3. XenCenter でプールマスターに接続し、すべての共有ストレージおよび仮想マシンが使用可能になっていることを確認します。
4. 新規インストールした残りのメンバーホストをプールに追加して、適切なホスト上で仮想マシンを起動します。

## 設定エラーによる障害への対処

ホストに物理的な障害がない場合でも、ソフトウェアやホスト設定の問題により障害が発生することがあります。

1. 次のコマンドを実行してホストのソフトウェアおよび設定を復元します:

```
1 xe host-restore host=host file-name=hostbackup
```

2. ホストをインストール CD から起動して、**[Restore from backup]** を選択します。

## 物理マシンの障害

物理ホストマシンに障害が発生した場合は、以下の適切な手順に従って回復します。

### 警告:

障害が発生したホスト上で実行されていた仮想マシンは、プールのデータベースでは (「Running」) としてマーク付けされます。この動作は安全のためです。2 つの異なるホストで仮想マシンを同時に起動すると、深刻なディスク破損が発生します。管理者は、マシン (および仮想マシン) がオフラインになっていることを確認してから、次のコマンドを実行して仮想マシンの電源状態 (「Halted」) 状態に変更できます:

```
xe vm-reset-powerstate vm=vm_uuid --force
```

仮想マシンはその後、XenCenter またはコマンドラインインターフェイスを使用して再起動できます。

障害が発生したプールマスターをメンバーホストを実行したまま交換するには:

1. 次のコマンドを実行します:

```
1 xe pool-emergency-transition-to-master
2 xe pool-recover-slaves
```

2. コマンドの実行に成功したら、仮想マシンを再起動します。

すべての障害が発生したホストにリソースプールを復元するには:

1. 次のコマンドを実行します:

```
1 xe pool-restore-database file-name=backup
```

### 警告:

このコマンドは、適切な名前を持つ NIC が適切な数だけそのホストにインストールされている場合にのみ成功します。

2. ターゲットマシンで元のマシンと異なるストレージ設定が使用されている場合は、`pbid-destroy` コマンドを実行してストレージ設定を変更します。次 `pbid-create` コマンドを実行してストレージ設定を再作成します。これらのコマンドについては、[PBD \(物理ブロッケデバイス\) コマンド](#) を参照してください。

3. ストレージ設定を作成したら、`pbid-plug`を使用するか、XenCenter の [ストレージ] > [ストレージリポジトリの修復] を選択してそのストレージ設定を使用します。
4. すべての仮想マシンを再起動します。

仮想マシンストレージを使用できないときに仮想マシンを復元するには:

1. 次のコマンドを実行します。

```
1 xe vm-import filename=backup metadata=true
```

2. メタデータのインポートに失敗した場合は、次のコマンドを実行します。

```
1 xe vm-import filename=backup metadata=true --force
```

このコマンドにより、仮想マシンメタデータの復元が「最大限の努力」で試行されます。

3. すべての仮想マシンを再起動します。

## トラブルシューティング

March 12, 2020

### サポート

Citrix では、次の 2 種類のサポートを提供しています: [シトリックスサポート](#)の Web サイトで無料セルフヘルプサポートを利用するか、このサイトからサポートサービスを購入できます。Citrix のテクニカルサポートを受けるには、オンラインでサポートケースを登録したり、サポート担当者に電話したりできます。

[Citrix Knowledge Center](#)では、想定外の動作、クラッシュ、およびその他のほかの問題が発生した場合に役立つリソースが提供されています。含まれるリソース: 製品のドキュメント、ナレッジベース、ホワイトペーパー、ディスカッションフォーラム、Hotfix やその他のほかのアップデート。

このセクションの目的は、Citrix Hypervisor サーバーについて技術的な問題が発生した場合に、可能であればお客様による問題の解決を手助けすることです。問題が解決できない場合は、このセクションの情報を使用して、ソリューションプロバイダーに問い合わせる場合に必要なアプリケーションログやその他の情報を収集してください。

Citrix Hypervisor のインストールの問題のトラブルシューティングについて詳しくは、「[インストールのトラブルシューティング](#)」を参照してください。仮想マシンの問題のトラブルシューティングについて詳しくは、「[仮想マシンの問題のトラブルシューティング](#)」を参照してください。

#### 重要:

ここで説明するトラブルシューティングを実行する場合、ソリューションプロバイダーまたはテクニカルサポ

ートの指示に従うことをお勧めします。

デバッグ時に、ホストのシリアルコンソールへのアクセスが必要になることがあります。このため、Citrix Hypervisor のセットアップ時にシリアルコンソールにアクセスできるように設定しておくことをお勧めします。ブレードサーバーなど、物理シリアルポートを搭載していないホストや、適切な物理インフラストラクチャを使用できない環境では、Dell DRAC や HP iLO などの埋め込み管理デバイスを設定できるかどうかを確認してください。

シリアルコンソールアクセスの設定について詳しくは、[CTX121442](#)を参照してください。

### ヘルスチェック

ヘルスチェック機能は、サーバーの状態レポートを生成して Citrix Insight Services (CIS) にアップロードし、XenCenter で CIS 分析レポートを受信するために使用します。

任意の対象のプールを XenCenter に接続すると、プールに対してヘルスチェックを有効にするように求められます。登録処理中に次のことができます：

- CIS にサーバーの状態レポートを自動的にアップロードするために使用するスケジュールを指定する
- プールとの接続を確立するために使用する Citrix Hypervisor の資格情報を入力する
- CIS へのアップロードの認証を受ける

ヘルスチェックにプールが正常に登録されると、プールの状態に関する通知が XenCenter に送信されます。この機能により、CIS が生成するレポートに基づいて、Citrix Hypervisor システムの状態を積極的に監視できます。

### 要件

ヘルスチェック機能を使用するには：

- プール内のすべてのホストで Citrix Hypervisor 8.1 を実行している必要があります。
- Citrix Hypervisor 8.1 の XenCenter を使用して Citrix Hypervisor プールに接続する必要があります。
- XenCenter がインターネットにアクセスできる必要があります。
- ヘルスチェックサービスが XenCenter マシンにインストールされ、実行されている必要があります。
- Active Directory (AD) を使用している場合、プールオペレータ以上の権限が必要です。

ヘルスチェックおよびプールをヘルスチェックに登録する手順について詳しくは、[ヘルスチェック](#)を参照してください。

### Citrix Hypervisor サーバーログ

Citrix Hypervisor サーバーの情報を収集するには、XenCenter を使用できます。

[ツール] メニューの [サーバーの状態レポート] を選択して、[サーバーの状態レポート] タスクを開きます。さまざまな種類の情報 (各種ログ、クラッシュダンプなど) を一覧から選択してレポートを作成できます。収集された情

報は、XenCenter を実行しているコンピュータ上にダウンロードされます。詳しくは、[XenCenter ドキュメント](#)を参照してください。

さらに、Citrix Hypervisor サーバーには、`xen-bugtool`ユーティリティを使用して、ログ出力やほかのシステム情報を照合するいくつかの CLI コマンドが用意されています。xe コマンド `host-bugreport-upload` を使用すると、該当するログファイルとシステム情報を収集して、サポート FTP サイトにアップロードできます。このコマンドとそのオプションパラメーターについて詳しくは、[\[host-bugreport-upload\] \(/ja-jp/citrix-hypervisor/command-line-interface.html#host-bugreport-upload\)](#) を参照してください。サポートチームにクラッシュダンプの提出を要求された場合は、xe コマンド `host-crashdump-upload` を使用します。このコマンドとそのオプションパラメーターについて詳しくは、[\[host-crashdump-upload\] \(/ja-jp/citrix-hypervisor/command-line-interface.html#host-crashdump-upload\)](#) を参照してください。

**重要:**

Citrix Hypervisor サーバーログには、機密情報が含まれている可能性があります。

### ホストログメッセージの中央サーバーへの送信

ログをコントロールドメインのファイルシステムに書き込まず、リモートサーバーに書き込むように Citrix Hypervisor サーバーを設定できます。この場合、リモートサーバー上で、ログを受信して適切に集約する `syslogd` デーモンが実行されている必要があります。`syslogd` デーモンは Linux と UNIX の標準的な機能で、Windows やその他のオペレーティングシステムで使用できるサードパーティ製のバージョンもあります。

`syslog_destination` パラメーターを、ログを書き込むリモートサーバーのホスト名または IP アドレスに設定します:

```
1 xe host-param-set uuid=BRAND_SERVER_host_uuid logging:
 syslog_destination=hostname
```

次のコマンドを実行します:

```
1 xe host-syslog-reconfigure uuid= BRAND_SERVER_host_uuid
```

これにより、変更内容が有効になります。このコマンドは、`host` パラメータを指定することで、リモートから実行することもできます。

### XenCenter のログ

XenCenter では、クライアント側のログも記録されます。このファイルには、XenCenter の使用中の全操作とエラーの説明がすべて含まれます。また、実行されたさまざまな操作の監査記録になる、イベントの情報ログも含まれます。XenCenter のログファイルは、プロファイルフォルダの次の場所に格納されます。XenCenter を Windows 2008 上にインストールした場合は、次のパスに格納されます。

%userprofile%\AppData\Citrix\XenCenter\logs\XenCenter.log

XenCenter を Windows 8.1 上にインストールした場合は、次のパスに格納されます。

%userprofile%\AppData\Citrix\Roaming\XenCenter\logs\XenCenter.log

XenCenter のログファイルを開いたりメールで送信したりするときは、XenCenter [ヘルプ] メニューの [アプリケーションログファイルの表示] を選択し、ログファイルを表示します。

## XenCenter と Citrix Hypervisor サーバー間の接続のトラブルシューティング

XenCenter で特定の Citrix Hypervisor サーバーに接続できない場合は、以下の点を確認してください：

- XenCenter のバージョンが、接続先の Citrix Hypervisor サーバーより古くないかどうか。

XenCenter アプリケーションには下位互換性があり、古いバージョンの Citrix Hypervisor サーバーとは問題なく通信できますが、古い XenCenter で新しい Citrix Hypervisor サーバーと通信することはできません。

この問題を修正するには、Citrix Hypervisor サーバーのバージョンと同じ、またはより新しいバージョンの XenCenter をインストールします。

- ライセンスが有効かどうか。

ライセンスアクセスコードの有効期限は、XenCenter で Citrix Hypervisor サーバーを選択して、[全般] タブの [ライセンス詳細] で確認できます。

ホストのライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

- Citrix Hypervisor サーバーは、HTTPS を使用して以下のポートで XenCenter と通信します：
  - ポート 443 (管理 API を使用したコマンドと応答の双方向接続)
  - ポート 5900 (準仮想化された Linux 仮想マシンとのグラフィカル VNC 接続)

Citrix Hypervisor サーバーと、クライアントソフトウェアが動作するマシン間にファイアウォールを設定している環境では、これらのポートからのトラフィックを許可してください。

## その他のトラブルシューティング情報

以下の記事では、製品の特定の領域に関するトラブルシューティング情報を提供しています：

- [インストールのトラブルシューティング](#)
- [仮想マシンのトラブルシューティング](#)
- [ネットワークのトラブルシューティング](#)
- [vSwitch Controller のトラブルシューティング](#)

## メジャーブートのサブリメンタルパック

December 30, 2019

Citrix Hypervisor メジャーブートのサブリメンタルパックを使用することで、起動時に Citrix Hypervisor ホストの主要コンポーネントを測定できます。また、リモート構成証明ソリューションを使用して、これらの測定値を安全に収集できる API を提供します。このサブリメンタルパックは Intel コンピューターシステムと互換性があり、*Trusted Execution Technology* (TXT) をサポートします。

サブリメンタルパックは[Citrix Hypervisor 8.1 Premium Edition](#)ページからダウンロードできます。

### 注:

メジャーブートのサブリメンタルパックは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。

## 背景

このサブリメンタルパックのインストール後、Citrix Hypervisor サーバーの次の起動時に、Intel の TXT は低レベルのシステムコンポーネント（ファームウェア、BIOS、Xen ハイパーバイザー、dom0 カーネル、dom0 initrd など）を測定します。これらの測定値は、*Trusted Platform Module* (TPM) というホスト上のセキュアな場所に格納されます。リモート構成証明ソリューションなど、これらの測定値を安全に収集するためのクライアント用の新しいインターフェイスが用意されています。

## リモート構成証明

リモート構成証明ソリューションは、「既知の良好な」クリーン状態である Citrix Hypervisor サーバーに接続することで機能します。低レベルの主要システム測定値一覧について Citrix Hypervisor サーバーの TPM にリモートかつセキュアに照会できます。これらの測定値は、「ホワイトリスト」または「既知の良好な」測定値一覧に格納されます。

ここで、リモート構成証明ソフトウェアは定期的に主要システム測定値を収集し、「既知の良好な」一覧と比較します。

以下の場合、ホストは「信頼できない」と見なされます:

- リモート構成証明ソフトウェアが測定値を収集できない場合
- 測定値が変化した場合
- 暗号化キーが有効でない場合

この場合、顧客は通知を受け取ります。CloudStack、OpenStack、ワークロードバランスソフトウェアなどの高レベルオーケストレーションソフトウェアによって、影響を受けたホストでインテリジェントなセキュリティ操作を実行できます。

## Citrix Hypervisor サーバーの準備

このサブリメンタルパックが正しく機能するには、データを収集する前に、ホストの BIOS で次の設定を編集します：

1. Citrix Hypervisor サーバーが従来モードで起動するようにセットアップします。

注：

メジャーブートでは、UEFI ブートモードはサポートされていません。

2. **Intel AES-NI** を有効にします。
3. **TPM Security** または **On with Pre-boot Measurements** を切り替えます。
4. TPM をクリアします。

この操作は、TPM に関連付けられた以前の設定とパスワードをすべて消去し、Citrix Hypervisor メジャーブートのサブリメンタルパックを使用して、TPM を制御できるようにします。

注：

この手順の後に、再起動する必要があります。

5. **TPM** を有効にします。
6. **Intel TXT** を有効にします。

注：

- 手順 5 と手順 6 の後に再起動する必要があります。
- BIOS 設定は、ハードウェアの製造元によって異なります。特定の環境で TPM と TXT を有効にする方法については、ハードウェアのマニュアルを参照してください。

## サブリメンタルパックのインストール

Citrix Hypervisor CLI を使用してこのサブリメンタルパックをインストールします。ソフトウェアのアップデートと同様、このサブリメンタルパックを適用する前に、データのバックアップを作成することをお勧めします。

サブリメンタルパックは、zip ファイルで転送できます。サブリメンタルパック ISO が zip ファイルに含まれている場合は、以下の手順を実行する前に、zip ファイルを解凍して、ディスク ISO イメージを生成します。

## 実行中の Citrix Hypervisor システムにインストール

1. サブリメンタルパックを直接アップデートする Citrix Hypervisor ホストにダウンロードします。

シトリックスでは、`/tmp/`ディレクトリに直接保存することをお勧めします。

また、ファイルをインターネットに接続されたコンピューターにダウンロードし、ISO イメージを CD に書き込むこともできます。

2. XenCenter で Citrix Hypervisor ホストのコンソールを開きます。または、SSH を使用して直接ログインします。
3. 最も簡単な方法は、ISO ファイルから直接インストールすることです。以下のコマンドを実行します。

```
1 xe-install-supplemental-pack /tmp/Citrix Hypervisor-8.1-measured-
boot.iso
```

または、ISO を CD 書き込むことを選択した場合は、ディスクをマウントする必要があります。たとえば、CD-ROM の場合は、次のように入力します。「path to cd-rom」は CD-ROM へのパスです：

```
1 mkdir -p /mnt/tmp
2 mount /dev/<path to cd-rom> /mnt/tmp
3 cd /mnt/tmp/
4 ./install.sh
5 cd /
6 umount /mnt/tmp
```

4. 変更を適用するには、ホストを再起動します。

#### 再インストール

以前のバージョンにこのサブメンタルパックをインストールする場合は、以前のインストールを上書きすることに同意します。xe-install-supplemental-packのインストール中、メッセージが表示されたらYを入力します。

#### デフォルトパスワードのアップデート

以前のバージョンのサブメンタルパックでは、デフォルトのパスワードはxenrootに設定され末尾で改行されました。このバージョンのサブメンタルパックにおける新しいデフォルトパスワードはxenrootで、末尾の改行は削除されました。

カスタムパスワードは/opt/xensource/tpm/configで設定でき、echo -n <password | sha1sumで生成されたプレーンテキストパスワードを SHA1 ハッシュにする必要があります。-nがこのコマンドラインから省略された場合、パスワードに末尾の改行が含まれます。

#### アセットタグを設定する

アセットタグは--tpm\_set\_asset\_tagおよび--tpm\_clear\_asset\_tagメソッドで/opt/xensource/tpm/xentpmバイナリを使用して設定できます。または、管理 API tpmプラグインとtpm\_set\_asset\_tag (「tag」引数使用) およびtpm\_clear\_asset\_tag関数を組み合わせて設定できます：

```
1 /opt/xensource/tpm/xentpm --tpm_set_asset_tag <tag_sha1>
2 /opt/xensource/tpm/xentpm --tpm_clear_asset_tag
3 xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
 tpm_set_asset_tag args:tag=<tag_sha1>
4 xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=
 tpm_clear_asset_tag
```

注:

この手順の後に、再起動する必要があります。

### 詳細情報の表示

メジャーブートのサブリメンタルパックをダウンロードするには、[Citrix Hypervisor 8.1 Premium Edition](#) ページを参照してください。

このサブリメンタルパックのインストールで問題が発生した場合は、[シトリックステクニカルサポート](#)にお問い合わせください。

Citrix Hypervisor 8.1 ドキュメントを参照するには、[シトリックス製品ドキュメントWeb](#) サイトにアクセスしてください。

### ワークロードバランス

December 30, 2019

Citrix Hypervisor のコンポーネントであるワークロードバランスは、以下の機能を提供する仮想アプライアンスとしてパッケージ化されています。

- Citrix Hypervisor 環境内の仮想マシンのパフォーマンスに関するレポートを作成する。
- リソースの負荷状況を評価して、仮想マシンの最適な再配置先ホストを検出する。

注:

- ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。
- ワークロードバランス 8.1 は、サポートされているすべてのバージョンの Citrix Hypervisor および XenServer と互換性があります。

ワークロードバランスによる仮想マシンワークロードの再配置を行わない場合でも、この機能によりワークロードレポートを生成して、リソースプールの管理に役立てることができます。ワークロードバランスによるワークロードの再配置では、以下の処理が行われます。

- 仮想マシンワークロードを Citrix Hypervisor のリソースプール内のホスト間で分散させる。
- 仮想マシンを起動するときに、最適なサーバーを決定する。
- シャットダウンした仮想マシンの再開に最適なホストを決定する。
- ホストに障害が発生した場合の仮想マシンの移行先を決定する。
- ホストを保守モードに切り替えたり保守モードから切り替えたりする場合の仮想マシンの移行先を決定する。

ワークロードバランスによるワークロードの最適化は、自動的に実行されるようにしたり、管理者が選択的に実行できるようにしたりできます。また、特定のスケジュールに従ってホストの電源が自動的に切断されるように設定することもできます（夜間の使用電力を抑える場合など）。

ワークロードバランスは、プール内の仮想マシンの使用状況进行评估します。ホストのパフォーマンスがしきい値を超えている場合、ワークロードバランスは仮想マシンをプール内の低負荷ホストに再配置します。仮想マシンを移行することで、各ホストでのリソース負荷を分散させます。

ワークロードバランスでは、最適化の目標として、リソースのパフォーマンスの向上、または仮想マシンの密度の最大化（1台のホスト上で最大数の仮想マシンを実行すること）を選択できます。これらの最適化モードは、特定のスケジュールに従って自動的に切り替えることも、常に同じモードにしておくこともできます。また、各リソースのメトリック（CPU、ネットワーク、ディスク、メモリ）のしきい値および重要度を調節して、環境に適した最適化が行われるように設定できます。

リソースプールの能力进行评估するには、ワークロードバランスの履歴レポートを参照して、リソースプールやホストのヘルス状態、最適化や仮想マシンのパフォーマンス、および仮想マシンの移行履歴を確認します。

### ワークロードに関するレポート

ワークロードバランスではパフォーマンスのデータが記録されるため、仮想環境について、ワークロードレポートと呼ばれるレポートを生成することができます。

このワークロードレポートには、リソースプールやホストの状態、監査、最適化、および仮想マシンの再配置（移行）履歴に関する情報が記述されます。また、仮想マシンの使用状況を示すチャージバックレポートを生成して、コストの評価と割り当てに役立てることもできます。

レポートを実行するために、ワークロードバランスを構成して配置の推奨項目を作成したり仮想マシンを移動したりする必要はありません。ただし、ワークロードバランスコンポーネントを設定する必要があります。リソース負荷（限界しきい値）は、プール内のホストのパフォーマンスが低下するときの値に設定するのが理想的です。

詳しくは、「[ワークロードレポートの生成](#)」を参照してください。

### ワークロードバランスの基本概念

仮想マシンを実行すると、物理ホスト上のリソース（CPU、メモリ、ネットワーク読み取り、ネットワーク書き込み、ディスク読み取り、およびディスク書き込み）が消費されます。仮想マシンのワークロードによっては、同じホスト

上のほかの仮想マシンよりも多くの CPU リソースが消費されます。ワークロードは、仮想マシン上で実行するアプリケーションやトランザクションで決まります。当然のことながら、使用可能なリソースの量は、ホスト上のすべての仮想マシンで消費されるリソースの総量の分だけ減少します。

ワークロードバランスでは、仮想マシンおよび物理ホストのリソースパフォーマンスデータが収集され、データベースに格納されます。これらのデータと管理者による設定に基づいて、リソースプールを最適化するために仮想マシンをどのホストに再配置（移行）するかが計算され、推奨項目として提示されます。

最適化とは、目標に合わせてホストを「改善」することです：ワークロードバランスで生成される推奨項目により、リソースプールのパフォーマンスまたは密度を改善できる、プール内での仮想マシンの再配置案が示されます。ワークロードバランスは、次の最終目標に合わせて推奨項目を生成します：プール内の仮想マシン間のバランスをとる。ワークロードバランスによる最適化とは、これらの推奨項目を適用する操作を指します。

ワークロードバランスでは、以下のいずれかの最適化モードを選択できます。

- パフォーマンス：サーバー上の物理リソース（CPU、メモリ、ネットワーク、およびディスク）の使用効率を最適化します。ワークロードバランスでパフォーマンスの最適化を選択すると、各仮想マシンが使用できるリソースの量が最大になるように再配置の推奨項目が作成されます。
- 密度：ホスト上の仮想マシンの数を最適化します。ワークロードバランスで密度の最適化を選択すると、リソースプール内で稼働するサーバーの数を最小化するように仮想マシンが配置されます。これにより、仮想マシンに十分な計算能力があることが保証されます。

ワークロードバランスは、高可用性の設定とは競合しません：これらの機能は互換性があります。

### リソースプールの要件

ワークロードバランスでリソースプールのワークロードを管理するには、プールのホストがライブマイグレーションの次の要件を満たしている必要があります：

- リモートの共有ストレージ
- 類似したプロセッサ構成
- ギガビットイーサネット

これらの要件を満たさないホストでは、ワークロードバランスによる仮想マシンの移行ができません。

#### 注

ワークロードバランスでは、vGPU 対応の仮想マシンを含むプールはサポートされていません。ワークロードバランスでは、vGPU が接続されている仮想マシンの容量を計画することはできません。

### ワークロードバランスの利用を開始する

March 12, 2020

このワークロードバランス仮想アプライアンスは、以下の手順で簡単にセットアップできます。

1. <http://www.citrix.com/downloads>からワークロードバランス仮想アプライアンスをダウンロードし、XenCenter を使ってインポートします。
2. ワークロードバランス仮想アプライアンスのコンソールで、テキストベースのウィザード (Workload Balancing Configuration wizard) の手順に従ってワークロードバランス仮想アプライアンスを設定します (ここではこのウィザードを「ワークロードバランスの設定ウィザード」と呼びます)。
3. リソースプールをワークロードバランス仮想アプライアンスに接続します。

ワークロードバランス機能を使用してプールのワークロードを管理するには、プールのホストがライブマイグレーションの要件を満たしている必要があります。詳細は、「[管理](#)」を参照してください。

### ワークロードバランス仮想アプライアンスのインポート

ワークロードバランス仮想アプライアンスは単一のインストール済み仮想マシンで構成されており、Citrix Hypervisor サーバー上で動作するように設計されています。この仮想アプライアンスをインポートする前に、以下の要件および注意事項について確認してください。

#### 前提条件

この仮想アプライアンスは、Citrix Hypervisor 7.1 またはそれ以降が動作するホスト用に設計されています。ただし、このワークロードバランス機能では、Citrix Hypervisor 5.5 またはそれ以降のホストが動作するリソースプールを管理できます。この仮想アプライアンスをインポートするには、XenCenter 管理コンソールを使用することをお勧めします。ワークロードバランス仮想アプライアンスを実行するには、2GB 以上の RAM と 20GB 以上のディスク領域が必要です。

#### 仮想アプライアンスをインポートする前の確認事項

仮想アプライアンスをインポートする前に、以下の事項を確認して、必要に応じて XenServer 環境を変更してください。また、ワークロードバランスのリリースノートを参照して、リリースの最新情報についても確認してください。

- 通信ポート: ワークロードバランスの設定ウィザードを起動する前に、ワークロードバランス仮想アプライアンスとの通信で使用されるポートを決定しておきます。ウィザードで、このポートの入力を求めるメッセージが表示されます。デフォルトでは、ワークロードバランスサーバーは 8012 を使用します。

#### 注:

ワークロードバランスの通信ポートとして 443 を使用しないでください。ポート 443 (標準の SSL/HTTPS ポート) からの接続は、ワークロードバランス仮想アプライアンスにより拒否されます。

- ワークロードバランスのアカウント：ワークロードバランスの設定ウィザードでは、ワークロードバランスアカウントおよびデータベースアカウントのユーザー名およびパスワードを入力する必要があります。ただし、ウィザードを起動する前にこれらのアカウントを作成しておく必要はありません。ウィザードにより適切なアカウントが作成されます。
- 異なるプールの管理：ワークロードバランス仮想アプライアンスをプールにインポートしたら、その仮想アプライアンスでほかのプールのワークロードを管理することもできます。たとえば、ワークロードバランス仮想アプライアンスをプール A にインポートして、プール B のワークロードを管理できます。

注：

ワークロードバランス仮想アプライアンスを実行する物理ホストと、管理対象のプールの時計が同期している必要があります。ただし、ワークロードバランス仮想アプライアンスの時計を変更することはできません。このため、この仮想アプライアンスの物理ホストと管理対象のプールで同じ NTP サーバーを使用することをお勧めしています。

- **Citrix Hypervisor** とワークロードバランスサーバーは、**HTTPS** を使用して通信します。XenServer とワークロードバランスとの通信は HTTPS で行われるため、ワークロードバランスの設定時に、自己署名入りの証明書が自動的に作成されます。この証明書の代わりに信頼された機関からの証明書を使用するか、Citrix Hypervisor で証明書が検証されるように設定できます。詳しくは、『ワークロードバランス管理者ガイド』を参照してください。
- 履歴データの保持とディスク容量：保持できる履歴データの量は、以下に基づいて決まります：
  - ワークロードバランスに割り当てられている仮想ディスクのサイズ（デフォルトは 20GB）
  - 必要な最小ディスク領域（デフォルトは 2,048MB。wlb.conf ファイルの `GroomingRequiredMinimumDiskSize` パラメーターで指定）

多くの履歴データを保持する必要がある場合は、以下のいずれかを実行してください：

- 「**管理**」の手順に従って履歴データをアーカイブします。
- ワークロードバランス仮想アプライアンスに割り当てられている仮想ディスクのサイズを増やします。

こうした操作が必要になるのは、たとえば、ワークロードバランスのプール監査記録機能を使用する場合や、レポートの詳細レベルを中以上に設定する場合などです。

仮想ディスクのサイズを増やすには、仮想アプライアンスをインポートしてから、『ワークロードバランス管理者ガイド』で説明されている手順に従ってサイズを変更します。

- ワークロードバランスの負荷分散：ワークロードバランス仮想アプライアンスでその仮想アプライアンス自体を管理する場合は、その仮想アプライアンスのインポート時にリモートの共有ストレージを指定します。

注：

ワークロードバランス仮想アプライアンスでその仮想アプライアンス自体を管理している場合、ワークロードバランスでこの仮想アプライアンスについて起動時の配置に関する推奨項目を作成することはできません。これは、その推奨項目の生成時にワークロードバランス仮想アプライアンスが既に実行されているためです。ただし、ほかの仮想マシンと同様に、ワークロードバランス仮想アプライアンスのワ

ワークロードを移動することは可能です。

## リソースプールのサイズ決定

大規模なリソースプールでワークロードバランスを使用するには、特定の設定が必要です。

## 仮想アプライアンスのダウンロード

ワークロードバランス仮想アプライアンスは、.xva形式でパッケージ化されています。この仮想アプライアンスは、シトリックスのダウンロードページ (<http://www.citrix.com/downloads>) からダウンロードできます。ローカルコンピュータ (XenCenter がインストールされているコンピュータ) のローカルハードドライブに XVA ファイルをダウンロードして、ダウンロードした .xva ファイルを XenCenter でリソースプールにインポートします。

## XenCenter への仮想アプライアンスのインポート

XenCenter を使用して、ワークロードバランス仮想アプライアンスをリソースプールにインポートします。

仮想アプライアンスを Citrix Hypervisor にインポートするには:

1. XenCenter を開きます。
2. インポート先のプールまたはホストを右クリックして [インポート] を選択します。
3. ダウンロードした `vpx-wlb.xva` パッケージを指定します。
4. ワークロードバランス仮想アプライアンスを実行するプールまたはホームサーバーを選択します。  
プールを選択すると、そのプール内の最適なホスト上で仮想アプライアンスが自動で起動します。  
ワークロードバランス仮想アプライアンスがワークロードバランスの管理対象に含まれないようにするには、その仮想アプライアンスのホームサーバーを設定します。これにより、仮想アプライアンスが常にそのホスト上で起動します。
5. ワークロードバランス仮想アプライアンスの仮想ストレージを格納するストレージリポジトリを選択します。  
20GB 以上の空き領域を持つストレージを選択してください。  
ローカルまたはリモートのストレージを選択できます。ただし、ローカルストレージを選択すると、ワークロードバランス仮想アプライアンス自体をワークロードバランスの管理対象にすることはできません。
6. ワークロードバランス仮想アプライアンスの仮想インターフェイスを定義します。このリリースでは、単一の仮想インターフェイスが使用されます。
7. 管理対象のプールに接続するためのネットワークを選択します。
8. [インポート後に VM を起動する] チェックボックスがオンになっていることを確認して、[完了] をクリックします。仮想アプライアンスのインポート処理が開始されます。

9. `.xva`ファイルのインポート処理が完了すると、XenCenterの [リソース] ペインにワークロードバランス仮想アプライアンスが表示されます。

#### ワークロードバランス仮想アプライアンスの設定

インポートしたワークロードバランス仮想アプライアンスを使用するには、その仮想アプライアンスを設定する必要があります。仮想アプライアンスの設定は、XenCenter上でウィザード形式の手順に従って行います。このウィザードを表示するには、[リソース] ペインで仮想アプライアンスを選択し、[コンソール] タブをクリックします。すべてのオプションで、Enter キーを押してデフォルト値を受け入れます。

1. インポートしたワークロードバランス仮想アプライアンスの [コンソール] タブをクリックします。
2. ライセンス契約書の内容を確認して、同意する場合は「yes」と入力します。同意しない場合は、「no」と入力します。

注:

ワークロードバランス仮想アプライアンスには、このアプライアンスの `/opt/vpx/wlb` ディレクトリに含まれているライセンス条項も適用されます。

3. ワークロードバランス仮想アプライアンスのルートパスワードを指定して、確認のため再入力します。安全なパスワードを使用することをお勧めします。

注:

コンソールにパスワードを入力するときに、アスタリスク (\*) などの文字は表示されません。

4. ワークロードバランス仮想アプライアンスに割り当てるホスト名を入力します。
5. 仮想アプライアンスのドメインサフィックスを入力します。

たとえば、仮想アプライアンスの FQDN (Fully Qualified Domain Name: 完全修飾ドメイン名) が `wlb-vpx-pos-pool.domain4.bedford4.ctx` の場合は、「`domain4.bedford4.ctx`」と入力します。

注:

ワークロードバランス仮想アプライアンスの FQDN が、DNS (Domain Name System: ドメインネームシステム) サーバーに自動で追加されることはありません。このため、プールをワークロードバランスに接続するときに FQDN を使用できるようにするには、ワークロードバランス仮想アプライアンスの FQDN を DNS サーバーに追加しておく必要があります。

6. ワークロードバランス仮想アプライアンスの IP アドレスを DHCP から自動的に取得する場合は、「y」と入力します。特定の静的 IP アドレスを指定する場合は、「n」と入力して、IP アドレス、サブネットマスク、およびゲートウェイを指定します。

注:

IP アドレスのリースが期限切れにならない場合に限り、DHCP を使用できます。仮想アプライアンスの IP アドレスが変更されないことが重要です。IP アドレスが変更されると、XenServer とワークロード バランス間の接続が切断されてしまいます。

7. ワークロードバランスデータベースのユーザー名を入力するか、**Enter** キーを押してデフォルトのユーザー名 (postgres) を使用します。

ここでは、ワークロードバランスデータベースのアカウントを作成します。ワークロードバランスサービスでは、このアカウントを使用してワークロードバランスデータベースの読み取りおよび書き込みを行います。ユーザー名とパスワードは記録しておいてください。これらは、ワークロードバランスの PostgreSQL データベースを直接管理する場合（データをエクスポートする場合など）に必要になります。

8. ワークロードバランスデータベースのパスワードを入力します。**Enter** キーを押すと、データベースオブジェクトのロード過程を示すメッセージが表示されます。
9. ワークロードバランスサーバーのユーザー名およびパスワードを入力します。

ここで作成するアカウントは、Citrix Hypervisor でワークロードバランスへ接続するときに使用されます。デフォルトのユーザー名は、**wlbuser** です。

10. ワークロードバランスサーバーのポート番号を入力します。ここで指定したポートが、ワークロードバランスサーバーの通信に使用されます。

デフォルトでは、ワークロードバランスサーバーは 8012 を使用します。標準の SSL ポートである 443 を指定することはできません。

注:

ここでポートを変更した場合は、リソースプールとワークロードバランスを接続するときにそのポート番号を指定してください。ポート番号の指定は、[**WLB** サーバーへの接続] ダイアログボックスなどで行います。

ここで指定するポートが、ファイアウォールでブロックされていないことを確認してください。

**Enter** キーを押すと、仮想アプライアンスの設定（自己署名入りの証明書の作成など）が続行されます。

11. この時点で、先ほど作成したアカウント（通常は **root**）を使用して、ワークロードバランス仮想アプライアンスにログインすることも可能になります。ただし、ログインは、ワークロードバランスコマンドを実行する場合か、ワークロードバランス設定ファイルを編集する場合にのみ必要です。

ワークロードバランスを設定したら、「ワークロードバランス仮想アプライアンスへの接続」の手順に従ってプールをワークロードバランス仮想アプライアンスに接続します。

必要であれば、ワークロードバランスの設定ファイルは、`/opt/vpx/wlb/wlb.conf` にあります。また、ワークロードバランスのログファイルは、`/var/log/wlb/LogFile.log` にあります。これらのファイルとその用途について詳しくは、『ワークロードバランス管理者ガイド』を参照してください。

## ワークロードバランス仮想アプライアンスへの接続

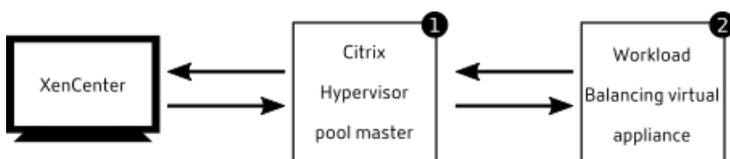
## 注:

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

ワークロードバランスの設定後、CLI (Command Line Interface: コマンドラインインターフェイス) または XenCenter を使用して、管理対象のリソースプールを WLB 仮想アプライアンスに接続します。

XenCenter でワークロードバランス仮想アプライアンスに接続するには、以下の情報が必要です。

- ワークロードバランス仮想アプライアンスの IP アドレスまたは FQDN と、通信用のポート番号。
- ワークロードバランスで監視するリソースプール (プールマスター) の資格情報。
- ワークロードバランスの設定時に作成したワークロードバランスアカウントの資格情報。Citrix Hypervisor は、このアカウントを使用してワークロードバランスと通信します。



ワークロードバランスサーバーへの接続時にワークロードバランス仮想アプライアンスの FQDN を指定する場合は、まず仮想アプライアンスのホスト名および IP アドレスを DNS サーバーに追加します。

ワークロードバランスに接続した直後では、デフォルトのしきい値および設定に基づいてワークロードが最適化されます。自動最適化モード、電源管理、および自動処理などの自動化機能は、デフォルトでは無効になっています。

## ワークロードバランスへの接続と証明書

ワークロードバランス仮想アプライアンスの設定時に作成されたデフォルトの証明書とは別の (信頼された) 証明書をアップロードする場合、または XenServer での証明書の検証を設定する場合は、プールをワークロードバランスに接続する前に、以下の点について注意してください。

- 自己署名入りのワークロードバランス証明書を Citrix Hypervisor で検証する場合は、IP アドレスを指定してワークロードバランス仮想アプライアンスに接続する必要があります。これは、この証明書がワークロードバランス仮想アプライアンスの IP アドレスに基づいて作成されているためです。
- 信頼された機関からの証明書を使用する場合は、FQDN を指定してワークロードバランス仮想アプライアンスに接続できます。ただし、**[WLB サーバーへの接続]** ダイアログボックスで静的 IP アドレスを指定することもできます。この IP アドレスを証明書のサブジェクトの別名 (SAN) として使用します。

証明書の設定について詳しくは、『ワークロードバランス管理者ガイド』を参照してください。

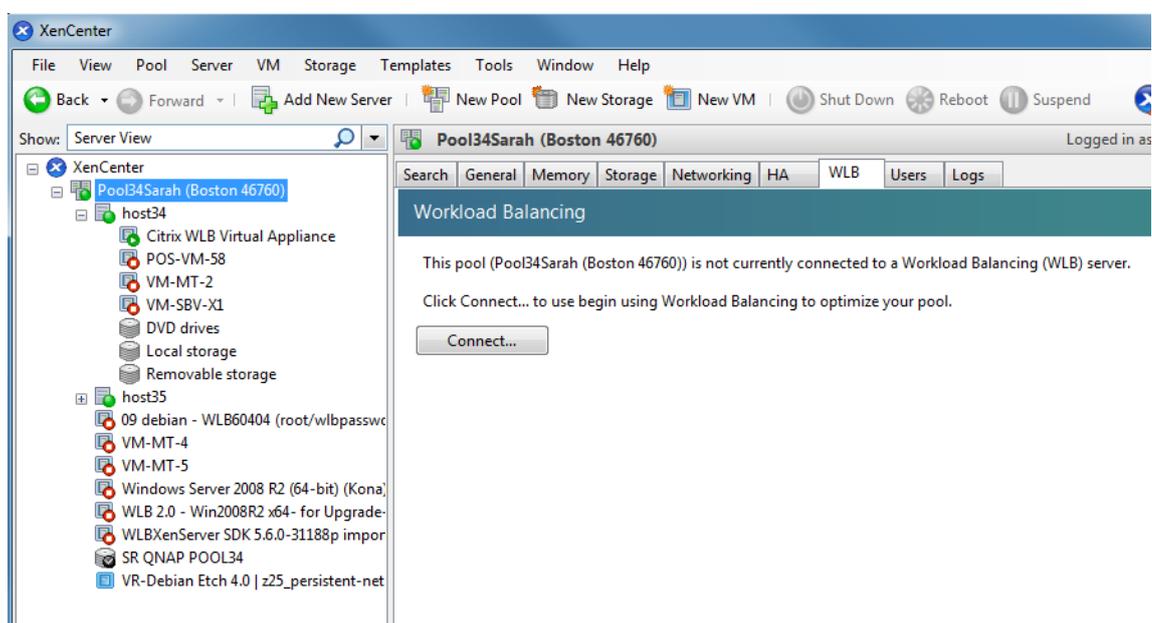
リソースプールをワークロードバランス仮想アプライアンスに接続するには

注:

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

1. 「XenCenter のインフラストラクチャペインで、[XenCenter] > your-resource-pool」を参照してください。
2. [プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブに [接続] ボタンが表示されます。



3. [WLB] タブの [接続] をクリックします。[WLB サーバーへの接続] ダイアログボックスが表示されます。

**Connect to WLB Server**

Server Address  
Enter the address of the Workload Balancing server this Citrix Hypervisor resource pool will use.

Address:

Port:  (Default is 8012)

WLB Server Credentials  
Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:

Citrix Hypervisor Credentials  
Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials

OK Cancel

4. [サーバーのアドレス] セクションで、以下の情報を入力します：

- a) [アドレス] ボックスに、ワークロードバランス仮想アプライアンスの IP アドレスまたは FQDN を入力します。たとえば、「`WLB-appliance-computername.yourdomain.net`」などを入力します。

ヒント：

詳しくは、「ワークロードバランス仮想アプライアンスの IP アドレスを調べるには」を参照してください。

- b) (オプション) ワークロードバランス仮想アプライアンスの設定時にポート番号を変更した場合は、[ポート] ボックスにその番号を入力します。Citrix Hypervisor は、このポートを使用してワークロードバランスと通信します。

Citrix Hypervisor のデフォルトでは、ポート 8012 が指定されています。

注：

ポート番号の変更は、ワークロードバランス仮想アプライアンスの設定時にポート番号を変更した場合のみ行ってください。[WLB サーバーへの接続] ダイアログボックスで指定するポート番号は、ワークロードバランス仮想アプライアンスの設定時に指定したもの（およびファイアウォール規則で指定したもの）と一致する必要があります。

5. [WLB サーバーの資格情報] セクションで、Citrix Hypervisor のリソースプール（プールマスタ）がワークロードバランス仮想アプライアンスに接続するときに使用するユーザー名およびパスワードを入力します。

Update Credentials

**WLB Server Credentials**

Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:

これらの資格情報は、ワークロードバランス仮想アプライアンスの設定時に作成したものである必要があります。デフォルトのユーザー名は、**wlbuser** です。

6. [Citrix Hypervisor の資格情報] セクションで、リソースプールにアクセスするためのユーザー名とパスワード（通常はプールマスターのパスワード）を入力します。これらの情報は、ワークロードバランス仮想アプライアンスがプールの各ホストに接続するときに使用されます。

**Citrix Hypervisor Credentials**

Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials

現在ログイン中の Citrix Hypervisor と同じ資格情報を使用するには、[現在の XenCenter の資格情報を使用する] チェックボックスをオンにします。RBAC（Roll-Based Access Control: 役割ベースのアクセス制御）で役割を割り当てたアカウントを使用する場合は、そのアカウントにワークロードバランス機能の管理許可が付与されていることを確認してください。詳しくは、『ワークロードバランス管理者ガイド』の RBAC に関するセクションを参照してください。

7. プールをワークロードバランス仮想アプライアンスに接続すると、デフォルトの最適化設定でプールの監視が開始されます。ワークロードバランス仮想アプライアンスへの接続直後に最適化設定やリソースの優先度を変更する場合は、少なくとも 60 秒待機してください。または、XenCenter のログに検出が完了したと表示されるまで待機してください。

**重要:**

ワークロードバランスをしばらく使用しても意図したとおりに推奨項目が生成されない場合は、「[管理](#)」に従って、パフォーマンスしきい値の設定を再評価してください。運用環境に合ったしきい値を設定することで、より適切な最適化推奨項目が作成されるようになります。

ワークロードバランス仮想アプライアンスの IP アドレスを調べるには

1. XenCenter の [リソース] ペインでワークロードバランス仮想アプライアンスを選択して、[コンソール] タブをクリックします。

2. 仮想アプライアンスにログインします。これを行うには、仮想アプライアンスのインポート時に作成したアカウント（root）とパスワードを使用します。
3. 次のコマンドを実行します。

```
1 ifconfig
```

## ワークロードバランス仮想アプライアンスの管理

March 12, 2020

この記事では、次の内容について説明します：

- ワークロードバランスを使って仮想マシンを最適なホスト上で起動する
- ワークロードバランスによる推奨項目を適用して仮想マシンを別のホストに移動する

注：

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

### ワークロードバランスの基本タスク

ワークロードバランスは高機能な Citrix Hypervisor コンポーネントであり、使用中の環境内のワークロードを最適化できるさまざまな機能を備えています。以下のタッチ操作が含まれます。

- ホストの電源管理
- 最適化モードのスケジュール化
- レポート生成

管理者は、各リソース負荷の測定基準を微調整して、適切な最適化推奨項目が生成されるようにワークロードバランス機能を設定できます。

ただし、ワークロードバランスが有効なリソースプールでは、管理者は日常的に以下の 2 つの基本タスクを実行することになります：

- 仮想マシンの起動に最適なサーバーを決定する
- ワークロードバランスにより提示された推奨項目を適用する

もう 1 つの一般的なタスクであるワークロードレポートの生成については、ワークロードレポートの生成を参照してください。

### 仮想マシンの起動に最適なサーバーを決定する

仮想マシンの再配置機能を使用すると、どのホストで仮想マシンを起動するかを指定できます。この機能により、電源がオフになっている仮想マシンを再起動したり、別のホストへ仮想マシンを移行したりすることができます。この機能は「配置推奨項目」と呼ばれ、Citrix Virtual Desktops 環境でも有用です。

### ワークロードバランスの推奨項目を適用する

ワークロードバランスをしばらく使用すると、環境を最適化するための推奨項目が生成されるようになります。たとえば、プール内で必要最小限のホストを稼働させるために、仮想マシンを特定のホスト上に集約するように提案する推奨項目が生成されます。自動モードを有効にしていない場合、これらの推奨項目を適用するかどうかを管理者が選択できます。

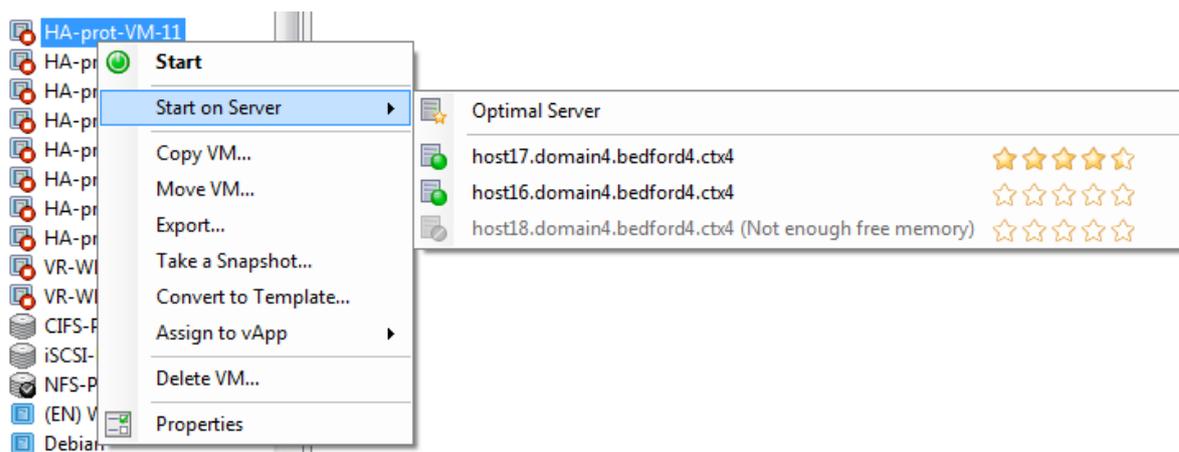
XenCenter のこれらの基本タスクについては、以下のセクションで詳しく説明します。

#### 重要:

ワークロードバランスをしばらく使用しても意図したとおりに配置推奨項目が生成されない場合は、パフォーマンスしきい値の設定を再評価してください。この評価については、「推奨項目を生成するしくみ」で説明されています。運用環境に合ったしきい値を設定することで、より適切な最適化推奨項目が作成されるようになります。

### 仮想マシンに最適なホストを選択する

ワークロードバランスを有効化してオフラインの仮想マシンを再起動すると、XenCenter により、仮想マシンの起動に最適なプールメンバーが提案されます。推奨起動サーバーは、星の数で示されます。



推奨起動ホストとは、ワークロードのホストとして最適な物理サーバーを指します。ワークロードバランスは、以下の点を考慮して推奨起動ホストを決定します:

- プール内の各ホストで使用可能なリソースの量。最適化モードとしてパフォーマンスの最大化が選択されている場合、すべての仮想マシンが良好なパフォーマンスで動作するように、各ホスト上にバランスよく仮想マシ

ンを配置しようとしています。密度の最大化が選択されている場合は、仮想マシンのリソースを維持したまま、ホスト上により多くの仮想マシンを配置しようとしています。

- プールで選択されている最適化モード（[パフォーマンスの最大化] または [密度の最大化]）。パフォーマンスの最大化が選択されている場合、その仮想マシンが必要とするリソースの負荷が最も低いホストにその仮想マシンが配置されます。密度の最大化が選択されている場合、別の仮想マシンがすでに実行されているホストに仮想マシンが配置されます。このアプローチにより、仮想マシンは可能な限り少ないホストで実行されます。
- 仮想マシンで必要とされるリソースの量とタイプ。ワークロードバランスは仮想マシンのメトリックを利用し、仮想マシンが必要とするリソースの種類に応じて推奨起動ホストを決定します。たとえば、ワークロードバランスでは、仮想マシンが必要とする場合、使用可能な CPU は少ないが使用可能なメモリが多いホストを選択する場合があります。

ワークロードバランスを有効化すると、XenCenter により、仮想マシンの起動に最適なホストが評価されます。この評価は、以下の場合にも提供されます：

- 電源オフの仮想マシンを起動するとき
- 一時中止中の仮想マシンを起動するとき
- 別のホストに仮想マシンを移行するとき（移行およびメンテナンスモード）

この機能では、推奨ホストの評価が星の数で示されます。ホスト名の横に白抜き星 (★) が 5 つ表示される場合は、仮想マシンのホストとして最も不適切であることを意味します。ホストで仮想マシンを起動、またはホストへ仮想マシンを移行できない場合、[起動サーバー] メニューコマンドで該当するホスト名が灰色で表示されます。ホスト名の横に、ホストで仮想マシンを使用できない理由が表示されます。

通常、ワークロードバランスで推奨されたホスト上で仮想マシンを起動すると、より効率的に推奨項目が生成され、不要な推奨項目が生成されなくなります。ホストの推奨項目に従う場合は、[起動サーバー] メニューから横に表示される星の数が 1 番多いホストを選択します。

最適なサーバーで仮想マシンを起動するには

1. XenCenter の [リソース] ペインで、起動する仮想マシンを選択します。
2. [VM] メニューの [起動サーバー] を選択し、以下のいずれかを選択します：
  - 最適なサーバー。選択した仮想マシンで要求されるリソースを持つ、ホストとして最も適したサーバーです。ワークロードバランスでは、パフォーマンス測定値の履歴レコードと選択されている最適化モードに基づいて最適なサーバーが決定されます。最適なサーバーの名前には、最も多くの星が表示されます。
  - [最適なサーバー] の下に表示される星付きのサーバー。5 つの星が表示されるサーバーは最も推奨されるサーバー（最適なサーバー）を示し、5 つの白抜き星が表示されるサーバーは推奨されないサーバーを示します。

ヒント:

[リソース] ペインで仮想マシンを右クリックして [起動サーバー] を選択することもできます。

最適なサーバーで仮想マシンを再開するには

1. XenCenter の [リソース] ペインで、再開する仮想マシンを選択します。
2. [VM] メニューの [再開サーバー] を選択し、以下のいずれかを選択します:
  - 最適なサーバー。選択した仮想マシンで要求されるリソースを持つ、ホストとして最も適したサーバーです。ワークロードバランスでは、パフォーマンス測定値の履歴レコードと選択されている最適化モードに基づいて最適なサーバーが決定されます。最適なサーバーの名前には、最も多くの星が表示されます。
  - [最適なサーバー] の下に表示される星付きのサーバー。5 つの星が表示されるサーバーは最も推奨されるサーバー（最適なサーバー）を示し、5 つの白抜きの星が表示されるサーバーは推奨されないサーバーを示します。

ヒント:

[リソース] ペインで仮想マシンを右クリックして [再開サーバー] を選択することもできます。

### 最適化推奨項目の適用

ワークロードバランスでは、リソースプールを最適化するために仮想マシンをどのように再配置（移行）すべきであるかというアドバイスが推奨項目として生成されます。最適化推奨項目は、XenCenter の [WLB 最適化] タブに表示されます。

#### Optimization Recommendations

[View History...](#)

| VM/Host                      | Operation                                                             | Reason           |
|------------------------------|-----------------------------------------------------------------------|------------------|
| HA-prot-VM-7                 | Relocate from 'host17.domain4.bedford4.ctx4' to 'host16.domain4.be... | Consolidation    |
| host17.domain4.bedford4.ctx4 | Power off                                                             | Release Resource |

Apply Recommendations

ワークロードバランスでは、以下の条件に基づいて推奨項目が生成されます:

- 管理者が設定した最適化モード。
- 物理ホスト上の CPU、メモリ、ネットワーク、およびディスクについて収集されたパフォーマンス測定値。
- リソースプール内でのホストの役割。プールマスタ上に仮想マシンを配置する推奨項目は、ほかのホスト上への配置が不可能な場合のみ生成されます。同様に、最適化モードとして密度の最大化が選択されているプールでは、仮想マシンの移行先としてプールマスターが選択されるのは最後になります。

[最適化の推奨項目] には以下の情報が表示されます:

- ワークロードバランスで再配置が推奨される仮想マシンの名前
- 仮想マシンが現在存在するホスト
- 新しい配置先としてワークロードバランスが推奨するホスト

また、仮想マシンの再配置が推奨される理由も示されます。たとえば、推奨理由が CPU 使用率の場合は「CPU」と表示されます。ワークロードバランスの電源管理が有効な場合は、電源を投入または切断すべきホストも示されます。この推奨項目は、特に集約化に関するものです。

[すべて実行] をクリックすると、Citrix Hypervisor は [最適化の推奨項目] の一覧に表示されたすべての処理を実行します。

ヒント:

プールの最適化モードを確認するには、XenCenter で目的のプールを選択します。[WLB] タブの [構成] セクションに、この情報が表示されます。

最適化推奨項目を適用するためには

1. XenCenter の [リソース] ペインで、推奨項目を確認するリソースプールを選択します。
2. [WLB] タブをクリックします。選択したリソースプールの最適化が必要な場合は、[WLB] タブの [最適化の推奨項目] に内容が表示されます。
3. 推奨項目を適用するためには、[すべて実行] をクリックします。Citrix Hypervisor により、[最適化の推奨項目] の [操作] 列のすべての処理が実行されます。

[すべて実行] をクリックすると、XenCenter は自動的に [ログ] タブを表示し、仮想マシンの移行状況を確認できます。

高可用性環境でのワークロードバランス

ワークロードバランス機能と Citrix Hypervisor の高可用性機能が有効なリソースプールでは、これらの 2 つの機能が相互にどのように影響するかを理解する必要があります。ワークロードバランスは、高可用性機能と競合しないように設計されています。ワークロードバランスで生成される推奨項目と高可用性設定が競合する場合は、常に高可用性機能の設定が優先されます。つまり、以下のようになります:

- 仮想マシンの移行先として高可用性プランで許可されないホストは、ワークロードバランスでは推奨起動ホストとして表示されません。
- [高可用性の構成] ダイアログボックスの [許可する障害数] ボックスの値を超える数のホストは、ワークロードバランスにより自動的に電源が切断されることはありません。
  - ただし、電源を切断することが推奨項目として提示される場合があります (たとえば、高可用性で許可する障害数として 1 が設定されている場合に、ワークロードバランスにより 2 台のホストのシャットダ

ウンが推奨されることがあります)。この推奨項目を適用しようとする、XenCenter に「高可用性が保証されなくなる」という内容のエラーメッセージが表示されます。

- 自動モードでワークロードバランスが動作する場合は、電源管理を有効にしても、高可用性で許可される障害数を超える数の推奨項目は無視されます。この場合、ワークロードバランスのログファイルに「高可用性が有効なため電源管理推奨項目を適用できない」という内容のメッセージが記録されます。

## ワークロードレポートの生成

このセクションでは、ワークロードバランスを使用して環境（ホストや仮想マシンなど）に関するレポートを生成する方法について説明します。以下の内容について説明します：

- レポートの生成方法
- ワークロードレポートの種類

注：

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

## ワークロードレポートの概要

ワークロードバランスレポートを使用すると、リソースプールの能力を評価したり、仮想マシンのヘルス状態を確認したり、設定したパフォーマンスしきい値の有効性を評価したりできます。

ワークロードバランスでは、物理ホスト、リソースプール、および仮想マシンに関するレポートを生成できます。以下の 2 種類のレポートが作成されます：

- 日別データを表示する履歴レポート
- 特定の項目に関する概要情報を表示するロールアップスタイルのレポート

ワークロードバランスでは、仮想マシンの移行回数などを記録した監査用のレポートも作成できます。

プールヘルスレポートを使用して、設定したしきい値の有効性を評価できます。ワークロードバランスでは各パフォーマンスしきい値にデフォルト値が設定されますが、環境によっては調整が必要な場合があります。これを行わないと、ワークロードバランスで適切な推奨項目が生成されません。

ワークロードバランスレポートを生成するには、ワークロードバランス仮想アプライアンスをインポートして、リソースプールをその仮想アプライアンスに接続しておく必要があります。さらに、有用なレポートを作成するには、ワークロードバランスによるデータ収集が十分な期間行われている必要があります。

## ワークロードバランスレポートの生成

1. XenCenter で、[プール] メニューの [ワークロードレポートを表示] を選択します。

ヒント:

[WLB] タブの [レポート] をクリックすることでも、[ワークロードレポート] ダイアログボックスを開くことができます。

2. [ワークロードレポート] ダイアログボックスの [レポート] ペインの一覧で、生成するレポートの種類を選択します。
3. レポート期間の開始日と終了日を選択します。選択したレポートの種類によっては、[ホスト] ボックスの一覧でレポート対象のホストを選択します。
4. [レポートの実行] をクリックします。レポートウィンドウにレポートが表示されます。各レポートの使用方法については、ワークロードバランスレポートの種類についてを参照してください。

## ワークロードバランスレポートの使用

レポートを生成したら、ツールバーのボタンを使用してさまざまなタスクを実行できます。ツールバーのボタンの名前は、マウスポインタをそのボタンに合わせると表示されます。

| ツールバーのボタン                                                                           | 説明                                                                                             |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
|  | [ドキュメントマップ] ボタンをクリックすると、サイズの大きなレポートを表示するときに便利なドキュメントマップが開きます。                                  |
|  | [ページ操作] ボタンを使用して、レポートの次のページや前のページ、または特定のページを表示できます。                                            |
|  | [元のレポートに戻る] ボタンをクリックすると、ドリルスルーレポートから元のレポートに戻ります。注: このボタンは、プールヘルスレポートなどのドリルスルーレポートでのみ使用可能になります。 |
|  | [生成停止] ボタンは、レポートの生成処理をキャンセルします。                                                                |
|  | [印刷] ボタンでは、一般的な印刷オプションを指定してレポートを印刷できます。これらのオプションには次が含まれます: プリンター、ページ数、およびコピー数。                 |

| ツールバーのボタン                                                                         | 説明                                                                                   |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
|  | [印刷レイアウト] ボタンをクリックすると、レポートの印刷プレビューを確認できます。印刷レイアウトを終了するには、もう一度 [印刷レイアウト] ボタンをクリックします。 |
|  | [ページ設定] では、用紙サイズ、印刷の向き、余白などの印刷オプションを指定できます。                                          |
|  | [エクスポート] をクリックすると、Acrobat (PDF) 形式または Excel (XLS) 形式のファイルとしてレポートをエクスポートできます。         |
|  | [検索] をクリックすると、仮想マシンの名前など、レポート内の特定の文字列を検索できます。                                        |

#### ワークロードバランスレポートの印刷

レポートを印刷するには、まずそのレポートを実行します。

1. (オプション) [印刷レイアウト] ボタン (下図) をクリックして、印刷プレビューを確認します:
2. (オプション) [ページ設定] ボタン (下図) をクリックして、用紙サイズ、印刷の向き、余白などの印刷オプションを指定します:
3. [印刷] ボタン (下図) をクリックします:

#### ワークロードバランスレポートのエクスポート

ワークロードバランスレポートは、Acrobat (PDF) 形式または Excel (XLS) 形式のファイルとしてエクスポートできます。

1. レポートを生成したら、[エクスポート] をクリックします。
2. [エクスポート] ボタンのメニューから、以下のいずれかを選択します。
  - Excel
  - Acrobat (PDF) ファイル

#### 注:

レポートをエクスポートする場合のデータ量は、エクスポート形式により異なります。Excel にエクスポートしたレポートには、「ドリルダウン」データを含め、レポートで利用可能なすべてのデータが含まれます。PDF に

エクスポートしたレポート、および XenCenter で表示するレポートに含まれるデータは、レポートの生成時に選択したもののみです。

### ワークロードバランスレポートの種類について

ここでは、ワークロードバランスの各レポートについて説明します。

### チャージバック使用解析

このレポート（「チャージバックレポート」）では、組織内の特定の部署で使用されたリソースの量を確認できます。具体的には、リソースプール内のすべての仮想マシンのアベイラビリティやリソース使用などの情報が含まれます。このレポートには仮想マシンのアップタイムが含まれるため、SLA（Service Level Agreement: サービス品質保証契約）に役立てることができます。

このレポートを使用して、課金用のシンプルなチャージバックソリューションを実装できます。特定のリソースについて顧客に課金するには、レポートを生成して Excel データとして保存し、そのスプレッドシートを編集したり、組織の課金システムにインポートしたりできます。

組織内の部署または外部の顧客に仮想マシンの使用料を請求する場合は、仮想マシンの名前に部署や顧客の名前を含めることを検討します。これにより、チャージバックレポートが読みやすくなります。

このレポートのリソース関連のデータは、個々の仮想マシンへの物理リソースの割り当てにより異なる場合があります。

レポートのメモリの平均データは、そのときに仮想マシンに割り当てられていたメモリ量により異なります。Citrix Hypervisor では、メモリ割り当てを固定したり、動的メモリ制御（DMC: Dynamic Memory Control）機能で自動化したりできます。

チャージバック使用解析レポートには、以下のデータ列が含まれます。

- **VM 名**: 仮想マシンの名前です。
- **VM アップタイム**: 仮想マシンの実行時間（XenCenter で緑色のアイコンで表示される時間）を分単位で示したものです。
- **vCPU 割り当て**: その仮想マシンに割り当てられている仮想 CPU の数です。各仮想 CPU には、そのホストの物理 CPU から均等に割り当てられます。たとえば、物理 CPU を 2 つ搭載した 1 台のホストに、仮想 CPU を 8 個設定しているとします。[vCPU 割り当て] 列の数値が「1」の場合、この値はホストの総処理能力の 16 分の 2 に相当します。
- **最小 CPU 使用率 (%)**: レポート期間内に記録された仮想 CPU 使用率の最小値です。仮想マシンの仮想 CPU 能力に対するパーセンテージとして示されます。この能力は、仮想マシンに割り当てられている仮想 CPU の数に基づきます。たとえば、仮想マシンに仮想 CPU を 1 つ割り当てている場合、[最小 CPU 使用率] には、記録された中で最も低い仮想 CPU の使用率が表示されます。仮想マシンに 2 つの仮想 CPU を割り当てている場合は、それらの合計能力に対する最小使用率が示されます。

この最小 CPU 使用率は、仮想 CPU が処理した最小ワークロードを示します。たとえば、仮想マシンに仮想 CPU を 1 つ割り当てており、ホストの物理 CPU は 2.4GHz である場合、仮想マシンには 0.3GHz が割り当てられます。ここで [最小 CPU 使用率] が 20% であった場合、この仮想マシンでの物理ホスト CPU の最小使用量が 60MHz であったことを示します。

- **最大 CPU 使用率 (%)** : レポート期間内に記録された仮想 CPU 使用率の最大値です。この値はその仮想マシンの仮想 CPU の能力に対するパーセンテージで示され、仮想 CPU の能力はその仮想マシンに割り当てられている仮想 CPU の数に基づきます。たとえば、仮想マシンに 1 つの仮想 CPU を割り当てた場合、その仮想 CPU 使用率の最大値が XenServer により記録され、最大 CPU 使用率として示されます。仮想マシンに 2 つの仮想 CPU を割り当てた場合は、それらの合計能力に対する最大使用率が示されます。
- **平均 CPU 使用率 (%)** : レポート期間内に記録された仮想 CPU 使用率の平均値です。この値はその仮想マシンの仮想 CPU の能力に対するパーセンテージで示され、仮想 CPU の能力はその仮想マシンに割り当てられている仮想 CPU の数に基づきます。仮想マシンに 2 つの仮想 CPU を割り当てた場合は、それらの合計能力に対する最大使用率が示されます。
- **ストレージ割り当て合計 (GB)** : レポート期間内にその仮想マシンに割り当てられていたディスク容量です。通常、この値は仮想マシンの作成時に割り当てたディスクのサイズを示します（作成後に変更していない場合）。
- **仮想 NIC 割り当て** : 仮想マシンに割り当てられている仮想インターフェイス (VIF) の数です。
- **現在の最小動的メモリ (MB)** :
  - **固定メモリ割り当て** : 仮想マシンに特定のメモリ量 (1,024MB など) を割り当てた場合、次の列には同じ値が表示されます: [現在の最小動的メモリ (MB)]、[現在の最大動的メモリ (MB)]、[現在のメモリ割り当て (MB)]、および [平均メモリ割り当て (MB)]。
  - **動的メモリ割り当て** : 動的メモリ制御を有効にした場合、Citrix Hypervisor は設定範囲内の最小メモリ量をこの列に表示します。範囲で設定している最小メモリが 1,024MB、最大メモリが 2,048 MB である場合、[現在の最小動的メモリ (MB)] 列には「1,024MB」と表示されます。
- **現在の最大動的メモリ (MB)** :
  - **動的メモリ割り当て** : Citrix Hypervisor で範囲に基づいて仮想マシンのメモリが自動調整されている場合は、その範囲の最大メモリ量がこの列に表示されます。たとえば、範囲内の最小メモリ値が 1,024MB、最大メモリ値が 2,048MB である場合、[現在の最大動的メモリ (MB)] には「2,048MB」と表示されます。
  - **固定メモリ割り当て** : 仮想マシンに特定のメモリ量 (1,024MB など) を割り当てた場合、次の列には同じ値が表示されます: [現在の最小動的メモリ (MB)]、[現在の最大動的メモリ (MB)]、[現在のメモリ割り当て (MB)]、および [平均メモリ割り当て (MB)]。
- **現在のメモリ割り当て (MB)** :
  - **動的メモリ割り当て** : 動的メモリ制御を有効にした場合、レポート対象期間内に Citrix Hypervisor が仮想マシンに割り当てたメモリ量が表示されます。

- 固定メモリ割り当て：仮想マシンに特定のメモリ量（1,024MB など）を割り当てた場合、次の列には同じ値が表示されます：[現在の最小動的メモリ（MB）]、[現在の最大動的メモリ（MB）]、[現在のメモリ割り当て（MB）]、および [平均メモリ割り当て（MB）]。

注：

仮想マシンのメモリ割り当てを変更した直後にこのレポートを実行した場合、この列には変更後の値が表示されます。

- 平均メモリ割り当て（**MB**）：

- 動的メモリ割り当て：動的メモリ制御を有効にした場合、レポート期間内に Citrix Hypervisor が仮想マシンに割り当てたメモリ量の平均値が表示されます。
- 固定メモリ割り当て：仮想マシンに特定のメモリ量（1,024MB など）を割り当てた場合、次の列には同じ値が表示されます：[現在の最小動的メモリ（MB）]、[現在の最大動的メモリ（MB）]、[現在のメモリ割り当て（MB）]、および [平均メモリ割り当て（MB）]。

注：

仮想マシンのメモリ割り当てを変更した直後にこのレポートを実行した場合、この列の値に変更内容が反映されない場合があります。この列には、指定した期間での平均値が表示されます。

- 平均ネットワーク読み取り（**bps**）：レポート期間内に仮想マシンが受信したデータ量（1秒あたりのビット数）の平均値です。
- 平均ネットワーク書き込み（**bps**）：レポート期間内に仮想マシンが送信したデータ量（1秒あたりのビット数）の平均値です。
- 平均ネットワーク使用（**bps**）：平均ネットワーク読み取りと平均ネットワーク書き込みの合計データ量（1秒あたりのビット数）です。レポート期間における仮想マシンの平均送信速度が1,027bps、平均受信速度が23,831bpsである場合、[平均ネットワーク使用]にはこれらの値を合計した次の値が表示されます：24,858bps。
- ネットワーク使用合計（**bps**）：レポート期間内に行われたネットワーク読み取りおよび書き込みトランザクションの合計値です。

#### ホストヘルス履歴

このレポートでは、特定のホスト上のリソース（CPU、メモリ、ネットワーク読み取り、およびネットワーク書き込み）のしきい値に対するパフォーマンスが示されます。

各しきい値は、色つきの線（赤、緑、黄色）で示されます。このレポートとプールヘルスレポートを使用して、特定ホストのパフォーマンスがリソースプールのパフォーマンスにどう影響しているかを評価できます。パフォーマンスしきい値を変更する場合は、このレポートでホストのパフォーマンスを確認します。

リソース使用のデータは、日別または時間別の平均値として表示できます。時間別の平均値では、その日のピーク時刻を確認できます。

時間別のデータを表示するには、[ホストヘルス履歴] の下の [クリックして特定期間内の時間別レポートデータを表示します] をクリックします。

このレポートには、指定した期間の時間別平均値が表示されます。つまり、データポイントは、指定期間のすべての日の特定時刻の平均使用量に基づいています。たとえば、2009年5月1日から2009年5月15日までのレポートの場合、[平均CPU使用率] のデータポイントはこの15日間の午後12時のすべてのリソース使用量を示します。値は平均値となります。5月1日の午後12時のCPU使用率が82%、5月2日の午後12時が88%、残りの日の午後12時がすべて75%だった場合、午後12時の平均値として76.3%が表示されます。

注:

ワークロードバランスでは、パフォーマンス測定値に急激な増加があっても平滑化されます。

### プール最適化パフォーマンス履歴

このレポートでは、最適化イベントがリソースプールの平均リソース使用に対して示されます。最適化イベントとは、管理者がリソースプールを最適化したときのことを指します。このレポートに表示されるリソース使用は、CPU、メモリ、ネットワーク読み取り、およびネットワーク書き込みです。

点線は、指定した期間のプール内の平均リソース使用を示します。青いバーは、プールを最適化した日を示します。

このレポートを使用して、設定したワークロードバランスが意図したとおりに動作しているかどうかを評価できます。また、何が最適化イベントの原因になっているか（つまりワークロードバランスの推奨項目生成前のリソース使用）を確認できます。

このレポートに示されるのは、対象日の平均リソース使用量です。システムに高負荷がかかった場合などのピーク時のデータは表示されません。また、ワークロードバランスの推奨項目を適用しなかった場合のプールのパフォーマンスを確認することもできます。

通常、最適化イベントの後はリソース使用量は低下するか、または一定の値になります。最適化してもリソース使用が改善しない場合は、しきい値の調整を検討します。また、リソースプールに配置している仮想マシンが多すぎないかどうかや、指定期間内に仮想マシンの新規追加や削除を行っているかどうかを調べてください。

### プール監査記録

このレポートには、Citrix Hypervisor の監査ログの内容が表示されます。監査ログは Citrix Hypervisor の一機能であり、承認されていないアクションの試みを記録し、承認するアクションを指定できます。こうしたアクションには以下のものがあります:

- インポートとエクスポート
- ホストとプールのバックアップ
- ゲストおよびサーバーからのコンソールへのアクセス

RBAC (Role Based Access Control: 役割ベースのアクセス制御) 機能での各 Citrix Hypervisor 管理者に役割を割り当てた環境では、このレポートでより詳しい情報を取得することができます。

### 重要:

監査ログレポートを実行するには、監査ログ機能を有効にする必要があります。デフォルトでは、ワークロードバランス仮想アプライアンスの監査ログ機能が常に有効になっています。

プール監査記録レポートでは、監査ログレポートに収集されるデータの詳細度を指定できます。また、特定のユーザー、オブジェクト、および時間を指定して監査記録ログの内容を検索したりフィルタとして適用したりできます。[プール監査記録レポートのデータ量] は、デフォルトで [最小] に設定されています。この設定により、ユーザーおよびオブジェクトの種類についての限定された量のデータが収集されます。この設定は、レポートに必要な情報の詳細度に応じていつでも変更できます。たとえば、監査ログのユーザー向けのレポートの場合は、詳細を [中] に設定します。詳細なレポートが必要な場合は [最大] に設定します。

### レポート項目

プール監査記録レポートに含まれる内容は以下のとおりです。

- 時間: Citrix Hypervisor でのユーザーアクションの記録日時です。
- ユーザー名: そのアクションを実行したときのセッションを作成した管理者のユーザーアカウントです。ユーザー ID が表示される場合もあります。
- イベントオブジェクト: アクションの対象オブジェクト (仮想マシンなど) です。
- イベントアクション: アクションの内容です。詳しくは、「監査記録でのイベント名」を参照してください。
- アクセス: その管理者に当該アクションの実行が許可されていたかどうかを示されます。
- オブジェクト名: 対象オブジェクトの名前 (仮想マシン名など) です。
- オブジェクト UUID: 対象オブジェクトの UUID (Universally Unique Identifier: 汎用一意識別子) (仮想マシンの UUID など) です。
- 成功: アクションの実行結果 (成功したかどうか) を示します。

### 監査ログでのイベント名

監査ログレポートには、Citrix Hypervisor のイベントやイベントオブジェクトだけでなく、インポートやエクスポート、ホストやプールのバックアップ、仮想マシンやサーバーのコンソールへのアクセスなどの操作が記録されます。次の表は、Citrix Hypervisor の監査ログレポートおよびプール監査記録レポートに出力される主なイベントの一覧です。また、これらのイベントのその出力データの量も示しています。

プール監査記録レポートの [Event Action] 列には、プール、仮想マシン、またはサーバーに関するイベントが出力されます。何に関するイベントかを確認するには、[Event Object] 列と [Object Name] 列を参照してください。そのほかのイベントについては、Citrix Web サイトで公開されている『Citrix Hypervisor Management API』(英文) を参照してください。

| プール監査記録でのデータ量 | イベントアクション                                | ユーザーアクション                                              |
|---------------|------------------------------------------|--------------------------------------------------------|
| 最小            | <code>pool.join</code>                   | 新規プールへのホストの追加                                          |
| 最小            | <code>pool.join_force</code>             | プールへのホストの（強制）追加                                        |
| 中             | <code>SR.destroy</code>                  | ストレージリポジトリの破棄                                          |
| 中             | <code>SR.create</code>                   | ストレージリポジトリの作成                                          |
| 中             | <code>VDI.snapshot</code>                | VDI の読み取り専用スナップショットの作成（そのスナップショットへの参照を返す）              |
| 中             | <code>VDI.clone</code>                   | VDI の完全複製の作成（その新規ディスクへの参照を返す）                          |
| 中             | <code>VIF.plugin</code>                  | 特定 VIF のホットプラグ。実行中の仮想マシンに動的に接続                         |
| 中             | <code>VIF.unplug</code>                  | 特定 VIF のホットアンプラグ。実行中の仮想マシンから動的に接続解除                    |
| 最大            | <code>auth.get_subject_identifier</code> | 人間が判読できるサブジェクト名からサブジェクト識別子を文字列として取得するための外部ディレクトリサービス照会 |
| 最大            | <code>task.cancel</code>                 | タスクのキャンセルの要求                                           |
| 最大            | <code>VBD.insert</code>                  | デバイスへの新規メディアの挿入                                        |
| 最大            | <code>VIF.get_by_uuid</code>             | 指定 UUID による VIF インスタンスへの参照取得                           |
| 最大            | <code>VDI.get_sharable</code>            | 指定 VDI の共有可能フィールドの取得                                   |
| 最大            | <code>SR.get_all</code>                  | システムで既知の全ストレージリポジトリ一覧の取得                               |
| 最大            | <code>pool.create_new_blob</code>        | このリソースプールに関連付けられた名前付きバイナリ BLOB 用のブレースホルダー作成            |
| 最大            | <code>host.send_debug_keys</code>        | デバッグキーとしての指定文字列の Xen への送信                              |

| プール監視記録でのデータ量 | イベントアクション                       | ユーザーアクション                                                            |
|---------------|---------------------------------|----------------------------------------------------------------------|
| 最大            | <code>VM.get_boot_record</code> | 仮想マシンの動的状態レコードの取得。仮想マシンの起動時に初期化され、実行時の構成内容の変更 (CPU ホットプラグなど) を反映して更新 |

## プールヘルス

プールヘルスレポートには、リソースプールおよびそのホストでの時間およびリソースの使用率が表示されます。これらの情報は、限界しきい値、高しきい値、中しきい値、および低しきい値の平均パーセンテージで示されます。

このレポートの内容は以下のとおりです。

- [中しきい値の平均] (青) は、最適化モードの設定にかかわらず、好ましいリソース使用を示します。同様に、円グラフの青い部分は、そのサーバーのリソース使用が良好だった期間を示します。
- [低しきい値の平均 (%) ] (緑) は、必ずしも好ましいリソース使用を示すとは限りません。低しきい値のリソース使用が好ましいかどうかは、最適化モードの設定によって異なります。最適化モードとして [密度を最大化] を選択したリソースプールで、ほとんどの期間のリソース使用が緑で示される場合、ワークロードバランスでホストまたはプールの仮想マシンの密度が最大化されていないことが考えられます。この場合は、リソース使用の多くが [中しきい値の平均] (青) で示されるようになるまで、パフォーマンスしきい値を調整します。
- [限界しきい値の平均 (%) ] (赤) は、平均リソース使用が限界しきい値以上になった期間を示します。

サーバーのリソース使用の円グラフをダブルクリックすると、XenCenter でそのサーバーのリソースについてのホストヘルス履歴レポートが表示されます。プールヘルス履歴レポートに戻るには、ツールバーの [元のレポートに戻る] をクリックします。

このレポートで示される値の大半が [中しきい値の平均] の範囲に収まらない場合は、このリソースプールのパフォーマンスしきい値を調整します。ワークロードバランスでは各パフォーマンスしきい値にデフォルト値が設定されますが、環境によっては調整が必要な場合があります。これを行わないと、ワークロードバランスで適切な推奨項目が生成されません。詳しくは、「しきい値の変更」を参照してください。

## プールヘルス履歴

このレポートでは、リソースプール内のすべての物理サーバーのリソース使用が線グラフで示されます。これにより、しきい値 (限界、高、中、および低) に関して、リソースの使用傾向を確認できます。このレポートのデータポイントの傾向を監視することで、設定したパフォーマンスしきい値の効果を評価できます。

ワークロードバランス仮想アプライアンスへの接続時に管理者設定したしきい値 (限界しきい値) に基づいて、高、中、および低しきい値の範囲が決定されます。プールヘルス履歴レポートはプールヘルスレポートに似ていますが、表示されるのは日別の平均リソース使用量です。各しきい値状態で動作した期間は示されません。

[平均空きメモリ] グラフを除き、データポイントの平均値が限界しきい値（赤線）以下に維持される必要があります。[平均空きメモリ] グラフの場合は、データポイントの平均値が限界しきい値（グラフの最下部）を下回ることはありません。これは、このグラフが空きメモリを示すためで、ほかのリソースのしきい値とは異なり、許容最小値を限界しきい値として設定するためです。

このレポートの内容は以下のとおりです。

- 平均使用量のグラフが [中しきい値の平均]（青線）に近い場合、リソース使用量は適切です。この表示は、最適化モードの設定に依存しません。
- [低しきい値の平均]（緑）に近い場合は、必ずしも好ましいリソース使用を示すとは限りません。低しきい値のリソース使用が好ましいかどうかは、最適化モードの設定によって異なります。以下のような場合があります：
  - 最適化モードを [密度の最大化] に設定している。
  - 平均使用量のグラフが多くの日で緑線以下であるこれらの場合、ワークロードバランスでプールの仮想マシンの密度が最大化されない可能性があります。この場合は、リソース使用の多くが [中しきい値の平均]（青）で示されるようになるまで、プールの低しきい値を調整します。
- リソースの平均使用のグラフが [限界しきい値の平均 (%) ]（赤）と交差する箇所は、リソースの平均使用が限界しきい値以上になった日を示します。

グラフのデータポイントが [中しきい値の平均] 範囲外に表示されているものの、プールで良好なパフォーマンスが得られる場合は、パフォーマンスしきい値の調整を検討します。詳しくは、「しきい値を変更する」を参照してください。

#### プールの最適化履歴

プールの最適化履歴レポートでは、ワークロードバランスによる最適化処理の内容が時系列で示されます。

最適化処理は、グラフおよび表で示されます。表の [日付] 列の [+] をクリックすると、その日に実行された最適化処理の詳細が表示されます。

このレポートの内容は以下のとおりです。

- VM 名: ワークロードバランスにより最適化された仮想マシンの名前です。
- 理由: 最適化の理由です。
- 方法: 最適化処理が成功したかどうかを示します。
- 移行元: 仮想マシンの移行元の物理サーバーです。
- 移動先: 仮想マシンの移行先の物理サーバーです。
- 時間: 最適化処理の実行時刻です。

#### ヒント:

プールの最適化履歴レポートは、[WLB] タブの [履歴を表示] をクリックすることでも生成できます。

### 仮想マシン移動履歴

この線グラフでは、リソースプールでの仮想マシンの移動（移行）数が示されます。仮想マシンの移行が推奨項目を適用した結果なのかどうか、および移行先のホストが表示されます。また、このレポートでは移行理由も示されます。このレポートを使用して、リソースプールの仮想マシンの移行を監査できます。

このレポートの内容は以下のとおりです。

- グラフの左側の数値は可能な移行数を示します。この値は、リソースプール内の仮想マシンの数に基づいています。
- レポートの [日付] 列の [+] をクリックすると、その日に実行された移行処理の詳細が表示されます。

### 仮想マシンパフォーマンス履歴

このレポートでは、特定ホスト上の各仮想マシンのパフォーマンスデータが示されます。ワークロードバランスでは、仮想マシンに割り当てられた仮想リソースの量に基づいてパフォーマンスデータが評価されます。たとえば、仮想マシンの平均 CPU 使用率が 67% の場合、対象期間に平均で仮想マシンの仮想 CPU の 67% が使用されたことになります。

このレポートの初期表示では、指定した期間でのリソース使用の平均値が示されます。

[+] をクリックすると、各リソースの線グラフが表示されます。これにより、特定期間でのリソースの使用傾向を確認できます。

このレポートには、CPU 使用率、空きメモリ、ネットワーク読み取り/書き込み、およびディスク読み取り/書き込みのデータが表示されます。

### ワークロードバランスの機能と設定の管理

このセクションでは、ワークロードバランスの設定を必要に応じて変更する方法について説明します。以下の操作が含まれます：

- 最適化モードを変更する
- 電源を自動的に最適化および管理する
- しきい値を変更する
- 測定基準の重要度を変更する
- 特定のホストを推奨項目の対象から除外する
- 詳細な自動処理オプション、およびデータストレージを設定する。
- プール監査記録レポートのデータ量設定を変更する。

このセクションの内容は、ワークロードバランス仮想アプライアンスへの接続が完了しているリソースプールを想定しています。ワークロードバランスを使用するために必要なワークロードバランス仮想アプライアンスの入手および

設定について詳しくは、「[導入](#)」を参照してください。また、ワークロードバランス仮想アプライアンスにリソースプールを接続する方法については、ワークロードバランス仮想アプライアンスへの接続を参照してください。

#### ワークロードバランス設定の変更

ワークロードバランス仮想アプライアンスに接続したら、必要に応じて、配置や推奨項目を計算するための設定を変更できます。

変更可能な最適化設定および再配置設定には以下のものがあります：

- 最適化モードの設定の変更
- 自動最適化および電源管理の設定
- パフォーマンスしきい値および測定基準の重要度の変更
- ホストの除外

ワークロードバランスの設定は、リソースプールに属するすべてのホストおよび仮想マシンに適用されます。

ネットワークやディスクのパフォーマンスがその環境のハードウェアに適したものである場合は、まずデフォルトの設定でワークロードバランスを使用します。

ワークロードバランス機能をしばらく運用した後で、パフォーマンスのしきい値を評価して、変更の必要性について検討することをお勧めしています。たとえば、以下の場合に設定の変更を検討します：

- 推奨項目が必要以上に生成される。この場合、適切な推奨項目が生成されるようになるまでしきい値を調整します。
- 意図したとおりに推奨項目が生成されない。たとえば、ネットワーク帯域幅が十分でないにもかかわらず推奨項目が生成されない場合は、設定の変更が必要かどうかを検討します。この場合、適切な推奨項目が生成されるようになるまでネットワークのしきい値を下げます。

しきい値を変更する前に、リソースプール内の各物理ホストについてホストヘルスレポートを作成することをお勧めします。

ワークロードバランス設定を変更するには、XenCenter の [ワークロードバランス設定] ダイアログボックスを使用します。

Citrix Hypervisor とワークロードバランスサーバーとの通信で使用される資格情報を変更する方法については、ワークロードバランス設定ファイルの編集を参照してください。

「XenCenter のインフラストラクチャペインで、[XenCenter] > [your-pool](#)」を参照してください。

[プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブの [設定] をクリックします。

#### 最適化モードを変更する

ワークロードバランスでは、仮想マシンの実行によるワークロードを再配置（つまり最適化）するための推奨項目が生成されます。この推奨項目は、管理者が選択する再配置設定に基づいて計算されます。再配置設定は、最適化モードとも呼ばれます。

最適化モードには、以下の2つがあります。

- パフォーマンスを最大化。（デフォルト）リソースプール内のすべての物理ホスト上に仮想マシンを均等に配置します。これにより、すべてのホストのCPU、メモリ、およびネットワーク負荷を最小化できます。この最適化モードでは、ホストが高しきい値に達すると最適化の推奨項目が生成されます。
- 密度を最大化。リソースプール内で稼働する物理ホストの数を最小化するために、1台の物理ホスト上に可能な限り多くの仮想マシンを配置します。

この最適化モードでは、[パフォーマンスを最大化] を選択した場合と同様のしきい値を使用できます。ただし、これらのしきい値は、1台のホストにどれだけ多くの仮想マシンを配置できるかを評価するために使用されます。この最適化モードでは、仮想マシンが低しきい値に達すると最適化の推奨項目が生成されます。

これらの最適化モードは、永続的に適用（固定）したり、特定のスケジュールに基づいて適用（スケジュール指定）したりできます。

- 最適化モードを固定すると、ワークロードバランスでは指定した最適化操作が常に行われます。この操作には、パフォーマンスの最大化か、密度の最大化を設定できます。
- 最適化モードのスケジュールを指定すると、指定したスケジュールに基づいてモードを切り替えることができます。たとえば、多くのエンドユーザーが作業する日中にはパフォーマンスを最大化するモードを適用します。使用電力を抑えるために、夜間は密度を最大化するモードを適用できます。

最適化モードのスケジュールを指定すると、その期間（曜日および時刻）に最適化モードが自動的に切り替わります。毎日、平日、週末、または特定の曜日を指定できます。また、特定の時刻を指定することもできます。

「XenCenter の [リソース] ペインで、[XenCenter] > [your-pool](#)」を参照してください。

[プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブの [設定] をクリックします。

左側のペインで [最適化モード] をクリックします。

[最適化モード] ページの [固定] セクションで、いずれかの最適化モードを選択します。

- パフォーマンスを最大化。（デフォルト）リソースプール内のすべての物理ホスト上に仮想マシンを均等に配置します。これにより、すべてのホストのCPU、メモリ、およびネットワーク負荷を最小化できます。
- 密度を最大化。1台の物理サーバー上に可能な限り多くの仮想マシンを配置します。これにより、リソースプール内で稼働する物理サーバーの数を最小化できます。ワークロードバランスでは、集約された仮想マシンのパフォーマンスも考慮され、ホストのリソースが限界しきい値に達すると、パフォーマンスを改善するための推奨項目が生成されます。

「XenCenter のインフラストラクチャペインで、[XenCenter] > [your-pool](#)」を参照してください。

[プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブの [設定] をクリックします。

ダイアログボックス左側の [最適化モード] をクリックします。

[最適化モード] ページで、[スケジュール指定] をクリックします。これにより、[スケジュール指定] セクションが使用可能になります。

[新規追加] をクリックします。

[モード] ボックスで、いずれかの最適化モードを選択します。

- パフォーマンスを最大化。リソースプール内のすべての物理ホスト上に仮想マシンを均等に配置します。これにより、すべてのホストの CPU、メモリ、およびネットワーク負荷を最小化できます。
- 密度を最大化。1 台の物理サーバー上に可能な限り多くの仮想マシンを配置します。これにより、リソースプール内で稼働する物理サーバーの数を最小化できます。

選択した最適化モードに切り替える曜日および時刻を選択します。

モード変更スケジュール（「タスク」）を必要な数だけ作成します。追加したタスクが1つのみの場合、そのスケジュールに基づいて切り替わった最適化モードが元に戻らなくなります。

[OK] をクリックします。

前述の手順 1. ～ 4. を実行して、[最適化モード] ページを開きます。

[スケジュール指定] の一覧で、削除または無効にするタスクを選択します。

次のいずれかを行います：

- タスクを削除する： [削除] ボタンをクリックします。
- タスクを一時的に停止する： タスクを右クリックして [無効化] をクリックします。

ヒント：

- タスクの有効化と無効化の切り替えは、タスクを選択して [編集] をクリックし、[最適化モードのスケジュール] ダイアログボックスの [タスクを有効にする] チェックボックスを選択することで行うこともできます。
- 無効にしたタスクを有効にするには、タスクを右クリックして [有効化] を選択します。

次のいずれかを行います：

- 編集するタスクを選択します。
- [編集] をクリックします。

[変更] ボックスで、別のモードを選択するか、必要に応じて他の変更を加えます。

注：

[ワークロードバランス設定] ダイアログボックスで行った変更内容は、このダイアログボックスの [OK] を押

すまで保存されません。たとえば、最適化モードの変更スケジュールを変更した後、[ワークロードバランス設定] ダイアログボックスで [キャンセル] をクリックすると、変更前の状態に戻ります。

### 電源を自動的に最適化および管理する

ワークロードバランスによる推奨項目が自動的に適用されるように設定することができ（ワークロードバランスの自動処理機能）、また、ホストの電源を自動的に投入したり切断したりすることもできます。余剰ホストの電源が自動的に切断されるようにするには、ワークロードバランスの電源管理機能を有効にして、さらに推奨項目を自動的に適用するオプションを有効にする必要があります。電源管理と自動化の両方については、以降のセクションで説明します。

### 最適化推奨項目を自動的に適用する

ワークロードバランスで生成された推奨項目を、管理者の介在なしに自動的に適用することができます。この最適推奨項目の自動適用機能を使用すると、生成される推奨項目に基づいて、自動的にパフォーマンスを最適化したりサーバーの電源を切断したりできます。ただし、仮想マシンの使用が減少したときにホストの電源を落として消費電力を抑えるには、自動処理のほか、電源管理と密度の最大化モードを設定する必要があります。

デフォルトでは、推奨項目は自動的に適用されません。生成された推奨項目が自動的に適用（実行）されるようにするには、自動処理機能を有効にします。この機能を有効にしない場合は、[すべて実行] をクリックして推奨項目を手動で適用する必要があります。

ワークロードバランスで生成された推奨項目が高可用性の設定と競合する場合、その推奨項目は自動的に適用されません。推奨項目の適用によりプールがオーバーコミット状態になる場合は、XenCenter にそれを適用するかどうかを確認するメッセージが表示されます。自動処理を有効にしても、高可用性で許可する障害数を超える数の電源管理推奨項目は無視され、自動的に適用されません。

自動処理機能が有効なワークロードバランスは、自動モードとも呼ばれます。

自動モードのワークロードバランスで推奨項目がどのように適用されるかを変更することができます。詳しくは、「推奨項目の自動適用の積極度」を参照してください。

### ワークロードバランスによる電源管理の有効化

ワークロードバランスの電源管理機能は、リソースプールの全体的なワークロードに応じて物理ホストの電源を投入したり切断したりするための機能です。

ホストでワークロードバランスの電源管理を構成するための要件は、以下の通りです：

- ホストのハードウェアがリモートからの電源投入/切断をサポートしている。
- ホストの電源投入機能が設定されている。
- ホストが電源管理の対象として明示的に選択されている。

また、ワークロードバランスでホストの電源を自動的に切断する場合は、以下の設定を行う必要があります：

- 最適化推奨項目を自動的に適用する

- 電源管理推奨項目を自動的に適用する

プール内で使用されていないリソースがワークロードバランスにより検出された場合、容量の超過が解消されるまでホストの電源を切断するよう求める推奨項目が作成されます。プール内のホスト容量が不足しておりホストの電源を切断できない場合は、プールのワークロードが十分に減少するまでホストを放置するように求められます。余剰ホストの電源を自動的に切断するように設定した場合は、電源を切るための推奨項目が自動的に適用されます。

電源管理の対象ホストを指定すると、そのホストの電源を投入したり切断したりするための推奨項目が生成されます。[パフォーマンスを最大化] モードに設定している場合は次のようになります：

- ホストの電源を自動で切断するようにワークロードバランスを設定している場合は、ホストのリソース使用量が [高] のしきい値を超えるとホストの電源が切断されます。
- ワークロードバランスにより電源投入されたホストの電源は、リソースに余剰が生じても切断されません。

これらの電源管理推奨項目の自動処理を有効にする場合、リソースプール全体に適用されます。ただし、電源管理の対象ホストは個別に選択できます。

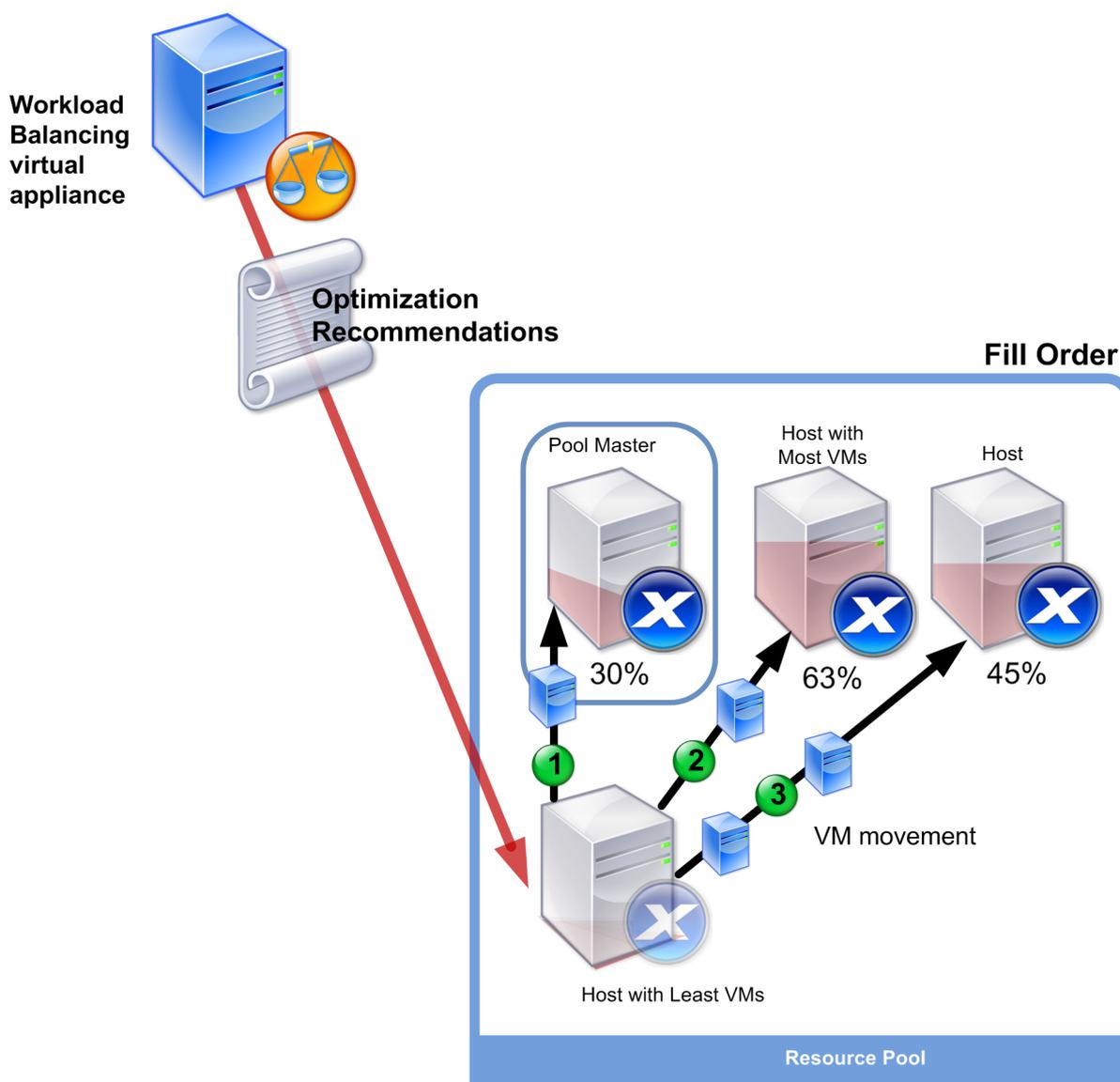
#### 電源管理のしくみ

ワークロードバランスによりホストの電源が切断される前に、そのサーバー上の仮想マシンの移行先ホストが選択されます。移行先ホストは、以下の順序で決定されます：

1. プールマスターが最初の移行先ホストになります。これは、プールマスターの電源が切断されることがないためです。
2. 次に、より多くの仮想マシンを実行しているホストが選択されます。
3. 以降、実行している仮想マシンの数が多いホストから順番に選択されます。

ワークロードバランスでプールマスターに仮想マシンを移行する場合、意図的に低いしきい値が使用されます。これにより、プールマスターが過負荷状態になるのを防ぎます。

この順序で仮想マシンをホストに移行することで、密度が高くなります。



最適化モードとして密度の最大化が選択されているプールでパフォーマンスに関する問題が検出されると、ワークロードバランスは電源投入済みのホスト間での仮想マシンの移行を推奨して問題を解決しようとします。この方法で問題が解決されない場合、シャットダウン状態のホストの電源を投入します。このとき、最適化モードとして [パフォーマンスの最大化] が設定された場合と同じ条件に基づいて、電源投入するホストが決定されます。

このとき、最適化モードとしてパフォーマンスの最大化が選択された場合と同じ条件に基づいて、電源投入するホストが決定されます。

仮想マシンを移行しているときに、オンライン状態のホストを増やすことでプール全体のパフォーマンスが改善するとワークロードバランスが判断した場合、自動的にホストの電源を投入したり、電源投入の推奨項目を生成したりします。

**重要:**

ワークロードバランスでは、推奨項目により電源が切断されたホストに対してのみ、電源投入の推奨項目を生成します。

#### 電源管理および仮想マシン集約のための環境設計

Citrix Hypervisor を実装して電源管理と仮想マシン集約を自動化する場合は、以下の点を考慮して環境を設計します。

- 異なる種類のワークロードを個別のプールに配置する：異なる種類のワークロードを実行する場合は、それらのワークロードに対応する仮想マシンを個別のプールに配置することを検討します。また、特定の種類のハードウェアでパフォーマンスが向上するタイプのアプリケーションをホストする仮想マシンを別のプールに分割することも検討してください。

電源管理機能および仮想マシンの集約はプールレベルで管理されるため、同じ比率で集約するワークロードが含まれるようにプールを設計します。この際には、「推奨項目の自動適用の制御」で説明されている点などを考慮に入れてください。

- 特定のホストをワークロードバランスから除外する：ホストの中には、常に電源をオンしておく必要があるものもあります。詳しくは、「特定のホストを推奨項目の対象から除外する」を参照してください。

#### 最適化推奨項目を自動的に適用するには

- 「XenCenter のインフラストラクチャペインで、[XenCenter] > [your-pool](#)」を参照してください。
- [プロパティ] ペインの [WLB] タブをクリックします。
- [WLB] タブの [設定] をクリックします。
- ダイアログボックス左側の [自動処理] をクリックします。
- 以下のオプションを設定します。
  - 最適化推奨項目を自動的に適用する：このチェックボックスをオンにすると、管理者の介在なしに最適化推奨項目を適用できます。ワークロードバランスにより自動的に最適化が行われ、仮想マシンが再配置されます。
  - 電源管理推奨項目を自動的に適用する：このチェックボックスによる動作は、リソースプールの最適化モードにより異なります。
    - パフォーマンスの最大化モード：[電源管理推奨項目を自動的に適用する] チェックボックスをオンにすると、ホストのパフォーマンスを改善するためにオフラインホストの電源が自動的に投入されます。
    - 密度の最大化モード：[電源管理推奨項目を自動的に適用する] チェックボックスをオンにすると、リソース使用量が [低] しきい値を下回ったホストの電源が自動的に切断されます。つまり、ホストは使用量が低い期間において、自動的に切断されることとなります。

6. (オプション) [ワークロードバランス設定] ダイアログボックスの [詳細] j ページで、以下のオプションを設定します:

- 最適化推奨項目が自動的に適用されるまでの作成回数を指定します。デフォルトでは、同じ推奨項目が3回生成された場合、3回目の推奨項目が自動的に適用されます。
- 自動的に適用する最適化推奨項目の最低重要度レベルを選択します。デフォルト値は [高] です。
- 最適化推奨項目をどれだけ積極的に自動適用するかを指定します。

また、移行したばかりの仮想マシンを最適化推奨項目に含めるまでの時間を分単位で指定できます。

これらのオプションについて詳しくは、推奨項目の自動適用の積極度を参照してください。

7. 次のいずれかを行います:

- 電源管理機能を設定するには、[自動処理] ページを開き、電源管理対象のホストを選択するにはの説明に従います。
- 電源管理を構成せずに自動化の構成が完了した場合は、[OK] をクリックします。

電源管理対象のホストを選択するには

1. [自動処理] ページの [電源管理] セクションで、ワークロードバランスの電源管理推奨項目の対象となるホストを選択します。

注:

[電源管理推奨項目を自動的に適用する] チェックボックスをオフにしたままこの一覧でホストを選択した場合、電源管理の推奨項目の提案は行われますが、自動的に適用されません。

2. [OK] をクリックします。リソースプール内にリモートからの電源管理をサポートするホストがない場合、ワークロードバランスの電源管理機能は動作しません。

推奨項目を生成するしくみ

ワークロードバランスでは、リソースプール内の物理ホストや仮想マシンのリソース負荷の測定基準が、そのしきい値と照合され評価されます。これらのしきい値は事前に設定されており、この値を超えると最適化の推奨項目が生成されます。事前設定値は [最高] に設定されています。ワークロードバランスでは、以下のプロセスで推奨項目を生成します:

1. リソースの負荷がしきい値を超えたことを検出する。
2. 最適化の推奨項目を生成するかどうかを評価する。
3. 移行先として適切なホストを決定する。このホストには、1つまたは複数の仮想マシンの再配置先として推奨されるホストが選ばれます。
4. 推奨項目を生成する。

ワークロードバランスは、最適化が必要であることを検出すると、推奨項目を作成する前にプール内のほかのホストを評価して、以下について決定します：

1. 最適化を行う順番（対象ホスト、対象仮想マシン）
2. 推奨項目の作成時に推奨する仮想マシンの移行先ホスト

これら 2 つのタスクを行うため、ワークロードバランスでは以下のしきい値および重要度が使用されます：

- しきい値：ワークロードバランスでプール内のリソース負荷の測定基準と照合される境界値です。推奨項目を生成するかどうか、および仮想マシンの移行先ホストを決定するために使用されます。
- 重要度：リソース負荷の各測定基準を評価するときの優先度で、この優先度に従って評価されます。ワークロードバランスは、推奨事項を決定した後、リソースの重要度に従って以下を決定します：
  - どのホストのパフォーマンスを優先するか
  - どの仮想マシンの移行を優先するか

ワークロードバランスで収集される各リソース負荷には、4 つのレベルのしきい値（限界、高、中、および低）があります。これらのしきい値により、推奨項目を生成するかどうか評価されます。

- 最適化モードとしてパフォーマンスの最大化が選択されているリソースプールでは、ホストの高しきい値を超えるリソース負荷が検出されると、仮想マシンを分散する推奨項目の生成が評価されます。
- 最適化モードとして密度の最大化が選択されているリソースプールでは、リソース負荷がホストの低しきい値を下回ると、仮想マシンを集約する推奨項目の生成が評価されます。
- 最適化モードとして密度の最大化が選択されているリソースプールでは、ホストの限界しきい値を超えるリソース負荷が検出されると、仮想マシンを分散する推奨項目の生成が評価されます。

たとえば、パフォーマンスの最大化が選択されたリソースプールで高しきい値が 80% の場合、ホストの CPU 使用率が 80.1% に達すると、仮想マシンを分散する推奨項目を生成するかどうか評価されます。

推奨項目を生成するかどうかを評価するときに、そのリソース測定基準の履歴も考慮されます。これにより、一時的な高負荷時などに推奨項目が生成されることを防ぐことができます。このため、ワークロードバランスは以下のタイミングでデータを収集し、履歴平均値測定基準を作成します。

| データが収集される期間               | 重要度 |
|---------------------------|-----|
| しきい値を超えた直後（つまりリアルタイムのデータ） | 70% |
| しきい値を超える 30 分前            | 25% |
| しきい値を超える 24 時間前           | 5%  |

午後 12 時 2 分にあるホストの CPU 使用率がしきい値を超えた場合、当日の午前 11 時 32 分と前日の午後 12 時 2 分の使用率がチェックされます。たとえば、CPU 使用率が以下のとおりである場合には、推奨項目は生成されません：

- 当日午後 12 時 2 分に 80.1%

- 当日午前 11 時 32 分に 50%
- 前日午後 12 時 32 分に 78%

これは、履歴平均値が 72.47% であり（高しきい値に達していない）、一時的な CPU 負荷であると判断されたためです。ただし、午前 11 時 32 分の使用率が 78% であった場合は、履歴平均値が 80.1% になるため推奨項目が生成されます。

#### 仮想マシンの分散および集約のプロセス

ワークロードバランスで推奨項目が生成される時のプロセスは、最適化モード（パフォーマンスの最大化または密度の最大化）により異なります。ただし、以下の 2 つの段階で行われる点は同じです：

1. 潜在的な最適化を決定する（そのホストから移行する仮想マシンの決定）。
2. 再配置の推奨項目を決定する（仮想マシンの移行先ホストの決定）。

注：

ワークロードバランスは、移行先に十分なストレージ領域があるかどうかなど、Citrix Hypervisor でのライブマイグレーションの要件を満たす仮想マシンに対してのみ最適化を行います。同様に、移行先のホストには、プールに設定されている最適化モードに基づいたしきい値を超えない範囲で仮想マシンを実行できるだけのリソースが必要です。たとえば、パフォーマンスの最大化では高しきい値以下、密度の最大化では限界しきい値以下などです。

ワークロードバランスが自動モードで動作する場合は、推奨項目を自動適用するときの設定を調整します。詳しくは、「推奨項目の自動適用の積極度」を参照してください。

#### パフォーマンスの最大化が選択されている場合の推奨項目の生成プロセス

パフォーマンスの最大化モードで実行している場合、ワークロードバランスは次のプロセスを使用して潜在的な最適化を決定します：

1. ワークロードバランスは、リソースプール内の各ホストのリソース使用を 2 分ごとに評価して、各ホストの各リソースに対する負荷が高しきい値を超えているかどうかをチェックします。高しきい値について詳しくは、しきい値を変更するを参照してください。

パフォーマンスの最大化が選択されているリソースプールでリソースの負荷が高しきい値を超えると、推奨項目を生成すべきかどうかの決定プロセスが開始されます。このときに、パフォーマンスの制約（高しきい値を超えたリソースの負荷など）が軽減されるかどうかを評価して、仮想マシンを分散させるための推奨項目を生成します。

たとえば、ホスト A の CPU リソースが足りないために仮想マシンのパフォーマンスが低下している場合を考えます。CPU 使用量の少ない別のホストがあった場合には、このホストへ仮想マシンを 1 つ以上移行するように求める推奨項目が生成されます。

2. ホストのリソース負荷がしきい値を超えたときに、以下の値から平均値（履歴平均値）を算出します：

- そのときの測定値
- 30 分前のデータ
- 24 時間前のデータ

この平均値がリソース負荷のしきい値を超えている場合に、最適化の推奨項目を生成します。

3. どのホストを先に最適化するかを決定するときに、測定基準の重要度が考慮されます。最も高い重要度を割り当てたリソースの負荷に基づいて、最適化の順番が決定されます。測定基準の重要度については、測定基準の重要度を変更するを参照してください。

4. 移行する仮想マシンをサポートできるホストを決定します。

このときに、仮想マシンのさまざまな組み合わせをホスト上に配置した場合のリソースへの影響を計算します (順列と呼ばれる方法が使用されます)。

この目的のため、ワークロードバランスは、ホストに仮想マシンを移行した場合の影響を予測するための単一の測定基準 (スコア) を作成します。このスコアにより、そのホストがより多くの仮想マシンの受け入れ先として適しているかどうかを示されます。

ホストのパフォーマンスの評価では、以下の測定基準が集計されます:

- ホストの現在の測定値
- 30 分前のホストの測定値
- 24 時間前のホストの測定値
- 仮想マシンの測定値

5. 次に、さまざまな組み合わせで仮想マシンを実行した場合を想定して、ホストの仮想モデルを作成します。このモデルにより、仮想マシンの移行先として最適なホストが決定されます。

パフォーマンスの最大化が選択されているリソースプールでは、測定基準の重要度に基づいて最初に最適化するホストおよび最初に移行する仮想マシンを決定します。ワークロードバランスは、測定基準の重要度に関するモデルに基づいています。たとえば、CPU 使用率に最も高い重要度が設定されている場合は、以下の基準でホストと仮想マシンの最適化の優先度が決定されます:

- CPU 使用率の影響を最も強く受けるホスト (現在の CPU 使用率がしきい値に最も近いホスト)
- CPU 使用率が最も高い仮想マシン (現在の CPU 使用率がしきい値に最も近い仮想マシン)

6. ワークロードバランスは最適化の計算を続行します。ホストの予測リソース使用量が高しきい値を下回るまで、ホストを潜在的な最適化の対象とみなし、仮想マシンを移行の対象とします。予測リソース使用量とは、ワークロードバランスにより仮想マシンを追加または削除されたホストで測定されると想定されるリソース負荷を指します。

密度の最大化が選択されている場合の仮想マシンの集約プロセス

ワークロードバランスの推奨項目は、移行先のホストで限界しきい値を超えずに追加の仮想マシンを実行できるかどうかに基づいて生成されます。

1. リソース負荷が低しきい値を下回ると、ワークロードバランスは潜在的な集約シナリオの計算を開始します。

2. 仮想マシンを集約できる方法を見つけたら、その集約先ホストが仮想マシンの実行に適しているかどうかを評価します。
3. パフォーマンスの最大化の場合と同様に、ホストのスコアを作成します。

WLB は、より少ないホストで仮想マシンを統合することを推奨する前に、仮想マシンがホストに再配置された後、それらのホストのリソース使用率が限界しきい値を下回っていることを確認します。

注:

測定基準の重要度は、仮想マシンを集約する推奨項目を生成するときには考慮されません。この重要度は、集約先ホストで十分なパフォーマンスを得るためだけに考慮されます。

4. 次に、さまざまな組み合わせで仮想マシンを実行した場合を想定して、ホストの仮想モデルを作成します。このモデルにより、仮想マシンの移行先として最適なホストが決定されます。
5. ホストのリソース負荷が限界しきい値を超えると予測されるまで、そのホストに仮想マシンを追加した場合の影響について計算します。
6. 集約の推奨項目では、プールマスタが最初の移行先ホストになります。これは、プールマスタの電源が切断されることがないためです。ただし、プールマスタが過負荷状態になるのを避けるため、いくらかの余裕を残して仮想マシンを移行します。
7. すべてのホストでリソース負荷が限界しきい値を超えるまで、推奨項目の生成を続行します。

#### しきい値を変更する

最適化の推奨項目の生成を制御するために、限界しきい値を変更できます。このセクションでは、以下に関するガイダンスを示します:

- プール内のホストで使用されるデフォルトの限界しきい値の変更方法
- 高しきい値、中しきい値、低しきい値に対する限界しきい値の影響

リソース負荷の履歴平均値がそのしきい値を超えると、ワークロードバランスで推奨項目が生成されます。パフォーマンスの最大化では高しきい値、密度の最大化では低しきい値または限界しきい値を超えたときに、ワークロードバランスの推奨項目が生成されます。詳しくは、「仮想マシンの分散および集約のプロセス」を参照してください。リソースに新しいしきい値を指定すると、ワークロードバランスによりその値は限界しきい値として設定され、それを基にリソースのほかのしきい値が相対的に決定されます (XenCenter で変更できるのは限界しきい値のみです)。

次の表は、各しきい値のデフォルト値を示しています。

| 測定基準       | 重大     | 高         | 中        | 低        |
|------------|--------|-----------|----------|----------|
| CPU 使用率    | 90%    | 76.5%     | 45%      | 22.5%    |
| 空きメモリ      | 51MB   | 63.75MB   | 510MB    | 1020MB   |
| ネットワーク読み取り | 25MB/秒 | 21.25MB/秒 | 12.5MB/秒 | 6.25MB/秒 |

| 測定基準       | 重大     | 高         | 中        | 低        |
|------------|--------|-----------|----------|----------|
| ネットワーク書き込み | 25MB/秒 | 21.25MB/秒 | 12.5MB/秒 | 6.25MB/秒 |
| ディスク読み取り   | 25MB/秒 | 21.25MB/秒 | 12.5MB/秒 | 6.25MB/秒 |
| ディスク書き込み   | 25MB/秒 | 21.25MB/秒 | 12.5MB/秒 | 6.25MB/秒 |

限界しきい値に以下の係数を乗じたものが、メモリを除くすべてのしきい値として設定されます：

- 高しきい値：0.85
- 中しきい値：0.50
- 低しきい値：0.25

たとえば、CPU 使用率の限界しきい値を 95% に変更した場合、高、中、および低のしきい値がそれぞれ 80.75%、47.5%、および 23.75% に変更されます。

空きメモリのしきい値は、限界しきい値に以下の係数を乗じたものが使用されます。

- 高しきい値：1.25
- 中しきい値：10.0
- 低しきい値：20.0

特定のしきい値についてこの計算を行うには、限界しきい値として指定した数値にこれらの数を乗じます。

高、中、または低しきい値 = 限界しきい値 \* しきい値

たとえば、[ネットワーク読み取り] のしきい値を 40MB/秒に変更した場合、低しきい値は  $40 \times 0.25 = 10\text{MB/秒}$  となります。中しきい値は  $40 \times 0.50$  で計算できます。

多くの推奨項目は限界しきい値に基づいて生成されますが、ほかのしきい値により推奨項目が生成される場合もあります。

- 高しきい値。
  - パフォーマンスを最大化。高しきい値を超えたときに、仮想マシンをリソース負荷の低いホスト上に移行するための推奨項目が生成されます。
  - 密度を最大化。追加の仮想マシンによりホストのいずれかのリソース使用量が高しきい値を超える場合、そのホスト上に仮想マシンを移行する推奨項目が生成されなくなります。
- 低しきい値。
  - パフォーマンスを最大化。推奨項目は生成されません。

- 密度を最大化。測定基準値が低しきい値を下回ると、仮想マシンをそのホスト上に集約するための推奨項目が生成されます。そのホストのいずれかのリソース負荷が高しきい値に達するまで、仮想マシンの集約先としてそのホストの推奨が続行されます。

ただし、仮想マシンの移行後に、新しいホストのリソース負荷が限界しきい値を超える場合があります。この場合は、パフォーマンスの最大化の場合と同様のロードバランスアルゴリズムにより、仮想マシンの新しい集約先が決定されます。リソースプール内のすべてのサーバーのリソース負荷が高しきい値を下回るまで、このアルゴリズムによる推奨項目の生成が続行されます。

しきい値を変更するには

1. 「XenCenter のインフラストラクチャペインで、[XenCenter] > [your-resource-pool](#)」を参照してください。
2. [プロパティ] ペインの [WLB] タブをクリックします。
3. [WLB] タブの [設定] をクリックします。
4. 左側のペインで [しきい値] を選択します。これらの値は、現在設定されている限界しきい値を示します。
5. [しきい値] ページでは、リソース使用量の限界しきい値を1つまたは複数設定できます。新しい限界しきい値に基づいて、高、中、および低しきい値が算出されます。

ワークロードバランスでは、仮想マシンの推奨再配置先を計算するときに、これらの限界しきい値が使用されます。各サーバーのリソース使用がこれらのしきい値を超えないように、仮想マシンによるワークロードを分散できます。

測定基準の重要度を変更する

ワークロードバランスでは、次の最適化モードに基づいて、どのホストや仮想マシンを先に最適化するかを決定するときに、各リソース測定基準の重要度が考慮されます：パフォーマンスの最大化または密度の最大化。

ワークロードバランスが最適化推奨項目を生成する際、ホストを最適化するための順番が算出されます。高い重要度が割り当てられている測定基準の値が比較され、ホストを最適化するための順番が決定されます。

通常、測定基準の重要度は、最適化モードとしてパフォーマンスの最大化が選択されているリソースプールで使用されます。ただし、密度の最大化が選択されている場合でも、限界しきい値を超えた測定基準では、その重要度が考慮されません。

パフォーマンスの最大化モード

[パフォーマンスの最大化] が選択されているリソースプールでは、ワークロードバランスで、測定基準の重要度により、どのホストのパフォーマンスを先に最適化するか、およびどの仮想マシンを先に移行するかが決定されます。

たとえば、[ネットワーク書き込み] を [重要度：高] に設定している場合、ネットワーク書き込み回数が最も多いホストが先に最適化の対象になります。[ネットワーク書き込み] を最重要として設定するには、[測定基準の重要度] スライダを右に設定し、ほかのスライダはすべて中央に設定します。

すべての測定基準の重要度が同じ場合、CPU 使用率、空きメモリの順に考慮されます。これは、これらのリソースに対する制約がホストのパフォーマンスに大きく影響するためです。すべての測定基準の重要度を同じにするには、すべての測定基準の [測定基準の重要度] スライダーを同じ位置に設定します。

### 密度の最大化モード

密度の最大化が選択されているリソースプールでは、ホストが限界しきい値に達した場合にのみ測定基準の重要度が考慮されます。ホストが限界しきい値に達すると、すべてのホストが限界しきい値を下回るまで、パフォーマンスの最大化と同じアルゴリズムが使用されます。このアルゴリズムでは、測定基準の重要度に基づいて、ホストを最適化するための順番が決定されます。

つまり、複数のホストで限界しきい値を超えている場合、その重要度がチェックされ、先に最適化するホストが決定されます。この場合には、重要度に基づいて、最初に最適化するホストと最初に移行する仮想マシンが決定されます。

たとえば、ホスト A とホスト B で構成されるリソースプールを例に説明します：

- ホスト A では CPU 使用率に最も高い重要度が設定されており（ [重要度： 高] ）、CPU 使用率が限界値を超えています。
- ホスト B ではメモリ使用率の重要度が最も低く設定されており（ [重要度： 低] ）、メモリ使用率が限界値を超えています。

この場合、高い重要度の測定基準が限界しきい値に達しているサーバー A が先に最適化の対象になります。次に、サーバー A 上の仮想マシンのうち、CPU 使用率の最も高いものを移行するための推奨項目が作成されます。CPU 使用率の重要度が最も高いため、仮想マシンの移行は CPU 率が一番高い仮想マシンから行われます。

ホスト A に対する推奨項目を生成したら、ホスト B が最適化の対象になります。ホスト B 上の仮想マシンに対しても、CPU 使用率の最も高いものを移行するための推奨項目が作成されます。

リソースプールにほかのサーバーがある場合は、サーバーの CPU 使用率が高いものから順に最適化が行われます。

デフォルトでは、すべての測定基準の重要度はスライダーの最も遠いポイント（ [重要度： 高] ）に設定されます。

#### 注：

測定基準の重要度は、相対的に処理されます。つまり、すべての測定基準の重要度が同じ場合、その重要度レベルは意味を持ちません。重要度の相対的な高低により、各測定基準の評価が決定されます。

### 測定基準の重要度を変更するには

1. 停止します。
2. 「XenCenter のインフラストラクチャペインで、[XenCenter] > `your-resource-pool`」を参照してください。
3. [WLB] タブの [設定] をクリックします。
4. 左側のペインで [測定基準の重要度] を選択します。

5. [測定基準の重要度] ページでは、必要に応じて各リソースの重要度を調節できます。

スライダを [重要度: 低] 側にドラッグすると、そのリソースの負荷は仮想マシンの再配置先の決定には影響しなくなります。

#### 推奨項目からのホストの除外

ワークロードバランスを設定する際、特定の物理ホストがワークロードバランスの最適化および配置の推奨項目（[起動] の配置を含む）から除外されるように指定できます。

以下の状況では、特定のホストを推奨項目の対象から除外することを検討してください：

- プールの最適化モードとして [密度の最大化] を使用するが、特定のホストをこの最適化（仮想マシンの集約化とホストのシャットダウン）から除外する場合。
- 2つの仮想マシンワークロードを常に同じホスト上で実行する必要がある場合（仮想マシンどうしのアプリケーション、ワークロードが相補的な場合など）。
- 移行すべきでないワークロードがある場合（ドメインコントローラやデータベースサーバーなど）。
- ホストの保守作業の間、そのホストをプールのネットワークに接続しておく必要がある場合。
- ハードウェアのコストよりもワークロードのパフォーマンスの方が重要な場合。
- 特定のホスト上で優先度の高いワークロード（仮想マシン）を実行し、それらの仮想マシンに高可用性機能の優先度を設定したくない場合。
- プール内のワークロードの実行に不適切なハードウェアを持つホストがある場合。

最適化モードのスケジュールを設定するかどうかに関係なく、最適化モードが変更されても除外サーバーは常に推奨項目の対象から除外されます。このため、ホストの電源が自動的に切断されるのを防ぐためだけの場合は、そのホストに対する電源管理機能を無効にすることを検討します。詳しくは、「電源を自動的に最適化および管理する」を参照してください。

ホストを推奨項目の対象から除外すると、そのホストがワークロードバランスの管理対象外になります。このように設定した場合、このホストに対する推奨項目は生成されなくなります。これに対し、特定のホストが電源管理の対象外であっても、そのホストに対する、電源管理以外の推奨項目が生成されます。

#### 特定のホストをワークロードバランスから除外するには

ワークロードバランスによる電源管理、仮想マシンの配置、ホスト評価、およびプールの最適化に関する推奨項目から特定のホストを除外するには、以下の手順に従います。

1. 「XenCenter の [リソース] ペインで、[XenCenter] > [your-resource-pool](#)」を参照してください。
2. [プロパティ] ペインの [WLB] タブをクリックします。
3. [WLB] タブの [設定] をクリックします。
4. 左側のペインで [除外ホスト] を選択します。

5. [除外ホスト] ページで、ワークロードバランスの推奨項目から除外するホストサーバーを選択します。

#### 推奨項目の自動適用の制御

ワークロードバランスの推奨項目を自動的に適用する機能（自動処理機能）には、いくつかの詳細設定オプションが用意されています。これらのオプションは、[ワークロードバランス設定] ダイアログボックスの [詳細] ページに表示されます。

「XenCenter の [リソース] ペインで、[XenCenter] > [your-resource-pool](#)」を参照してください。

[プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブの [設定] をクリックします。

左側のペインで [詳細] を選択します。

#### 推奨項目の自動適用の積極度

自動モードで実行する場合、最適化と集約化の推奨項目の頻度、およびそれらが自動的に適用されるまでの時間は、以下を含む複数の要因に基づきます：

- 移行後の仮想マシンを次の推奨項目に含めるまでの時間
- 推奨項目を自動的に適用するまでの作成回数（VM 移行間隔）
- 推奨項目を自動適用するときの最低重要度レベル（最適化の重要度）
- 推奨項目を自動適用するときの推奨項目の一貫性レベル（移動する仮想マシンや移動先サーバーとして同じものが推奨されるかどうか）

#### 重要：

通常、上記要素の設定変更は以下の場合にのみ行うようにしてください：

- Citrix テクニカルサポートからの指示がある場合
- ワークロードバランスを有効化した状態でプールの挙動を詳細にテストする場合

これらの設定を誤って構成すると、ワークロードバランスで推奨項目が作成されない場合があります。

#### VM 移行間隔

移行後の仮想マシンについて、ワークロードバランスの最適化推奨項目に含めるまでの時間を分単位で指定できます。

仮想マシンの移行間隔は、人為的な操作（一時的な高負荷時など）が原因で推奨項目が生成されるのを防ぐために設定します。

ワークロードバランスの自動処理機能を有効にした場合は、仮想マシンの移行間隔を特に慎重に決定する必要があります。継続的および反復的に負荷が増加する環境で頻度を増やす（小さい値を設定する）と、多くの推奨項目が生成され、仮想マシンの再配置が頻繁に発生します。

注:

この設定は、前回と同じホストを仮想マシンの起動または再開先ホスト、および保守モードの推奨項目に含むかどうかの決定には影響しません。

### 推奨項目の回数

ワークロードバランスでは、そのリソースプールで推奨項目の生成が必要かどうかを2分ごとにチェックされます。ワークロードバランスの自動処理機能では、推奨項目をいくつ生成したら自動的に適用するかを指定できます。これを行うには、[推奨項目の回数]を設定します。[推奨項目の回数]と[最適化の積極度]の設定により、推奨項目をどのように自動適用するかを微調整できます。

上記の「推奨項目の自動適用の積極度」で説明したように、ワークロードバランスでは、推奨項目の類似性に基づいて以下のチェックを行います:

1. 推奨項目が必要かどうか
2. 仮想マシンの移行先ホストのパフォーマンスが長時間安定しているかどうか（移行先ホストが安定していないと仮想マシンの再移行が必要になるため）

[推奨項目の回数]では、推奨項目を自動適用するまでの作成回数を指定します。同じ推奨項目の生成がこの回数に達すると、その推奨項目が自動的に適用されます。

この設定は、以下のように使用されます:

1. 推奨項目の回数は、[最適化の積極度]で指定した一貫性要件を満たす推奨項目が生成されるたびに増加します。一貫性要件を満たさない推奨項目が生成されると、(最適化の積極度で説明されている要因によっては)推奨項目の回数が0にリセットされます。
2. 一貫性要件を満たす推奨項目の生成数(連続推奨数)が[推奨項目の回数]の値に達すると、その推奨項目が自動的に適用されます。

この設定を変更する場合は、その環境に最適な値を決定する必要があります。以下のシナリオを検討してください:

- ホストの負荷およびアクティビティが極端に急増する環境では、[推奨項目の回数]の値を大きくします。推奨項目の生成が必要かどうかは、2分ごとにチェックされます。推奨項目を適用するまでの作成回数として**3**を設定すると、6分後に推奨項目が自動適用されます。
- ホストの負荷およびアクティビティが段階的に増加する環境では、[推奨項目の回数]の値を小さくします。

推奨項目を適用すると仮想マシンの再配置処理が発生し、システムリソースに負担がかかってパフォーマンスが影響を受けます。[推奨項目の回数]の値を大きくすると、推奨項目が自動適用されるまでに、同様の推奨項目が多く生成されることになります。つまり、より慎重で一貫した推奨項目だけが適用され、仮想マシンが不適切に移行される可能性が低くなります。デフォルトでは、このような値が設定されています。

この値の変更は運用環境への影響が大きいため、変更する場合は必ず細心の注意を払ってください。変更する場合は、ワークロードバランスの動作について詳細にテストするか、Citrix テクニカルサポート担当者からの指示に従ってください。

### 最適化の重要度

すべての最適化推奨項目には、推奨項目の重要性を示す重要度（重大、高、中、低）が含まれています。この重要度レベルは、以下の要素を組み合わせで決定されます：

- 設定されているオプション（パフォーマンスしきい値や重要度など）
- ワークロードで使用可能なリソース
- リソース使用履歴データ

推奨項目の重要度レベルは、[WLB] タブの [最適化の推奨項目] の一覧に表示されます。

ワークロードバランスの推奨項目が自動的に適用されるように設定した場合、指定した最低重要度レベルを満たす推奨項目だけが適用されます。

### 最適化の積極度

自動モードで動作するワークロードバランスでは、推奨項目の一貫性を判断するためのいくつかの基準が使用されます。これは、一時的または異常な負荷の増加により仮想マシンの移行が行われなくするためのものです。自動モードでは、最初に生成された推奨項目は自動適用されません。ホストや仮想マシンでその動作が継続的に発生することが検出されるまで、自動適用は行われません。つまり、同じホストや仮想マシンが原因で推奨項目が生成される場合、その推奨項目は一貫していると判断されます。

ワークロードバランスでは、一貫性を判断するための条件と、同じ推奨項目をいくつ生成したかにより、その環境の動作の一貫性が決定されます。一貫性をどれだけ厳密に評価するかを制御するには、[最適化の積極度] を設定します。

この [最適化の積極度] 設計は、主にデモ用として設計したのですが、このオプションにより運用環境の安定性を制御することができます。デフォルトでは、積極度が低く設定されています。積極度を高くすると、推奨項目の類似性を評価するときの厳密度が低くなり、運用環境の安定性が低下します。多くの場合、高い積極度は適切ではありません。このため、デフォルトでは [低] が設定されています。

ワークロードバランスは、最大で 4 つの条件を使用して推奨項目の一貫性を判断します。使用される条件の数は、[最適化の積極度] で設定されている積極度レベルにより異なります。積極度レベルが [低] または [中] の場合、推奨項目は積極的には自動適用されません。つまり、積極度レベルが低いと最適化条件が厳密に評価され、それらに合致しないと自動適用は行われません。

たとえば、積極度レベルとして [低] を設定すると、このレベルの条件に合致する推奨項目の数が [推奨項目の回数] の値に達するまで、その推奨項目は自動適用されません。

[推奨項目の回数] に「3」を設定した場合、低レベル用のすべての条件に合致する推奨項目が連続して 3 回生成されたときに、その推奨項目が自動適用されます。この設定により、長時間安定して動作している最適なホストに仮想マシンが移行されるようになり、移行先ホストのパフォーマンスの低下によりその仮想マシンが再移行されるという可能性が低くなります。デフォルトでは、積極度レベルとして [低] が設定されています。

[最適化の積極度] を高くしてホストの最適化頻度を上げることは推奨していません。サーバーの最適化がより高速または頻繁に行われるようにするには、パフォーマンスしきい値の調整を検討します。この調整では、プールヘルスレポートを参考にしてください。

各種極度レベルでは、以下の条件を評価して推奨項目の一貫性が判断されます。

低:

- 後続の推奨項目に含まれる仮想マシン (UUID) が、直前の推奨項目とすべて同じである。
- 後続の推奨項目で、移行先ホストがすべて同じである。
- 最初の推奨項目とその直後の推奨項目が同じである (異なる場合、連続推奨数が1にリセットされる)。

中:

- 後続の推奨項目に含まれるすべての仮想マシンが、直前の推奨項目と同じホスト上で動作している。ただし、最初の推奨項目と異なる仮想マシンであっても構わない。
- 後続の推奨項目で、移行先ホストがすべて同じである。
- 最初の推奨項目と後続の2つの推奨項目のいずれかが同じである (異なる場合、連続推奨数が1にリセットされる)。

高:

- 推奨項目に含まれるすべての仮想マシンが同じホスト上で動作している。ただし、各推奨項目の仮想マシンが互いに異なっても構わない。
- 仮想マシンの移動元ホストが、各推奨項目で同じである。
- 最初の推奨項目の後続の2つの推奨項目が異なっても、連続推奨数は1にリセットされない。

例

ここでは、[最適化の積極度] と [推奨項目の回数] の設定が、推奨項目の自動適用にどのように影響するかについて例を挙げて説明します。

次の表で、最初の列は推奨項目の生成順を示します。「推奨項目」の列は、ワークロードバランスにより生成される推奨項目の内容 (移行する仮想マシンと移行先ホスト) です。各推奨項目で、ホスト A 上の3つの仮想マシンの移行が推奨されています。右側の3つの列では、[最適化の積極度] の設定 (高、中、低) により、推奨項目の回数 (連続推奨数) がどのように増分されるかを示しています。各行のグループには、「推奨項目 #1」のように番号が付けられます。これらの列の番号は、その積極度レベルでの連続推奨数です。たとえば、「推奨項目 #2」行「積極度: 中」列の「1」は、推奨項目 #1 と推奨項目 #2 の一貫性が十分でないことを示しています。このため、連続推奨数が1にリセットされています。

この表から、[最適化の積極度] で [高] を設定した場合、推奨項目 #1、#2、および #3 の連続推奨数が増分されることがわかります。この増分は、各推奨項目の内容が異なっている (異なる仮想マシンやホストが推奨されている) 場合にも行われます。この場合、推奨項目 #3 が生成されたときに、[推奨項目の回数] で設定されている連続推奨数「3」に達しています。つまり、ホスト A について一貫した推奨項目が連続して3回生成されたとみなされ、推奨項目 #3 が自動適用されます。

これに対し、[最適化の積極度] で [低] を設定した場合、最初の4つの推奨項目 (#1 ~ #4) で連続推奨数が増分されていません。これらの推奨項目に含まれている仮想マシンおよび移行先ホストが異なるため、連続推奨数は1にリ

セットされます。この積極度レベルでは、推奨項目 #4 とまったく同じ内容の推奨項目 #5 が生成されるまで連続推奨数が増分されません。さらに、まったく同じ内容の推奨項目 #6 で連続推奨数が「3」に達するため、この推奨項目が自動適用されます。

**推奨項目 #1:**

- VM1 をホスト A からホスト B に移動
- VM3 をホスト A からホスト B に移動
- VM5 をホスト A からホスト C に移動

積極度: 高、推奨項目の回数: 1

積極度: 中、推奨項目の回数: 1

積極度: 低、推奨項目の回数: 1

**推奨項目 #2:**

- VM1 をホスト A からホスト B に移動
- VM3 をホスト A からホスト C に移動
- VM7 をホスト A からホスト C に移動

積極度: 高、推奨項目の回数: 2

積極度: 中、推奨項目の回数: 1

積極度: 低、推奨項目の回数: 1

**推奨項目 #3:**

- VM1 をホスト A からホスト B に移動
- VM3 をホスト A からホスト C に移動
- VM5 をホスト A からホスト C に移動

積極度: 高、推奨項目の回数: 3 (適用)

積極度: 中、推奨項目の回数: 1

積極度: 低、推奨項目の回数: 1

**推奨項目 #4:**

- VM1 をホスト A からホスト B に移動
- VM3 をホスト A からホスト B に移動
- VM5 をホスト A からホスト C に移動

積極度: 高、推奨項目の回数: 2

積極度: 低、推奨項目の回数: 1

**推奨項目 #5:**

- VM1 をホスト A からホスト B に移動

- VM3 をホスト A からホスト B に移動
- VM5 をホスト A からホスト C に移動

積極度：中、推奨項目の回数：3（適用）

積極度：低、推奨項目の回数：2

推奨項目 #6:

- VM1 をホスト A からホスト B に移動
- VM3 をホスト A からホスト B に移動
- VM5 をホスト A からホスト C に移動

積極度：低、推奨項目の回数：3（適用）

最適化推奨項目の間隔を設定するには

1. 「XenCenter の [リソース] ペインで、[XenCenter] >your-pool」を参照してください。
2. [プロパティ] ペインの [WLB] タブをクリックします。
3. [WLB] タブの [設定] をクリックします。
4. ダイアログボックス左側の [詳細] をクリックします。
5. [VM 最適化間隔] セクションで、以下の設定を行います：
  - [分] ボックスに、移行後の仮想マシンを最適化推奨項目に含めるまでの時間を分単位で指定します。
  - [回] ボックスに、最適化推奨項目が自動的に適用されるまでの作成回数を指定します。
  - [最適化の重要度] で、最適化推奨項目の最低重要度レベルを指定します。このレベルに達すると、推奨項目が自動的に適用されます。
  - [最適化の積極度] で、最適化推奨項目をどれだけ積極的に自動適用するかを指定します。自動適用の積極度を高くすると、自動適用される推奨項目の一貫性（対象の仮想マシンや再配置先ホストなどの一貫性）が低下します。最適化の積極度の設定により、推奨項目の回数（つまり [回] ボックス）が直接入力されます。

注:

[回] に「1」と入力した場合、[最適化の積極度] は無視されます。

プール監査記録レポートのデータ量設定を変更するには

以下の手順に従って、データ量設定を変更します。

1. [インフラストラクチャ] ビューでプールを選択して [WLB] タブをクリックし、[設定] をクリックします。
2. ダイアログボックス左側の [詳細] をクリックします。
3. [詳細] ページの [プール監査記録レポートのデータ量] の一覧から、データ量のオプションを選択します。

**重要:**

レポートに必要な情報の詳細度に適したオプションを選択してください。たとえば、[最小] に設定すると、特定のユーザーおよびオブジェクトの種類についての限定された量のデータのみが収集されます。[中] に設定すると、監査ログレポートがユーザーにとって読みやすい程度の量になります。[最大] に設定すると、監査ログの詳細なレポートが生成されます。ただし、これによりワークロードバランスサーバーでより多くのディスク領域およびメモリが消費される点に注意してください。

4. [OK] をクリックして変更を適用します。

## XenCenter のオブジェクトに基づいたプール監査記録レポートを表示するには

次の手順で、選択したオブジェクトに基づいたプール監査記録のレポートを実行して表示します。

1. [プール監査記録レポートのデータ量] 設定を設定した後、[レポート] をクリックします。[ワークロードレポート] ページが開きます。
2. 左側のペインで [プール監査記録] を選択します。
3. [オブジェクト] リストから特定のオブジェクトを選択して、対象オブジェクトに基づいたレポートを実行して表示します。たとえば、リストから [ホスト] を選択して、ホストのみのレポートを取得します。

## ワークロードバランスの管理

このセクションでは、次の内容について説明します：

- ワークロードバランス仮想アプライアンスの変更
- ワークロードバランス仮想アプライアンスからの切断とワークロードバランスの一時停止
- データベースのグルーミング
- 設定オプションの変更

**注:**

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

## ワークロードバランスの管理と保守

ワークロードバランス機能をしばらく実行すると、その効果を最適に保つための保守・管理タスクが必要になる場合があります。たとえば、環境に変更があった場合 (IP アドレスや資格情報の変更など)、ハードウェアをアップグレードした場合、および日常的な保守作業の結果これらのタスクが必要になります。

ワークロードバランスでは、以下の管理タスクが必要になることもあります。

- ワークロードバランス仮想アプライアンスへの接続または再接続
- プールで使用するワークロードバランス仮想アプライアンスの変更
- ワークロードバランスユーザーアカウントの変更
- ワークロードバランス仮想アプライアンスの切断
- ワークロードバランス仮想アプライアンスの削除
- 役割ベースのアクセス制御（RBAC）の実装

ワークロードバランスの一部の動作は、設定ファイル `wlb.conf` を使用して変更できます。

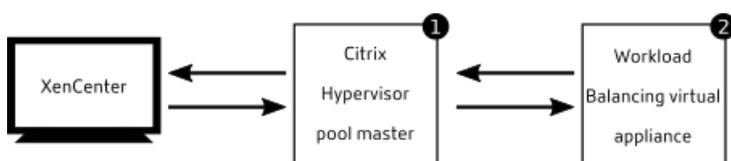
以降のセクションでは、ワークロードバランスデータベースを管理する方法についても説明します。

#### ワークロードバランス仮想アプライアンスへの接続

ワークロードバランス仮想アプライアンスの設定が完了したら、管理対象のリソースプールをワークロードバランス仮想アプライアンスに接続します。これを行うには、コマンドラインインターフェイス（Command Line Interface: CLI）または XenCenter を使用します。同様に、ある時点で同じ仮想アプライアンスに再接続する必要がある場合があります。

XenCenter でワークロードバランス仮想アプライアンスに接続するには、以下の情報が必要です。

- ワークロードバランス仮想アプライアンスのホスト名（または IP アドレス）とポート番号。
- リソースプールにアクセスするための資格情報。
- ワークロードバランス仮想アプライアンス上で作成したアカウントの情報。このアカウントはワークロードバランスユーザーアカウントとも呼ばれます。Citrix Hypervisor はこのアカウントをワークロードバランスとの通信に使用します。（このアカウントは、ワークロードバランス仮想アプライアンスの設定時に作成します）。



ワークロードバランス仮想アプライアンスのホスト名を指定する場合は、事前に仮想アプライアンスのホスト名および IP アドレスを DNS サーバーに追加しておきます。

証明機関から入手した証明書を使用する場合は、有効期限のない IP アドレスまたは FQDN を使用することをお勧めします。

ワークロードバランスに接続した直後では、デフォルトのしきい値および設定に基づいてワークロードが最適化されます。自動最適化モード、電源管理、および自動処理などの自動化機能は、デフォルトでは無効になっています。

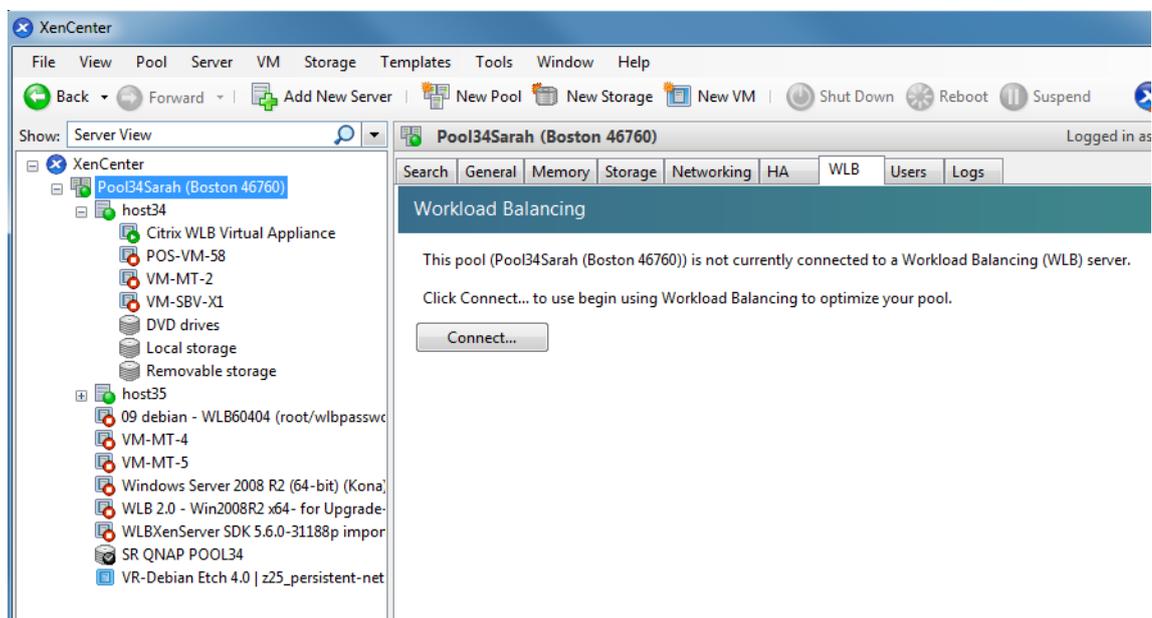
注:

ワークロードバランス機能は、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

リソースプールをワークロードバランス仮想アプライアンスに接続するには

1. 「XenCenter の [リソース] ペインで、[XenCenter] > `your-resource-pool`」を参照してください。
2. [プロパティ] ペインの [WLB] タブをクリックします。

[WLB] タブに [接続] ボタンが表示されます。



3. [WLB] タブの [接続] をクリックします。

[WLB サーバーへの接続] ダイアログボックスが表示されます。

**Connect to WLB Server**

Server Address  
Enter the address of the Workload Balancing server this Citrix Hypervisor resource pool will use.

Address:

Port:  (Default is 8012)

WLB Server Credentials  
Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:

Citrix Hypervisor Credentials  
Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials

OK Cancel

4. [サーバーのアドレス] セクションで、以下の情報を入力します：

- a) [アドレス] ボックスに、ワークロードバランス仮想アプライアンスの IP アドレスまたは FQDN (your-WLB-appliance-computername.yourdomain.netなど) を入力します。

ヒント：

詳しくは、「ワークロードバランス仮想アプライアンスの IP アドレスを調べるには」を参照してください。

- b) [ポート] ボックスにポート番号を入力します。このポートを使用して、Citrix Hypervisor がワークロードバランスと通信します

デフォルトでは、Citrix Hypervisor はワークロードバランスサーバー（この場合は Web Service Host サービス）にポート 8012 で接続します。ワークロードバランス仮想アプライアンスの設定時にポートを変更した場合は、そのポート番号を入力します。

注：

ワークロードバランス仮想アプライアンスの設定時にポート番号を変更した場合のみ、ここでポート番号を変更してください。[WLB サーバーへの接続] ダイアログボックスで指定するポート番号は、ワークロードバランス仮想アプライアンスの設定時に指定したもの（およびファイアウォール規則で指定したもの）と一致する必要があります。

5. [WLB サーバーの資格情報] で、ユーザー名 (wlbuserなど) とパスワードを入力します。これらの情報は、リソースプールがワークロードバランス仮想アプライアンスに接続するときに使用されます。

Update Credentials

**WLB Server Credentials**

Enter the credentials Citrix Hypervisor will use to connect to the Workload Balancing server.

Username:

Password:



これらの資格情報は、ワークロードバランス仮想アプライアンスの設定時に作成したものである必要があります。デフォルトのユーザー名は、`wlbuser`です。

6. [Citrix Hypervisor の資格情報] セクションで、プールにアクセスするためのユーザー名とパスワードを入力します。ワークロードバランスは、この情報を使用してリソースプールの Citrix Hypervisor サーバーに接続します。

**Citrix Hypervisor Credentials**

Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor.

Username:

Password:

Use the current XenCenter credentials



現在ログイン中の Citrix Hypervisor と同じ資格情報を使用するには、[現在の XenCenter の資格情報を使用する] チェックボックスをオンにします。役割ベースのアクセス制御 (RBAC) で役割を割り当てたアカウントを使用する場合は、そのアカウントにワークロードバランス機能の管理許可が付与されていることを確認してください。詳しくは、「役割ベースのアクセス制御とワークロードバランス」を参照してください。

7. プールをワークロードバランス仮想アプライアンスに接続すると、デフォルトの最適化設定でプールの監視が開始されます。ワークロードバランス仮想アプライアンスへの接続直後に最適化設定やリソースの優先度を変更する場合は、60 秒以上 (XenCenter のログに検出の完了が示されます) 待機する必要があります。詳しくは、「ワークロードバランス設定の変更」を参照してください。

ワークロードバランス仮想アプライアンスの **IP** アドレスを調べるには

1. XenCenter の [リソース] ペインでワークロードバランス仮想アプライアンスを選択して、[コンソール] タブをクリックします。
2. 仮想アプライアンスにログインします。これを行うには、仮想アプライアンスのインポート時に作成したアカウント (`root`) とパスワードを使用します。
3. 次のコマンドを実行します。

```
1 ifconfig
```

## 役割ベースのアクセス制御とワークロードバランス

環境に役割ベースのアクセス制御（RBAC）が実装されている場合、すべてのユーザーロールに [WLB] タブを表示できます。ただし、実行可能なタスクは、管理者の役割によって異なります。次の表は、ワークロードバランス機能の各タスクを実行するために必要な役割を示しています。\*\*

| タスク                               | 必要な役割     |
|-----------------------------------|-----------|
| WLB の構成、初期化、有効化、および無効化            | プールオペレーター |
| ワークロードバランス最適化推奨項目の適用（[WLB] タブで）   | プールオペレーター |
| WLB レポートサブスクリプションの変更              | プールオペレーター |
| ワークロードバランス配置推奨項目の承諾（「星」付きの推奨）     | VM パワー管理者 |
| ワークロードバランスレポート（プール監査記録レポートを含む）の生成 | 読み取り専用    |
| WLB 構成の表示                         | 読み取り専用    |

## アクセス権の定義

各アクセス権の内容は以下のとおりです。

| 権限                                | 許可されるタスク                                                 |
|-----------------------------------|----------------------------------------------------------|
| WLB の構成、初期化、有効化、および無効化            | WLB の構成<br>WLB の初期化と WLB サーバーの変更<br>WLB の有効化<br>WLB の無効化 |
| ワークロードバランス最適化推奨項目の適用（[WLB] タブで）   | [WLB] タブに表示されるすべての最適化推奨項目の適用                             |
| WLB レポートサブスクリプションの変更              | 生成する WLB レポートおよびその送信先の変更                                 |
| ワークロードバランス配置推奨項目の承諾（「星」付きの推奨）     | ワークロードの配置先として（「星」で）提示された推奨サーバーからの選択                      |
| ワークロードバランスレポート（プール監査記録レポートを含む）の生成 | プール監査記録レポートを含む WLB レポートの表示および実行                          |
| WLB 構成の表示                         | [WLB] タブに表示されるプールの WLB 設定の表示                             |

必要な役割レベルが付与されていない管理者がワークロードバランスタスクを実行しようとする、昇格用のダイアログボックスが開きます。役割ベースのアクセス制御については、「[役割ベースのアクセス制御](#)」を参照してください。

#### ワークロードバランス仮想アプライアンスの状態の確認

ワークロードバランス仮想アプライアンスの状態を確認するには、`service workloadbalancing status` コマンドを使用します。詳しくは、ワークロードバランスコマンドを参照してください。

#### プールで使用するワークロードバランス仮想アプライアンスの変更

必要な場合は、リソースプールのワークロードバランス仮想アプライアンスを変更できます。

この場合、変更後も古いワークロードバランス仮想アプライアンスによりプールのデータが収集されるのを防ぐため、事前に古い仮想アプライアンスを切断しておく必要があります。

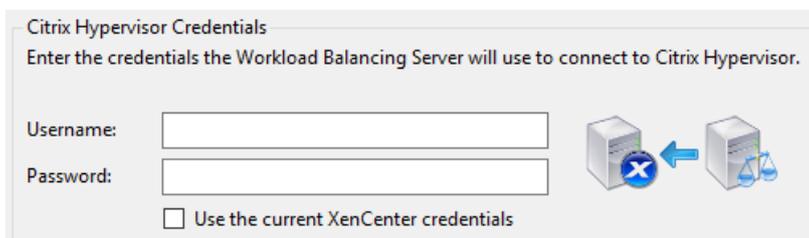
プールで古いワークロードバランス仮想アプライアンスを切断したら、新しいワークロードバランス仮想アプライアンスの名前を指定して接続します。これを行うには、以下の手順に従います。

使用するワークロードバランス仮想アプライアンスを変更するには：

1. [プール] メニューの [ワークロードバランスサーバーの切断] を選択し、確認メッセージが表示されたら [切断] をクリックします。
2. [WLB] タブの [接続] をクリックします。[WLB サーバーへの接続] ダイアログボックスが表示されます。
3. [アドレス] ボックスに、新しいワークロードバランスサーバーの IP アドレスまたは FQDN を入力します。
4. [WLB サーバーの資格情報] セクションで、Citrix Hypervisor のリソースプール（プールマスタ）がワークロードバランス仮想アプライアンスに接続するときに使用するユーザー名およびパスワードを入力します。

これらの資格情報は、このワークロードバランス仮想アプライアンスの設定時に作成したものである必要があります。デフォルトのユーザー名は、`wlbuser`です。

5. [Citrix Hypervisor の資格情報] セクションで、リソースプールにアクセスするためのユーザー名とパスワード（通常はプールマスターのパスワード）を入力します。これらの情報は、ワークロードバランス仮想アプライアンスがプールの各ホストに接続するときに使用されます。



The image shows a dialog box titled "Citrix Hypervisor Credentials". The text inside reads: "Enter the credentials the Workload Balancing Server will use to connect to Citrix Hypervisor." There are two input fields: "Username:" and "Password:". Below the password field is a checkbox labeled "Use the current XenCenter credentials". To the right of the input fields is an icon showing two server racks with a blue arrow pointing from the left one to the right one, and a blue 'X' over the left server rack.

現在ログイン中の Citrix Hypervisor と同じ資格情報を使用するには、[現在の XenCenter の資格情報を使用する] チェックボックスをオンにします。役割ベースのアクセス制御 (Roll Based Access Control:

RBAC) で役割を割り当てたアカウントを使用する場合は、そのアカウントにワークロードバランス機能の管理許可が付与されていることを確認してください。詳しくは、「役割ベースのアクセス制御とワークロードバランス」を参照してください。

#### ワークロードバランスの資格情報の変更

Citrix Hypervisor とワークロードバランス仮想アプライアンス間の通信で使用される資格情報を変更するには、以下のプロセスを実行します：

1. [WLB] タブで [一時停止] をクリックして、ワークロードバランス機能を一時停止します。
2. `wlbconfig` コマンドを使用して、ワークロードバランスの資格情報を変更します。詳しくは、「ワークロードバランスコマンド」を参照してください。
3. ワークロードバランスを再有効化して、新しい資格情報を指定します。
4. 進行状況バーが完了したら、[接続] をクリックします。  
[WLB サーバーへの接続] ダイアログボックスが表示されます。
5. [資格情報を変更する] をクリックします。
6. [サーバーアドレス] セクションで、必要に応じて次の内容を変更します。
  - [アドレス] ボックスに、ワークロードバランス仮想アプライアンスの IP アドレスまたは FQDN を入力します。
  - (オプション) ワークロードバランス仮想アプライアンスの設定時にポートを変更した場合は、そのポート番号を入力します。このポートにより、Citrix Hypervisor とワークロードバランスが通信します。

Citrix Hypervisor のデフォルトでは、ポート 8012 が指定されています。

#### 注：

この値を変更するのは、ワークロードバランスの設定ウィザードで別のポート番号を指定した場合のみとしてください。[WLB サーバーへの接続] ダイアログボックスで指定するポート番号は、ワークロードバランスのインストールウィザードで指定したポート番号と同じである必要があります。

7. [WLB サーバーの資格情報] で、ワークロードバランスサーバーに接続するときに Citrix Hypervisor で使用するユーザー名 (`wlbuser` など) およびパスワードを入力します。
8. [Citrix Hypervisor の資格情報] セクションで、リソースプールにアクセスするためのユーザー名とパスワード (通常はプールマスターのパスワード) を入力します。ワークロードバランスは、この情報を使用して Citrix Hypervisor のリソースプールのサーバーに接続します。
9. [Citrix Hypervisor の資格情報] セクションで、プールにアクセスするためのユーザー名とパスワードを入力します。ワークロードバランスは、この情報を使用して Citrix Hypervisor のリソースプールのサーバーに接続します。

現在ログイン中の Citrix Hypervisor と同じ資格情報を使用するには、[現在の XenCenter の資格情報を使用する] チェックボックスをオンにします。

### ワークロードバランスの IP アドレスの変更

ワークロードバランスの IP アドレスを変更するには、以下の手順に従います。

1. ワークロードバランスサービスを停止します。これを行うには、ワークロードバランス仮想アプライアンス上で `service workloadbalancing stop` コマンドを実行します。
2. ワークロードバランスの IP アドレスを変更します。これを行うには、仮想アプライアンス上で `ifconfig` コマンドを実行します。
3. ワークロードバランスを有効にして、新しい IP アドレスを指定します。
4. ワークロードバランスサービスを起動します。これを行うには、ワークロードバランス仮想アプライアンス上で `service workloadbalancing start` コマンドを実行します。

### ワークロードバランスの停止

ワークロードバランスはプールレベルで設定されるため、プールの管理を停止する場合は、次のいずれかを実行する必要があります：

- ワークロードバランスを一時停止する：ワークロードバランス機能を一時停止すると、そのプールに対する推奨項目が XenCenter に表示されなくなります。ワークロードバランス機能を短期間停止して、再度設定することなくプールの管理を再開させる場合は、ワークロードバランスを一時停止します。ワークロードバランスを一時停止すると、再開するまでそのプールからのデータ収集が停止します。
- プールをワークロードバランス仮想アプライアンスから切断する：プールをワークロードバランス仮想アプライアンスから切断すると、可能な場合、ワークロードバランスデータベースからそのプールに関するデータが削除されます。さらに、これによりそのプールからのデータ収集が停止します。

1. XenCenter の [リソース] ペインで、ワークロードバランス機能を無効化するリソースプールを選択します。
2. [WLB] タブで [一時停止] をクリックします。ワークロードバランスが一時停止状態であることを示すメッセージが [WLB] タブに表示されます。

ヒント：

監視を再開するには、[WLB] タブの [再開] ボタンをクリックします。

3. XenCenter の [インフラストラクチャ] ペインで、ワークロードバランス機能を停止するリソースプールを選択します。
4. [インフラストラクチャ] メニューの [ワークロードバランスサーバーの切断] を選択します。[ワークロードバランスサーバーの切断] ダイアログボックスが開きます。
5. [切断] をクリックします。これにより、ワークロードバランスによるプールの監視が完全に停止します。

ヒント：

ワークロードバランス仮想アプライアンスから切断した後でこの機能を再度有効にするには、ワークロードバランス仮想アプライアンスに再接続する必要があります。詳しくは、ワークロードバランス仮想アプライアンス

スへの接続を参照してください。

### ワークロードバランスが有効なときの保守モード

ワークロードバランスが有効なリソースプールでは、物理ホストを保守モードに切り替えると、Citrix Hypervisorはそのホスト上で実行されているすべての仮想マシンを自動的にほかの適切なホストに移行します。Citrix Hypervisorは、仮想マシンの移行先ホストを、ワークロードバランスが最適化モードとパフォーマンスしきい値の設定、およびパフォーマンス測定値に基づいて計算した推奨項目により決定します。

移行先ホストが使用できない状態である場合は、[保守モードへの切り替え] ダイアログボックスに「ここをクリックして VM を一時停止します」というメッセージが表示されます。この場合、十分なリソースを持つホストがないため、ワークロードバランスでは推奨再配置先が提示されません。管理者は、仮想マシンを一時停止するか、保守モードを終了してほかのホスト上のワークロードを軽減する（仮想マシンを一時停止するなど）などの処置を行います。次に、[保守モードへの切り替え] ダイアログボックスを再度入力すると、ワークロードバランスは、移行に適したホスト候補を一覧表示できる場合があります。

#### 注:

ワークロードバランスが有効なリソースプールでホストを保守モードにすると、[保守モードへの切り替え] ウィザードに「ワークロードバランスが有効」と表示されます。

ワークロードバランスが有効なときに保守モードに切り替えるには:

1. XenCenter の [リソース] ペインで、オフラインにする物理ホストを選択します。[サーバー] メニューの [保守モードへの切り替え] を選択します。
2. [保守モードへの切り替え] ダイアログボックスで、[保守モードへの切り替え] をクリックします。これにより、そのホスト上で実行中のすべての仮想マシンが、最適化モードとパフォーマンスしきい値の設定、およびパフォーマンス測定値に基づいて決定される最適なホストに自動的に移行されます。

ホストを保守モードから切り替えるには、目的のホストを右クリックして、[保守モードからの切り替え] を選択します。これにより、Citrix Hypervisor はそのホストで実行されていたすべての仮想マシンを自動的に復元します。

### ワークロードバランス仮想アプライアンスのディスクサイズの変更

ここでは、ワークロードバランス仮想アプライアンスの仮想ディスクのサイズを変更する方法について説明します。以下の手順を行うには、まずワークロードバランス仮想アプライアンスをシャットダウンしてください。この間、ワークロードバランス機能は停止します。

#### 警告:

この手順を行う前に、仮想アプライアンスのスナップショットを作成しておくことをお勧めします。これらの手順を誤って実行すると、ワークロードバランス仮想アプライアンスが破損する可能性があります。

1. ワークロードバランス仮想アプライアンスをシャットダウンします。

XenCenter の [リソース] ペインで、ワークロードバランス仮想アプライアンスを選択します。

2. [ストレージ] タブをクリックします。
3. 一覧で [vdi\_xvda] ディスクを選択し、[プロパティ] をクリックします。
4. [vdi\_xvda プロパティ] ダイアログボックスで [サイズと場所] を選択します。
5. サイズを変更して、[OK] をクリックします。
6. ワークロードバランス仮想アプライアンスを起動して、ログインします。
7. ワークロードバランス仮想アプライアンス上で、次のコマンドを実行します。

```
1 resize2fs /dev/xvda
```

注:

resize2fsツールがインストールされていない場合は、インターネット接続を確認してから、次のコマンドを使用してインストールしてください:

```
yum install -y --enablerepo=base,updates --disablerepo=citrix-*
e2fsprogs
```

インターネットに接続できない場合。

1. [https://centos.pkgs.org/7/centos-x86\\_64/](https://centos.pkgs.org/7/centos-x86_64/)からダウンロードします。
  - libss-1.42.9-7.el7.i686.rpm
  - e2fsprogs-libs-1.42.9-7.el7.x86\_64.rpm
  - e2fsprogs-1.42.9-7.el7.x86\_64.rpm
2. SCP または適切なツールで、WLB 仮想マシンにこれらをアップロードします。
3. WLB 仮想マシンで次のコマンドを実行します。

```
1 rpm -ivh libss-*.rpm e2fsprogs-*.rpm
```

これで、resize2fsツールがインストールされました。

4. df -hコマンドを実行して、ディスクサイズが変更されたことを確認します。

#### ワークロードバランス仮想アプライアンスの削除

ワークロードバランス仮想アプライアンスを削除する場合、XenCenter で仮想マシンを削除するときと同じ方法を使用することをお勧めします。

ワークロードバランス仮想アプライアンスを削除すると、ワークロードバランスデータベース (PostgreSQL データベース) も削除されます。このデータを保存する場合は、ワークロードバランス仮想アプライアンスを削除する前にデータベースを移行しておく必要があります。

### ワークロードバランスデータベースの管理

ワークロードバランスデータベースは PostgreSQL データベースです。PostgreSQL は、オープンソースのリレーショナルデータベースの 1 つです。PostgreSQL に関するドキュメントは、インターネット上を検索して入手できます。

以下の手順は、データベース管理者およびデータベース管理タスクを理解している PostgreSQL ユーザーを対象にしています。PostgreSQL について詳しくない場合、このデータベースソフトウェアについて理解してから以下の手順を実行することをお勧めします。

デフォルトの PostgreSQL ユーザー名は `postgres` です。このアカウントのパスワードは、ワークロードバランス仮想アプライアンスの設定時に指定したものです。

保持できる履歴データの量は、ワークロードバランスに割り当てられている仮想ディスクのサイズ（と、必要な最小ディスク容量により決定されます。デフォルトで割り当てられている仮想ディスクのサイズは 20GB です。詳しくは、「データベースグルーミングのパラメータ」を参照してください。

保持される履歴データを増やす（たとえば、プール監査記録レポートを有効にする場合）には、以下のいずれかを行います：

- ワークロードバランス仮想アプライアンスに割り当てられている仮想ディスクのサイズを増やします。これを行うには、仮想アプライアンスをインポートした後で、ワークロードバランスのディスクサイズの変更で説明されている手順に従います。
- データベースへのリモートクライアントアクセスを有効にして、サードパーティ製データベース管理ツールを使用してデータの複製バックアップコピーが定期的に作成されるように設定します。

また、データベースのグルーミングを設定して、データにより消費されるディスク領域を制御することもできます。

### データベースへのアクセス

ワークロードバランス仮想アプライアンスでは、ファイアウォールが設定されています。このため、データベースにアクセスできるようにするには、`postgresql` サーバポートを `iptables` に追加する必要があります。

ワークロードバランス仮想アプライアンスのコンソールで、次のコマンドを実行します。

```
1 iptables -A INPUT -i eth0 -p tcp -m tcp --dport 5432 -m \
2 state --state NEW,ESTABLISHED -j ACCEPT
```

(任意) 仮想アプライアンスを再起動してもこの設定が適用されるようにするには、次のコマンドを実行します：

```
1 iptables-save > /etc/sysconfig/potables
```

### データベースグルーミングの制御

ワークロードバランスデータベースでは、ワークロードバランスの動作に必要な空きディスク容量が足りなくなると、古いものからデータが自動的に削除されます。ワークロードバランスに必要な空き容量（最小ディスク容量）は、デフォルトで 1,024MB に設定されています。

wlb.conf ファイルを編集することで、ワークロードバランスデータベースのグルーミングをカスタマイズできます。

ワークロードバランス仮想アプライアンスの仮想ディスクに十分な空き容量がなくなると、履歴データのグルーミングが自動的に実行されます。このときのプロセスは、以下のとおりです：

1. 事前に定義されたグルーミング間隔で、グルーミングが必要かどうかワークロードバランスデータコレクターによりチェックされます。データベースデータの増大により、ディスクの空き容量がワークロードバランスの最小ディスク容量より少なくなると、グルーミングが必要になります。最小ディスク容量は、`GroomingRequiredMinimumDiskSizeInMB`により設定します。

グルーミング間隔は、`GroomingIntervalInHour`で変更できます。デフォルトでは、1時間ごとに空き容量がチェックされます。

2. グルーミングが必要になると、最も古い日付（デフォルトで1日分、`GroomingDBDataTrimDays`パラメータで設定）のデータが削除されます。削除後、ワークロードバランスの動作に必要な最小ディスク容量が確保されたかどうかチェックされます。
3. 最初のグルーミングで最小ディスク容量が確保されない場合、`GroomingIntervalInHour`のグルーミング間隔を待たずに`GroomingRetryCounter`で指定された回数までグルーミングが繰り返されます。
4. 最初のグルーミングで十分なディスク容量が確保された場合は、`GroomingIntervalInHour`で指定されたグルーミング間隔の後、手順1.に戻ります。
5. `GroomingRetryCounter`で指定された回数のグルーミングで十分なディスク容量が確保されなくても、`GroomingIntervalInHour`で指定されたグルーミング間隔の後、手順1.に戻ります。

#### データベースグルーミングのパラメータ

wlb.confファイルには、データベースのグルーミングを制御するための、以下に示す5つのパラメータがあります。

- 「`GroomingIntervalInHour`」を参照してください。グルーミングが必要かどうかをチェックする間隔を制御します。この間隔は、1時間単位で指定します。たとえば、「1」を指定すると、1時間に1回の頻度でチェックされます。「2」を指定すると、2時間に1回の頻度でチェックされます。
- 「`GroomingRetryCounter`」を参照してください。グルーミングにより最小ディスク容量が確保されない場合に、自動的に繰り返されるグルーミングの回数を制御します。
- 「`GroomingDBDataTrimDays`」を参照してください。グルーミング時に削除されるデータの日数を制御します。デフォルト値は1日です。
- 「`GroomingDBTimeoutInMinute`」を参照してください。グルーミングクエリのタイムアウトを分単位で制御します。ここで指定した時間内にグルーミングクエリが完了しない場合、そのタスクはキャンセルされます。デフォルトでは0が指定されており、タイムアウトによるキャンセルは発生しません。
- 「`GroomingRequiredMinimumDiskSizeInMB`」を参照してください。ワークロードバランス仮想アプライアンスの動作に必要な最小空きディスク容量を制御します。データの増大により、仮想ディスクの空き容

量がこの値（最小ディスク容量）に達すると、データベースのグルーミングが開始されます。デフォルト値は 2,048MB です。

これらのパラメータの編集については、ワークロードバランス設定ファイルの編集を参照してください。

#### データベースパスワードの変更

wlb.conf ファイルを編集してワークロードバランスデータベースのパスワードを変更することもできますが、wlbconfig コマンドを使用することをお勧めしています。詳しくは、「ワークロードバランス設定オプションの変更」を参照してください。

#### データベースデータのアーカイブ

古い履歴データが削除されないようにするために、必要に応じて、データベースからデータをコピーしてアーカイブ化できます。これを行うには、以下のタスクを行います。

1. データベースで、クライアント認証を有効にします。
2. 任意の PostgreSQL データベース管理ツールを使用して、アーカイブをセットアップします。

#### データベースに対するクライアント認証を有効にします

ワークロードバランス仮想アプライアンスのコンソールからデータベースに直接アクセスすることもできますが、PostgreSQL データベース管理ツールを使用することもできます。データベース管理ツールをダウンロードして、ワークロードバランス仮想アプライアンス上のデータベースに接続できるシステムにインストールします。たとえば、XenCenter を実行するのと同じコンピューターなどにインストールします。

データベースへのリモートクライアント認証を有効にする前に、以下を行います。

1. データベース設定ファイル (pg\_hba.conf と postgresql.conf) を編集して、接続を許可します。
2. ワークロードバランスサービスを停止し、データベースを再起動してから、ワークロードバランスサービスを起動します。
3. データベース管理ツールで、データベースの IP アドレス（つまりワークロードバランス仮想アプライアンスの IP アドレス）およびデータベースパスワードを設定します。

#### データベース設定ファイルの編集

データベースでクライアント認証を有効にするには、ワークロードバランス仮想アプライアンスの 2 つのファイル: pg\_hba.conf ファイルと postgresql.conf ファイルを変更する必要があります。

**pg\_hba.conf** ファイルを編集するには:

1. pg\_hba.conf ファイルを変更します。ワークロードバランス仮想アプライアンスのコンソールで、vi などのテキストエディタを使って pg\_hba.conf ファイルを開きます。次に例を示します:

```
1 vi /var/lib/pgsql/9.0/data/pg_hba.conf
```

- IPv4 が使用されるネットワークでは、接続元コンピューターの IP アドレスを `pg_hba.conf` ファイルの以下のセクションに追加します。次に例を示します：

##IPv4 `local connections`行の下に、以下の行を入力します：

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** 0.0.0.0/0
- **METHOD:** trust

- `CIDR-ADDRESS` フィールドには実際の IP アドレスを入力します。

注：

「0.0.0.0/0」の箇所を編集して、実際の IP アドレスの最終オクテットの部分を「0/24」に変更したものを入力できます。末尾の「24」はサブネットマスクで、そのサブネットマスク内の IP アドレスからの接続のみが許可されます。

`Method` フィールドに「`trust`」と入力すると、パスワードを入力しなくても認証されるようになります。パスワードが要求されるようにするには、`Method` フィールドに「`password`」と入力します。

- IPv6 が使用されるネットワークでは、接続元コンピューターの IP アドレスを `pg_hba.conf` ファイルの以下のセクションに追加します。次に例を示します：

##IPv6 `local connections`行の下に、以下の内容を入力します：

- **TYPE:** host
- **DATABASE:** all
- **USER:** all
- **CIDR-ADDRESS:** ::0/0
- **METHOD:** trust

`CIDR-ADDRESS` フィールドには実際の IPv6 アドレスを入力します。この例のように「`::0/0`」と入力すると、任意の IPv6 アドレスからデータベースに接続できるようになります。

- ファイルを保存してテキストエディタを終了します。
- データベースを再起動して変更を適用します。次のコマンドを実行します。

```
1 service postgresql-9.0 restart
```

**postgresql.conf** ファイルを編集するには：

- `postgresql.conf` ファイルを変更します。ワークロードバランス仮想アプライアンスのコンソールで、`vi` などのテキストエディタを使って `postgresql.conf` ファイルを開きます。次に例を示します：

```
1 vi /var/lib/pgsql/9.0/data/postgresql.conf
```

2. このファイルでは、ローカルホストだけではなく、すべてのポートからの接続が許可されるように設定します。次に例を示します:

- a) 以下の行を見つけます。

```
1 # listen_addresses='localhost'
```

- b) この行のコメントを解除（##を削除）して、次のように変更します:

```
1 listen_addresses='*'
```

3. ファイルを保存してテキストエディタを終了します。
4. データベースを再起動して変更を適用します。次のコマンドを実行します。

```
1 service postgresql-9.0 restart
```

#### データベース保守時間の変更

ワークロードバランスにより、毎日グリニッジ標準時（GMT）の午前 0:05 にデータベース保守が自動的に実行されます。この間、データの収集は続行されますが、データの記録に遅延が生じることがあります。また、この間も XenCenter でワークロードバランスのユーザーインターフェイスを使用でき、推奨項目も生成されます。

##### 注:

ワークロードバランスの損失を回避するには:

- メンテナンスウィンドウ中に、ワークロードバランスサーバーが再起動します。これと同時に仮想マシンを再起動しないよう注意してください。
- 今回とは別に、プール内のすべての仮想マシンを再起動するときは、ワークロードバランスサーバーを再起動しないでください。

この保守により、未使用のディスク領域が解放され、データベースが再インデックス化されます。この処理は、6～8分で完了します。ただし、大規模なリソースプールでは、ワークロードバランスでの検出処理に応じて保守に時間がかかることがあります。

この保守時間は、運用する場所のタイムゾーンに合わせて変更することができます。たとえば、デフォルトの設定では、日本標準時（JST）の午前 9:05 に保守が実行されてしまいます。また、夏時間を採用している地域では、その移行を考慮した保守時間を設定できます。

保守時間を変更するには:

1. ワークロードバランス仮想アプライアンスのコンソールで、任意のディレクトリから次のコマンドを実行します。

```
1 crontab -e
```

次の行が表示されます。

```
1 05 0 * * * /opt/vpx/wlb/wlbmaintenance.sh
```

「05 0」という値は、ワークロードバランスが保守を実行する時刻（05分過ぎ、0時）を示します（アスタリスク（\*）はこのジョブを実行する日、月、年です。このフィールドを編集しないでください）。05 0は、毎日グリニッジ標準時（GMT）の午前 0:05 に保守が実行されることを意味します。この設定は、ニューヨークに住んでいる場合、冬の間は午後 7:05、夏の間は午後 8:05 に保守が実行されることを意味します。

重要:

3つのアスタリスク（\*）で示される日、月、および年を変更しないでください。データベースの保守は毎日実行する必要があります。

2. 保守の実行時刻を、GMTで入力します。たとえば、深夜 0 時に保守を実行するには、以下のように変更します。

| タイムゾーン                       | UTC との時差 | ローカルの午前 0:05 に<br>保守を実行する場合 | 夏時間  |
|------------------------------|----------|-----------------------------|------|
| 米国太平洋標準時（PST、<br>カリフォルニア州など） | UTC-08   | 05 8                        | 05 7 |
| 日本標準時（JST）                   | UTC+09   | 05 15                       | -    |
| 中国標準時（CST）                   | UTC+08   | 04 15                       | -    |

1. ファイルを保存してテキストエディタを終了します。

#### ワークロードバランスのカスタマイズ

ワークロードバランス機能では、以下のカスタマイズが可能です。

- スクリプト用のコマンドライン：ワークロードバランスコマンドを参照してください。
- ホスト電源投入スクリプトのサポート：ホスト電源投入スクリプトを使用してワークロードバランスの機能を間接的にカスタマイズすることもできます。

#### ワークロードバランスのアップグレード

ワークロードバランスのオンラインでのアップグレードは、セキュリティ上の理由で廃止されました。yum repoによるアップグレードはできなくなりました。最新バージョンのワークロードバランスへのアップグレードは、<https://www.citrix.com/downloads/citrix-hypervisor/product-software/>から最新の WLB VPX をダウンロードしインポートしてください。

## ワークロードバランスのトラブルシューティング

ここでは、ワークロードバランスの問題を解決するための手順について説明します。

### 一般的なトラブルシューティングのヒント

- まず、ワークロードバランスのログファイル (LogFile.log および wlb\_install\_log.log) を参照します。デフォルトでは、ワークロードバランス仮想アプライアンスの以下の場所にログファイルが作成されます。

- /var/log/wlb

- また、XenCenter の [ログ] タブに表示される情報も参照してください。
- ワークロードバランス仮想アプライアンスのビルド番号を確認するには、その仮想アプライアンスが監視しているリソースプールのホスト上で、次のコマンドを実行します:

```
1 xe pool-retrieve-wlb-diagnostics | more
```

出力の上部に、ワークロードバランスのバージョン番号が表示されます。

### エラーメッセージ

ワークロードバランス機能のエラーメッセージは、XenCenter のダイアログボックスや [ログ] タブに表示されます。

エラーメッセージが表示された場合は、XenCenter のイベントログを参照します。詳しくは、[XenCenter ドキュメント](#)を参照してください。

### ワークロードバランスの資格情報入力時の問題

[WLB サーバーへの接続] ダイアログボックスで入力したワークロードバランス仮想マシンのユーザー名およびパスワードで接続できない場合は、以下の点を確認してください:

- ワークロードバランス仮想アプライアンスがインポートされており、正しく設定されていることを確認します。また、すべてのサービスが実行されていることを確認します。詳しくは、「[wlb-start](#wlb-start)」を参照してください。
- 入力した資格情報が正しいことを確認します。デフォルトの資格情報は、『ワークロードバランスクイックスタートガイド』に記載されています。
- [アドレス] ボックスにはホスト名も入力できますが、ここにはワークロードバランス仮想アプライアンスの完全修飾ドメイン名 (Fully Qualified Domain Name: FQDN) を入力する必要があります。仮想アプライアンスをホストする物理サーバーのホスト名は入力しないでください。たとえば、yourcomputername のようになります。ホスト名を入力して問題が生じる場合は、ワークロードバランス仮想アプライアンスの IP アドレスを入力してください。

- ホストで正しい DNS サーバーが使用されていることと、Citrix Hypervisor サーバーで FQDN を使ってワークロードバランス仮想アプライアンスに接続できることを確認します。この確認を行うには、Citrix Hypervisor サーバーから FQDN を指定して ping コマンドを実行します。たとえば、Citrix Hypervisor サーバーコンソールで次のコマンドを実行します：

```
1 ping wlb-vpx-1.mydomain.net
```

#### ファイアウォールの問題

ワークロードバランス仮想アプライアンスがファイアウォールで隔たれており、ファイアウォールが正しく設定されていない場合、「ワークロードバランスサーバーへの接続中にエラーが発生しました。<プール名>。[WLB の初期化] をクリックして接続設定を再初期化してください」というエラーメッセージが表示されます。このメッセージは、ワークロードバランス仮想アプライアンスとの接続でほかの問題がある場合にも表示されます。

#### 解決方法：

ワークロードバランス仮想アプライアンスとの間にあるファイアウォールで、ポート 8012 を開放します。

また、Citrix Hypervisor がワークロードバランスに接続するときのポート（デフォルトで 8012）が、ワークロードバランスの設定ウィザードで指定したものと同じである必要があります。

#### ワークロードバランスとの接続の消失

ワークロードバランスを設定して接続した後接続エラーが発生した場合、資格情報が無効になる可能性があります。この問題を解決するには、以下を行います：

- [WLB サーバーへの接続] ダイアログボックスに入力した資格情報と、以下の情報が一致していることを確認します。
  - ワークロードバランスの設定ウィザードで指定した資格情報
  - Citrix Hypervisor（プールマスタ）の資格情報
- [WLB サーバーへの接続] ダイアログボックスに入力した、ワークロードバランス仮想アプライアンスの IP アドレスまたは FQDN を確認します。
- ワークロードバランス構成時に作成したユーザー名が、[WLB サーバーへの接続] ダイアログボックスに入力したものと一致していることを確認します。

#### ワークロードバランスの接続エラー

[WLB] タブの [ワークロードバランスの状態] に接続エラーが表示される場合は、リソースプールのワークロードバランスを再設定してください。

これを行うには、[WLB] タブの [接続] をクリックして、サーバーの資格情報を再入力します。

ワークロードバランスが停止する場合

ワークロードバランスが機能しない場合（設定に対する変更内容が保存されないなど）、ワークロードバランスのログファイルに以下のエラーメッセージが記録されていないかどうかを確認します：

```
1 dwmdatacolsvc.exe: Don't have a valid pool. Trying again in 10 minutes.
```

原因：

通常、このエラーはプール内の仮想マシンに何らかの問題があると発生します。仮想マシンに問題がある場合は、以下のような現象が見られます：

- **Windows:** Windows 仮想マシンでブルースクリーンエラーが発生している。
- **Linux:** Linux 仮想マシンのコンソールが応答不能になり、シャットダウンなどができない。

回避方法：

1. 仮想マシンの強制シャットダウンを実行します。これを行うには、以下のいずれかを実行します。
  - XenCenter で仮想マシンを選択して、[VM] メニューの [強制シャットダウン] を選択します。
  - `vm-shutdown xe` コマンドに `force=true` を指定して実行します（『Citrix Hypervisor 管理者ガイド』を参照）。次に例を示します：

```
1 xe vm-shutdown force=true uuid=vm_uuid
```

ホストの UUID は、XenCenter の [全般] タブ、または `host-list xe` コマンドを実行して確認できます。仮想マシンの UUID は、仮想マシンの [全般] タブ、または `vm-list xe` コマンドを実行して確認できます。詳しくは、「[コマンドラインインターフェイス](#)」を参照してください。

2. クラッシュした仮想マシンの Citrix Hypervisor サーバーの `xsconsole`、または XenCenter を使用してそのホスト上のすべての仮想マシンをほかのホストに移行してから、`xe-toolstack-restart` コマンドを実行します。

ワークロードバランスサーバーの変更時の問題

リソースプールのワークロードバランスで使用するワークロードバランス仮想アプライアンスを変更するときに、元の仮想アプライアンスから切断してから新しい仮想アプライアンスに接続する必要があります。これを行わないと、両方の仮想アプライアンスでプールのデータが収集されます。

この問題を解決するには、次のいずれかの操作を実行します：

- ワークロードバランス仮想アプライアンスをシャットダウンして削除する。
- ワークロードバランスサービスを手動で停止する（Analysis Engine、Data Collection Manager、Web Services Host）。

注:

`pool-deconfigure-wlb` xe コマンドを使ってワークロードバランス仮想アプライアンスを切断したり、`pool-initialize-wlb` xe コマンドを使ってほかの仮想アプライアンスを指定したりしないでください。

## ワークロードバランスコマンド

ここでは、各ワークロードバランスコマンドの機能と、指定可能なパラメータ、構文などについて説明します。これらのコマンドは、Citrix Hypervisor サーバーやコンソールからワークロードバランスを制御したり、Citrix Hypervisor サーバーでワークロードバランス設定するときを使用します。ここでは、サービスコマンドについても説明します。

以下のサービスコマンドは、ワークロードバランス仮想アプライアンス上で実行します。このためには、ワークロードバランス仮想アプライアンスに接続する必要があります。

### ワークロードバランス仮想アプライアンスへのログイン

サービスコマンドを実行したり `wlb.conf` ファイルを編集したりするには、ワークロードバランス仮想アプライアンスにログインする必要があります。このためには、ユーザー名とパスワードを入力する必要があります。仮想アプライアンスにユーザーアカウントを追加していない場合は、ルートユーザーアカウントでログインします。使用するアカウントは、(ワークロードバランスとリソースプールを接続する前に) [ワークロードバランスの設定] ウィザードで指定したものになります。または、XenCenter の [コンソール] タブからログインすることもできます。

ワークロードバランス仮想アプライアンスにログインするには:

1. `name-of-your-WLB-VPX` ログインプロンプトに、アカウントのユーザー名を入力します。次の例の `wlb-vpx-pos-pool` には、ワークロードバランス仮想アプライアンスの名前を入力します:

```
1 wlb-vpx-pos-pool login: root
```

2. パスワードプロンプトに、アカウントのパスワードを入力します:

```
1 wlb-vpx-pos-pool login: root
```

注:

ワークロードバランス仮想アプライアンスからログオフするには、コマンドプロンプトで「`logout`」と入力します。

## **wlb restart**

`wlb restart` コマンドをワークロードバランス仮想アプライアンスの任意の場所で実行すると、Workload Balancing Data Collection サービス、Web Service サービス、Data Analysis サービスが停止され再起動されます。

## wlb start

`wlb start` コマンドをワークロードバランス仮想アプライアンスの任意の場所で実行すると、Workload Balancing Data Collection サービス、Web Service サービス、Data Analysis サービスが開始されます。

## wlb stop

`wlb stop` コマンドをワークロードバランス仮想アプライアンスの任意の場所で実行すると、Workload Balancing Data Collection サービス、Web Service サービス、Data Analysis サービスが停止されます。

## wlb status

`wlb status` コマンドをワークロードバランス仮想アプライアンスの任意の場所で実行すると、ワークロードバランスサーバーの状態が確認されます。このコマンドを実行すると、3つのワークロードバランスサービス（Web Service、Data Collection Service、Data Analysis Service）のステータスが表示されます。

### ワークロードバランス設定オプションの変更

データベース設定オプションやウェブサービス設定オプションなど、ワークロードバランス設定の多くは `wlb.conf` ファイルに記録されています。この `wlb.conf` ファイルが、ワークロードバランス仮想アプライアンスの設定ファイルとなります。

頻繁に使用されるオプションを簡単に変更できるように、`wlb config` コマンドが用意されています。ワークロードバランス仮想アプライアンス上で `wlb config` コマンドを実行すると、ワークロードバランスのユーザーアカウント名の変更、パスワードの変更、PostgreSQL パスワードの変更を行うことができます。このコマンドを実行すると、ワークロードバランスサービスが再起動します。

**wlb config** コマンドを実行するには:

1. コマンドプロンプトから次を実行します:

```
1 wlb config
```

この画面には、ワークロードバランスのユーザー名とパスワード、および PostgreSQL のパスワードを変更するための一連の質問が表示されます。これらの質問に従って変更を行います。

#### 重要:

`wlb.conf` ファイルに値を入力する場合は、必ず入念に確認してください: ワークロードバランスでは `wlb.conf` ファイルの値の検証は行われません。このため、指定したパラメータが所定の範囲にない場合でも、エラーログは生成されません。

## ワークロードバランス設定ファイルの編集

ワークロードバランスの設定オプションは、ワークロードバランス仮想アプライアンスの/opt/vpx/wlb ディレクトリに保存されている wlb.conf ファイルを編集することで変更できます。通常は、Citrix 担当者からの指示がある場合のみ変更するようにしてください。ただし、必要に応じて変更可能な設定カテゴリが 3 つあります：

- ワークロードバランスのアカウント名とパスワード：これらの資格情報は、`wlb config` コマンドを実行して簡単に変更できます。
- データベースパスワード：この値は、wlb.conf ファイルで変更できます。ただし、`wlb config` を使用すれば wlb.conf ファイルが更新され自動でデータベースのパスワードが変更されるため、こちらのコマンドを使用することをお勧めします。代わりに wlb.conf ファイルを変更することを選択した場合は、クエリを実行して、新しいパスワードでデータベースを更新する必要があります。
- データベースグルーミングのパラメータ：このファイルでは、データベースのグルーミングパラメータ（データベースのグルーミング間隔など）を変更できます。方法についてはデータベースの管理に関するセクションの手順を参照してください。ただし、変更する場合は注意することをお勧めします。

現時点では、wlb.conf ファイルの上記以外の設定については、Citrix 担当者から特別な指示がない限りデフォルトのままにすることが推奨されます。

**wlb.conf** ファイルを編集するには：

1. ワークロードバランス仮想アプライアンス上で、コマンドプロンプトから次のコマンドを実行します（例として vi を使用）：

```
1 vi /opt/vpx/wlb/wlb.conf
```

画面上に、さまざまな設定オプションが表示されます。

2. 設定オプションを変更して、エディタを終了します。

wlb.conf ファイルの編集後にワークロードバランスサービスを再起動する必要はありません。変更内容は、エディタを閉じるとすぐに反映されます。

### 重要：

wlb.conf ファイルに値を入力する場合は、必ず入念に確認してください：ワークロードバランスでは wlb.conf ファイルの値の検証は行われません。このため、指定したパラメータが所定の範囲にない場合でも、エラーログは生成されません。

## ワークロードバランスログの詳細度の変更

ワークロードバランスログには、分析エンジン、データベース、監査ログに対する操作など、ワークロードバランス仮想アプライアンスで発生したイベントの一覧が記録されます。このログファイルは次の場所にあります：  
`/var/log/wlb/LogFile.log`。

必要に応じて、ワークロードバランスログが提供する詳細レベルを上げることができます。これを行うには、次の場所にあるワークロードバランス設定ファイル (wlb.conf) の「Trace flags」セクションを編集します：  
/opt/vpx/wlb/wlb.conf。各トレースについて、「1」または「true」と入力するとログ記録が有効化され、「0」または「false」と入力すると無効化されます。たとえば、分析エンジンのログ記録を有効にするには次のように入力します：

```
1 AnalEngTrace=1
```

Citrix テクニカルサポートに問題を報告する場合や、トラブルシューティングを行う場合には、ログ記録の詳細度を上げることをお勧めします。

| ログオプション       | トレースフラグ                          | メリットまたは用途                                                                                        |
|---------------|----------------------------------|--------------------------------------------------------------------------------------------------|
| 分析エンジントレース    | <code>AnalEngTrace</code>        | 分析エンジンの計算の詳細を記録します。分析エンジンの決定内容を確認し、ワークロードバランスで推奨項目が生成されない理由を把握できます。                              |
| データベーストレース    | <code>DatabaseTrace</code>       | データベースの読み取り/書き込みの詳細を記録します。このトレースを有効にすると、ログファイルのサイズが急激に増加します。                                     |
| データ収集トレース     | <code>DataCollectionTrace</code> | メトリックの取得処理を記録します。この値から、ワークロードバランスで取得され、データストアに保存された測定値を確認できます。このトレースを有効にすると、ログファイルのサイズが急激に増加します。 |
| データ圧縮トレース     | <code>DataCompactionTrace</code> | メトリックデータの圧縮にかかった時間がミリ秒単位で記録されません。                                                                |
| データイベントトレース   | <code>DataEventTrace</code>      | ワークロードバランスが XenServer から取得したイベントの詳細を記録します。                                                       |
| データグルーミングトレース | <code>DataGroomingTrace</code>   | データベースグルーミングの詳細を記録します。                                                                           |
| データメトリックトレース  | <code>DataMetricsTrace</code>    | メトリックデータの解析の詳細を記録します。このトレースを有効にすると、ログファイルのサイズが急激に増加します。                                          |

| ログオプション       | トレースフラグ              | メリットまたは用途                                                                                             |
|---------------|----------------------|-------------------------------------------------------------------------------------------------------|
| キュー管理トレース     | QueueManagementTrace | データ収集におけるキュー管理プロセスの詳細を記録します（内部使用向けのオプションです）。                                                          |
| データ保存トレース     | DataSaveTrace        | データベースに保存されているリソースプールの詳細を記録します。                                                                       |
| ホストスコア付けトレース  | ScoreHostTrace       | ワークロードバランスでのホストのスコア付けの詳細を記録します。このトレースには、仮想マシンの移行先に最適なサーバーの評価を計算するときにワークロードバランスが生成したスコアが示されません。        |
| 監査ログトレース      | AuditLogTrace        | 監査ログデータの記録処理および書き込み処理が記録されます（このオプションは内部専用であり、監査ログに記録される情報は記録されません）。このトレースを有効にすると、ログファイルのサイズが急激に増加します。 |
| スケジュールタスクトレース | ScheduledTaskTrace   | スケジュールされたタスクの詳細を記録します。たとえば、モード変更スケジュールが機能しない場合に、このトレースから原因を探ることができます。                                 |
| Web サービストレース  | WlbWebServiceTrace   | Web サービスインターフェイスとの通信の詳細を記録します。                                                                        |

## ワークロードバランスの証明書

March 12, 2020

このセクションでは、証明書の安全性を向上させるための以下の方法について説明します。

- Citrix Hypervisor が信頼された機関からの証明書を検証するように設定する。

- Citrix Hypervisor がデフォルトのシトリックスワークロードバランス自己署名証明書を検証するように設定する。

## 概要

Citrix Hypervisor とワークロードバランスサーバーは、HTTPS を使用して通信します。このため、ワークロードバランス仮想アプライアンスの設定時に、ウィザードにより自己署名入りのテスト証明書が自動的に作成されます。このテスト証明書により、ワークロードバランスと Citrix Hypervisor との SSL 接続が確立されます。

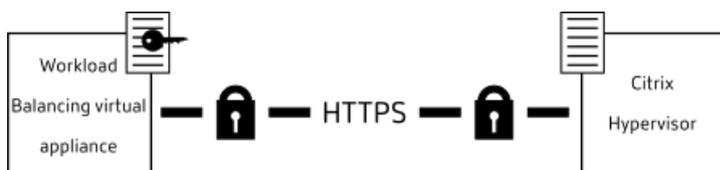
### 注:

自己署名入りのテスト証明書は HTTPS 通信を行うための代替証明書であり、信頼された証明機関からの証明書ではありません。セキュリティを向上させるために、信頼された証明機関からの証明書を使用することをお勧めします。

この SSL 接続は、Citrix Hypervisor でデフォルトで自動的に作成されます。ワークロードバランス仮想アプライアンスの設定時および設定後に追加の証明書設定を行う必要はありません。

ただし、証明機関からの証明書を使用する場合は、ワークロードバランス仮想アプライアンスと Citrix Hypervisor でその証明書が使用されるように設定する必要があります。

デフォルトでは、ワークロードバランスでどのような証明書を使用しても、Citrix Hypervisor がその仮想アプライアンスとの接続を確立するときに、証明書の同一性は検証されません。Citrix Hypervisor が特定の証明書を検証するには、その証明書の署名に使用されたルート証明書をエクスポートして、それを Citrix Hypervisor にコピーし、Citrix Hypervisor がその証明書を検証するように設定します。この場合、Citrix Hypervisor はクライアントとして動作し、ワークロードバランス仮想アプライアンスはサーバーとして動作します。



環境のセキュリティポリシーに応じて、以下のいずれかを行います。

- Citrix Hypervisor が自己署名入りのテスト証明書を検証するように設定する。「Citrix Hypervisor で自己署名証明書の検証を設定する」を参照してください。
- Citrix Hypervisor が信頼された証明機関からの証明書を検証するように設定する。「Citrix Hypervisor で証明機関からの証明書の検証を設定する」を参照してください。

## Citrix Hypervisor で自己署名証明書の検証を設定する

Citrix Hypervisor がワークロードバランス仮想アプライアンスとの接続を確立するときに、Citrix Hypervisor がシトリックスワークロードバランス自己署名証明書を検証するように設定できます。

**重要:**

自己署名入りの証明書を XenServer で検証する場合は、ホスト名を指定してワークロードバランス仮想アプライアンスに接続する必要があります。ワークロードバランスのホスト名を確認するには、仮想アプライアンス上で `hostname` コマンドを実行します。

Citrix WLB 自己署名証明書が検証されるように設定するには、以下の手順に従います。

**Citrix Hypervisor** で自己署名証明書が検証されるように設定するには:

1. ワークロードバランス仮想アプライアンス上の自己署名入り証明書をプールマスタにコピーします。自己署名入りの証明書は、`is stored at /etc/ssl/certs/server.pem` に格納されています。プールマスタ上で次のコマンドを実行して、この証明書をコピーします。

```
1 scp root@wlb-ip:/etc/ssl/certs/server.pem .
```

2. ワークロードバランス仮想アプライアンスの IP アドレス (`wlb-ip`) の信頼性を確認できないという内容のメッセージが表示されたら、「`yes`」と入力して続行します。
3. ワークロードバランス仮想アプライアンスのルートパスワードを入力すると、証明書が現在のディレクトリにコピーされます。
4. 証明書をインストールします。これを行うには、PEM ファイルをコピーしたディレクトリで `pool-certificate-install` コマンドを実行します。次に例を示します:

```
1 xe pool-certificate-install filename=server.pem
```

5. プールマスタで `pool-certificate-list` コマンドを実行して、証明書が正しくインストールされたことを確認します:

```
1 xe pool-certificate-list
```

証明書が正しくインストールされた場合は、エクスポートされたルート証明書 (`server.pem` など) が表示されます (このコマンドを実行すると、インストールされているすべての SSL 証明書が一覧表示されます)。

6. プールマスタで `pool-certificate-sync` コマンドを実行して、証明書をほかのホストに同期します:

```
1 xe pool-certificate-sync
```

プールマスタ上で `pool-certificate-sync` コマンドを実行すると、証明書および証明書失効一覧がプール内で同期されます。これにより、リソースプール内のすべてのホストで同じ証明書が使用されるようになります。

このコマンドを実行しても、何も出力されません。このコマンドが正しく実行されていない場合、次の手順も機能しません。

7. ワークロードバランス仮想アプライアンスとの接続を確立するときに、Citrix Hypervisor が証明書を検証するように設定します。これを行うには、プールマスタで次のコマンドを実行します。

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

ヒント:

プールの UUID は、Tab キーを押すと自動で入力されます。

8. (オプション) このコマンドが正しく実行されたことを確認するには、以下の手順に従います:

- a) プール内のホストに証明書が同期されたことを確認するには、そのホストで `pool-certificate-list` コマンドを実行します。
- b) Citrix Hypervisor が証明書を検証するように設定されていることを確認するには、`pool-param-get` コマンドに `param-name=wlb-verify-cert` パラメーターを指定して実行します。次に例を示します:

```
1 xe pool-param-get param-name=wlb-verify-cert uuid=uuid_of_pool
```

## Citrix Hypervisor で証明機関からの証明書の検証を設定する

Citrix Hypervisor がワークロードバランス仮想アプライアンスとの接続を確立するとき、信頼された証明機関からの証明書を検証するように設定できます。

信頼された機関からの証明書を Citrix Hypervisor で使用するには、公開キーを含んだ PEM ファイルとしてエクスポートした証明書または証明書チェーン（中間証明書とルート証明書）が必要です。

信頼された機関からの証明書が XenServer で検証されるように設定するには、以下のタスクを行います。

1. 信頼された証明機関から、署名入りの証明書を入手します。「タスク 1: 証明機関から証明書を入手する」を参照してください。
2. 入手した証明書を指定および適用します。詳しくは、タスク 2: 新しい証明書を指定するを参照してください。
3. 入手した証明書をインストールして、プールマスタでその証明書が検証されるように設定します。「タスク 3: 証明書チェーンをプールにインポートする」を参照してください。

これらのタスクを実行する前に、以下の点を確認します:

- Citrix Hypervisor プールマスタの IP アドレスが必要です。
- Citrix Hypervisor でワークロードバランス仮想アプライアンスのホスト名を解決できる必要があります (Citrix Hypervisor プールマスタのコンソールでワークロードバランス仮想アプライアンスの FQDN を指定して ping を実行できるなど)。

重要:

IP アドレスを使ってワークロードバランス仮想アプライアンスに接続する場合は、証明書の生成時にその IP アドレスを SAN (Subject Alternative Name: サブジェクトの別称) として指定する必要があります。

## タスク 1: 証明機関から証明書を入手する

証明機関から証明書を取得するには、証明書署名要求 (CSR) を生成する必要があります。ワークロードバランス仮想アプライアンスの証明書署名要求を生成するには、秘密キーを作成し、それを使用して証明書署名要求を生成します。これらの作業は、ワークロードバランス仮想アプライアンス上で行います。

### 証明書の一般名について

CSR の作成時に指定する一般名 (CN: Common Name) は、ワークロードバランス仮想アプライアンスの FQDN (完全修飾ドメイン名: Fully Qualified Domain Name)、および [WLB サーバーへの接続] ダイアログボックスの [アドレス] ボックスで指定した FQDN または IP アドレスと正確に一致させる必要があります。

CN を指定するときは、以下のいずれかのガイドラインに従います。

- [WLB サーバーへの接続] ダイアログボックスで指定したものと同一 CN を指定する。たとえば、ワークロードバランス仮想アプライアンスの名前が「wlb-vpx.yourdomain」である場合は、[WLB サーバーへの接続] ダイアログボックスで「wlb-vpx.yourdomain」と指定し、証明書署名要求の生成時にも「wlb-vpx.yourdomain」と指定します。
- IP アドレスを使用してプールをワークロードバランスに接続した場合は、FQDN を共通名として使用し、IP アドレスをサブジェクトの別名 (SAN) として指定します。ただし、このような証明書では問題が生じる場合もあります。

#### 注:

証明書の検証機能は、不正な接続を防ぐ目的で設計されています。このため、ワークロードバランス証明書が厳密な要件を満たさない場合、証明書の検証に失敗し、Citrix Hypervisor とワークロードバランス仮想アプライアンスの接続が確立されません。また、証明書を検証するには、Citrix Hypervisor が特定できる適切な場所に証明書が格納されている必要があります。

秘密キーファイルを作成するには:

1. 次のコマンドを実行して、秘密キーファイルを作成します。

```
1 openssl genrsa -des3 -out privatekey.pem 2048
```

2. 次のコマンドを実行して、パスワードを削除します:

```
1 openssl rsa -in privatekey.pem -out privatekey.nop.pem
```

#### 注:

不正なパスワードを入力すると、ユーザーインターフェイスエラーが発生したという内容のメッセージが表示されます。このメッセージは無視して構いません。そのままコマンドを実行して秘密キーファイルを作成します。

証明書署名要求を生成するには:

1. 以下の手順に従って、証明書署名要求を生成します。

a) 次のコマンドで秘密キーを指定して、証明書署名要求を生成します。

```
1 openssl req -new -key privatekey.nop.pem -out csr
```

b) 画面のメッセージに従って以下の情報を入力し、証明書署名要求を生成します。

**Country Name:** SSL 証明書の国コードを入力します。日本の国コードは「JP」です。国コードの一覧については、インターネット上を検索して入手できます。

**State or Province Name (full name):** プールが動作する場所の都道府県名を入力します。たとえば、東京の場合は「Tokyo」と入力します。

**Locality Name:** プールが動作する場所の市区町村名を入力します。

**Organization Name:** 所属組織または会社の名前を入力します。

**Organizational Unit Name:** 部門や部署の名前を入力します。この情報は入力しなくても構いません。

**Common Name:** ワークロードバランス仮想アプライアンスの FQDN を入力します。プールでワークロードバランス仮想アプライアンスに接続するときに使用した情報を入力する必要があります。

**Email Address:** 証明書に含めるメールアドレスを入力します。

c) 任意の属性を指定するか、Enter キーを押して次のステップに進みます。

現在のディレクトリに証明書署名要求が生成され、「csr」という名前で保存されます。

2. ワークロードバランスのアプライアンスコンソールで次のコマンドを実行して、コンソールウィンドウに CSR を表示します:

```
1 cat csr
```

3. 証明書署名要求の全内容をコピーして、証明機関に証明書を要求します。

## タスク 2: 新しい証明書を指定する

この手順を使用して、ワークロードバランスが証明機関からの証明書を使用するように指定します。この手順により、ルート証明書と中間証明書（該当する場合）がインストールされます。

新しい証明書を指定するには:

1. 証明機関から、署名入り証明書、ルート証明書、および中間証明書（証明機関により提供される場合）をダウンロードします。
2. ワークロードバランス仮想アプライアンス以外のコンピューターに証明書をダウンロードした場合は、次のいずれかを行います:

- a) Windows コンピューターにダウンロードした場合は、WinSCP などのコピーユーティリティを使用して証明書ファイルをワークロードバランス仮想アプライアンスにコピーします。

この場合、ホスト名として IP アドレスを指定して、デフォルトのポートを使用します。ユーザー名およびパスワードは、通常 root アカウントのものを使用します（ワークロードバランス仮想アプライアンスの設定時に指定したもの）。

- a) Linux コンピューターにダウンロードした場合は、SCP などのコピーユーティリティを使用して証明書ファイルをワークロードバランス仮想アプライアンスにコピーします。次に例を示します：

```
1 scp root_ca.pem root@wlb-ip:/path_on_your_WLB
```

3. ワークロードバランス仮想アプライアンスで、すべての証明書（ルート証明書、中間証明書（インストールされている場合）、および署名入り証明書）の内容を統合します。次に例を示します：

```
1 cat signed_cert.pem intermediate_ca.pem root_ca.pem > server.pem
```

4. 次のコマンドを実行して、既存の証明書およびキーの名前を変更します。

```
1 mv /etc/ssl/certs/server.pem /etc/ssl/certs/server.pem_orig
2 mv /etc/ssl/certs/server.key /etc/ssl/certs/server.key_orig
```

5. 次のコマンドを実行して、統合した証明書をコピーします。

```
1 mv server.pem /etc/ssl/certs/server.pem
```

6. 次のコマンドを実行して、先ほど作成した秘密キーをコピーします：

```
1 mv privatekey.nop.pem /etc/ssl/certs/server.key
```

7. ルートユーザーだけが秘密キーを読み取れるようにします。これを行うには、`chmod`コマンドを実行します。

```
1 chmod 600 /etc/ssl/certs/server.key
```

8. `stunnel`を再起動します：

```
1 killall stunnel
2 stunnel
```

### タスク 3: 証明書チェーンをプールにインポートする

証明書を入手したら、Citrix Hypervisor プールマスタ上にインポート（インストール）して、プール内のすべてのホストでそれらの証明書が使用されるように同期します。その後で、ワークロードバランスからの接続時に証明書が検証されるように、Citrix Hypervisor を設定します。

1. 署名入り証明書、ルート証明書、および中間証明書（証明機関により提供される場合）を Citrix Hypervisor プールマスタにコピーします。
2. 次のコマンドを実行して、ルート証明書をプールマスタにインストールします。

```
1 xe pool-certificate-install filename=root_ca.pem
```

3. 中間証明書を使用する場合は、それもプールマスタにインストールします。

```
1 xe pool-certificate-install filename=intermediate_ca.pem
```

4. 証明書が正しくインストールされたことを確認します。これを行うには、プールマスタで次のコマンドを実行します。

```
1 xe pool-certificate-list
```

このコマンドにより、インストールされているすべての SSL 証明書が一覧表示されます。インストールした証明書がこの一覧に含まれていることを確認します。

5. 次のコマンドを実行して、証明書をほかのホストに同期します。

```
1 xe pool-certificate-sync
```

プールマスタ上で `pool-certificate-sync` コマンドを実行すると、証明書および証明書失効一覧がプール内で同期されます。これにより、リソースプール内のすべてのホストで同じ証明書が使用されるようになります。

6. ワークロードバランス仮想アプライアンスとの接続を確立するときに、Citrix Hypervisor が証明書を検証するように設定します。これを行うには、プールマスタで次のコマンドを実行します。

```
1 xe pool-param-set wlb-verify-cert=true uuid=uuid_of_pool
```

ヒント:

プールの UUID は、Tab キーを押すと自動で入力されます。

7. 証明書の検証を有効化する前に、[WLB への接続] ダイアログボックスで IP アドレスを指定している場合は、プールとワークロードバランスを再接続するように求められます。

この場合は、[WLB サーバーへの接続] ダイアログボックスの [アドレス] ボックスに、ワークロードバランス仮想アプライアンスの **FQDN**（証明書の CN と同じもの）を入力します（証明書の CN は、ワークロードバランス仮想アプライアンスの FQDN、および Citrix Hypervisor で [WLB サーバーへの接続] ダイアログボックスの [アドレス] ボックスに入力した FQDN と一致する必要があります）。

### トラブルシューティングのヒント

- 証明書の検証の設定後にプールとワークロードバランスを接続できなくなった場合は、「`xe pool-param -set wlb-verify-cert=false uuid=uuid_of_pool`」を実行して証明書の検証を無効化し、接続できるか確認してください。証明書の検証を無効にして接続できる場合は、証明書の設定に問題があります。証明書の検証を無効にしても接続できない場合は、ワークロードバランス仮想アプライアンスの資格情報またはネットワーク接続の問題が考えられます。
- 一部の証明機関では、証明書のインストールを確認するためのツールが提供されています。ここで説明したタスクで問題が生じた場合は、これらのツールを使用して問題を特定してください。これらのツールで SSL ポートを指定する必要がある場合は、8012 またはワークロードバランス仮想アプライアンスの設定時に指定したポート番号を使用します。
- ここで説明したタスクを実行した後で [WLB] タブに「ワークロードバランスサーバーへの接続中にエラーが発生しました」というメッセージが表示された場合は、証明書の CN とワークロードバランス仮想アプライアンス名が一致していることを確認してください。ワークロードバランス仮想アプライアンス名および証明書の共通名は正確に一致する必要があります。

## VMware ワークロードの変換

December 30, 2019

XenCenter および Citrix Hypervisor Conversion Manager 仮想アプライアンスを使用すると、VMware の仮想マシンのバッチを環境 Citrix Hypervisor に移動することで、VMware のワークロードを Citrix Hypervisor に移行できます。

この移行の中で、XenCenter は仮想マシンのネットワーク設定やストレージ接続の変更などの移行作業を容易にします。XenServer Conversion Manager による変換処理が完了すると、その仮想マシンはほぼ実行可能な状態になります。

注:

Citrix Hypervisor 8.0 以前のバージョンでは、別の Conversion Manager コンソールが提供されています。この機能は Citrix Hypervisor 8.1 から XenCenter に統合されています。

### 概要

Citrix Hypervisor により以下を実行できます:

- 1 つのシンプルなウィザードを使用して複数の仮想マシンを変換する
- VMware と Citrix Hypervisor の間でネットワーク設定をマップし、変換した仮想マシンを適切なネットワーク設定で起動し実行できるようにする

- 新しい Citrix Hypervisor 仮想マシンを実行するストレージの場所を選択する

注:

- XenCenter は、既存の VMware 環境を削除または変更しません。仮想マシンは Citrix Hypervisor 環境で複製され、VMware から削除されることはありません。
- Citrix Hypervisor Conversion Manager 仮想アプライアンスは、シンプロビジョニング、シックプロビジョニング、IDE、SCSI などのさまざまなストレージを使用する VMware 仮想マシンの変換をサポートします。
- Citrix Hypervisor Conversion Manager 仮想アプライアンスでは、ソース仮想マシンに VMware Tools がインストールされている必要はありません。VMware 仮想マシンに VMware Tools がインストールされているかどうかに関係なく変換を実行できます。
- Citrix Hypervisor Conversion Manager 仮想アプライアンスは、4 つ以上のディスクを持つ VMWare 仮想マシンを Citrix Hypervisor 仮想マシンに変換することはできません。VMWare 仮想マシンには、3 つ以下のディスクが必要です。
- Citrix Hypervisor Conversion Manager 仮想アプライアンスは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor 8.1 のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト](#)にアクセスしてください。

### Citrix Hypervisor について

環境を変換する前に、Citrix Hypervisor のコンセプトに精通することをお勧めします。詳しくは、「[製品の技術概要](#)」を参照してください。

Citrix Hypervisor 環境で VMware の仮想マシンを正常に変換するには、次のタスクを実行します:

- Citrix Hypervisor をインストールするなど、基本的な Citrix Hypervisor 環境を設定する。詳しくは、「[クイックスタート](#)」および「[インストール](#)」を参照してください。
- Citrix Hypervisor でネットワークを作成して、IP アドレスをネットワークインターフェイスカードに割り当てる。詳しくは、「[クイックスタート](#)」を参照してください。
- ストレージに接続する。詳しくは、「[クイックスタート](#)」を参照してください。

### VMware と Citrix Hypervisor の用語の比較

次の表に、一般的な VMware の機能、コンセプト、およびコンポーネントにおおよそ相当する Citrix Hypervisor の用語を示します:

| VMware の用語            | Citrix Hypervisor の相当語                         |
|-----------------------|------------------------------------------------|
| VMware vSphere Client | XenCenter (Citrix Hypervisor の管理コンソール)         |
| クラスター/リソースプール         | リソースプール                                        |
| データストア                | ストレージリポジトリ                                     |
| vMotion               | ライブマイグレーション                                    |
| 分散リソーススケジュール (DRS)    | ワークロードバランス                                     |
| 高可用性 (HA)             | 高可用性 (HA)                                      |
| vCenter Converter     | Citrix Hypervisor Conversion Manager 仮想アプライアンス |
| 役割ベースのアクセス制御 (RBAC)   | 役割ベースのアクセス制御 (RBAC)                            |

## 変換の概要

XenCenter および Citrix Hypervisor Conversion Manager 仮想アプライアンスは対象の各仮想マシンのコピーを作成します。同等のネットワーク設定とストレージ接続で対象の仮想マシンを Citrix Hypervisor 仮想マシンに変換した後、XenCenter はその仮想マシンを Citrix Hypervisor プールまたはホストにインポートします。1 つまたは 2 つの仮想マシンだけを変換することも、環境全体の一括変換を実行することもできます。

### 注:

vSphere から仮想マシンを変換する前に、vSphere で仮想マシン (変換対象のもの) をシャットダウンする必要があります。Citrix Hypervisor Conversion Manager 仮想アプライアンスでは、コピーしたメモリを使用して実行中の仮想マシンを vSphere から Citrix Hypervisor に変換することはできません。

また、変換する前に、VMware 仮想マシンにネットワークと記憶域コントローラーが存在することを確認してください。

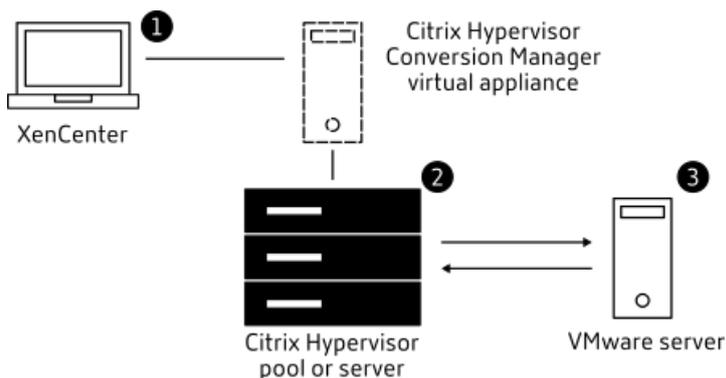
変換プロセスには以下の 4 つのコンポーネントが必要です:

- **XenCenter** - Citrix Hypervisor 管理インターフェイスには、変換オプションを設定して変換を制御する変換ウィザードが含まれています。XenCenter は Windows デスクトップでインストールできます。XenCenter は Citrix Hypervisor および Citrix Hypervisor Conversion Manager 仮想アプライアンスに接続できる必要があります。
- **Citrix Hypervisor Conversion Manager** 仮想アプライアンス - 事前にパッケージされた仮想マシン。変換した仮想マシンを実行する Citrix Hypervisor ホストまたはプールにインポートします。仮想アプライアンスは、VMware 仮想マシンのコピーを Citrix Hypervisor 仮想マシンフォーマットに変換します。変換後、これらのコピーを Citrix Hypervisor プールまたはホストにインポートします。
- **Citrix Hypervisor** スタンドアロンのホストまたはプール - 変換した仮想マシンを実行する Citrix

Hypervisor 環境。

- **VMware** サーバー。Citrix Hypervisor Conversion Manager には、変換する仮想マシンを管理する VMware サーバーへの接続が必要です。接続先の VMware サーバーは、vCenter Server、ESXi Server、または ESX Server である必要があります。仮想マシンは VMware サーバーから削除されません。代わりに、Citrix Hypervisor Conversion Manager 仮想アプライアンスはこれらの仮想マシンのコピーを作成して、Citrix Hypervisor 仮想マシンフォーマットに変換します。

次の図では、これらのコンポーネントの関係性を示しています：



この図は以下を示しています：

1. XenCenter と Citrix Hypervisor Conversion Manager 仮想アプライアンスの通信の仕組み
2. Citrix Hypervisor Conversion Manager 仮想アプライアンスによる VMware サーバーの認証の仕組み
3. 変換中 VMware サーバーが Citrix Hypervisor Conversion Manager 仮想アプライアンスに応答する仕組み

VMware サーバーは、アプライアンスが VMware サーバーにクエリを実行する際にのみ、変換を通した環境の情報とディスクデータについて Citrix Hypervisor Conversion Manager 仮想アプライアンスと通信を行います。

#### 仮想マシン変換方法の概要

以下の簡単な手順で Citrix Hypervisor Conversion Manager 仮想アプライアンスを設定して仮想マシンの変換を開始できます：

1. [Citrix Hypervisor 8.1 Premium Edition のページ] から Citrix Hypervisor Conversion Manager 仮想アプライアンスをダウンロードします。
2. XenCenter を使用して、Citrix Hypervisor Conversion Manager 仮想アプライアンスを Citrix Hypervisor にインポートします。
3. Citrix Hypervisor Conversion Manager 仮想アプライアンスの設定は、XenCenter を使用して行います。
4. XenCenter から変換ウィザードを起動して、仮想マシンの変換を開始します。

以下のセクションでは、これらの手順について詳しく説明します。

## 環境の準備

VMware 環境を変換する前に、対象の Citrix Hypervisor スタンドアロンホスト、つまり変換した VMware 仮想マシンを実行するプールを作成して準備する必要があります。環境の準備には以下のことが含まれています：

1. VMware 環境をどのように変換するか戦略を定義する。1 つまたは 2 つの仮想マシンを変換するのか、環境全体を変換するのか、設定が正しいことを確認するために最初にパイロットを作成するのか、両方の環境を並行して実行するのか、Citrix Hypervisor に変換するときに既存のクラスター設計を維持するのか、など。
2. ネットワーク設定の構成を計画する。同じ物理ネットワークに接続するのか、ネットワーク設定の構成を単純化したり変更したりするのか、など。
3. プールに含めるホストに Citrix Hypervisor をインストールする。理想的には、インストールを開始する前に、ホストのネットワークインターフェイスカードを物理ネットワークに挿入します。
4. プールを作成して、基本的なネットワーク設定の構成を実行する。たとえば、次のようにします：
  - Citrix Hypervisor ホスト上の VMware クラスターに接続するネットワークを構成します（クラスターが Citrix Hypervisor ホストと同じネットワーク上にない場合）。
  - ストレージアレイに接続するネットワークを構成します。つまり、IP ベースのストレージを使用する場合は、ストレージアレイの物理ネットワークに接続する Citrix Hypervisor ネットワークを作成します。
  - プールを作成して、このプールにホストを追加します。
5. (共有ストレージおよび Citrix Hypervisor プールの場合) 仮想ディスクを格納する共有ストレージを準備して、ストレージ（プールのストレージリポジトリ：SR）への接続を作成する。
6. (オプション) 変換の要件ではありませんが、VMware サーバーの管理者アカウントと一致するように、Citrix Hypervisor プールの管理者アカウントを構成できます。Active Directory アカウントの役割ベースのアクセス制御の構成について詳しくは、「[役割ベースのアクセス制御](#)」を参照してください。

## Citrix Hypervisor のインストールとプールの作成

VMware 仮想マシンを変換するには、変換した仮想マシンを実行する Citrix Hypervisor プールまたはホストを作成してください。このプールには、VMware サーバーに接続できるように構成したネットワーク設定が必要です。VMware クラスターに含まれている Citrix Hypervisor プールと同じ物理ネットワークを構成することも、ネットワーク設定の構成を単純化することもできます。変換した仮想マシンをプールで実行する場合は、変換前にストレージリポジトリを作成して、共有ストレージをプールに追加します。

Citrix Hypervisor を初めて利用される場合、基本的なインストールや構成など、Citrix Hypervisor の基本については「[クイックスタート](#)」でご覧いただけます。

## Citrix Hypervisor 環境に関する考慮事項

Citrix Hypervisor のインストールと仮想アプライアンスのインポートの前に、変換戦略に影響する可能性のある次の要素を検討してください:

**Citrix Hypervisor Conversion Manager** 仮想アプライアンスを実行するホストの選択。仮想アプライアンスを stand-alone ホスト、または変換した仮想マシンを実行するプール内のホストにインポートします。

プールの場合、ホストのストレージが記憶要件を満たせば、プール内の任意のホストで仮想アプライアンスを実行できます。

変換した仮想マシンを実行するプールまたはホストで構成されるストレージは、特定の要件を満たす必要があります。新しく変換した仮想マシンをプールで実行する場合は、その仮想ディスクが共有ストレージに格納されている必要があります。ただし、変換した仮想マシンを（プールではなく）1台のスタンドアロンのホストで実行する場合は、仮想ディスクにローカルストレージを使用できます。

変換した仮想マシンをプールで実行する場合は、ストレージリポジトリを作成して、共有ストレージをプールに追加してください。

変換をサポートするゲストオペレーティングシステム。Citrix Hypervisor Conversion Manager 仮想アプライアンスでは、Citrix Hypervisor でサポートされているすべての Windows ゲストオペレーティングシステムの VMware 仮想マシンの変換がサポートされています。Citrix Hypervisor によってサポートされる Windows ゲストオペレーティングシステムの一覧については、「[ゲストオペレーティングシステムのサポート](#)」を参照してください。次の Linux オペレーティングシステムもサポートされています。

- RHEL 7.0
- CentOS 7.0
- Ubuntu 16.04

### ネットワーク設定要件の適合

VMware 仮想マシンを変換するには、Citrix Hypervisor Conversion Manager 仮想アプライアンスが VMware サーバーと接続できる物理ネットワークまたは VLAN に接続できる必要があります。(以下のセクションでは、このネットワークを「VMware ネットワーク」と呼びます)

VMware サーバーが、Citrix Hypervisor プール内のホストと異なる物理ネットワーク上にある場合、変換前にそのネットワークを Citrix Hypervisor に追加します。

### 既存のネットワーク構成のマッピング

Citrix Hypervisor Conversion Manager 仮想アプライアンスには、既存の VMware 仮想マシンを Citrix Hypervisor に変換した後に必要な手作業によるネットワーク設定の構成を少なくする機能があります。たとえば、Citrix Hypervisor Conversion Manager 仮想アプライアンスによって以下が行われます:

- VMware 仮想マシンの仮想 MAC アドレスを保持し、変換後の Citrix Hypervisor 仮想マシンで再利用します。仮想ネットワークアダプタに関連付けられた MAC アドレス（仮想 MAC アドレス）を保持すると、以下に役立ちます：
  - DHCP を使用する環境での IP アドレスの保持
  - ライセンスが仮想 MAC アドレスを参照するソフトウェアプログラム
- (仮想) ネットワークアダプタをマップします。Citrix Hypervisor Conversion Manager 仮想アプライアンスは、仮想マシンが変換された後、仮想ネットワークインターフェイスがそれに応じて接続されるように、VMware ネットワークを Citrix Hypervisor ネットワークにマッピングできます。

たとえば、VMware の「仮想ネットワーク 4」を Citrix Hypervisor の「ネットワーク 0」にマップした場合、変換後、「仮想ネットワーク 4」に接続する仮想アダプタを持つすべての VMware 仮想マシンが「ネットワーク 0」に接続されます。Citrix Hypervisor Conversion Manager 仮想アプライアンスは、ハイパーバイザーネットワーク設定を変換または移行しません。ウィザードは、提供されたマッピングに基づいて、変換された仮想マシンの仮想ネットワークインターフェイス接続のみを変更します。

**注:**

すべての VMware ネットワークを対応する Citrix Hypervisor ネットワークにマップする必要はありません。ただし、必要に応じて、新しい Citrix Hypervisor 構成で、仮想マシンが使用するネットワークを変更したり、ネットワークの数を減らしたり、集約したりすることができます。

これらの機能を最大限に活用するために、以下を実行することをお勧めします:

- Citrix Hypervisor をインストールする前に、適切なスイッチ上のネットワーク（ポート）にそのホストを接続します。
- 目的のネットワークが Citrix Hypervisor プールから参照できることを確認します。つまり、VMware クラスタと同じネットワークにアクセスできるスイッチポートに Citrix Hypervisor ホストを接続します。

Citrix Hypervisor ネットワークインターフェイスカードを VMware ホストのネットワークインターフェイスカードと同じネットワークに差し込むほうが簡単ですが、必須ではありません。ネットワークインターフェイスカードとネットワークの関係を変更する場合は、Citrix Hypervisor ネットワークインターフェイスカードを別の物理ネットワークに差し込むことができます。

### **Citrix Hypervisor Conversion Manager 仮想アプライアンスネットワーク設定要件の準備**

変換を実行するときには、VMware サーバーがあるネットワークへのネットワーク接続を作成する必要があります。この接続は、Citrix Hypervisor Conversion Manager 仮想アプライアンスが Citrix Hypervisor ホストと VMware サーバー間の変換トラフィックに使用します。

このネットワーク接続を作成するには、次の 2 つのタスクを実行する必要があります:

- Citrix Hypervisor Conversion Manager 仮想アプライアンスをインポートするときに、仮想ネットワークインターフェイスとして変換トラフィック用に追加したネットワークを指定します。指定は、インターフェイス 1 を構成することで行い、この指定でインターフェイス 1 がそのネットワークに接続します。
- 変換ウィザードを実行する前に、ネットワークに接続している VMware と Citrix Hypervisor を、変換した仮想マシンを実行する Citrix Hypervisor ホストに追加します。

デフォルトでは、Citrix Hypervisor Conversion Manager 仮想アプライアンスをインポートするときに、XenCenter が、ネットワーク 0 と NIC0 (eth0) に関連付けた仮想ネットワークインターフェイスを作成します。ただし、デフォルトでは、Citrix Hypervisor のセットアップは NIC0 を管理インターフェイス、Citrix Hypervisor の管理トラフィックに使用されるネットワークインターフェイスカードとして設定します。その結果、変換用にネットワークを追加するときに、NIC0 以外のネットワークインターフェイスカードを選択することもできます。別のネットワークを選択すると、トラフィック量の多いプールのパフォーマンスが向上する場合があります。管理インターフェイスについて詳しくは、「[ネットワーク](#)」を参照してください。

次にネットワークを追加するには **Citrix Hypervisor**:

1. XenCenter の [リソース] ペインで、Citrix Hypervisor Conversion Manager 仮想アプライアンスを実行するプールを選択します。
2. [ネットワーク] タブをクリックします。
3. [ネットワークの追加] をクリックします。
4. [種類の選択] ページで、[外部ネットワーク] を選択して [次へ] をクリックします。
5. [名前] ページで、ネットワークのわかりやすい名前（「VMware ネットワーク」など）と説明を入力します。
6. [インターフェイス] ページで以下を指定します：
  - **NIC**: ネットワークの作成に Citrix Hypervisor で使用するネットワークインターフェイスカード。VMware サーバーの物理ネットワークまたは論理ネットワークに接続されているネットワークインターフェイスカードを選択します。
  - **VLAN**: VMware ネットワークが VLAN である場合は、その VLAN の ID（または「タグ」）を入力します。
  - **MTU**: VMware ネットワークでジャンボフレームが使用されている場合は、MTU (Maximum Transmission Unit: 最大転送単位) の値を 1500 ~ 9216 で入力します。ジャンボフレームが使用されていない場合は、デフォルトの 1500 を使用します。

注:

[このネットワークを新規 VM に自動的に追加する] チェックボックスはオンにしないでください。

7. [完了] をクリックします。

記憶要件の適合

VMware 仮想マシンのバッチを変換する前に、記憶要件を検査します。変換した仮想マシンのディスクは、Citrix Hypervisor ストレージリポジトリに格納されます。

このストレージリポジトリには、そのプールで実行する変換済み仮想マシンの仮想ディスクをすべて格納するのに十分な容量が必要です。変換したマシンをスタンドアロンホストでしか実行しない場合は、変換した仮想ディスクの場所として、ローカルストレージまたは共有ストレージのいずれかを指定できます。変換したマシンをプールで実行する場合は、共有ストレージのみを指定できます。

ストレージリポジトリを作成するには：

1. XenCenter の [リソース] ペインで、Citrix Hypervisor Conversion Manager 仮想アプライアンスを実行するプールを選択します。
2. [ストレージ] タブをクリックします。
3. [新規ストレージリポジトリ] をクリックして、ウィザードの手順に従って処理を進めます。詳しくは、**F1** キーを押してオンラインヘルプを参照してください。

### Citrix Hypervisor の要件

このリリースの Citrix Hypervisor Conversion Manager で変換した仮想マシンは、以下のバージョンの Citrix Hypervisor で実行できます：

- XenServer 7.1 Cumulative Update 2
- XenServer 7.6
- Citrix Hypervisor 8.0
- Citrix Hypervisor 8.1

### VMware の要件

Citrix Hypervisor Conversion Manager 仮想アプライアンスは、以下のバージョンの VMware から VMware 仮想マシンを変換できます：

- vCenter Server 5.5.0、6.0.0、6.5.0
- vSphere 5.5.0、6.0.0、6.5.0
- ESXi 5.5.0、6.0.0、6.5.0

注：

Citrix Hypervisor Conversion Manager 仮想アプライアンスは、4 つ以上のディスクを持つ VMWare 仮想マシンを Citrix Hypervisor 仮想マシンに変換することはできません。VMWare 仮想マシンには、3 つ以下のディスクが必要です。

VMware 仮想マシンにもネットワークとストレージコントローラーが構成されている必要があります。

### 仮想アプライアンスをインポートする準備

仮想アプライアンスをインポートする前に、以下の事項を確認して、必要に応じて XenServer 環境を変更してください。

### 仮想アプライアンスのダウンロード

Citrix Hypervisor Conversion Manager 仮想アプライアンスは XVA フォーマットでパッケージ化されています。この仮想アプライアンスは、[Citrix Hypervisor 8.1 Premium Edition のページ](#)からダウンロードできます。ファイルをダウンロードするときに、このファイルをローカルコンピューター（通常は XenCenter がインストールされているコンピューターですが、必ずしもそうである必要はありません）のローカルハードドライブのフォルダーに保存します。.xva ファイルをハードドライブに置くと、XenCenter にインポートできるようになります。

#### 注:

Citrix Hypervisor Conversion Manager 仮想アプライアンスは、Citrix Hypervisor Premium Edition ユーザー、または Citrix Virtual Apps and Desktops 権限により Citrix Hypervisor にアクセスするユーザーが使用できます。Citrix Hypervisor ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。Citrix Hypervisor 8.1 のライセンスをアップグレードまたは購入するには、[シトリックス Web サイト] にアクセスしてください。

### 仮想アプライアンスの前提条件

Citrix Hypervisor Conversion Manager 仮想アプライアンスの最低要件:

- XenServer 7.1 Cumulative Update 2、XenServer 7.6、Citrix Hypervisor 8.0、または Citrix Hypervisor 8.1
- ディスクスペース: 30GB のディスクスペース
- メモリ: 6.5GB
- 仮想 CPU 割り当て: 1vCPU

### 仮想アプライアンスのインポートと構成

Citrix Hypervisor Conversion Manager 仮想アプライアンスは単一のインストール済み仮想マシンであり、Citrix Hypervisor ホスト上で動作するように設計されています。インポートする前に、「仮想アプライアンスの準備とインポート」というセクションの前提条件情報と考慮事項を確認してください。

### **Citrix Hypervisor** への仮想アプライアンスのインポート

Citrix Hypervisor Conversion Manager 仮想アプライアンスを、変換した仮想マシンを実行するプールまたはホストにインポートするには、XenCenter インポートウィザードを使用します:

1. XenCenter を開きます。インポート先のプールまたはホストを右クリックして [インポート] を選択します。
2. 参照して、仮想アプライアンスパッケージを検索します。
3. Citrix Hypervisor Conversion Manager 仮想アプライアンスを実行するプールまたはホームサーバーを選択します。

注:

ホームサーバーとは、プール内の仮想マシンにリソースを提供するホストを指します。可能な間、Citrix Hypervisor は他のホストを試行する前に、そのホストで仮想マシンを起動しようとします。ホストを選択した場合、Citrix Hypervisor Conversion Manager 仮想アプライアンスはこのホストをホームサーバーとして使用します。プールを選択した場合、仮想アプライアンスはそのプール内の最適なホストで自動的に起動します。

4. Citrix Hypervisor Conversion Manager 仮想アプライアンスの仮想ディスクを格納するストレージリポジトリを選択して、[インポート] をクリックします。ストレージリポジトリをプールに追加する場合は、「記憶要件の適合」というセクションを参照してください。ローカルストレージまたは共有ストレージのいずれかを選択できます。
5. 変換に使用するネットワーク (VMware サーバーと Citrix Hypervisor ホストを接続するネットワーク) が、インターフェイス 1 (「仮想 NIC 1」) が関連付けられているネットワークとして選択されていることを確認します。
  - 正しいネットワークがインターフェイス 1 の横に表示されない場合は、[ネットワーク] 列の一覧を使用して別のネットワークを選択します。
  - プールとは異なる物理ネットワークにある VMware ネットワークを追加していない場合は、以下を実行します:
    - a) ウィザードを終了します。
    - b) ネットワークをプールに追加します。
    - c) ウィザードを再実行します。

詳しくは、「にネットワークを追加するには **Citrix Hypervisor**」を参照してください。

警告:

顧客ネットワークに対して NICO を設定しないでください。NICO は「ホスト内部管理ネットワーク」にのみ割り当てます。

6. [インポート後に **VM** を起動する] チェックボックスがオンになっていることを確認して、[完了] をクリックします。仮想アプライアンスのインポート処理が開始されます。
7. `.xva` ファイルをインポートすると、Citrix Hypervisor Conversion Manager 仮想アプライアンスが XenCenter の [リソース] ペインに表示されます。

## Citrix Hypervisor Conversion Manager 仮想アプライアンスの構成

Citrix Hypervisor Conversion Manager 仮想アプライアンスを VMware 仮想マシンの変換に使用するには、インポートした後に構成する必要があります。XenCenter [コンソール] タブの指示に従います。

1. インポートした Citrix Hypervisor Conversion Manager 仮想アプライアンスの [コンソール] タブをクリックします。
2. ライセンス契約書の内容を確認して、同意する場合は「**yes**」と入力します。同意しない場合は、「**no**」と入力します。
3. Citrix Hypervisor Conversion Manager 仮想アプライアンスの新しいルートパスワードを入力して確認します。安全なパスワードを使用することをお勧めします。
4. Citrix Hypervisor Conversion Manager 仮想アプライアンスのホスト名を入力します。
5. 仮想アプライアンスのドメインサフィックスを入力します。たとえば、仮想アプライアンスの FQDN (Fully Qualified Domain Name: 完全修飾ドメイン名) が `citrix-migrate-vm.domain4.example.com` の場合は、「`domain4.example.com`」と入力します。
6. Citrix Hypervisor Conversion Manager 仮想アプライアンスの IP アドレスを DHCP から自動的に取得する場合は、「**y**」と入力します。特定の静的 IP アドレスを指定する場合は、「**n**」と入力して、仮想マシンの IP アドレス、サブネットマスク、およびゲートウェイを指定します。
7. ホスト名とネットワーク設定を確認し、プロンプトが表示されたら「**y**」と入力します。この手順で Citrix Hypervisor Conversion Manager 仮想アプライアンス構成プロセスが完了します。
8. アプライアンスを正常に構成すると、ログインプロンプトが表示されます。ログイン資格情報を入力して Enter キーを押し、Citrix Hypervisor Conversion Manager 仮想アプライアンスにログインします。

## VMware 仮想マシンの変換

VMware 仮想マシンを変換すると、マシンは、Citrix Hypervisor Conversion Manager 仮想アプライアンスを実行している Citrix Hypervisor プールまたはスタンドアロンホストにインポートされます。変換した仮想マシンには、元の VMware の仮想プロセッサと仮想メモリの設定が残ります。

変換手順を開始する前に、以下の条件が満たされていることを確認してください：

- Citrix Hypervisor プール（またはスタンドアロンホスト）の資格情報を持っていること。ルートアカウントの資格情報、またはプール管理者の役割が構成されている役割ベースのアクセス制御 (RBAC) アカウントを使用できます。
- 変換する仮想マシンを含む VMware サーバーの資格情報を持っていること。変換手順では、Citrix Hypervisor Conversion Manager コンソールとこの VMware サーバーを接続する必要があります。
- 変換する VMware 仮想マシンの電源がオフであること。
- 変換する VMware 仮想マシンに、ネットワークとストレージコントローラーが構成されていること。

- 変換した仮想マシンを実行する Citrix Hypervisor プール（またはホスト）にストレージリポジトリが接続されていること。ストレージリポジトリには、変換した仮想ディスクを格納するための十分な領域が必要です。
- 新しく変換した仮想マシンをプールで実行する場合、そのストレージリポジトリは共有ストレージである必要があります。ただし、変換した仮想マシンを（プールではなく）1台のスタンドアロンのホストで実行する場合は、ローカルストレージを使用できます。
- 変換する仮想マシンの仮想ディスクのサイズが 2TiB 未満であること。
- Citrix Hypervisor プール（またはホスト）に変換した仮想マシンが使用するネットワークが含まれていること。

**VMware** 仮想マシンを、**Citrix Hypervisor** 環境で実行できる仮想マシンに変換するには以下を行います：

1. 仮想アプライアンスがインストールされ、仮想マシンをインポートする Citrix Hypervisor サーバーまたはプールで実行されていることを確認します。
2. XenCenter で、[プール] > [**Conversion Manager**] に移動します。  
[変換の管理] ウィンドウが開きます。ウィザードが仮想アプライアンスに接続するまで待ちます。
3. [新しい変換] をクリックします。
4. 新しい変換ウィザードで、VMware サーバーの資格情報を入力します：
  - サーバー。Citrix Hypervisor に変換する仮想マシンを保持している VMware サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。
  - ユーザー名。この VMware サーバーにアクセスするためのユーザー名を入力します。VMware の管理者アカウントまたは Root ロールが必要です。
  - パスワード。[ユーザー名] ボックスで指定したユーザーアカウントのパスワードを入力します。[次へ] をクリックします。XenCenter が VMware サーバーに接続します。
5. [仮想マシン] ページで、VMware サーバーでホストされている仮想マシンのリストから、変換する仮想マシンを選択します。[次へ] をクリックします。
6. [ストレージ] ページで、変換中に使用するストレージリポジトリを選択します。このストレージリポジトリで、作成する仮想マシンと仮想ディスクが永久に保存されます。  
このタブは、変換された仮想マシンの仮想ディスクが消費する使用可能なストレージの割合を示します。
7. [ネットワークング] ページで、リストされている各 VMware ネットワークについて、マッピングする Citrix Hypervisor ネットワークを選択します。仮想 MAC アドレスを保存するかどうかを選択できます。[次へ] をクリックします。
8. 変換プロセス用に構成したオプションを確認します。オプションを変更するには、[戻る] をクリックします。表示されている構成で続行するには、[完了] をクリックします。  
変換プロセスが開始されます。ESXi または vSphere からの変換は、仮想ディスクのサイズによっては数分かかる場合があります。

[変換の管理] ウィンドウには、進行中の変換と完了した変換が表示されます。

## 変換後の手順

変換後、XenCenter で新しく変換した仮想マシンで以下の手順を実行します：

### Windows マシンの場合：

1. Windows 仮想マシンでは、Microsoft のライセンスモデルによっては、仮想マシンの Windows ライセンスを再度有効にする必要があります。この再有効化は、Windows オペレーティングシステムが変換をハードウェアの変更として認識するために実行されます。
2. Windows 仮想マシンでは Citrix VM Tools をインストールすることで I/O が高速化され、ディスクとネットワークのパフォーマンスが向上します。また、仮想マシンを正しくシャットダウン/再起動/一時停止する機能やライブマイグレーションなど、Citrix VM Tools をインストールしないと有効にならない機能もあります。

Citrix VM Tools がインストールされていない仮想マシンを使用した場合、[全般] ペインの [全般] タブに Citrix VM Tools がインストールされていないというメッセージが表示されます。Windows 仮想マシンでは、このテキストをクリックして仮想マシンコンソールに切り替え、Citrix VM Tools ISO イメージをダウンロードして、Citrix VM Tools のインストールウィザードを起動することができます。

#### 注：

仮想マシンが完全にサポートされる構成にするには、各仮想マシンに Citrix VM Tools をインストールする必要があります。Citrix VM Tools がなくても仮想マシンは機能しますが、パフォーマンスに影響が出る可能性があります。

### Linux マシンでの VNC の有効化

Linux 仮想マシンでは、VNC サーバーを構成します。詳しくは、「[Linux 仮想マシンの VNC 設定](#)」を参照してください。

#### 注：

VNC パスワードは、6 文字以上にする必要があります。

### その他の変換タスク

[変換の管理] ウィンドウを使用すると、仮想マシンの変換に関連する他のタスクを実行できます。その他のタスクの例には、ジョブのクリア、ジョブの結果内容の保存、ジョブの再試行、ジョブのキャンセル、ログファイルの表示などがあります。

すべてのジョブをクリアするには：

1. [すべてクリア] を選択します。
2. このアクションの確認を求められたら、[はい] をクリックして続行します。

ジョブの結果内容を保存するには：

1. [すべてをエクスポート] をクリックします。
2. CSV ファイルを保存する場所を指定します。
3. [保存] をクリックします。

ジョブを再試行するには:

1. リストからジョブを選択します。
2. [再試行] をクリックします。

注:

[再試行] は、失敗したジョブまたはキャンセルされたジョブに対してのみ使用可能になります。

ジョブをキャンセルするには:

1. リストからジョブを選択します。
2. [キャンセル] をクリックします。

注:

[ジョブのキャンセル] は、待機中のジョブまたは実行中のジョブに対してのみ使用可能になります。

単一のジョブの変換ログファイルを保存するには:

1. リストからジョブを選択します。
2. ログメニューから、[選択したログを取得] をクリックします。
3. ログファイルを保存する場所を指定します。

すべてのジョブの変換ログファイルを保存するには:

1. ログメニューから、[すべてのログを取得] をクリックします。
2. ログファイルを保存する場所を指定します。

変換詳細を表示するには:

1. リストからジョブを選択します。  
情報は [詳細] パネルに表示されます。

## 変換のトラブルシューティング

このセクションでは、変換プロセスと変換した仮想マシンのトラブルシューティングについての情報を提供します。

### 変換した仮想マシンの起動に関する問題

通常、変換はスムーズに実行され、Citrix Hypervisor Conversion Manager 仮想アプライアンスによって問題なく仮想マシンが変換されます。ただし、まれに、変換した仮想マシンを開こうとしたときにエラーが発生することがあります。以下のセクションでは、エラーやその他の問題を解決するための手引きをいくつか提供します。

停止コード **0x0000007B** で **Windows** がブルースクリーンになる

この停止コードは、Citrix Hypervisor Conversion Manager 仮想アプライアンスが、Citrix Hypervisor の初回起動にとって重要な Windows デバイスを構成できなかったことを示します。より詳しい手引きをご希望の場合は、ログを保存して Citrix テクニカルサポートにお送りください。

### Windows 製品のライセンス認証

ライセンスモデルによっては、Windows 仮想マシンを起動しようとする、システムのライセンス認証に関するエラーメッセージが表示されることがあります。

### Windows 仮想マシンのネットワーク設定が失われる

ESXi サーバーから Citrix Hypervisor に Windows 仮想マシンをインポートした場合、IPv4/IPv6 ネットワークの設定が失われることがあります。ネットワーク設定を保持するには、変換を完了した後に IPv4/IPv6 設定を再構成します。

### VMware SCSI ディスクを起動できない

VMware 仮想マシンを SCSI ディスクから起動しても、IDE ハードディスクが構成されていた場合、仮想マシンが起動しないことがあります (Citrix Hypervisor に変換した場合)。この問題は、移行プロセスで IDE ハードディスクが SCSI ディスクより小さいデバイス番号に割り当てられることが原因で発生します。しかし、Citrix Hypervisor はデバイス 0 に割り当てられているハードディスクから起動します。この問題を解決するには、XenCenter の仮想ディスクの場所を再調整して、仮想マシンがオペレーティングシステムを含む仮想ディスクから再起動するようにします。

オペレーティングシステムを含む仮想ディスクの場所を変更するには:

1. XenCenter [リソース] ペインで電源オフ状態のゲスト仮想マシンを選択します。
2. [ストレージ] タブを選択します。
3. [仮想ディスク] リストで、オペレーティングシステムを含む仮想ディスクを選択して、[プロパティ] をクリックします。
4. 仮想ディスクの [プロパティ] ダイアログボックスで、[vm\_name] タブをクリックしてデバイスオプションを表示します。
5. [デバイスの場所] 一覧で、[0] を選択して、[OK] をクリックします。

### 変換中の問題

仮想マシンの変換中に問題またはエラーが発生した場合は、VMware 仮想マシンを OVF パッケージとしてエクスポートしてみてください。VMware 仮想マシンを OVF パッケージとしてエクスポートできない場合、Conversion Manager はこの仮想マシンを変換できません。仮想マシンを OVF パッケージとしてエクスポートしようとしたとき

に表示されるエラーメッセージを使用して、VMware 仮想マシンに関する問題のトラブルシューティングと修正を行います。たとえば、仮想マシンを変換または OVF パッケージとしてエクスポートする前に、ネットワークまたはストレージコントローラーを構成する必要がある場合があります。VMware 仮想マシンのトラブルシューティングの詳細については、[VMware ドキュメント](#)を参照してください。

Linux 仮想マシンの変換で問題が発生した場合は、変換した仮想マシンを削除して、Citrix Hypervisor Conversion Manager 仮想アプライアンスを再起動してから、再試行してください。

失敗した変換のログは Citrix Hypervisor Conversion Manager 仮想アプライアンスに保存され、[変換の管理] ウィンドウで [すべてのログを取得] をクリックして取得できます。シトリックスサポートに問題を報告する場合、トラブルシューティングのために変換ログファイルと、完全なサーバステータスレポートを提供することをお勧めします。詳しくは、「[サーバーの状態レポートの作成](#)」を参照してください。

## vSwitch と Controller

January 20, 2020

vSwitch は、Citrix Hypervisor の仮想ネットワーク環境に可視性、セキュリティ、コントロールを提供します。vSwitch は以下のコンポーネントで構成されています：

- 各 Citrix Hypervisor 上で動作する、仮想化に対応したスイッチ (vSwitch)。
- 単一の vSwitch の外観を実現するために、個々の vSwitch の動作を管理および調整する集中管理型サーバー (vSwitch Controller)。

vSwitch Controller では、セキュリティポリシーを使用した VM へのトラフィック出入力の詳細なフロー制御がサポートされています。仮想ネットワーク環境内のすべてのトラフィックの動作とパフォーマンスの詳細を表示します。vSwitch は、環境内の IT 管理を大幅に簡素化します。vSwitch を使用する場合、VM の構成と統計は、ある物理ホストから別の物理ホストに移行しても VM にバインドされたままになります。

注：

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

### 導入

#### 要件

- XenCenter で構成された 1 つ以上の Citrix Hypervisor のリソースプール
- vSwitch Controller 仮想アプライアンスの展開に必要なプール内の容量

Controller を実行するホストの要件については、次のセクションで説明します。

## プロセス

vSwitch Controller のセットアップには、以下のタスクが含まれます：

1. vSwitch Controller 仮想アプライアンスの展開
2. vSwitch Controller へのアクセス
3. vSwitch Controller の IP アドレスの構成
4. リソースプールの追加
5. 高可用性の構成（オプション）

注：

このバージョンの vSwitch Controller は、Citrix Hypervisor のサポートされているすべてのバージョンと互換性があります。

## vSwitch Controller 仮想アプライアンスの展開

vSwitch Controller を実行する Citrix Hypervisor サーバーは、以下の最小要件を満たしている必要があります：

- 2つの CPU
- 2GB の DRAM
- 16GB のディスク

vSwitch Controller アプライアンスの最小許容 VM 構成と、インポート時のデフォルト構成は以下のとおりです：

- 2つの vCPU
- 2GB の DRAM
- 16GB のディスク

この構成では、最大 16 個の Citrix Hypervisor サーバーのプールと vSwitch Controller に接続された 256 個の仮想ネットワークインターフェイス (VIF) がサポートされます。より大きなプール（サポートされる全プール合計上限数は 64 個の Citrix Hypervisor サーバーと 1024 個の VIF）の場合、VM 構成を以下のように変更します：

- 4つの vCPU
- 4GB の DRAM
- 16GB のディスク

注：

- アプライアンスのディスクがネットワークストレージに格納され、基盤となる Citrix Hypervisor ホストのネットワークトラフィックを制御している場合、ロードされた状態でデッドロックが発生し、プール全体のネットワークトラフィックが停止することがあります。これを防ぐには、DVSC ディスクをローカルストレージに格納するか、その DVSC によって制御されていない別のプールにアプライアンスを移動することを強くお勧めします。
- プールごとに、プールサイズを制限してホストを 16 個以下にする必要があります。

- vSwitch Controller は、Citrix Hypervisor PVS アクセラレータ機能を使用するプールではサポートされていません。

vSwitch Controller VM は、管理するリソースプール内で実行できます。通常、この構成は、vSwitch Controller VM が別々に動作しているかのように動作します。ただし、Controller の移行または再起動時に、すべての vSwitch を接続するまで少し時間がかかる場合があります（最大 2 分）。この時間は、個々の vSwitch による制御接続の接続方法が異なるために発生します。

vSwitch Controller をインストールするには、指定の仮想アプライアンス VM イメージを Citrix Hypervisor のリソースプールにインポートします。インポート中に、インポートする VM の VIF を、制御したいホストまたはプールに到達できるネットワークに接続します。

VM をインポートした後、VM を起動して DVS の構成プロセスを開始します。

### vSwitch Controller のコマンドラインインターフェイスへのアクセス

vSwitch Controller のコマンドラインインターフェイス（CLI）には、XenCenter 内部から、または SSH クライアントを使用してリモートからアクセスできます。vSwitch Controller VM が最初に起動すると、XenCenter 内のコンソールには、Controller へのリモートアクセスに使用する IP アドレスが表示されます。VM が IP アドレスを受信しなかった場合、テキストコンソールには、CLI を介してアドレスを割り当てる必要がある旨が表示されます。いずれの場合でも、テキストコンソールには、XenCenter コンソールでローカルに CLI にログインするためのログインプロンプトが表示されます。使用可能な CLI コマンドについての完全なドキュメントは、「[コマンドラインインターフェイス](#)」にあります。

### vSwitch Controller GUI へのアクセス

Web ブラウザー、またはローカルの XenCenter コンソールを使用して、vSwitch Controller GUI にリモートアクセスします。

#### 重要:

vSwitch Controller に初めてログインするときは、コンソールではなく GUI を使用してログインすることをお勧めします。vSwitch Controller の GUI では、パスワードをデフォルト値から変更するよう求められます。環境のセキュリティを保護するために、強力な管理者パスワードを設定してください。

vSwitch Controller VM が起動すると、XenCenter 内のコンソールには、リモートで GUI にアクセスするための IP アドレスが表示されます。VM が IP アドレスを受信しなかった場合、IP アドレスが割り当てられるまでは GUI をローカルやリモートで使用できません。コンソールには、コマンドラインインターフェイスを使用してローカルで IP アドレスを設定する方法が表示されます。Controller VM に IP アドレスが割り当てられたら、XenCenter コンソール内でローカルに GUI にアクセスできます。

#### 注:

VNC が無効の場合、vSwitch Controller GUI には Web ブラウザーからのみアクセスできます。

## vSwitch Controller GUI へのリモートアクセス

vSwitch Controller インターフェイスにリモートからアクセスするには:

1. Web ブラウザーを開き、次の URL を入力します。サーバーには Controller VM インターフェイスの IP アドレス、またはホスト名を入力します: `https://server-name:443/`
2. ユーザー名とパスワードを入力し、**[Login]** をクリックします。デフォルトの管理者ユーザー名とパスワードはそれぞれ **admin** と **admin** です。
3. 初めて GUI でログインする場合、パスワードをデフォルト値から変更するように求められます。環境のセキュリティを保護するために、強力な管理者パスワードを設定してください。

注:

デフォルトでは、vSwitch Controller の Web サーバーは自己署名証明書を使用します。証明書により、GUI に接続する際に Web ブラウザーにセキュリティエラーが表示されることがあります。エラーを無視して Web ブラウザーに証明書をインストールしても問題ありません。

次の Web ブラウザーがサポートされています: Firefox 3.x、Safari 4.x、Internet Explorer 7 および 8。同様の機能を備えた最新の Web ブラウザー (Opera や Google Chrome など) はサポートされていませんが、動作する可能性はあります。Internet Explorer 9 はメモリとリソースのリークに関する既知の問題を解決しています。ただし、完全なテストを受けたわけではありません。

## vSwitch Controller の IP アドレスの構成

vSwitch Controller は初めて起動するときに、DHCP を使用して IP アドレスを取得しようとします。ただし、静的 IP アドレスを割り当てることをお勧めします。DHCP が構成されている場合、リソースプールはフェールセーフモードに設定できません。

静的 IP アドレスを割り当てるには:

1. vSwitch Controller インターフェイスにローカルからアクセスします。
2. **[Settings]** タブを選択してから、サイドパネルの **[IP Configuration]** を選択します。現在の設定が表示されます。
3. **[Modify Configuration]** を選択し、新しい IP アドレス情報を指定して、**[Make Changes]** を選択します。
4. vSwitch Controller 仮想アプライアンスを再起動します。

## リソースプールの追加

リソースプールを追加することで、vSwitch Controller がそのプール内の全 Citrix Hypervisor サーバーの管理を自動的に開始できるようになります。

リソースプールを追加するには:

1. **[Visibility & Control]** で **[Status]** タブを開き、リソースツリー内の **[All Resource Pools]** を選択して、すべてのリソースプールの **[Status]** ページを開きます。
2. **[Add Resource Pool]** をクリックします。別のリソースプールを追加するための適切なライセンスがない場合、エラーメッセージが表示されます。
3. **[Pool Master Server (DNS/IP)]** ボックスに、マスターの Citrix Hypervisor サーバーの IP アドレスまたは DNS 名を入力します。
4. サーバーへの管理アクセス用のユーザー名とパスワードを入力します。

このユーザーは、リソースプール内のすべての管理機能を使用できる必要があります。このアカウントの機能が制限されている場合、vSwitch Controller はプールを適切に管理できません。

通常、このアカウントのユーザー名は `root` になっていますが、Citrix Hypervisor プラットフォームの RBAC 機能を使用している場合は異なる名前になっている場合があります。
5. このリソースプールについての既存の vSwitch Controller 構成を上書きする場合のみ、**[Steal]** チェックボックスをオンにします。
6. **[Connect]** をクリックします。

vSwitch Controller は指定されたユーザー名とパスワードを使用して、XAPI プロトコルでプールマスターサーバーと通信します。通信が確立されると、関連付けられたすべてのリソースとともに、新しいリソースプールがリソースツリーに追加されます。vSwitch Controller VM がプールマスターと通信できない場合は、失敗を示すエラーメッセージが表示されます。

注:

Citrix Hypervisor のリソースプールと通信する vSwitch Controller の場合、その Citrix Hypervisor のリソースプールでは後方互換性モードを使用する必要があります。このモードがデフォルトです。この設定は、XenCenter の **[Pool Properties]** ページで指定できます。詳しくは、[XenCenter ドキュメント](#) を参照してください。

## 高可用性の構成

Citrix Hypervisor サーバーがアクティブな vSwitch Controller に常に到達できるようにするには、vSwitch Controller VM 用に Citrix Hypervisor の高可用性を使用します。Citrix Hypervisor で高可用性を有効にする方法について詳しくは、「[高可用性](#)」を参照してください。vSwitch Controller が継続して動作することは、すべての VM のネットワーク操作にとってきわめて重要です。vSwitch Controller VM の高可用性を確保するには、その `restart-priority` を 1 に、`ha-always-run` を true に設定します。

## vSwitch の管理

March 12, 2020

vSwitch Controller GUI により、以下のようなさまざまな管理タスクを実行できます：

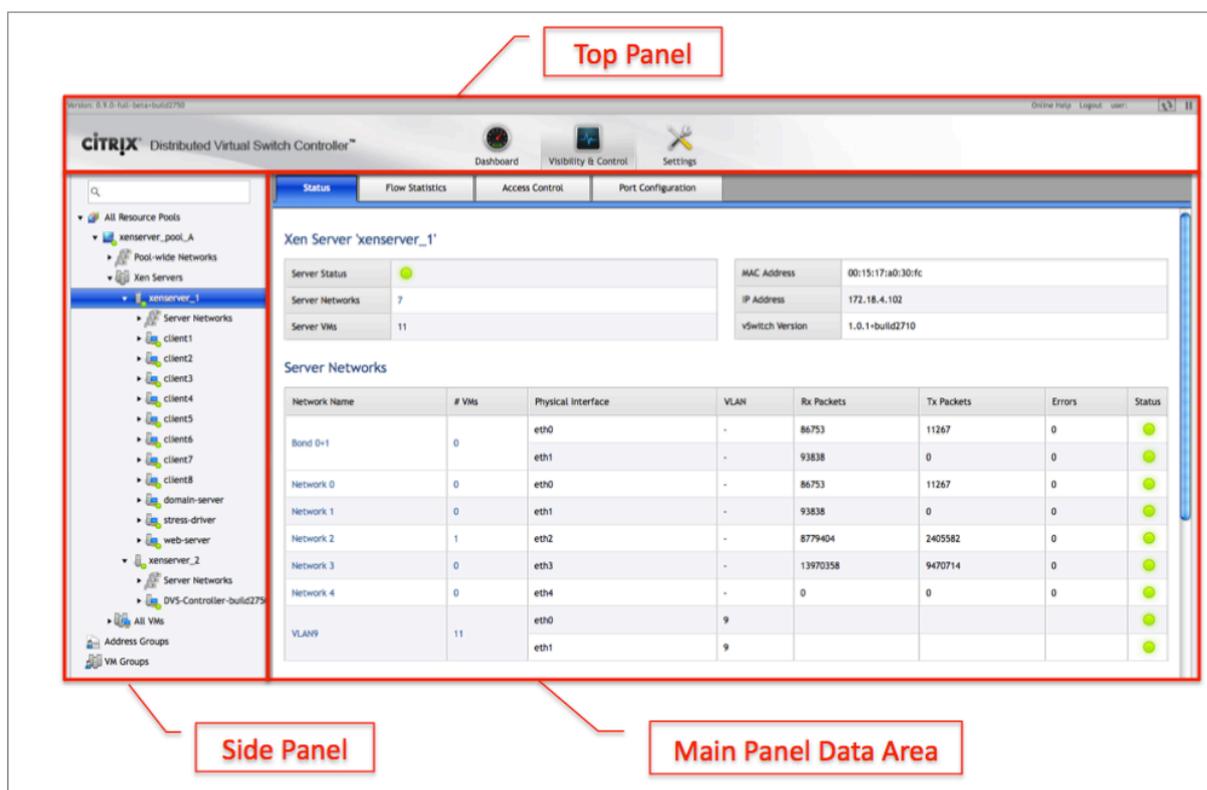
- 仮想ネットワーク内の要素のステータスおよびフローの統計情報を表示する
- VM アクセス制御、QoS（サービス品質）、およびトラフィックミラーリングポリシーを設定する
- vSwitch Controller 仮想アプライアンスの構成を変更する

注：

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

### インターフェイスの概要

vSwitch Controller GUI には、3 つの異なるパネルがあります。これらのパネルを次の図に示します。



### トップパネル

トップパネルは GUI を使用しているときは常に表示され、これにはステータスバーとメインナビゲーションアイコンのセットが表示されています。

## ステータスバー

vSwitch Controller ウィンドウの上部にある灰色のステータスバーには、以下の情報と機能が含まれています（左から右）:

- **Version:** 現在の vSwitch Controller のバージョン。
- **Online Help:** クリックすると、Controller ウィンドウ上部のオンラインヘルプ領域を表示または閉じます。
- **Logout:** クリックすると、vSwitch Controller GUI からログアウトします。
- **User:** 現在ログインしているユーザーのユーザー名を表示します。
- **Refresh アイコン:** クリックすると、ページ上の情報を更新します。
- **Play/Pause:** クリックすると、GUI の背景の更新により画面上のデータを自動的に更新する/しないを切り替えます。Play モードでは、表示されるデータは 15 秒ごとに自動的に更新されます。Pause モードでは、ほとんどのデータは更新されません。ただし、リソースツリーなどいくつかの要素は更新されます。Pause モードでは、ボタンの後ろにあるステータスバーの背景がオレンジ色に変わり、ステータスバーに「データ更新の一時停止」インジケーターが表示されます。

## 上部のアイコン

上部のアイコンをクリックすると、GUI 内の主な機能にアクセスできます。

- **Dashboard:** ネットワークと管理イベントに関する概要統計や情報を表示します。「ダッシュボードでのネットワークステータスの監視」を参照してください。
- **Visitility and Control:** 仮想ネットワークにおける、ネットワークのステータスと統計を表示、または、アクセス制御、QoS、トラフィックミラーリングポリシーを構成します。「[仮想ネットワークの可視性と制御](#)」を参照してください。
- **Settings:** vSwitch Controller の保守と管理の機能を実行します。「[vSwitch Controller の管理と保守](#)」を参照してください。

## サイドパネル

サイドパネルは [Visitility and Control] セクションと [Settings] セクションでのみ使用できます。

[Visitility and Control] セクションのサイドパネルには、仮想ネットワーク環境内のネットワーク要素の参照に使用できるリソースツリーが含まれています。XenCenter 内のリソースツリーと同様、要素は階層で整理され、これによりシステム内の要素を簡単に参照できます。リソースツリーのセクションを展開するには、ノードのテキストの横にある横向きの矢印をクリックします。展開されたノードには下向きの矢印が表示されます。この矢印をクリックすると折りたたむことができます。

リソースツリーから要素を選択すると、メインパネルにツリー内のノードのステータスと構成データが表示されます。たとえば、リソースツリーから VM を選択して [Visitility and Control] セクションの [Status] を選択した場合、メインパネルには選択した VM に関するステータス情報が表示されます。

リソースツリーでは検索を行うことができます。検索文字列に基づいて内容をフィルタリングするには、検索フィールドにテキストを入力し **Enter** キーを押します。検索をクリアするには **[X]** 記号をクリックします。検索ではワイルドカード文字（1つまたは複数の文字の場合は\*、1文字のみの場合は?）を使用できます。ワイルドカードを使用しない場合、検索文字列の先頭と末尾にワイルドカード文字「\*」が付けられた部分文字列として検索が実行されます。たとえば、「Lab」で検索すると、「Laboratory-1」や「New-Lab-5」などのように、名前に「Lab」が含まれているすべての項目が検索されます。

[Settings] セクションのサイドパネルには、vSwitch Controller 構成の各領域を選択するためのアイコンがあり、ユーザーはそこから表示または変更を行うことができます。

## リソースツリーの使用

リソースツリーの最上位レベルでは、以下の項目が表示されます：

- **All Resource Pools:** 使用可能なすべてのリソースプールのリスト。このリストには、各リソースプールの一部であるすべての Citrix Hypervisor サーバー、ネットワーク、VM、および VIF を検索するためのトップレベルのリソースが表示されています。
- **Address Groups:** IP アドレスとサブネット範囲の名前付きセット。これらのグループは、以下の目的で使用されます：
  - アクセス制御セクションで規則の適用を制限する
  - **[Flow Statistics]** セクションのクエリの範囲を制限する
- **VM Groups:** 特定の VM コレクションのステータスおよびフローの統計を簡略化して表示するための VM の名前付きセット。

リソースツリーでリソースプールを展開すると、以下の項目が表示されます：

- **Pool-wide networks:** このリストにはリソースプール内のすべてのネットワークが表示されます。これは XenCenter の [Network] タブに表示されるリストに似ています。このリストを展開して個々のネットワークを表示したり、ネットワークを展開してそのネットワーク上の VM を表示したり、VM を展開してそのネットワーク上の VIF を表示したりすることができます。
- **Citrix Hypervisor サーバー:** このリストは、XenCenter のサーバー階層に似ています。このリストを展開してプール内のすべてのサーバーを表示、単一のサーバーエントリを展開してサーバーに関連付けられたネットワーク、VM、VIF を表示できます。サーバーネットワークのリストは、XenCenter のサーバーをクリックして [Network] タブを選択したときに表示されるリストに似ています。
- **All VMs:** このリストには、VM が単一のサーバー用に構成されているかどうかにかかわらず、リソースプール内のすべての VM が表示されます。リストを展開して個々の VM を表示したり、VM を展開して VIF を表示したりすることができます。

ほとんどのノードでは、ノードのコンテキストメニューを右クリックしてリソースツリー内の項目を簡単に追加、変更、削除できます。

## 色分けされたアイコン

リソースツリーの色分けされたアイコンは、トップレベルの [All Resource Pools] ノードの下にあるツリーノードのステータスを示します。XenCenter と同様、これらの色分けは、各プールマスタから XAPI を経由して取得したデータに基づいています。ノードのステータスが変更されたとき、アイコンは以下のように更新されます：

- 緑色：緑色のアイコンは、そのリソースがネットワーク上でアクティブであり、vSwitch Controller によって適切に管理されていることを示しています。
- 赤色：[Resource Pool] ノードの場合、赤色のアイコンは、プールマスタに XAPI 接続を確立できないことを示しています。[Resource Pool] ノードが緑色の場合、その下のノードの赤色のアイコンは、その要素がネットワーク上で現在アクティブではないことを示しています。たとえば、要素の電源が切られているか、または要素が切断されています。
- オレンジ色：オレンジ色のアイコンは、ノードまたはその子ノードのいずれかが正しく接続されていない、または管理されていないことを示しています。関連リソースのステータスページに、問題を説明したエラーメッセージが表示されます。

ノードの [Status] ページには、ツリーメニュー項目のカラーコードも表示されます。カラーコードとステータス情報について詳しくは、「[vSwitch Controller の問題のトラブルシューティング](#)」を参照してください。

#### メインパネルのデータ領域

メインパネルのデータ領域には、ステータス情報、統計情報、構成設定が表示されます。

- **Dashboard**：サイドメニューはなく、メインパネルのデータ領域がトップパネルの下の全領域を占めています。ダッシュボードのメインパネルには、vSwitch Controller により管理されるすべての仮想ネットワークの概要が表示されます。
- **Visibility and Control**：メインパネルがトップパネルの下のウィンドウの右側を占めています。このパネルの上部には、以下の主要な可視性と制御の機能に対応するタブがあります：
  - **Status**：選択したリソースツリーノードの詳細なステータス情報が表示されます。
  - **Flow Statistics**：選択したノードのネットワークアクティビティに関するグラフとデータが表示されます。
  - **Access Control**：選択したノードのアクセス制御ポリシーを設定します。
  - **Port Configuration**：選択したノードの QoS（サービス品質）とトラフィックミラーリングポリシーを設定します。
- **Settings**：メインパネルがトップパネルの下のウィンドウの右側を占めています。設定のメインパネルには、サイドパネルで選択したサブセクションに基づいて vSwitch Controller の設定を表示または構成するための詳細が表示されます。

[Visibility and Control] セクションでは、メインパネルに表示されるデータが変更されると、階層レベルと、サイドパネルで選択した特定の項目が反映されます。

たとえば、サイドパネルでリソースプールを選択して [Access Control] タブをクリックすると、メインパネルに以下の情報が表示されます：

- グローバルアクセス制御セキュリティポリシー

- 選択したリソースプールのポリシー

サイドパネルから仮想ネットワークインターフェイス (VIF) を選択して [Access Control] タブをクリックすると、メインパネルが表示されます:

- グローバルアクセス制御セキュリティポリシー
- VIF を含むリソースプールのポリシー
- VIF を含む VM のポリシー
- 選択した VIF のポリシー

### ダッシュボードでのネットワークステータスの監視

ダッシュボードには、仮想ネットワーク環境内のイベントに関する概要統計と情報が表示されます。ダッシュボードを表示するには、vSwitch Controller インターフェイスの上部にある [**Dashboard**] アイコンをクリックします。ダッシュボードは、このセクションで説明する領域に分かれています。情報は数秒ごとに自動的に更新されます。

### サーバー統計

このセクションでは、vSwitch Controller に関する、以下の一般的な情報を示します。

- Up Time: vSwitch Controller が最後に起動されてから今に至るまでの時間。
- CPU Load: vSwitch Controller 仮想アプライアンスの現在の CPU 使用率。

### ネットワーク統計

このセクションでは、ネットワーク要素 (リソースプール、Citrix Hypervisor サーバー、ネットワーク、VM) のイベントリを示します。以下の各カテゴリがあります:

- Managed: XAPI に従って実行状態にあり、現在 vSwitch Controller により管理されているこのタイプの要素の数。
- Active: XAPI に従って実行状態にあるこのタイプの要素の数。管理対象と非管理対象の要素が含まれます。
- Total: XAPI 経由で存在することがわかっている、このタイプ (アクティブまたは非アクティブ) の要素の数。

システムが正しく構成されており正常に動作している場合、管理対象の数とアクティブの数は同じです。Total 数は、常に管理対象およびアクティブの数と同数以上になります。電源がオフになっているコンポーネントは、Controller の管理対象として表示されません。

### 最近のネットワークイベント

このセクションでは、vSwitch Controller が最後に再起動されてから管理対象の仮想ネットワーク内で発生した最新のイベントを示します。右のスクロールバーを使用してリストをスクロールします。最新のイベントがリストの最初に表示されます。時間が経つと、古いイベントがリストから削除されます。

ネットワークイベントごとに、以下の情報が報告されます：

- **Priority:** イベントの相対的重要度。
- **Date/Time:** イベントが発生した日時。
- **Event:** イベントの説明。イベントの説明にあるハイパーリンクをクリックすると、イベントに記載されているネットワーク要素の [Visibility and Control Status] ページにアクセスできます。

より永続的に記録するために、ネットワークイベントを syslog サーバーにエクスポートできます。詳しくは、「[Syslog ファイルのエクスポート](#)」を参照してください。

#### 最近の管理イベント

このセクションでは、vSwitch Controller 内で発生したイベントを示します。このイベントは、多くの場合 GUI 内で管理者が設定を変更したことが原因で発生します。右のスクロールバーを使用してリストをスクロールします。最新のイベントがリストの最初に表示されます。時間が経つと、古いイベントがリストから削除されます。

管理イベントごとに、以下の情報が報告されます：

- **Priority:** イベントの相対的重要度。
- **Date/Time:** イベントが発生した日時。
- **Event:** イベントの説明。イベントの説明にあるハイパーリンクをクリックすると、イベントに記載されているネットワーク要素の [Visibility and Control Status] ページにアクセスできます。

より永続的に記録するために、ネットワークイベントを syslog サーバーにエクスポートできます。詳しくは、「[Syslog ファイルのエクスポート](#)」を参照してください。

#### スループット、フロー、ビットレートのグラフ

これらのグラフには、最もアクティブな VM とプロトコルの動作に関する情報が表示されます。

グラフには、以下の情報が表示されます：

- 過去1時間のスループット（ビット/秒）の集計
- 過去1時間のパケットレート（パケット/秒）の集計
- 過去1時間の接続レート（フロー/秒）の集計

#### 仮想ネットワークの可視性と制御

March 12, 2020

[Visibility and Control] セクションでは、ネットワークの動作を監視し、ネットワークポリシーを設定できます。このページにアクセスするには、vSwitch Controller インターフェイスの上部にある **[Visibility and Control]** アイコンを選択します。

注:

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

### 状態の表示

**[Status]** タブでは、リソースツリーで選択したノードに関する詳細な情報がテーブル形式で表示されます。表示される情報のタイプは、選択したノードによって異なります。ほとんどの個別のテーブルエントリはリンクです。これらのリンクをクリックすると、そのテーブルエントリに適用されるステータスページを表示できます。

すべてのバイト数とエラー数は、Citrix Hypervisor サーバーの再起動時、または VM の再起動時や移行時にも加算され続けます。カラーコードは、サイドパネルのカラーコードと同じ規則に従います。「[色分けされたアイコン](#)」を参照してください。

### グローバルレベル

グローバルレベルでは、すべてのリソースプールを表示したテーブルが **[Status]** ページに表示され、以下の情報を確認できます:

- **Resource pool:** リソースプールの名前。
- **# Servers:** プール内のサーバーの数。
- **# Networks:** プール内のネットワークの数。
- **# VMs:** プール内の VM の数。
- **\Status:** 現在のプールの状態を示す色分けされたアイコン

行の右側にある歯車のアイコンをクリックすると、リソースプールを変更するオプションが表示されます。

このページでは、ポート構成ポリシーに使用できるターゲット VLAN を指定することもできます。「[ポート構成ポリシーの設定](#)」を参照してください。

### リソースプールレベル

選択したリソースプールの **[Status]** ページには、以下の情報が表示されます:

- **Status:** 現在のプールの状態を示す色分けされたアイコン
- **Pool Master:** プール内のマスターサーバーの IP アドレスまたは DNS 名
- **Pool-Wide Networks:** プール内のネットワークの数
- **Citrix Hypervisor:** プール内のサーバーの数
- **All VMs:** プール内の VM の数
- **Server list:** サーバー名、ネットワーク数、VM 数、ステータスなどを含む、プール内のサーバーのリスト。

ステータス情報を確認するだけでなく、プール内の Citrix Hypervisor サーバーによる Netflow データの転送方法を構成できます。必要に応じて以下のチェックボックスをオンにして、**[Save Netflow Configuration]** をクリックします:

- vSwitch Controller (デフォルトで選択): GUI の [Flow Statistics] セクションで使用される Netflow 情報を vSwitch Controller に転送します。このチェックボックスをオフにすると、Netflow データは vSwitch Controller に送信されず、[Flow Statistics] ページにはデータが表示されません。
- External Netflow Controller: 外部のサードパーティ製 Netflow コレクターに Netflow データを転送できます。外部のコレクターの IP アドレスを入力します。

#### フェールセーフモード

[Fail Mode] セクションで、vSwitch Controller に接続できない場合の vSwitch のアクセス制御規則の適用方法を構成できます。データ損失を避けるために、vSwitch Controller の可用性を高いレベルに維持することが重要です。vSwitch Controller が利用できない場合、次の失敗モードが適用されます:

- Fail-open: すべてのトラフィックが許可され、以前定義した ACL は vSwitch が vSwitch Controller に再接続できるまで適用されません。
- Fail-safe: 既存の ACL が引き続き適用されます。

通常の動作では、vSwitch は構成済みの vSwitch Controller との接続を維持し、ネットワーク管理とステータス情報を交換します。vSwitch Controller が使用できなくなると、vSwitch は、無操作状態によるタイムアウトでネットワークトラフィックが切断されるまで待機します。無操作状態によるタイムアウト後、vSwitch は構成されたフェールモードに入ります。

フェールセーフモードでは、vSwitch が構成済みの vSwitch Controller への接続を失った後は、既存の ACL が引き続き適用されます。既存の ACL と一致しないトラフィックは拒否されます。Controller によって提示されるポリシー階層のどのレベルでも、vSwitch の VIF に関する規則のセットとしてすべての ACL が適用されます。その結果、Controller が使用できないときにフェールセーフモードで表示される新しい VIF は、Controller が再び使用可能になるまで通信できません。プラグを抜いてから再接続した既存の VIF は、新しい VIF と同じ動作をします。この状況は、通信を可能にする上位の ACL ポリシー規則（グローバル、リソース単位プール、ネットワーク単位、または VM 単位）が既存の VIF に存在する場合でも発生します。さらに、vSwitch Controller は、学習した IP アドレスに基づいて ACL を定義できます。フェールセーフモードでは、使用できなくなる前に VM に関連付けられていない Controller の IP アドレスで VM が送信したパケットは拒否されます。たとえば、新しい IP アドレスを使用する既存の VM は、Controller が再び到達可能になるまで通信できません。フェールセーフモードでトラフィックが拒否されるその他の例を以下に示します:

- 新しく接続された VIF
- 新しい VM
- 移行された VM (例: ライブマイグレーションやワークロードバランス)
- プールに追加されたホスト上の VM
- ルーターのように動作するアプリケーション

vSwitch がフェールセーフモードで再起動し、vSwitch の起動後も Controller が使用できない場合は、すべての ACL が失われ、すべてのトラフィックが拒否されます。vSwitch は、Controller との接続が再確立され、ACL が Controller によって vSwitch まで引き下げられるまで、フェールセーフモードにとどまります。

### 警告:

フェールセーフモードで vSwitch Controller の管理からリソースプールを削除すると、vSwitch がネットワーク接続を失い、緊急リセットの状況が発生する可能性があります。このような状況を回避するには、ステータスが緑色の間にリソースプールを削除するだけです。

このページのポート構成ポリシーに使用可能なターゲット VLAN を指定することもできます。詳しくは、「ポート構成ポリシーの設定」を参照してください。

### サーバーレベル

選択したサーバーの [Status] ページには、以下の情報が表示されます:

- **Server Status:** 現在のサーバーのステータスを示す色分けされたアイコン。
- **Server Networks:** リソースプール内のネットワークの数。
- **MAC Address:** サーバー管理インターフェイスの MAC アドレス。
- **IP Address:** サーバー管理インターフェイスの IP アドレス。
- **vSwitch Version:** この Citrix Hypervisor で実行中の vSwitch のビルドとバージョン番号。
- **Server Networks:** サーバーに関連付けられているすべてのネットワークのリスト。この情報には、以下が含まれます:
  - そのネットワークを使用するサーバー上の VM の数
  - 関連する物理インターフェイス
  - VLAN
  - 送受信されたバイト数
  - エラーの数
  - ステータス
- **Server VMs:** サーバーに関連付けられたすべての VM のリスト。VM 上の各 VIF には、以下の情報も含まれます:
  - MAC アドレス
  - ネットワーク
  - IP アドレス
  - VM が起動されてから送受信された合計バイト数
  - ステータス

このページでは、ポート構成ポリシーに使用できるターゲット VLAN を指定することもできます。「ポート構成ポリシーの設定」を参照してください。

### ネットワークレベル

プール全体のネットワークの [Status] タブには、リソースプール内の各ネットワークに関する概要情報が表示されます。個々のネットワークの [Status] タブには、ネットワーク自体に関する情報が表示されます。このタブには、

現在ネットワークに接続されている物理インターフェイスと VM インターフェイスに関するハイパーリンクテーブルが含まれています。

ステータスアイコンは、以下の色で表示できます：

- 緑色（ネットワークがアクティブで、vSwitch Controller により適切に管理されている場合）
- 赤色（接続されたインターフェイスがネットワークにない場合）
- オレンジ色（エラー状態がある場合）。関連するテキストでエラーが説明されています。

プール全体のネットワークの場合は、以下の情報が表示されます：

- Network name: 特定のネットワーク。
- VMs: ネットワークに関連付けられた VM の数。
- Citrix Hypervisor: ネットワーク用サーバー。
- Physical Interface: ネットワークのサーバーインターフェイス。
- Transmit (Tx) and receive (Rx) packets: 指定されたネットワーク上のすべての VIF 間で集計されたパケット数。
- Errors: 指定したネットワーク上のすべての VIF 間で集計されたエラー数。
- Status: 現在のネットワークを示す色分けされたアイコン。

選択したネットワークについて、以下の情報が表示されます：

- Network Status: 現在のネットワークを示す色分けされたアイコン。
- VMs: ネットワークに関連付けられた VM の数。
- Physical interfaces: VLAN、送受信されたバイト数、エラー、ステータスなどを含む物理インターフェイスのリスト。
- Switching Citrix Hypervisor (サーバー間のプライベートネットワークのみ): ネットワークの現在アクティブなスイッチングホストを指定します。

サーバー間のプライベートネットワークは、物理ネットワークの追加構成を必要とせずに、同じリソースプール内の仮想マシン間の通信を可能にします。VM は異なるホスト上で実行できます。この機能は、「スイッチングホスト」がプール内の他の各ホストへの GRE トンネルを確立することによって実現されます。GRE トンネルはスタートポロジでセットアップされています。他のホストには、プライベートネットワーク上で実行中のアクティブな VM があります。

スイッチングホストが使用できなくなるか削除されると、新しいスイッチングホストが自動的に選択され、新しい GRE トンネルが設定されます。詳しくは、「[ネットワーク](#)」を参照してください。

- VM interfaces: MAC アドレス、IP アドレス、送受信されたバイト数、ステータスなどを含む VM のリスト。

このページでは、ポート構成ポリシーに使用できるターゲット VLAN を指定することもできます。詳しくは、「[ポート構成ポリシーの設定](#)」を参照してください。

## 仮想マシン (VM) レベル

すべての VM について、以下の情報が表示されます：

- VM name: 特定の VM の名前。

- MAC address: VM に割り当てられた MAC アドレス。
- Network name: VM が割り当てられているネットワーク。
- Detected IP address: VM に割り当てられた IP アドレス。
- Transmit (Tx) and receive (Rx) packets: 指定された VM 上のすべての VIF 間で集計されたパケット数。
- Errors: 指定した VM 上のすべての VIF 間で集計されたエラー数。

選択した VM の [Status] ページには、以下の情報が表示されます:

- Status: 現在の VM ステータスを表示する色分けされたアイコン。
- Resource Pool: VM が属するリソースプール。
- Server Name: VM が割り当てられているサーバーの名前。この情報は、VM が実行されておらず特定のサーバーに関連付けられていない場合は、空白になります。
- VM Group Membership: VM が割り当てられている管理グループのリスト。
- VM interfaces: VM 上の VIF のリスト。この情報には、以下が含まれます:
  - MAC アドレス
  - ネットワーク名
  - 検出された IP アドレス
  - 送受信バイト、パケット、エラー数
  - ステータス
- Network Events: 優先順位、日付/時刻、説明などを含む、VM に関連するネットワークイベントのリスト。

#### 仮想インターフェイス (VIF) レベル

選択した VIF の [Status] ページには、以下の情報が表示されます:

- Status: 現在の VIF ステータスを示す色分けされたアイコン。
- Resource Pool: VIF が属するリソースプール。
- Network: VIF が属するネットワーク。
- VM Name: VIF が属する VM。
- MAC Address: VIF の MAC アドレス。
- IP Address: VIF の IP アドレス。
- Transmit and Receive bytes, packets, and errors: VIF のトラフィック数。
- Switch Port ACL Statistics: 送受信数とは異なり、ACL ヒット数は、現在の vSwitch の ACL 規則統計から読み取られた即時統計です。そのため、ポリシーの変更や、停止、シャットダウン、移行などの VM アクションによって、これらの統計情報はリセットされます。  
vSwitch ACL 統計では、IP アドレスをネットワーク上で識別し、IP ベースのプロトコルの統計を収集できるようにする必要があります。IP ベースの規則に数値が表示されない場合は、IP アドレスのフィールドに IP アドレスが表示されているかを確認します。

## フロー統計情報の表示

デフォルトでは、各管理対象 Citrix Hypervisor 上の vSwitch は Netflow データを vSwitch Controller に送信します。この Controller は、このデータを使用して [Flow Statistics] テーブルとチャートを生成します。vSwitch は、5 秒間アクティビティがなかった、または 60 秒間の全アクティビティを集計した後、すべての IPv4 フローの Netflow レコードを生成します。

フローのデータレートは、フローが継続した期間の平均のフロー総トラフィックとして表されます。たとえば、フローが 10 秒間継続し、最初の 1 秒間に 900KB 送信され、残りの 9 秒間に 10KB 送信された場合、結果のデータレートはフロー期間全体で 100KB/秒であるかのようにプロットされます。

Netflow は、スイッチとコレクター（vSwitch Controller など）の間で NetFlow レコードを転送するために、UDP データグラムを使用します。NetFlow は UDP データグラムを使用するため、NetFlow レコードが受信されなかった理由をコレクターが把握する方法は通常ありません。拒否されたレコードは、[Flow Statistics] テーブルまたはチャートで非決定性データになる場合があります。たとえば、1 秒間に 10 回のフローを生成するネットワークで、10 秒間継続する単一の 1GB のファイル転送があるとします。このネットワークは、合計 202 のフロー（100 の hping 刺激、100 の hping 応答、1 のファイル転送刺激、1 のファイル転送応答）を生成します。UDP データグラムの 50% が拒否された場合、コレクターがデータを 1GB と 2KB のいずれかで報告する確率は 50/50 です。

プール内の各 vSwitch は Netflow レコードを生成するため、異なる Citrix Hypervisor サーバーで実行された送信元と送信先は 2 つのレコードになり、統計の数値が倍になります。

NetFlow レコードを送信するために使用される vSwitch Controller 仮想アプライアンスおよびネットワークのオーバーロードを避けるために、100 を超える VM 環境でフロー可視性を無効にします。

**[Flow Statistics]** タブには、選択したノードのフローを表示するためのグラフと関連テーブルが表示されます。



ページの上にあるリストを使用して、以下を指定します：

- 方向：Bidirectional（送受信）、Inward（受信）、Outbound（送信）
- 単位：Bytes（バイト）、Bits（ビット）、Packets（パケット）、Flows（フロー）
- 以下のいずれかのグループの Top（上位）または Bottom（下位）の項目（最高値または最低値）：
  - VMs: リソースプール内に属しているトラフィックの送信元または送信先としての VM
  - IP Addresses: トラフィックの送信元または送信先としての IP アドレス
  - Protocols: ICMP、TCP、UDP などの IP プロトコルトラフィック

注：

結果の生成に使用される Netflow プロトコルを制限するため、イーサネットレイヤープロトコル（ARP など）は表示されません。

- Application: TCP/UDP ポートまたは ICMP タイプ/コードで識別される「アプリケーション」レベルのプロトコルトラフィック

- Traffic (タイプ別): VM、IP アドレス、プロトコル、アプリケーション (プロトコルのタイプとポート番号で示されます。この情報によりサービスを推測できます)
- 時間間隔

グラフの下の表には、リストで選択されている項目のタイプに応じて、以下の情報の一部またはすべてが表示されます:

- 仮想マシン
- IP
- 受信バイト数
- 受信データレート (Kbit/秒)
- 送信バイト数
- 送信データレート (Kbit/秒)
- 合計バイト数
- 合計データレート (bps)

NetFlow が vSwitch Controller に転送されていない場合は、[Flow Statistics] タブの下に青色の警告ステータステキストが表示されます: `One or more selected pools are not configured to forward NetFlow records to vSwitch Controller`

転送を再構成するには、この青色のステータステキストをクリックしてリソースプールのリストを表示します。リストから目的のリソースプールを選択して、プールステータスページに移動します。ステータスページから、NetFlow データ転送を構成できます。

## アドレスグループの管理

アドレスグループを設定して、ACL およびフロー統計情報レポートの送信元または送信先として使用する IP アドレスを指定できます。

アドレスグループを追加するには:

1. **[Visibility & Control]** で、サイドパネルにあるリソースツリーの **[Address Groups]** を選択し、すべてのアドレスグループの **[Status]** ページを開きます。
2. **[Create Group]** をクリックします。
3. グループを識別するための名前と、オプションの説明を入力します。
4. **[Create Group]** をクリックします。新しいグループがアドレスグループのリストに追加されます。
5. リソースツリーで新しいグループを選択して、その **[Status]** ページを開きます。
6. **[Add Members]** ボタンをクリックします。
7. ポップアップウィンドウで、1 つまたは複数の IP アドレスやサブネット (コンマ区切り) を指定します。例: 192.168.12.5、192.168.1.0/24
8. **[追加]** をクリックします。必要に応じて、さらにネットワークを追加します。アドレスの各セットは、アドレスグループリストのネットワークの下にノードとして追加されます。

新しいアドレスグループは、ACL ポリシーおよびフロー統計情報で使用できるようになりました。

このアドレスグループの [All Address Groups] 行にある [Remove] リンクをクリックすると、既存のアドレスグループを削除できます。

また、グループの名前や説明を更新することもできます：

1. リソースツリーで新しいグループを選択して、その [Status] ページを開きます。
2. [Modify Group] ボタンをクリックします。
3. 表示されるダイアログボックスで、名前と説明を変更します。
4. [Modify Group] ボタンをクリックして、変更を保存します。

## 仮想マシングループの管理

VM グループは、ステータスとフローの統計情報を表示するための、グループとして識別される VM セットです。VM グループ内の各 VM は、すでにリソースプール内に存在する必要があります。それ以外は、グループはリソースプールとサーバーから独立しています。

VM グループを追加するには：

1. [Visibility & Control] で、サイドパネルにあるリソースツリーの [VM Groups] を選択し、すべての VM グループの [Status] ページを開きます。
2. [Create Group] ボタンをクリックします。
3. グループを識別するための名前と、オプションの説明を入力します。
4. [Create Group] をクリックします。新しいグループが VM グループのリストに追加されます。
5. リソースツリーで新しいグループを選択して、その [Status] ページを開きます。
6. [Add Member] をクリックします。
7. ポップアップウィンドウで、リストから VM を選択します。
8. [追加] をクリックします。必要に応じて、さらに VM を追加します。各 VM は、VM グループリストのグループの下にサブノードとして追加されます。

各 VM グループでは、以下の右クリックオプションを使用できます：

- Add VM to group: 新しいグループメンバーを追加します。
- Modify Name/Description: 名前または説明を変更します。
- Remove Group: グループを削除します。

## DVS ポリシー構成階層

[Visibility & Control] 内の [Access Control and Port Configuration] タブを使用して、仮想マシン環境内のアクセス制御、QoS (サービス品質)、トラフィックミラーリングポリシーを構成します。すべてのポリシーは VIF レベルで適用されますが、vSwitch Controller では、VIF コレクション全体のデフォルトポリシーの宣言をサポートする階層型ポリシーモデルを使用します。また、vSwitch Controller では、必要に応じてきめ細かな例外を作成することにより、このデフォルトポリシーを上書きすることもできます。たとえば、デフォルトのリソースプールポリシーから特定の VM を除外できます。

リソースツリーで使用されている階層と同様に、ポリシー階層には以下のレベルがあります：

- Global (最も一般的なレベル)：すべてのリソースプールにすべての VIF が含まれます。
- Resource pools： 特定のリソースプール内のすべての VIF。
- Networks： 特定のネットワークに接続されているすべての VIF。
- VMs： 特定の VM に接続されているすべての VIF。
- VIF (最も具体的なレベル)： 単一の VIF。

注：

リソースプール内の Citrix Hypervisor が VM を実行しているかどうかにかかわらずポリシーが適用される必要があるため、Citrix Hypervisor サーバーはポリシー階層には含まれません。

## アクセス制御ポリシーの設定

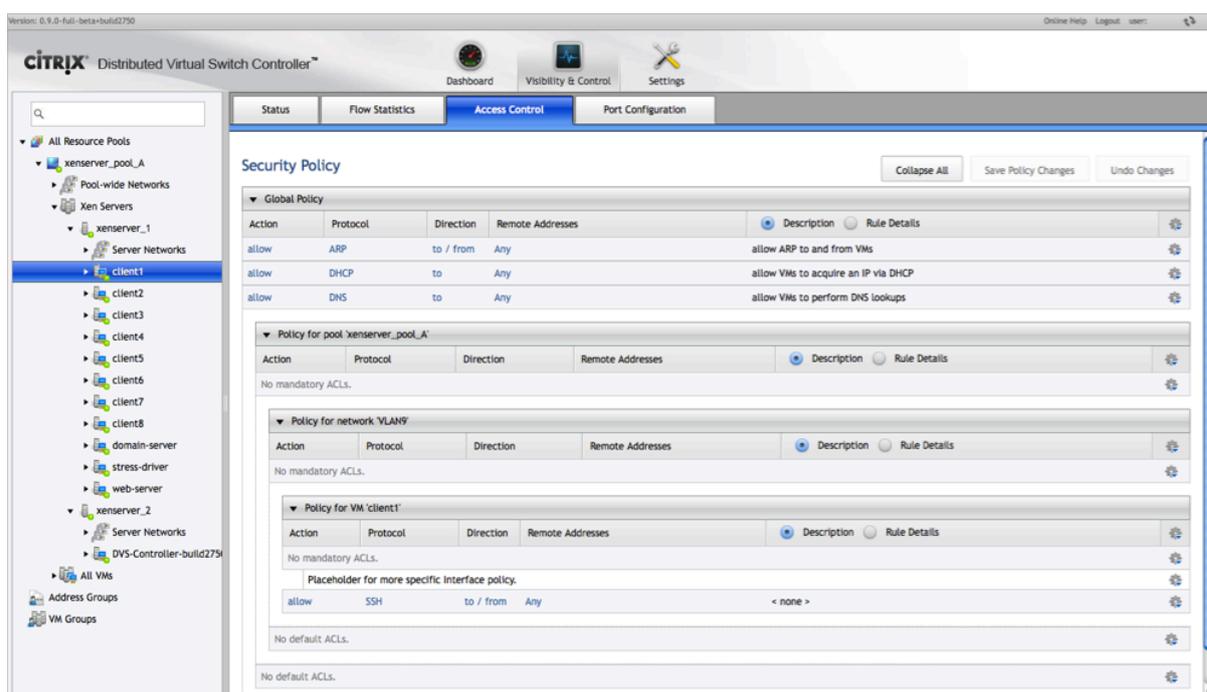
**[Access Control]** タブを選択して、パケット属性に基づいて VM トラフィックを許可または拒否するポリシーを設定します。

ACL ポリシーは規則のセットで構成され、それぞれに以下の情報が含まれます：

- Action： 規則に一致するトラフィックが許可される (Allow) か拒否される (Deny) かを示します。
- Protocol： 規則が適用されるネットワークプロトコル。規則をすべてのプロトコル (Any) に適用、既存のプロトコルリストから選択、または、新しいプロトコルを指定できます。
- Direction： 規則が適用されるトラフィックの方向。Read the text of the rules from left to right: 「to」は VM からの送信トラフィックを意味し、「from」は VM への受信トラフィックを意味します。
- Remote Addresses： 規則が、リモート IP アドレスの特定のセットとの間のトラフィックに制限されているかどうかを示します。

ACL ポリシーの管理は、リソースツリー階層に厳密に従います。サポートされている階層レベルでポリシーを指定できます。各レベルで、規則は以下のように整理されます：

- 必須規則： これらの規則は、子ポリシー規則の前に評価されます。これらに優先する唯一の規則は、親 (あまり具体的ではない) ポリシーの必須規則です。必須規則は、子 (より具体的な) ポリシーでは上書きできない規則を指定するために使用されます。
- 子規則： 子ポリシーブレースホルダーは、子ポリシーの規則が評価される順序における場所を示します。これにより、必須規則がデフォルトの規則と分類されます。
- デフォルトの規則： これらの規則は、すべての必須規則とすべての子ポリシーのデフォルトの規則の後に、最後に評価されます。これらの規則は、親ポリシーのデフォルトの規則に対してのみ優先されます。競合する動作がより具体的な子ポリシーで指定されていない場合にのみ適用される動作を指定するために、これらの規則を使用します。



## グローバルアクセス制御リスト（ACL）規則

グローバル ACL 規則を設定するには、リソースツリーの **[All Resource Pools]** をクリックします。このページには、グローバルレベルで定義されているすべての ACL 規則が表示されます。

## リソースプールのアクセス制御リスト（ACL）規則

リソースプールの ACL 規則を設定するには、リソースツリーでリソースプールを選択します。

このページには、グローバルポリシーの展開可能なバーと、リソースプール規則の展開された領域が表示されます。**[Expand All]** ボタンをクリックすると、グローバルポリシーの枠内にリソースプール規則が組み込まれている様子を確認できます。

## ネットワークアクセス制御リスト（ACL）規則

ネットワークレベルで ACL 規則を設定するには、リソースツリーでネットワークをクリックします。

このページには、以下の情報が表示されます：

- グローバル規則の展開可能なバー
- ネットワークが属するリソースプールの展開可能なバー
- ネットワーク規則の展開された領域

**[Expand All]** をクリックすると、リソースプールの枠内およびグローバルポリシーの枠内にネットワークポリシーが組み込まれている様子を確認できます。

## VM アクセス制御リスト (ACL) 規則

VM レベルでポリシーを設定するには、リソースツリーで VM をクリックします。

このページには、以下の情報が表示されます：

- グローバル規則の展開可能なバー
- VM が属するリソースプールとネットワークの展開可能なバー
- VM 規則の展開された領域

**[Expand All]** ボタンをクリックすると、ネットワーク、リソースプール、グローバルの枠内に VM 規則が組み込まれている様子を確認できます。

複数のネットワーク上にある VIF が VM に含まれている場合、ネットワークのサンプルバーの右側に [Change Network] リンクが表示されます。このリンクをクリックすると、その VM 上の VIF に適用される可能性がある各ネットワークレベルポリシーの規則を表示できます。

## VIF アクセス制御リスト (ACL) 規則

VIF レベルでポリシーを設定するには、リソースツリーで VIF をクリックします。ポリシーは VIF レベルでのみパッケージ化され適用されるため、VIF ページを表示してポリシーのすべてのコンテキストを表示する必要があります。

このページには、以下の情報が表示されます：

- グローバル規則の展開可能なバー
- VIF が属するリソースプール、ネットワーク、VM の展開可能なバー
- VIF 規則の展開された領域

**[Expand All]** ボタンをクリックすると、VM、ネットワーク、リソースプール、グローバルの枠内に VIF 規則が組み込まれている様子を確認できます。

## アクセス制御リスト (ACL) 規則の適用順序

ACL はポリシー構成階層のさまざまなレベルで定義できますが、ACL は VIF 単位で適用されます。実際に適用される場合、このセクションで説明されている順序で階層が結合され、各 VIF に適用されます。VIF および関連する統計情報に現在適用されている規則を確認するには、リソースツリーで VIF を選択します。[Status] タブで ACL リストを表示します。

適用順序は以下のとおりです：

1. グローバルレベルでの必須規則
2. VIF を含むリソースプールの必須規則
3. VIF を含むネットワークの必須規則
4. VIF を含む VM の必須規則
5. VIF を含む VIF の規則

6. VIF を含む VM のデフォルト規則
7. VIF を含むネットワークのデフォルト規則
8. VIF を含むリソースプールのデフォルト規則
9. VIF を含むグローバルのデフォルト規則

一致する最初の規則が実行され、それ以外の規則は評価されません。

注:

vSwitch Controller が使用できない場合、リソースプールは構成済みのフェールモードに基づいてアクセス制御規則を適用します。リソースプールのフェールモードについて詳しくは、「ステータスの表示」の「リソースプールレベル」セクションを参照してください。

#### アクセス制御リスト (ACL) 規則の定義

新しい ACL 規則を定義するには、リソースツリーを使用して、ポリシー構成階層の適切なレベルにあるノードを選択します。レベルごとに、そのレベルおよび上位のレベルの規則を追加できます。たとえば、リソースプールを選択した場合は、そのリソースプールの規則とグローバル規則を追加できます。

ポリシー構成階層のレベルに対応していないリソースツリーノードを選択すると、メッセージが表示されます。このメッセージには、別のレベルを選択するためのリンクがあります。

新しい規則は、以下の方法で追加できます:

- 必須規則を追加するには、そのレベルのヘッダーバーにある歯車アイコンをクリックし、**[Add New Mandatory ACL]** を選択します。
- デフォルト規則を追加するには、そのレベルのヘッダーバーにある歯車アイコンをクリックし、\*\* [Add New Default ACL] \*\* を選択します。
- 既存の規則エントリの上に規則を追加するには、そのエントリの歯車アイコンをクリックし、**[Add New ACL Above]** を選択します。
- 既存の規則エントリの下に規則を追加するには、そのエントリの歯車アイコンをクリックし、**[Add New ACL Below]** を選択します。

次のデフォルト設定で新しいルールがページに追加されます:

- Action: Allow
- Protocol: Any
- Direction: To/From
- Remote Addresses: Any
- Description: None

規則内の特定のフィールドを変更するには、現在のフィールド値を表すリンクをクリックし、以下のリストの説明に従って変更を適用します。変更を適用すると、規則が更新されて値が表示されます。

- **Action:** リンクをクリックして **[Change Action to Deny]** または **[Change Action to Allow]** を選択します。

- **Protocol:** 以下のオプションのいずれかをクリックして選択します:
  - 規則をすべてのプロトコルに適用するには **[Match Any Protocol]** を選択します。
  - プロトコルを指定するには **[Use an Existing Protocol]** を選択します。リストからプロトコルを選択し、**[Use Protocol]** をクリックします。
  - カスタムプロトコル特性を指定するには **[Use a New Protocol]** を選択します。ポップアップウィンドウで以下の情報を指定し、**[Save & Use]** をクリックします:
    - \* Ethertype: IP を選択するか、別の Ethertype を入力します。
    - \* IP Protocol: リスト表示されたプロトコルのいずれかを選択するか、別のプロトコルを入力します。
    - \* Destination Port (TCP/UDP のみ): ポート番号を入力するか、**[Any]** を指定します。
    - \* Source Port (TCP/UDP のみ): ポート番号を入力するか、**[Any]** を指定します。ウェルノウンサーバーポートを使用するアプリケーションを定義する場合は、ウェルノウンポートを Destination Port (送信先ポート) に定義し、Source Port (送信元ポート) は **[Any]** のままにします。たとえば、ポート 80 を使用する HTTP をこのように定義できます。
    - \* ICMP Type (ICMP のみ): **[Any]** を選択するか、特定の ICMP タイプのプロトコル (ICMP) タイプを入力します。
    - \* ICMP Code (ICMP のみ): **[Any]** を選択するか、特定の ICMP コードを入力します。
    - \* Match reply traffic: リターントラフィックが規則の一部として自動的に許可されるかどうかを示します。たとえば、VM から指定のリモートアドレスへの UDP 送信先ポート 7777 トラフィックを規則で許可して **[Match reply traffic]** を選択している場合は、リモートアドレスの送信元ポート 7777 から VM への UDP トラフィックも許可されます。双方向通信が必要な UDP プロトコルの場合は、このオプションを有効にします (このオプションは TCP の場合は常に有効になります)。
    - \* One-time Use vs. Multiple Uses: このプロトコルを現在の規則に対してのみ使用するか、プロトコルメニューのプロトコルのリストに追加するかを選択します。
  - 既に定義されたプロトコルの特性を変更するには、**[View/Modify Current Protocol]** を選択します。
- **Direction:** 指定のリモートアドレスを **from** (送信元)、**to** (送信先)、またはその両方として選択し、規則を適用します。
- **Remote Addresses:** リモートアドレスを指定するには:
  1. **[Any]** リンクをクリックして、使用可能なアドレスグループを表示するポップアップウィンドウを開きます。
  2. 1 つまたは複数のアドレスグループを選択し、矢印を使用して **[Selected]** 列にアドレスグループを移動します。
  3. **[All]** ボタンを使用して、すべてのグループを選択または選択解除します。
  4. 既存のアドレスグループの一部ではない IP アドレスまたはサブネットを指定するには、アドレスまたはサブネット (x.x.x.x または x.x.x.x/n) を入力します。 **[追加]** をクリックします。アドレスの追加を繰り返します。
  5. **[完了]** をクリックします。
- **Description:** 規則の説明テキストを追加するには:

1. **[Description]** ボタンをクリックします。
2. エントリをクリックします（現在説明がない場合は **<None>**）。テキスト入力領域が表示されます。テキストを入力し、キーを押します。 **Enter**。

- **Rule Details:** **[Rule Details]** ボタンをクリックして、規則の概要を表示します。

**[Save Policy Changes]** をクリックして、新しい規則を適用します。適用すると、仮想ネットワーク環境内で変更が直ちに反映されます。ルールをまだ保存していない場合は、**[変更を元に戻す]** をクリックして名前を付けた変更を元に戻します。

ACL を変更すると、vSwitch Controller GUI のすべての背景の更新が一時停止します。別の管理者が同時にポリシーを変更して先に変更を確定した場合は、ページを更新してサーバーから新しいポリシーを取得します。その後、変更を再入力します。

規則の歯車アイコンをクリックして **[Move Up]** または **[Move Down]** を選択すると、1つのレベルで規則の順序を変更できます。階層内のレベル間で規則を移動することはできません。規則を削除するには、歯車アイコンをクリックして **[Delete]** を選択します。 **[Description]** ボタンをクリックして、ACL の説明を表示します。または、 **[Rule]** ボタンをクリックして、作成した ACL の規則を表示します。

ACL 規則は、ポリシー階層の上位に構成されている場合でも、常に VM の仮想インターフェースの観点から解釈されます。この動作は、規則の **[Remote Addresses]** フィールドの意味を考えると重要になります。

たとえば、プール内の VM の IP アドレスが 10.1.1.1 の場合、VM に到達するトラフィックを防ぐために「IP 10.1.1.1 に対するすべてのプロトコルを拒否する」というプール上の規則を想定することがあります。この動作は、VM が送信するときに各 VM がこの規則を適用するため、リソースプール内の他のすべての VM の場合に当てはまります。ただし、リソースプールの外部にあるマシンは、IP アドレス 10.1.1.1 の VM と通信できます。このように動作するのは、外部マシンの送信動作を制御する規則がないためです。また、IP アドレスが 10.1.1.1 の VM の VIF には、そのアドレスの送信トラフィックを拒否する規則がないためです。ただし、この規則はそのアドレスの受信トラフィックを拒否しません。

ポリシーの動作が予想できない場合は、すべてのポリシーレベルの規則セット全体が視覚化されている仮想インターフェースの **[Status]** タブを表示します。

## ポート構成ポリシーの設定

**[Port Configuration]** タブを使用して、VIF ポートに適用するポリシーを構成します。以下のポリシータイプがサポートされています：

- **QoS:** QoS (Quality of Service: サービス品質) ポリシーは、DVS ポートに接続された VM の最大送信レートを制御します。
- **Traffic Mirroring:** RSPAN (Remote Switched Port Analyzer: リモートスイッチポートアナライザー) ポリシーは、トラフィック監視アプリケーションをサポートするために、VIF 上で送受信されたトラフィックの VLAN へのミラーリングをサポートします。
- **Disable MAC address spoof check:** MAC アドレスなりすましチェックポリシーは、VIF からのトラフィックの発信に対して MAC アドレスを適用するかどうかを制御します。vSwitch Controller が VIF からの MAC

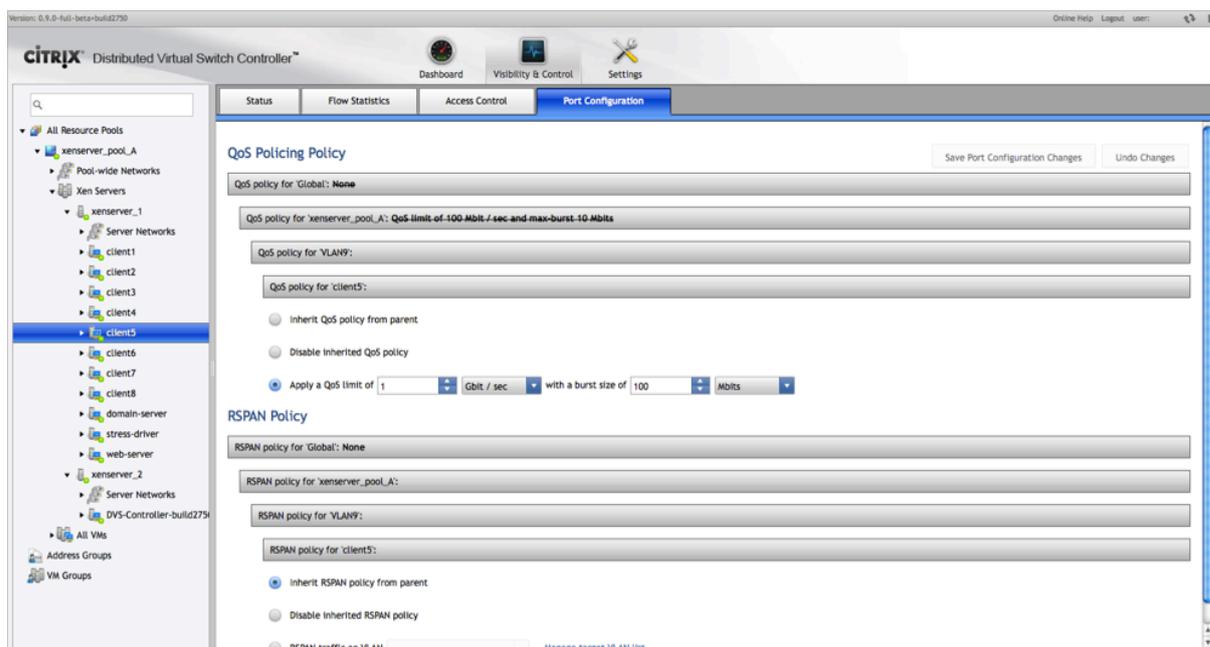
アドレス不明のパケットを検出すると、VIF からのパケットとそれ以降のすべてのトラフィックを拒否します。MAC アドレスなりすましチェックポリシーは、デフォルトでオンになっています。Microsoft Windows サーバーでネットワーク負荷分散などのソフトウェアを実行している VIF では、これらのポリシーを無効にしません。

**警告:**

物理ネットワークと仮想ネットワークを正しく構成せずに RSPAN を有効にすると、重大なネットワーク停止状態が発生する可能性があります。この機能を有効にする前に、「RSPAN の構成」の指示を注意深く確認してください。

グローバル、リソースプール、ネットワーク、VM、および VIF レベルで QoS およびトラフィックミラーリングポートポリシーを構成できます。リソースツリーでノードを選択し **[Port Configuration]** タブを選択すると、階層内のそれぞれの親レベルの構成が表示されます。ただし、変更できるのは選択したポリシーレベルの構成のみです。たとえば、VM を選択すると、**[Port Configuration]** タブには、グローバル、リソースプール、ネットワークのレベルで構成された値が表示されます。このタブでは、仮想マシンレベルで値を変更できます。

特定レベルでの [QoS] と [Traffic Mirroring] の構成は、上位レベルの構成より優先されます。構成が優先された場合、その構成の **[Port Configuration]** タブに表示される上位の構成は、取り消し線付きで表示されます。たとえば、次の図は、リソースプールレベルの構成に優先するネットワークレベルの QoS 構成を示しています。



ポートポリシーを構成するには、リソースツリーのノードを選択して **[Port Configuration]** タブを選択します。ポート構成ポリシーをサポートしていないノードを選択した場合、ポート構成をサポートしているノードへのリンクが記載されたメッセージが表示されます。

## QoS の構成

QoS ポリシーでは、以下のオプションを選択します：

- **Inherit QoS policy from parent** (デフォルト)：より上位の（つまり、あまり具体的ではない）階層レベルからポリシーを適用します。このオプションは、グローバルレベルにはありません。
- **Disable inherited QoS policy**：より上位の（つまり、あまり具体的ではない）レベルで設定されたポリシーを無視して、選択したポリシーレベルに含まれるすべての VIF が QoS 構成を持たないようにします。
- **Apply a QoS limit**：レート制限（単位付き）とバーストサイズ（単位付き）を選択します。選択したポリシーレベルに含まれるすべての VIF へのトラフィックを指定のレートに制限し、個々のバーストを指定のパケット数に制限します。

### 警告：

レート制限に対してバーストサイズを小さくしすぎると、VIF がそのレート制限に到達するだけの十分なトラフィックを送信できなくなります。この動作は、TCP などの輻輳制御を行うプロトコルで特に発生しやすくなります。

バーストレートは少なくとも、ローカルネットワークの MTU (Maximum Transmission Unit: 最大転送単位) より大きい数値である必要があります。

vSwitch Controller が管理しているインターフェイスで QoS に不適切に低いバーストレートを設定すると、vSwitch Controller とのすべての通信が失われる可能性があります。この通信ロスにより、緊急リセット状況に陥ります。

継承されないようにするには、VM レベルで QoS ポリシーを無効にします。

[**Save Port Configuration Changes**] をクリックして変更を反映するか、[**Undo Changes**] をクリックして保存していない変更を削除します。ポリシーは保存後すぐに有効になります。

## RSPAN の構成

### 警告：

VLAN を把握していないスイッチにサーバーが接続されている場合、または、RSPAN VLAN をサポートするよう適切に構成されていない場合に RSPAN を構成すると、トラフィックの重複やネットワークの停止状態を発生させることがあります。RSPAN 機能を有効にする前に、ドキュメントと物理スイッチの構成を確認してください。複数の物理スイッチが関与する可能性がある階層の上位レベルでは、この確認が特に重要になります。

RSPAN を有効にするには、以下に示す一連の手順が必要です：

### RSPAN VLAN の特定

RSPAN が VIF で有効になっている場合、その VIF の vSwitch は各パケットのコピーをその VIF に対して、またはその VIF から送信します。この vSwitch は、ターゲット VLAN と呼ばれる VLAN 値がタグ付けされたパケットのコピーを送信します。次に、管理者は、ターゲット VLAN を使用するよう構成したスイッチポートに、監視を実行する

ホストを配置します。監視ホストのインターフェイスで無作為検出モードを使用する場合は、RSPAN を使用する構成にした VIF との間で送受信されるすべてのトラフィックを確認できます。

#### ターゲット VLAN を使用する物理ネットワークの構成

ネットワークの停止を避けるためには、物理ネットワークを正しく構成して RSPAN トラフィックを把握することが極めて重要です。RSPAN が有効なすべての VIF に接続している物理スイッチインフラストラクチャが、ターゲット VLAN 上のラーニングを無効化する構成にできる場合のみ、RSPAN を有効にします。詳しくは、スイッチの製造元のドキュメントを参照してください。

また、ターゲット VLAN 上で送信されるトラフィックは、各 vSwitch から監視ホストに転送される必要があります。物理インフラストラクチャが1つの階層内に多くのスイッチを含んでいる場合、この転送を行うには、異なるスイッチ間でターゲット VLAN をトランク接続する必要があります。詳しくは、スイッチの製造元のドキュメントを参照してください。

#### ターゲット VLAN を使用する vSwitch Controller の構成

RSPAN ポート構成用の VLAN ID を使用する前に、vSwitch Controller に各ターゲット VLAN について知らせます。使用可能なターゲット VLAN ID を、リソースプール、ネットワーク、またはサーバーのレベルで指定できます。階層内の1つのレベルに追加されたターゲット VLAN は、そのレベル、およびその階層内のすべての下位レベルで、RSPAN ポート構成を構成する際に使用できます。ターゲット VLAN を指定したレベルが正しいかどうかは、物理インフラストラクチャがターゲット VLAN を把握できるようどれだけ幅広く構成したかによります。

使用可能なターゲット VLAN を指定するには：

1. **[Visibility & Control]** で、すべてのリソースプール、指定したリソースプール、指定したサーバー、または指定したネットワークの **[Status]** タブを開きます。
2. **[RSPAN Target VLAN IDs]** 領域で、**[+]** をクリックし、VLAN ID を入力します。
3. VLAN ID の追加を繰り返します。
4. **[Save Target VLAN Change]** をクリックします。

このセクションで説明したとおり、VLAN は **[Port Configuration]** タブで選択できます。

#### ポート構成を変更し VIF セット用に RSPAN を有効化

**[Port Configuration]** タブ内で RSPAN ポリシーを構成するには、リソースツリーで適切なノードを選択し、以下からオプションを選択します：

- **Inherit RSPAN policy from parent** (デフォルト)：次の上位の（つまり、あまり具体的ではない）階層レベルからポリシーを適用します。
- **Disable inherited RSPAN policy**：より上位の（つまり、あまり具体的ではない）レベルで設定されたポリシーを無視して、選択したポリシーレベルに含まれるすべての VIF が RSPAN 構成を持たないようにします。
- **RSPAN traffic on VLAN**：ターゲット VLAN のリストから VLAN を選択します。リストに表示されるターゲット VLAN は、現在選択中のノードがあるポリシーレベルに構成された VLAN のみです。

### MAC アドレスなりすましチェックの構成

MAC アドレスの適用を無効にするには、**[MAC address spoof checking]** を選択します。適用は VIF 単位でのみ構成でき、継承や、親の構成より優先させることはできません。

#### 変更の保存

**[Save Port Configuration Changes]** をクリックして変更を反映するか、**[Undo Changes]** をクリックして保存していない変更を削除します。ポリシーは保存後すぐに有効になります。

## vSwitch Controller の管理と保守

December 30, 2019

**[Settings]** ページで vSwitch Controller の管理と保守の機能を実行します。**[Settings]** ページにアクセスするには、vSwitch Controller ウィンドウの上部パネルにある **[Settings]** アイコンをクリックします。

注:

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

### IP アドレス設定の構成

**[IP Configuration]** ページで、vSwitch Controller の IP アドレスを確認および構成します。vSwitch Controller は最初の起動時に、DHCP 経由で IP アドレスを取得します。ただし、静的 IP アドレスを割り当てることをお勧めします。DHCP が構成されている場合、リソースプールはフェールセーフモードに設定できません。

Controller の IP アドレスを表示および構成するには:

1. **[Settings]** で **[IP Configuration]** を選択し、現在の構成を表示します。
2. 構成を変更するには、**[Modify Configuration]** をクリックします。
3. **[Manual Configuration]** を選択し、静的 IP アドレスを割り当てます。
4. 次の情報を入力します:
  - 新しい IP アドレス
  - ネットマスク
  - ゲートウェイの IP アドレス
  - (オプション) 1 つまたは 2 つの DNS サーバー IP アドレス

注:

Controller で名前解決を有効にするには、最低 1 つの DNS サーバーの IP アドレスを指定する必要があります。

5. **[Make Changes]** をクリックし、変更を反映します。

警告:

vSwitch Controller の IP アドレスを変更すると、次のエラーメッセージが表示されることがあります: Pool Managed By *old\_ip\_address*。このエラーメッセージは、vSwitch Controller が管理するプールの **[Status]** 列に表示されます。このメッセージが表示された場合は、プールの管理を再開するよう Controller に指示する必要があります。

**[All Resource Pools]** タブで、リソースプールの **[Status]** 列の横にある歯車アイコンをクリックします。**[Steal Pool]** を選択します。

デフォルトでは、vSwitch Controller 仮想アプライアンスは、自己署名 SSL 証明書を使用して各 Citrix Hypervisor で実行される vSwitch と接続します。vSwitch 接続用の署名入り証明書を提供する認証機関を取得できます。署名する公開キー/秘密キーのペアを生成するときに使用する予定の認証機関の指示に従います。キーを認証機関に送信します。認証機関から署名入り証明書を入手したあと、このセクションの手順に従います。

**[Settings]** で、**[Server and Certificate Maintenance]** をクリックします。

**[Update OVS Certificate]** をクリックします。

SSL /TLS 証明書ファイルを参照して選択します。

ファイルをアップロードしたら、**[Update Certificate]** をクリックします。

vSwitch SSL セキュリティ証明書に関する情報を表示するには:

1. **[Settings]** で、**[Server and Certificate Maintenance]** をクリックします。
2. **[View OVS Certificate]** をクリックします。

この情報には、証明書の有効期限も含まれています。

vSwitch SSL 証明書を更新したあと、管理用に新しいプールを追加すると、プール内の各サーバーの vSwitch が自動的に新しい証明書をダウンロードします。ただし、管理下にある既存のプールで実行されている vSwitch では、SSL 証明書を手動で更新する必要があります。

Citrix Hypervisor サーバーで、SSL 証明書を `/etc/openvswitch/vswitchd.cacert` にコピーします。

Citrix Hypervisor サーバーを再起動します。

## Controller のホスト名の構成

Controller のホスト名と DNS ドメインを確認および構成するには、**[IP Configuration]** ページを使用します。デフォルトでは、Controller のホスト名は `dvsc` であり、DNS ドメイン名は割り当てられていません。

**[Settings]** で **[IP Configuration]** を選択し、現在の構成を表示します。

**[Modify Host Settings]** をクリックします。

該当するフィールドに、希望のホスト名とドメイン名を入力します。

ドメイン名の値は、修飾されていないホスト名を検索するために、ホストのドメイン名とドメインの両方で使用されます。

**[Make Changes]** をクリックして変更を保存するか、**[Cancel]** を選択します。

#### トラブルレポートのための情報収集

トラブルレポートのための情報を収集するには：

1. **[Settings]** で **[Server and Certificate Maintenance]** をクリックします。
2. **[Collect & Zip All Logs]** をクリックして、関連するすべての vSwitch Controller ログを ZIP ファイルに追加してダウンロードします。
3. ZIP の操作が完了したら、ポップアップウィンドウのこちらのリンクをクリックして、dump.tar.gz ファイルをダウンロードします。
4. ダウンロードしたら、**[Close]** をクリックしてポップアップウィンドウを閉じます。

#### vSwitch Controller ソフトウェアの再起動

vSwitch Controller ソフトウェアを再起動するには、**[Settings]** で **[Server and Certificate Maintenance]** をクリックし、次に **[Restart Network Controller]** をクリックします。再起動が完了すると、ログインページが開きます。

#### 管理アカウントの管理

複数のユーザーアカウントを使用して、特定のユーザーに GUI アクセス時の制限付き特権を与えることができます。管理イベントログのエントリには、アクションを実行したユーザーの名前が含まれます。複数のユーザーがいると、最近構成を変更したユーザーを特定するのに役立ちます。

vSwitch Controller へのアクセス用にユーザーアカウントを追加し、ユーザーパスワードを変更するには：

1. **[Settings]** で **[Administrative Accounts]** を選択します。
2. **[Create Account]** をクリックします。
3. ユーザー名とパスワードを入力し、確認のためにパスワードを再入力します。以下のユーザー特権レベルのいずれかを指定します：
  - Superuser: すべての特権。
  - Read-write: 他のユーザーアカウントを変更しスナップショットを復元する権限を除く、すべての特権。
  - Read-Only: GUI でほとんどの情報を見ることができますが、vSwitch Controller ではユーザー自身のパスワード以外は変更できません。
4. **[Add User]** をクリックします。

ユーザーパスワードを変更するには、そのユーザーの **[Password]** リンクをクリックします。新しいパスワードを入力して確認し、**[Change Password]** をクリックします。

ユーザーを削除するには、そのユーザーの **[Remove]** リンクをクリックします。管理ユーザーは削除できません。

## 構成スナップショットの管理

スナップショットにより、現在の vSwitch Controller 構成を保存し、後でその構成を正確に復元することができます。主要な構成変更を行う前に、システムのスナップショットを作成しておく役に立つ場合があります。デフォルトでは、12 時間ごとに自動的に自動スナップショットが作成されます。

**[Settings]** で **[Configuration Snapshots]** をクリックして、構成バックアップのリストを表示し、バックアップから復元します。このページには最近のすべてのバックアップが記載されており、最新のバックアップが最初に表示されています。自動バックアップは、1 日に 2 回、および vSwitch Controller が再起動されるたびに、実行されます。バックアップから復元する場合、vSwitch Controller の現在の IP 構成は更新されません。vSwitch Controller の IP アドレスを変更する方法については、「IP アドレス設定の構成」を参照してください。

バックアップから構成を復元するには、スナップショットの歯車アイコンをクリックして、**[Restore to Snapshot]** を選択します。続行するかどうか尋ねられたら、**[Yes, Restore]** をクリックします。

オンデマンドでバックアップを作成するには、**[Create New Snapshot]** をクリックします。スナップショットを識別するために、オプションとして説明を入力できます。**[Create Snapshot]** をクリックします。新しいバックアップがリストの一番上に追加されます。

別のシステムに保存するためにスナップショットをダウンロードするには、そのスナップショットの歯車アイコンをクリックし、**[Download]** を選択します。ポップアップウィンドウの指示に従って、スナップショットファイルを保存します。

以前に保存したスナップショットを Controller にアップロードするには、**[Upload Snapshot]** をクリックします。スナップショットファイルを参照して選択し、**[Upload Snapshot]** をクリックします。アップロードされたスナップショットは、**[Configuration Snapshots]** ページのリストに追加されます。

スナップショットを削除するには、そのスナップショットの歯車アイコンをクリックし、**[Delete Snapshot]** を選択します。続行するかどうか尋ねられたら、**[Delete Snapshot]** をクリックします。

スナップショットテーブルには、ソフトウェアのバージョンと互換性に関する情報も含まれています。互換性は、スナップショット内のデータが現在のソフトウェアバージョンと互換性があるかどうかを示します。互換性がある場合は緑色のインジケータが表示され、互換性がない場合は赤色のインジケータが表示されます。互換性のないスナップショットに戻すには、まず **[Software Version]** 列に表示されている互換性のあるバージョンにソフトウェアを変更する必要があります。

デフォルトでは、12 時間ごとに構成スナップショットが作成されます。これらのスナップショットは、**[Automatic periodic snapshot]** という説明ラベルでリストに表示されます。また、vSwitch Controller を再起動するたびに構成スナップショットが作成されます。これらのスナップショットは、**[Startup snapshot]** という説明ラベルでリストに表示されます。システム起動のスナップショットは、30 日以上経過すると自動で削除されます。手動でス

ナップショットを作成する場合は、一意の説明ラベルを入力することで、システム起動のナップショットと混同されることがなくなり、30 日後に削除されなくなります。システム起動のナップショットを 30 日を超えて保存する必要がある場合は、そのナップショットをダウンロードしてから、一意の説明ラベルを付けて再アップロードします。

## ネットワークタイムプロトコル (NTP) サーバーの追加

vSwitch Controller 仮想アプライアンスは、外部のネットワークタイムプロトコル (NTP) サーバーに接続して時間設定を管理します。Controller にはデフォルトのサーバーが既に構成されています。これらの NTP サーバーはご使用の環境に最適ではない可能性があるため、以下の手順に従ってローカル NTP サーバーに置き換えることができます。

NTP サーバーを追加するには:

1. **[Settings]** で **[Time & NTP]** を選択します。
2. **[Add Server]** をクリックします。
3. サーバーの IP アドレスを入力し、**[Add]** をクリックします。
4. 必要に応じてサーバーを追加します。

NTP サーバーを削除するには、**[Remove]** リンクをクリックします。

## Syslog ファイルのエクスポート

システムが生成する管理メッセージとネットワークイベントメッセージで構成されるリモート syslog メッセージを受信するサーバーを、**[Syslog]** ページに追加します。最新の syslog エントリもダッシュボードに表示されます。

syslog サーバーを追加するには:

1. **[Settings]** で **[Syslog]** を選択します。
2. **[Add Server Address]** をクリックします。
3. サーバーの IP アドレスを入力し、**[Add]** をクリックします。
4. 必要に応じてサーバーを追加します。

サーバーを削除するには、**[Remove]** リンクをクリックします。

## コマンド

December 30, 2019

このセクションでは、vSwitch Controller の CLI コマンドについて説明します。XenCenter 内の Controller VM のテキストコンソールから、ローカルで CLI にアクセスできます。リモートで CLI にアクセスするには、SSH クライアントアプリケーションを使用し、ポート 22 で Controller VM のホスト名または IP アドレスに接続します。

注:

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

CLI セッション中に、以下のいずれかの方法で CLI コマンドのヘルプを表示できます:

- 「**help**」と入力してから **Enter** キーを押します。
- コマンドの一部に続けて、スペースと疑問符 (?) を入力してから **Enter** キーを押します。

このインターフェイスでは、コマンド引数を **Tab** キーで終了できます。通常、コマンドを各レベルで最も短い一意の文字列に短縮することで入力文字数を減らすことができます。矢印キーを押すと、現在のセッション内のコマンド履歴にアクセスできます。

ライフサイクルコマンド

**vSwitch Controller** を停止するには

```
1 halt controller
```

このコマンドで Controller を正常にシャットダウンすることにより、vSwitch Controller アプライアンスを停止します。

**Controller** を再起動するには

```
1 restart controller appliance
```

このコマンドにより、Controller アプライアンス全体をシャットダウンして再起動します。

このコマンドは、主にトラブルシューティング用です。通常、**halt** コマンドは Controller アプライアンスの電源をオフにするために使用されます。

**Controller** デーモンを再起動するには

```
1 restart controller daemon
```

このコマンドにより、Controller 機能を実装するプロセスをシャットダウンして再起動します。

このコマンドは、主にトラブルシューティング用です。

## 設定コマンド

vSwitch Controller を設定するには、次のコマンドを使用します。

**Controller** アプライアンスのホスト名を設定するには

```
1 set controller hostname hostname
```

このコマンドにより、Controller アプライアンスのホスト名を設定します。

指定のホスト名に1つまたは複数のピリオド文字 (.) が含まれている場合、アプライアンスのホスト名は最初のピリオドの前の文字列に設定されます。アプライアンスのドメイン名は、最初のピリオドの後の文字列に設定されます。

**DHCP** 経由で **Controller** 管理インターフェイスの **IP** アドレスを設定するには

```
1 set controller management-interface config dhcp
```

このコマンドにより、Controller 管理インターフェイスの IP アドレスが DHCP で設定されるようになります。DHCP が構成されている場合、リソースプールはフェールセーフモードに設定できません。

このコマンドは実行時に有効になるため、アドレスが変更されると CLI へのリモートアクセスが失われる場合があります。

**Controller** 管理インターフェイスの静的 **IP** アドレスを設定するには

```
1 set controller management-interface config static
2 IP-address
3 netmask
4 gateway-IP
5 [dns-server-IP]
6 [dns-server-IP2
7 dns-search]]'
```

このコマンドにより、Controller 管理インターフェイスの静的 IP アドレスを設定します。DNS 構成情報はオプションです。DNS 検索パスを指定するには、2 つの DNS サーバーを指定する必要があります。

このコマンドは実行時に有効になるため、アドレスが変更されると CLI へのリモートアクセスが失われる場合があります。

## 表示コマンド

現在の vSwitch Controller 設定に関する情報を表示するには、次のコマンドを使用します。

現在の **Controller** のホスト名を表示するには

```
1 show controller hostname
```

現在の構成の概要と管理インターフェイスのステータスを表示するには

```
1 show controller management-interface
```

管理インターフェイスの構成値を表示するには

```
1 show controller management-interface config
```

**Controller** の現在のデフォルトゲートウェイを表示するには

```
1 show controller management-interface default-gateway
```

**Controller** の現在の **DNS** 構成を表示するには

```
1 show controller management-interface dns-server
```

**Controller** 管理インターフェイスの現在の **IP** アドレスを表示するには

```
1 show controller management-interface ip-address
```

**Controller** 管理インターフェイスの現在のネットマスクを表示するには

```
1 show controller management-interface netmask
```

**Controller** のソフトウェアバージョンを表示するには

```
1 show controller version
```

## その他のコマンド

現在の **CLI** セッションを終了するには

```
1 exit
```

コマンドに関する情報を取得するには

```
1 help
```

**Controller** の既存のバージョンをアップグレードまたはダウングレードするには

```
1 install controller software-update scp-format-remote-filename
```

このコマンドにより、指定したリモートの場所から **Controller** の更新ファイルを安全にコピーし、既存のバージョンの代わりにそのバージョンをインストールします。

このコマンドを使用して、アップグレードとダウングレードの両方のソフトウェアバージョンをインストールできます。アップグレードにより、構成が自動的に新しいバージョンに移行されます。ダウングレードにより、互換性のあるスナップショットが存在しない場合は、互換性のある最新の構成スナップショットまたは空の構成に戻ります。

指定したリモートシステムを **ping** するには

```
1 ping name-or-IP-address [count]
```

このコマンドにより、名前または IP アドレスで識別されるリモートシステムに ICMP エコー要求を送信し、応答を待ちます。回数が指定されていない場合、Ctrl+C キーで中断されるまで、1 秒に 1 回要求が送信されます。回数が指定されている場合、その数の ping が送信されます。

## vSwitch Controller の問題のトラブルシューティング

December 30, 2019

このセクションには、vSwitch Controller の問題のトラブルシューティングに役立つ情報が記載されています。

注:

vSwitch Controller は Citrix Hypervisor 8.1 で廃止され、今後のリリースから削除されます。

## リソースツリーノードのステータス

以下の表に、各リソースタイプのステータスアイコンを示します。これらのアイコンは、リソースツリーと、項目の [Status] ページに表示されます。

| 項目/ステータスアイコン             | 説明                                                                                                         |
|--------------------------|------------------------------------------------------------------------------------------------------------|
| <b>VIF</b>               |                                                                                                            |
| 赤                        | 関連する仮想マシン (VM) がシャットダウンまたは到達不能です。                                                                          |
| 緑                        | 仮想ネットワークインターフェイス (VIF) が動作しており、管理されています。                                                                   |
| オレンジ                     | VM は実行中ですが、VIF が属する Citrix Hypervisor が vSwitch Controller に接続されていません。                                     |
| <b>仮想マシン</b>             |                                                                                                            |
| 赤                        | VM がシャットダウンしている、または到達不能です。                                                                                 |
| 緑                        | VM は実行中であり、VIF が管理されています。                                                                                  |
| オレンジ                     | VM は実行中ですが、VM が属する Citrix Hypervisor が vSwitch Controller に正しく接続されていません。このステータスは、それぞれの VIF の共有状態によって異なります。 |
| <b>サーバーネットワーク</b>        |                                                                                                            |
| 赤                        | Citrix Hypervisor がシャットダウンしているまたは到達不能、あるいはネットワークに関連付けられた VIF が VM にありません。                                  |
| 緑                        | Citrix Hypervisor が vSwitch Controller に正しく接続されています。                                                       |
| オレンジ                     | Citrix Hypervisor の vSwitch Controller への接続が正しく構成されていません (関連付けられた物理インターフェイスと VIF の共有状態によって異なります)。          |
| <b>Citrix Hypervisor</b> |                                                                                                            |

| 項目/ステータスアイコン | 説明                                                                                                  |
|--------------|-----------------------------------------------------------------------------------------------------|
| 赤            | Citrix Hypervisor がシャットダウンしている、または到達不能です。                                                           |
| 緑            | Citrix Hypervisor が vSwitch Controller に正しく接続されています。                                                |
| オレンジ         | Citrix Hypervisor の vSwitch Controller への接続が構成されていません（関連付けられた物理インターフェイスと VIF の共有状態によって異なります）。       |
| プール全体のネットワーク |                                                                                                     |
| 赤            | マスターの Citrix Hypervisor がシャットダウンしている、または到達不能です。                                                     |
| 緑            | マスターの Citrix Hypervisor の vSwitch Controller への接続が構成されており、その接続が確立して動作しています。                         |
| オレンジ         | マスターの Citrix Hypervisor の vSwitch Controller への接続が構成されていません（関連付けられた物理インターフェイスと VIF の共有状態によって異なります）。 |
| リソースプール      |                                                                                                     |
| 赤            | マスターの Citrix Hypervisor がシャットダウンしている、または到達不能です。                                                     |
| 緑            | マスターの Citrix Hypervisor の vSwitch Controller への接続が構成されており、その接続が確立して動作しています。                         |
| オレンジ         | マスターの Citrix Hypervisor の vSwitch Controller への接続が構成されていません（関連付けられた物理インターフェイスと VIF の共有状態によって異なります）。 |

## アクセスポリシーの問題のトラブルシューティング

アクセス制御ポリシーが正しく動作していない場合は、以下の提案事項がトラブルシューティングに役立ちます。

1. ポリシーが影響を与えると思われる VM の VIF の **[Status]** ページを選択します。ポリシーが正しく処理されないトラフィックを生成する間に、各規則のヒット数を表示します。トラフィックがヒットしていると思われる規則ではなく、実際にヒットしている規則を特定します。デバッグのために、グローバルレベルで最も優

先度が低いデフォルト規則として、すべてのトラフィックと一致するデフォルト規則を追加できます。

注:

デバッグ中、必要なネットワーク動作に応じた許可または拒否のアクションをこの規則に設定することができます。デバッグ後は、この規則を削除してください。

2. トラフィックが予想よりも低い優先度の規則にヒットした場合は、規則一致基準を慎重に確認してください。トラフィックの方向が正しく指定されていますか。リモートホストは正しく識別されていますか。プロトコルが正しく定義されていますか。たとえば、プロトコルが TCP ポートではなく UDP ポートを指定している、またはその逆になっていることはありませんか。
3. トラフィックが予想よりも高い優先度の規則にヒットした場合は、この規則と、トラフィックがヒットすると予想される規則との間の競合を解決します。競合を解決するには、規則をある程度詳細に再定義するか、2つの規則の相対的な優先順位を変更します。たとえば、規則を特定のリモート IP アドレスのセットにのみ適用するよう変更できます。
4. 仮想マシンに複数の VIF がある場合、ポリシーを適用する VIF でトラフィックが送受信されていることを確認します。必要に応じて、RSPAN を使用して、VIF からネットワークアナライザーへのトラフィックをミラーリングします。このミラーリングされたトラフィックを使用して、規則に一致するはずのトラフィックが存在することを確認できます。

注:

vSwitch Controller が使用できない場合、リソースプールは構成済みのフェールモードに基づいてアクセス制御規則を適用します。リソースプールのフェールモードについて詳しくは、「ステータスの表示」の「リソースプールレベル」セクションを参照してください。

## トラブルレポートの作成

問題を効率的に解決するには、問題に関連する Citrix Hypervisor と vSwitch Controller から情報を収集します。問題の発生後、できるだけ早くこの情報を収集します。トラブルレポートとともにこの情報を提出します。

- この問題に関連する各 Citrix Hypervisor のサーバーの状態レポートを同梱します。サーバーの状態レポートの生成に関する情報については、「ヘルスチェック」を参照してください。
- **[Server & Certificate Maintenance Settings]** ページの **[Collect and Zip All Logs]** をクリックして、vSwitch Controller からのログバンドルを含めます。詳しくは、「[トラブルレポートのための情報収集](#)」を参照してください。

## Controller のエラーメッセージ

以下のエラーメッセージが表示される場合があります:

- **Connecting to Pool** - 新しいプールが追加され、vSwitch Controller がプールマスタにまだ正常に接続していない場合に表示されます。または、vSwitch Controller が再起動し、まだプールマスタに正常に接

続していないときに表示されます。正常な接続が 30 秒以内に確立されない場合、このメッセージは「Pool Connection Failed」に置き換えられます。

- **Network control channels disconnected** - Citrix Hypervisor が vSwitch Controller に正しく接続されていません。
- **Missing Pool Address** - プールに使用できる DNS 名または IP アドレスがありません。
- **Pool Connection Failed** - このメッセージは、以下の状況で表示されます:
  - Controller とプールマスタの間にネットワークの問題がある
  - DNS 名前解決に失敗した
  - 無効な DNS 名またはプールマスタの IP アドレスがある
  - プールマスタがダウンしている、または構成ミスがある
- **Unsupported Pool Version** - プールに構成された DNS 名または IP アドレスが、Citrix Hypervisor の互換バージョンの名前解決になっていません。
- **Duplicate Pool: Pool Disabled** - プールが、vSwitch Controller データベースに既に存在する別のプールと同じ XAPI UUID を報告しています。
- **Pool Authentication Failure** - 提供されたユーザー名とパスワードでは、vSwitch Controller のプールマスタへの認証に失敗しました。
- **Pool Identity Changed** - プールが再インストールされ、一致するプールのステータスと一致しません。
- **Pool Synchronization Error** - XAPI を使用してプールマスタと通信するときに、サポートされていない操作が確認されました。
- **Unknown Error** - エラーの原因は不明です。

## コマンドラインインターフェイス

March 12, 2020

xe CLI を使用すると、システム管理タスクをスクリプト化して自動化できます。CLI を使用することで、Citrix Hypervisor を既存の IT インフラストラクチャに統合できます。

### xe CLI のインストール

xe コマンドラインインターフェイスは、すべての Citrix Hypervisor サーバーにデフォルトでインストールされ、XenCenter にも含まれています。Linux の場合、スタンドアロンのリモート CLI も使用できます。

### Windows の場合

Windows では、`xe.exe` コマンドが XenCenter と一緒にインストールされています。

`xe.exe`コマンドを使用するには、Windows のコマンドプロンプトを開き、ディレクトリを`xe.exe`ファイルが保存されているディレクトリに変更します（通常は`C:\Program Files\Citrix\XenCenter`）。`xe.exe`のインストール先をシステムパスに追加する場合は、ディレクトリを変更することなくコマンドを使用できます。

### Linux の場合

RPM ベースのディストリビューション（Red Hat など）では、メインの Citrix Hypervisor インストール ISO イメージの「`client_install/xapi-xe-BUILD.x86_64.rpm`」という名前の RPM からスタンドアロン `xe` コマンドをインストールできます。

RPM からインストールするには、次のコマンドを使用します：

```
1 rpm -ivh xapi-xe-BUILD.x86_64.rpm
```

コマンドラインでパラメーターを使用すると、`xe` コマンドの実行時に使用する Citrix Hypervisor サーバー、ユーザー名、およびパスワードを定義できます。または、パラメーターではなく環境変数として設定することもできます。次に例を示します：

```
1 export XE_EXTRA_ARGS="server=<host name>,username=<user name>,password=<password>"
```

#### 注：

セキュリティで保護された接続を介してファイル転送を行うコマンドを実行しようとする、Linux 上のリモート `xe CLI` が動作を停止することがあります。この場合は、`--no-ssl`パラメーターを使用することで、セキュリティで保護されない接続を介して Citrix Hypervisor サーバーにコマンドを実行できます。

### `xe` コマンドのヘルプの表示

ホスト上の CLI の基本ヘルプを表示するには、次のコマンドを実行します。

```
1 xe help command
```

使用頻度の高い `xe` コマンドの一覧を表示するには、次のコマンドを実行します：

```
1 xe help
```

また、すべての `xe` コマンドの一覧を表示するには、次のコマンドを実行します：

```
1 xe help --all
```

## 基本構文

Citrix Hypervisor のすべての xe コマンドの基本構文は、次のとおりです。

```
1 xe command-name argument=value argument=value
```

各コマンドには、`argument=value`という形式で指定する引数のセットがあります。一部のコマンドには必須の引数があり、多くのコマンドにはオプションの引数があります。通常、オプションの引数を指定せずにコマンドを実行すると、各引数のデフォルト値が適用されます。

xe コマンドがリモートで実行されると、接続と認証に追加の引数が使用されます。これらの引数も、`argument=argument_value`形式で指定します。

`server` 引数では、コマンドの実行先のホスト名または IP アドレスを指定します。`username` 引数と `password` 引数では、認証情報（ユーザー名とパスワード）を指定します。

`password-file` 引数は、パスワードを直接入力する代わりに指定できます。この場合、xe コマンドは指定されたファイルからパスワードの読み取りを試み、そのパスワードを使用して接続します（ファイルの最後にある行末の CR および LF はすべて削除されます）。この方法は、コマンドラインでパスワードを直接指定するよりも安全です。

オプションの `port` 引数を使用して、リモートの Citrix Hypervisor サーバーのエージェントポート（デフォルトで 443）を指定できます。

例：ローカルの Citrix Hypervisor サーバーで、次のコマンドを実行します：

```
1 xe vm-list
```

例：リモートの Citrix Hypervisor サーバーで、次のコマンドを実行します：

```
1 xe vm-list -user username -password password -server hostname
```

リモート接続用の引数では、以下の省略構文も使用できます。

- `-u`: ユーザー名
- `-pw`: パスワード
- `-pwf`: パスワードファイル
- `-p`: ポート
- `-s`: サーバー

例：リモートの Citrix Hypervisor サーバーで、次のコマンドを実行します：

```
1 xe vm-list -u myuser -pw mypassword -s hostname
```

また、引数は、環境変数 `XE_EXTRA_ARGS` からコンマ区切りのキー/値ペアの形式でも取得されます。たとえば、リモートの Citrix Hypervisor サーバーで実行されるコマンドを入力するには、まず次のコマンドを実行します：

```
1 export XE_EXTRA_ARGS="server=jeffbeck,port=443,username=root,password=pass"
```

このコマンドを実行した後は、実行する各 `xe` コマンドでリモートの Citrix Hypervisor サーバーパラメーターを指定する必要はありません。

また、環境変数 `XE_EXTRA_ARGS` を使用すると、リモートの Citrix Hypervisor サーバーに `xe` コマンドを実行するときに、`Tab` キーによる自動補完機能を使用できるようになります。この機能はデフォルトでは無効になっています。

### 特殊文字と構文

`xe` コマンドで引数/値ペアを指定するには、次の形式を使用します: `argument=value`

値にスペースが含まれている場合を除き、引用符を使用しないでください。また、引数名、等号 (=)、および値の間にスペースを挿入しないでください。この形式に従っていない引数はすべて無視されます。

スペースを含む値の場合、次のように記述します: `argument="value with spaces"`

Citrix Hypervisor サーバーで CLI を使用する場合、標準的な Linux bash シェルに類似した、`Tab` キーによる自動補完機能を使用できます。たとえば、「`xe vm-l`」と入力してから **Tab** キーを押すと、コマンドの残りの部分が表示されます。ただし、`vm-l` で始まるコマンドが複数ある場合は、**Tab** キーをもう 1 回押すと、それらのコマンドが一覧表示されます。この機能は、コマンド内でオブジェクトの UUID を指定する場合に便利です。

#### 注:

リモートの Citrix Hypervisor サーバーに対してコマンドを実行する場合、通常この自動補完機能は無効です。ただし、コマンドを入力するマシンで `XE_EXTRA_ARGS` 変数を設定すると、自動補完機能が有効になります。詳しくは、「基本構文」を参照してください。

### コマンドの種類

CLI コマンドは 2 つに分けることができます。低レベルコマンドは、API オブジェクトのリスティングとパラメーター操作に関係しています。高レベルコマンドは、より抽象的なレベルの仮想マシンまたはホストと対話するために使用されます。

低レベルコマンドは、以下のとおりです。

- `class-list`
- `class-param-get`
- `class-param-set`
- `class-param-list`

- *class-param-add*
- *class-param-remove*
- *class-param-clear*

ここで、*class* は以下のいずれかです:

- *bond*
- *console*
- *host*
- *host-crashdump*
- *host-cpu*
- *network*
- *patch*
- *pbid*
- *pif*
- *pool*
- *sm*
- *sr*
- *task*
- *template*
- *vbd*
- *vdi*
- *vif*
- *vlan*
- *vm*

これらの *class* 値ですべての *class-param-action* コマンドを使用できるわけではありません。*class* 値の一部には、コマンドセットがより小さいものもあります。

#### パラメーターの種類

xe コマンドで操作するオブジェクトには、それを識別したり状態を定義したりするためのパラメータセットがあります。

ほとんどのパラメータでは、1つの値を取ります。たとえば、仮想マシンの`name-label`パラメーターでは、1つの文字列値を指定します。`xe vm-param-list`のようなパラメーターリストコマンドからの出力では、かっこ内の値は、パラメーターが読み取り/書き込み (RW) か読み取り専用 (RO) かを示します。

特定の仮想マシンに対する`xe vm-param-list`コマンドによる出力には、以下の行が含まれることがあります：

```
1 user-version (RW): 1
2 is-control-domain (RO): false
```

1つ目のパラメーター`user-version`は書き込み可能であり、値は1です。2つ目の`is-control-domain`は読み取り専用で、値は`false`です。

ほかの2種類のパラメーターでは、複数の値を取ります。`set`パラメーターには、値の一覧が含まれます。`map`パラメーターには、キー/値ペアのセットが含まれます。たとえば、以下は、特定の仮想マシンに対する`xe vm-param-list`コマンドのサンプル出力の一部です

```
1 platform (MRW): acpi: true; apic: true; pae: true; nx: false
2 allowed-operations (SRO): pause; clean_shutdown; clean_reboot; \
3 hard_shutdown; hard_reboot; suspend
```

`platform`パラメーターには、キー/値ペアを表す項目のリストがあります。キー名の後にはコロン文字 (:) が付きます。キー/値の各ペアは、セミコロン文字 (;) で区切られます。MRWのMはマップパラメーターであることを示し、RWは読み取りと書き込みが可能であることを示します。`allowed-operations`パラメーターには、項目セットを構成するリストがあります。SROのSはセットパラメータであることを示し、ROは読み取り専用であることを示します。

マップパラメーターをフィルタする、つまりマップパラメーターを設定する場合は、マップパラメーター名とキー/値ペアの間にコロン (:) を挿入して区切ります。たとえば、仮想マシンの`other-config`パラメーターの`foo`キーの値を`baa`に設定する場合、コマンドは次のようになります。

```
1 xe vm-param-set uuid=VM uuid other-config:foo=baa
```

#### 注：

以前のリリースでは、ハイフン文字 (-) を使用してマップパラメーターを指定していました。このバージョンでも従来の構文を使用できますが、将来廃止予定です。

## 低レベルパラメーターコマンド

`class-param-get`、`class-param-set`、`class-param-add`、`class-param-remove`、`class-param-clear`、および `class-param-list` は、オブジェクトのパラメータを操作するコマンドです。これらのコマンドは、`uuid`パラメーターを取って、特定のオブジェクトを指定します。これらのコマンドは低レベルのコマンドとみなされるため、仮想マシンの名前ラベルではなく、UUID を指定する必要があります。

- `class-param-list uuid=uuid`

すべてのパラメータとその値のリストを出力します。`class-list` コマンドとは異なり、「expensive」フィールドの値のリストが出力されます。

- `class-param-get uuid=uuid param-name=parameter param-key=key`

特定のパラメータの値を返します。マップパラメータの場合、`param-key` を指定すると、マップのキーに対応する値が取得されます。`param-key` を指定しない場合、またはパラメータがセットの場合は、セットまたはマップの文字列表現が返されます。

- `class-param-set uuid=uuid param=value`

1つまたは複数のパラメータの値を設定します。

- `class-param-add uuid=uuid param-name=parameter key=value param-key=key`

マップまたはセットパラメータに値を追加します。マップパラメータの場合は、`key=value` 構文を使用してキー/値ペアを追加します。パラメータがセットの場合は、`param-key=key` 構文でキーを追加します。

- `class-param-remove uuid=uuid param-name=parameter param-key=key`

マップパラメータのキー/値ペアまたはセットパラメータのキーを削除します。

- `class-param-clear uuid=uuid param-name=parameter`

セットまたはマップを完全にクリアします。

#### 低レベルリストコマンド

`class-list` コマンドでは、`class` で指定する種類のオブジェクトのリストが出力されます。デフォルトでは、このタイプのコマンドはすべてのオブジェクトをリストし、パラメータのサブセットを出力します。この動作は、次の方法で変更できます：

- サブセットのみを出力するようにオブジェクトをフィルタリングできます。
- 出力されるパラメータは変更できます。

出力されるパラメータを変更するには、必要なパラメータのコンマ区切り一覧として引数 `params` を指定します。次に例を示します：

```
1 xe vm-list params=name-label,other-config
```

すべてのパラメータのリストを出力するには、次の構文を使用します。

```
1 xe vm-list params=all
```

計算のために多くのリソースを消費するパラメータは、`list` コマンドで表示されない場合があります。この場合、そのパラメータは次のように示されます：

```
1 allowed-VBD-devices (SR0): <expensive field>
```

これらのフィールドを取得するには、`class-param-list` コマンドまたは `class-param-get` コマンドを使用します。

特定のパラメータ値を持つオブジェクトだけを出力する（つまりリストをフィルターする）には、そのパラメータ—および値をコマンドラインで指定します。次に例を示します：

```
1 xe vm-list HVM-boot-policy="BIOS order" power-state=halted
```

この例では、`power-state` フィールドに値 `halted` を持ち、さらに `HVM-boot-policy` フィールドに値 `BIOS order` を持つ仮想マシンだけが出力されます。

マップのキーの値、またはセットに値が存在するかどうかを指定してリストをフィルタすることもできます。マップのキーに基づくフィルタリングの構文は、`map-name:key=value` です。セットに存在する値に基づくフィルタリングの構文は、`set-name:contains=value` です。

スクリプトを作成する場合は、コマンドラインに `--minimal` を渡すことで、`xe` で最初のフィールドだけをコンマ区切りで出力できます。たとえば、3つの仮想マシンがインストールされたホスト上で `xe vm-list --minimal` を実行すると、次のように3つの仮想マシンの UUID がコンマ区切りで出力されます：

```
1 a85d6717-7264-d00e-069b-3b1d19d56ad9,aaa3eec5-9499-bcf3-4c03-af10baea96b7, \
2 42c044de-df69-4b30-89d9-2c199564581d
```

## シークレット

Citrix Hypervisor ではシークレット機能によって、パスワードがコマンドライン履歴または API オブジェクトにプレーンテキストで保存されないようにします。XenCenter では、この機能が自動的に使用されます。また、パスワードが必要なコマンドの `xe CLI` でも、この機能を使用できます。

### 注

パスワードのシークレットを使って、`xe CLI` のリモートインスタンスから Citrix Hypervisor ホストで認証することはできません。

シークレットオブジェクトを作成するには、Citrix Hypervisor ホストで以下のコマンドを実行します。

```
1 xe secret-create value=my-password
```

シークレットが作成され、Citrix Hypervisor ホストに格納されます。このコマンドを使用すると、シークレットオブジェクトの UUID が出力されます。たとえば、`99945d96-5890-de2a-3899-8c04ef2521db` のようになります。`_secret` を `password` 引数の名前に追加し、この UUID がパスワードが必要なコマンドに渡されるようにします。

例：シークレットを作成した Citrix Hypervisor ホストで、以下のコマンドを実行できます：

```
1 xe sr-create device-config:location=sr_address device-config:type=cifs device-config:username=cifs_username \
```

```
2 device-config:cifspassword_secret=secret_uuid name-label="CIFS ISO
SR" type="iso" content-type="iso" shared="true"
```

## xe コマンドリファレンス

このセクションでは、コマンドが扱うオブジェクトによってコマンドをグループ化します。これらのオブジェクトはアルファベット順に表示されます。

### アプライアンスコマンド

vApp とも呼ばれる仮想アプライアンス (appliance オブジェクト) を作成または変更します。詳しくは、「[vApp](#)」を参照してください。

### appliance オブジェクトのパラメーター

appliance オブジェクトには、以下のパラメーターがあります:

| パラメーター名          | 説明            | 種類    |
|------------------|---------------|-------|
| uuid             | アプライアンスの UUID | 必須    |
| name-description | アプライアンスの説明文字列 | オプション |
| paused           |               | オプション |
| force            | 強制シャットダウン     | オプション |

### appliance-assert-can-be-recovered

```
1 appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid
=vd-uuid
```

この仮想アプライアンス/vApp を回復するためのストレージが使用可能かどうかをテストします。

### appliance-create

```
1 appliance-create name-label=name-label [name-description=name-
description]
```

仮想アプライアンス/vApp を作成します。次に例を示します:

```
1 xe appliance-create name=label=my_appliance
```

アプライアンスに仮想マシンを追加します。

```
1 xe vm-param-set uuid=VM-UUID appliance=appliance-uuid
```

### **appliance-destroy**

```
1 appliance-destroy uuid=appliance-uuid
```

仮想アプライアンス/vApp を破棄します。次に例を示します：

```
1 xe appliance-destroy uuid=appliance-uuid
```

### **appliance-recover**

```
1 appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [
 paused=true | false]
```

指定した VDI のデータベースから仮想アプライアンス/vApp を回復します。

### **appliance-shutdown**

```
1 appliance-shutdown uuid=appliance-uuid [force=true | false]
```

仮想アプライアンス/vApp のすべての仮想マシンをシャットダウンします。次に例を示します：

```
1 xe appliance-shutdown uuid=appliance-uuid
```

### **appliance-start**

```
1 appliance-start uuid=appliance-uuid [paused=true | false]
```

仮想アプライアンス/vApp を起動します。次に例を示します：

```
1 xe appliance-start uuid=appliance-uuid
```

## 監査コマンド

リソースプールの RBAC 監査ファイルのすべての記録をファイルとしてダウンロードします。オプションの `since` パラメーターを指定すると、その日時以降の記録のみがダウンロードされます。

### `audit-log-get` パラメーター

`audit-log-get` には次のパラメーターがあります

| パラメーター名               | 説明                                               | 種類    |
|-----------------------|--------------------------------------------------|-------|
| <code>filename</code> | プールの監査ログを <code>filename</code> で指定するファイルに書き込みます | 必須    |
| <code>since</code>    | 特定の日時以降の記録のみをダウンロードします                           | オプション |

### `audit-log-get`

```
1 audit-log-get [since=timestamp] filename=filename
```

指定した日時（ミリ秒単位）以降の監査ログをダウンロードします。

次のコマンドを実行します。

```
1 xe audit-log-get since=2009-09-24T17:56:20.530Z filename=/tmp/auditlog-pool-actions.out
```

## ボンディングコマンド

物理インターフェイスのフェールオーバーによる障害許容力のために、ネットワークボンドを操作します。詳しくは、「[ネットワーク](#)」を参照してください。

`bond` オブジェクトは、`master` と `member` の PIF を結合する参照オブジェクトです。master PIF は、`bond` オブジェクトを参照するために総体的な PIF として使用されるボンディングインターフェイスです。member PIF は、2 つ以上の物理インターフェイスのセットであり、高レベルのボンディングインターフェイスとして結束されています。

### `bond` オブジェクトのパラメーター

`bond` オブジェクトには、以下のパラメーターがあります。

| パラメーター名              | 説明                          | 種類     |
|----------------------|-----------------------------|--------|
| <code>uuid</code>    | ボンディングの一意の識別子/オブジェクト参照      | 読み取り専用 |
| <code>master</code>  | ボンドマスタ PIF の UUID           | 読み取り専用 |
| <code>members</code> | ボンディングを構成する PIF の UUID のセット | 読み取り専用 |

## **bond-create**

```
1 bond-create network-uuid=network_uuid pif-uuids=pif_uuid_1,pif_uuid_2
 ,...
```

既存の PIF オブジェクトをリストで指定して、指定したネットワーク上にボンディングネットワークインターフェイスを作成します。コマンドは、次のいずれかの場合に失敗します：

- PIF が既に別のボンドにある場合
- いずれかのメンバーに VLAN タグが設定されている場合
- 参照される PIF が同じ Citrix Hypervisor サーバーにない場合
- PIF が 2 個未満の場合

## **bond-destroy**

```
1 bond-destroy uuid=bond_uuid
```

UUID で指定したボンディングインターフェイスをホストから削除します。

## **bond-set-mode**

```
1 bond-set-mode uuid=bond_uuid mode=bond_mode
```

ボンディングモードを変更します。

## **CD** (仮想ネットワーク) コマンド

Citrix Hypervisor サーバー上の物理 CD/DVD ドライブ (cd オブジェクト) を操作します。

**cd** オブジェクトのパラメーター

cd オブジェクトには、以下のパラメーターがあります。

| パラメーター名                           | 説明                                                             | 種類               |
|-----------------------------------|----------------------------------------------------------------|------------------|
| <code>uuid</code>                 | CD の一意の識別子/オブジェクト参照                                            | 読み取り専用           |
| <code>name-label</code>           | CD の名前                                                         | 読み取り/書き込み        |
| <code>name-description</code>     | CD の説明文字列                                                      | 読み取り/書き込み        |
| <code>allowed-operations</code>   | この CD 上で実行できる操作のリスト                                            | 読み取り専用のセットパラメーター |
| <code>current-operations</code>   | この CD 上で現在処理中の操作のリスト                                           | 読み取り専用のセットパラメーター |
| <code>sr-uuid</code>              | この CD が属しているストレージリポジトリの一意の識別子/オブジェクト参照                         | 読み取り専用           |
| <code>sr-name-label</code>        | この CD が属しているストレージリポジトリの名前                                      | 読み取り専用           |
| <code>vbd-uuids</code>            | この CD に接続している仮想マシン上の VBD の一意の識別子のリスト                           | 読み取り専用のセットパラメーター |
| <code>crashdump-uuids</code>      | CD では使用されません。クラッシュダンプは CD に書き込むことができないため                       | 読み取り専用のセットパラメーター |
| <code>virtual-size</code>         | 仮想マシンに表示された CD のサイズ (バイト数)                                     | 読み取り専用           |
| <code>physical-utilisation</code> | ストレージリポジトリ上での CD イメージの物理スペース (バイト数)                            | 読み取り専用           |
| <code>type</code>                 | CD のユーザーに設定                                                    | 読み取り専用           |
| <code>sharable</code>             | CD ドライブが共有可能かどうか。デフォルトは <b>false</b> です。                       | 読み取り専用           |
| <code>read-only</code>            | CD が読み取り専用かどうか。 <b>false</b> の場合は書き込み可能。CD は常に <b>true</b> です。 | 読み取り専用           |

| パラメーター名                    | 説明                                                           | 種類                    |
|----------------------------|--------------------------------------------------------------|-----------------------|
| <code>storage-lock</code>  | このディスクがストレージレベルでロックされている場合は <b>true</b> 。                    | 読み取り専用                |
| <code>parent</code>        | この CD がチェーンの一部である場合は、親ディスクへの参照                               | 読み取り専用                |
| <code>missing</code>       | ストレージリポジトリのスキャン操作によりこの CD がディスク上に存在しないと認識された場合値は <b>true</b> | 読み取り専用                |
| <code>other-config</code>  | CD の追加構成パラメーターを指定するキー/値ペアのリスト                                | 読み取り/書き込み可のマッピングパラメータ |
| <code>location</code>      | このデバイスがマウントされているパス                                           | 読み取り専用                |
| <code>managed</code>       | デバイスが管理されている場合は <b>true</b>                                  | 読み取り専用                |
| <code>xenstore-data</code> | <code>xenstore</code> ツリーに挿入されるべきデータ                         | 読み取り専用のマッピングパラメータ     |
| <code>sm-config</code>     | ストレージマネージャーデバイス設定キーの名前と説明                                    | 読み取り専用のマッピングパラメータ     |
| <code>is-a-snapshot</code> | このテンプレートが CD スナップショットの場合は <b>true</b>                        | 読み取り専用                |
| <code>snapshot_of</code>   | このテンプレートのスナップショット元の CD の UUID                                | 読み取り専用                |
| <code>snapshots</code>     | この CD から作成されたすべてのスナップショットの UUID                              | 読み取り専用                |
| <code>snapshot_time</code> | スナップショット作成日時                                                 | 読み取り専用                |

## cd-list

```
1 cd-list [params=param1,param2,...] [parameter=parameter_value]
```

Citrix Hypervisor サーバーまたはリソースプール上の CD と ISO (CD イメージファイル) のリストを、オプションの引数 `params` に基づいてフィルターして出力します。

オプションの引数 `params` を使用して特定のパラメーター値を持つオブジェクトだけを出力する (つまりリストをフィルタする) 場合は、そのオブジェクトのパラメーターのリストを含む文字列を値として指定します。または、キー

ワード `all` を指定してすべてのパラメーターのリストを出力することもできます。 `params` を使用しない場合、使用可能なすべてのパラメーターのうち、デフォルトのサブセットが出力されます。

オプションの引数には、 `cd` オブジェクトのパラメーターから任意の数を指定できます。

## クラスターコマンド

クラスター化されたプールを操作します。

クラスター化されたプールは、クラスタリング機能が有効になっているリソースプールです。GFS2 ストレージリポジトリと共にこれらのプールを使用します。詳しくは、「[クラスター化プール](#)」を参照してください。

クラスターおよびクラスターホストのオブジェクトのリストは、標準オブジェクトリストコマンド (`xe cluster-list` および `xe cluster-host-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「[低レベルパラメーターコマンド](#)」を参照してください。

クラスター化されたプールを操作します。

## クラスターパラメーター

クラスターには次のパラメーターがあります：

| パラメーター名                         | 説明                                                                         | 種類               |
|---------------------------------|----------------------------------------------------------------------------|------------------|
| <code>uuid</code>               | クラスターの一意の識別子/オブジェクト参照                                                      | 読み取り専用           |
| <code>cluster-hosts</code>      | クラスター内のホストの一意の識別子/オブジェクト参照のリスト                                             | 読み取り専用のセットパラメーター |
| <code>cluster-token</code>      | <code>xapi-clusterd</code> が他のホスト上で自身と通信するときに使用する秘密キー                      | 読み取り専用           |
| <code>cluster-stack</code>      | クラスタリング機能を提供するテクノロジスタック。使用できる値は <code>corosync</code> です。                  | 読み取り専用           |
| <code>allowed-operations</code> | 現在の状態で可能な操作のリスト。このリストは参考用で、クライアントがこのフィールドを読み取る時点でクラスターの状態が変更されている可能性もあります。 | 読み取り専用のセットパラメーター |

| パラメーター名                                | 説明                                                                                | 種類                   |
|----------------------------------------|-----------------------------------------------------------------------------------|----------------------|
| <code>current-operations</code>        | 現在処理中の操作のリスト。このリストは参考用で、クライアントがこのフィールドを読み取る時点でクラスターの状態が変更されている可能性もあります。           | 読み取り専用のセットパラメーター     |
| <code>token-timeout</code>             | <code>corosync</code> トークンのタイムアウト (秒単位)                                           | 読み取り専用               |
| <code>token-timeout-coefficient</code> | <code>corosync</code> トークンのタイムアウト係数 (秒単位)                                         | 読み取り専用               |
| <code>pool-auto-join</code>            | 新しいプールメンバーをクラスターに自動的に参加させる場合は <code>true</code> 。これは <code>true</code> に設定されています。 | 読み取り専用               |
| <code>cluster-config</code>            | クラスターの追加構成パラメーターを指定するキー/値ペアのリスト                                                   | 読み取り専用のマップパラメーター     |
| <code>other-config</code>              | クラスターの追加構成パラメーターを指定するキー/値ペアのリスト                                                   | 読み取り/書き込み可のマップパラメーター |

## cluster-host-create

```
1 cluster-host-create cluster-uuid=cluster_uuid host-uuid=host_uuid pif-uuid=pif_uuid
```

既存のクラスターにホストを追加します。

## cluster-host-destroy

```
1 cluster-host-destroy uuid=host_uuid
```

クラスターホストを破棄して、クラスターを効果的に残します。

## cluster-host-disable

```
1 cluster-host-disable uuid=cluster_uuid
```

有効なクラスターホストのクラスターメンバーシップを無効にします。

### **cluster-host-enable**

```
1 cluster-host-enable uuid=cluster_uuid
```

無効になっているクラスターホストのクラスターメンバーシップを有効にします。

### **cluster-host-force-destroy**

```
1 cluster-host-force-destroy uuid=cluster_host
```

クラスターホストオブジェクトを強制的に破棄して、クラスターを効果的に残します。

### **cluster-pool-create**

```
1 cluster-pool-create network-uuid=network_uuid [cluster-stack=
cluster_stack] [token-timeout=token_timeout] [token-timeout-
coefficient=token_timeout_coefficient]
```

プール全体のクラスターを作成します。

### **cluster-pool-destroy**

```
1 cluster-pool-destroy cluster-uuid=cluster_uuid
```

プール全体のクラスターを破棄します。プールは引き続き存在しますが、クラスター化されなくなり、GFS2 ストレージレポジトリを使用できなくなります。

### **cluster-pool-force-destroy**

```
1 cluster-pool-force-destroy cluster-uuid=cluster_uuid
```

プール全体のクラスターを強制的に破棄します。

### **cluster-pool-resync**

```
1 cluster-pool-resync cluster-uuid=cluster_uuid
```

プール全体でクラスターを再同期します。

## コンソールコマンド

コンソール (console オブジェクト) を操作します。

console オブジェクトのリストは、標準オブジェクトリストコマンド (`xe console-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### console オブジェクトのパラメーター

console オブジェクトには、以下のパラメーターがあります。

| パラメーター名                    | 説明                                                                                                                                                                    | 種類                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <code>uuid</code>          | コンソールの一意の識別子/オブジェクト参照                                                                                                                                                 | 読み取り専用                 |
| <code>vm-uuid</code>       | このコンソールを開いている VM の一意の識別子/オブジェクト参照                                                                                                                                     | 読み取り専用                 |
| <code>vm-name-label</code> | このコンソールを開いている VM の名前                                                                                                                                                  | 読み取り専用                 |
| <code>protocol</code>      | このコンソールが使用するプロトコル。 <code>vt100</code> : VT100 ターミナル、 <code>rfb</code> : Remote Framebuffer プロトコル (VNC で使用)、または <code>rdp</code> : Remote Desktop Protocol (RDP) のいずれか | 読み取り専用                 |
| <code>location</code>      | このコンソールのサービスの URI                                                                                                                                                     | 読み取り専用                 |
| <code>other-config</code>  | コンソールの追加構成パラメーターを指定するキー/値ペアのリスト                                                                                                                                       | 読み取り/書き込み可のマッピングパラメーター |

### console

```
1 console
```

特定のコンソールに接続します。

## 診断コマンド

診断情報を Citrix Hypervisor から収集するためのコマンドです。

### **diagnostic-compact**

```
1 diagnostic-compact
```

主要な GC 収集とヒープの圧縮を実行します。

### **diagnostic-db-log**

```
1 diagnostic-db-log
```

データベース操作のロギングを開始します。警告：一度起動すると停止できません。

### **diagnostic-db-stats**

```
1 diagnostic-db-stats
```

データベース統計を出力します。

### **diagnostic-gc-stats**

```
1 diagnostic-gc-stats
```

GC 統計を出力します。

### **diagnostic-license-status**

```
1 diagnostic-license-status
```

プール全体のライセンス問題を診断するのに役立ちます。

### **diagnostic-net-stats**

```
1 diagnostic-net-stats [uri=uri] [method=method] [params=param1,param2
...]
```

ネットワーク統計を出力します。

### **diagnostic-timing-stats**

```
1 diagnostic-timing-stats
```

タイミング統計を出力する。

### **diagnostic-vdi-status**

```
1 diagnostic-vdi-status uuid=vdi_uuid
```

VDI のロックおよび共有状態を照会します。

### **diagnostic-vm-status**

```
1 diagnostic-vm-status uuid=vm_uuid
```

VM が起動できるホストを照会し、すべての VBD の共有/ロック状態を確認します。

### **障害回復コマンド**

障害発生後に仮想マシンを回復するコマンドです。

### **drtask-create**

```
1 drtask-create type=type sr-whitelist=sr-white-list device-config=device
-config
```

障害回復タスクを作成します。たとえば、障害回復の準備タスクとして特定の iSCSI ストレージリポジトリに接続するには、次のコマンドを実行します。

```
1 xe drtask-create type=lvmoiscsi device-config:target=target-ip-address
 \
2 device-config:targetIQN=targetIQN device-config:SCSIid=SCSIid \
3 sr-whitelist=sr-uuid-list
```

注:

コマンド `sr-whitelist` はストレージリポジトリ UUID をリストします。`drtask-create` コマンドは、ホワイトリストに登録された UUID の 1 つを持つストレージリポジトリのみを導入して接続します

### **drtask-destroy**

```
1 drtask-destroy uuid=dr-task-uuid
```

障害回復タスクを破棄してストレージリポジトリの接続を消去します。

### **vm-assert-can-be-recovered**

```
1 vm-assert-can-be-recovered uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

特定の仮想マシンを回復するためにストレージを使用できるかどうかをテストします。

### **appliance-assert-can-be-recovered**

```
1 appliance-assert-can-be-recovered uuid=appliance-uuid database:vdi-uuid
=vdi-uuid
```

仮想アプライアンス/vApp ディスクを格納しているストレージが使用可能かどうかをチェックします。

### **appliance-recover**

```
1 appliance-recover uuid=appliance-uuid database:vdi-uuid=vdi-uuid [force
=true | false]
```

指定した VDI のデータベースから仮想アプライアンス/vApp を回復します。

**vm-recover**

```
1 vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid [force=true|false]
```

指定した VDI のデータベースから仮想マシンを回復します。

**sr-enable-database-replication**

```
1 sr-enable-database-replication uuid=sr-uuid
```

指定した（共有）ストレージリポジトリへの XAPI データベースの複製を有効にします。

**sr-disable-database-replication**

```
1 sr-disable-database-replication uuid=sr-uuid
```

指定したストレージリポジトリへの XAPI データベースの複製を無効にします。

## 使用例

ここでは、障害回復コマンドの使用例を順に挙げます。

プライマリサイトで、データベースの複製を有効にします。

```
1 xe sr-database-replication uuid=sr-uuid
```

障害発生後、セカンダリサイトでストレージリポジトリに接続します。device-config コマンドには sr-probe と同じフィールドがあります。

```
1 xe drtask-create type=lvmoiscsi \
2 device-config:target=target ip address \
3 device-config:targetIQN=target-iqn \
4 device-config:SCSIid=scsi-id \
5 sr-whitelist=sr-uuid
```

ストレージリポジトリ上のデータベース VDI を見つけます。

```
1 xe vdi-list sr-uuid=sr-uuid type=Metadata
```

データベース VDI から仮想マシンを照会します。

```
1 xe vm-list database:vdi-uuid=vdi-uuid
```

仮想マシンを回復します。

```
1 xe vm-recover uuid=vm-uuid database:vdi-uuid=vdi-uuid
```

障害回復タスクを破棄します。このタスクによりイントロデュースされ、かつ仮想マシンで使用されないすべてのストレージリポジトリを破棄します：

```
1 xe drtask-destroy uuid=drtask-uuid
```

## イベントコマンド

イベント (event オブジェクト) を操作します。

### event オブジェクトのクラス

event オブジェクトには、以下のクラスがあります。

| クラス名    | 説明                                                      |
|---------|---------------------------------------------------------|
| pool    | 物理ホストのリソースプール                                           |
| vm      | 仮想マシン                                                   |
| host    | 物理ホスト                                                   |
| network | 仮想ネットワーク                                                |
| vif     | 仮想ネットワークインターフェイス                                        |
| pif     | 物理ネットワークインターフェイス (NIC に関連付けられた各 VLAN は個別の PIF として表されます) |
| sr      | ストレージレポジトリ                                              |
| vdi     | 仮想ディスクイメージ                                              |
| vbd     | 仮想ブロックデバイス                                              |
| pbd     | ホストがストレージレポジトリへのアクセスに使用する物理ブロックデバイス                     |

### event-wait

```
1 event-wait class=class_name [param-name=param_value] [param-name=/=param_value]
```

このコマンドでは、コマンドラインで指定した条件を満たすオブジェクトが存在するようになるまで、ほかのコマンドの実行をブロックします。`x=y`は「フィールド `x` の値が `y` になるまで待機する」、`x!=y`は、「フィールド `x` の値が `y` 以外になるまで待機する」を意味します。

例：特定の仮想マシンが実行状態になるまで待機する場合は、次のコマンドを実行します。

```
1 xe event-wait class=vm name-label=myvm power-state=running
```

このコマンドでは、`myvm`という名前の仮想マシンの`power-state`が「`running`」になるまで、ほかのコマンドの実行をブロックします。

例：特定の仮想マシンが再起動するまで待機する場合は、次のコマンドを実行します。

```
1 xe event-wait class=vm uuid=$VM start-time!=$(xe vm-list uuid=$VM
 params=start-time --minimal)
```

このコマンドでは、UUID が `$VM` の仮想マシンが再起動するまで、ほかのコマンドの実行をブロックします。このコマンドは`start-time`の値で仮想マシンがいつ再起動するかを決定します。

クラス名は、このセクションの冒頭に挙げられているevent オブジェクトのクラスから選ぶことができます。パラメーターは、CLI コマンドの `class-param-list` にリストされているパラメーターから選ぶことができます。

## GPU コマンド

物理 GPU (pgpu)、GPU グループ (gpu-group)、および仮想 GPU (vgpu) を操作します。

GPU オブジェクトは、次の標準的なオブジェクトリストコマンドでリストできます：`xe pgpu-list`、`xe gpu-group-list`、`xe vgpu-list`。パラメーターは標準パラメーターコマンドで操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### 物理 GPU のパラメーター

物理 GPU (pGPU) には、以下のパラメーターがあります：

| パラメーター名                  | 説明                      | 種類     |
|--------------------------|-------------------------|--------|
| <code>uuid</code>        | 物理 GPU の一意の識別子/オブジェクト参照 | 読み取り専用 |
| <code>vendor-name</code> | 物理 GPU ベンダの名前           | 読み取り専用 |
| <code>device-name</code> | ベンダが物理 GPU モデルに割り当てた名前  | 読み取り専用 |

| パラメーター名                           | 説明                                                                                                     | 種類                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------|
| <code>gpu-group-uuid</code>       | この物理 GPU が Citrix Hypervisor により自動的に割り当てられた GPU グループの一意の識別子/オブジェクト参照。プール内のすべてのホスト上の同一物理 GPU がグループ化されます | 読み取り専用                |
| <code>gpu-group-name-label</code> | この物理 GPU が割り当てられた GPU グループの名前                                                                          | 読み取り専用                |
| <code>host-uuid</code>            | この物理 GPU が接続している Citrix Hypervisor サーバーの一意の識別子/オブジェクト参照                                                | 読み取り専用                |
| <code>host-name-label</code>      | この物理 GPU が接続している Citrix Hypervisor サーバーの名前                                                             | 読み取り専用                |
| <code>pci-id</code>               | PCI identifier                                                                                         | 読み取り専用                |
| <code>dependencies</code>         | 同一仮想マシンにパススルーされる依存 PCI デバイスのリスト                                                                        | 読み取り/書き込み可のマッピングパラメータ |
| <code>other-config</code>         | 物理 GPU の追加構成パラメーターを指定するキー/値ペアのリスト                                                                      | 読み取り/書き込み可のマッピングパラメータ |
| <code>supported-VGPU-types</code> | ハードウェアでサポートされる仮想 GPU の一覧                                                                               | 読み取り専用                |
| <code>enabled-VGPU-types</code>   | この物理 GPU で有効な仮想 GPU の一覧                                                                                | 読み取り/書き込み             |
| <code>resident-VGPUs</code>       | この物理 GPU で実行中の仮想 GPU の一覧                                                                               | 読み取り専用                |

### **`pgpu-disable-dom0-access`**

```
1 pgpu-disable-dom0-access uuid=uuid
```

dom0 への PGPU アクセスを無効にします。

### **`pgpu-enable-dom0-access`**

```
1 pgpu-enable-dom0-access uuid=uuid
```

dom0 への PGPU アクセスを有効にします。

### gpu-group オブジェクトのパラメーター

gpu-group オブジェクトには、以下のパラメーターがあります。

| パラメーター名              | 説明                                      | 種類                   |
|----------------------|-----------------------------------------|----------------------|
| uuid                 | GPU グループの一意的識別子/オブジェクト参照                | 読み取り専用               |
| name-label           | GPU グループの名前                             | 読み取り/書き込み            |
| name-description     | GPU グループの説明文字列                          | 読み取り/書き込み            |
| VGPU-uuids           | GPU グループ内の仮想 GPU の一意的識別子/オブジェクト参照の一覧    | 読み取り専用のセットパラメーター     |
| PGPU-uuids           | GPU グループ内の物理 GPU の一意的識別子/オブジェクト参照のリスト   | 読み取り専用のセットパラメーター     |
| other-config         | GPU グループの追加構成パラメーターを指定するキー/値ペアのリスト      | 読み取り/書き込み可のマップパラメーター |
| supported-VGPU-types | ハードウェアでサポートされるすべての仮想 GPU の一覧            | 読み取り専用               |
| enabled-VGPU-types   | 物理 GPU で有効なすべての仮想 GPU の一覧               | 読み取り専用               |
| allocation-algorithm | グループ内の物理 GPU に割り当てられた仮想 GPU の深さ優先/幅優先設定 | 読み取り/書き込み可の列挙型パラメーター |

### GPU グループの操作

GPU グループを操作するコマンド

#### gpu-group-create

```
1 gpu-group-create name=label=name_for_group [name-description=
description]
```

物理 GPU が移動できる新規（空の）GPU グループを作成します。

### gpu-group-destroy

```
1 gpu-group-destroy uuid=uuid_of_group
```

GPU グループを破棄します。対象は空のグループのみです。

### gpu-group-get-remaining-capacity

```
1 gpu-group-get-remaining-capacity uuid=uuid_of_group vgpu-type-uuid=
uuid_of_vgpu_type
```

GPU グループでインスタンス化できる、指定した種類の仮想 GPU の数を返します。

### gpu-group-param-set

```
1 gpu-group-param-set uuid=uuid_of_group allocation-algorithm=breadth-
first|depth-first
```

GPU グループが仮想 GPU を物理 GPU に割り当てるために使用するアルゴリズムを変更します。

### gpu-group-param-get-uuid

```
1 gpu-group-param-get-uuid uuid=uuid_of_group param-name=supported-vGPU-
types|enabled-vGPU-types
```

この GPU グループでサポートされるかまたは有効な種類を返します。

仮想 **GPU** のパラメーター

仮想 GPU には、以下のパラメーターがあります。

| パラメーター名           | 説明                      | 種類     |
|-------------------|-------------------------|--------|
| <code>uuid</code> | 仮想 GPU の一意の識別子/オブジェクト参照 | 読み取り専用 |

| パラメーター名                           | 説明                                              | 種類                     |
|-----------------------------------|-------------------------------------------------|------------------------|
| <code>vm-uuid</code>              | この仮想 GPU が割り当てられた仮想マシンの一意の識別子/オブジェクト参照          | 読み取り専用                 |
| <code>vm-name-label</code>        | この仮想 GPU が割り当てられた仮想マシンの名前                       | 読み取り専用                 |
| <code>gpu-group-uuid</code>       | この仮想 GPU を含んでいる GPU グループの一意の識別子/オブジェクト参照        | 読み取り専用                 |
| <code>gpu-group-name-label</code> | この仮想 GPU を含んでいる GPU グループの名前                     | 読み取り専用                 |
| <code>currently-attached</code>   | GPU パススルーを使用する仮想マシンが実行中の場合は true、そうでない場合は false | 読み取り専用                 |
| <code>other-config</code>         | 仮想 GPU の追加構成パラメーターを指定するキー/値ペアのリスト               | 読み取り/書き込み可のマッピングパラメーター |
| <code>type-uuid</code>            | この仮想 GPU の仮想 GPU の種類の一意的識別子/オブジェクト参照            | 読み取り/書き込み可のマッピングパラメーター |
| <code>type-model-name</code>      | 仮想 GPU に関連付けられているモデル名                           | 読み取り専用                 |

#### 仮想 GPU のパラメーター

注:

GPU ベンダーが提供するサポートされるソフトウェアおよびグラフィックカードがないと、GPU パススルーおよび仮想 GPU は、ライブマイグレーション、ストレージライブマイグレーションおよび仮想マシンの一時停止で機能しません。つまり、このサポートがなければダウンタイムを回避するために仮想マシンを移行することはできません。NVIDIA vGPU とライブマイグレーション、ストレージライブマイグレーション、および仮想マシンの一時停止との互換性については、「[グラフィック](#)」を参照してください。

仮想 GPU の種類には、以下のパラメーターがあります。

| パラメーター名                  | 説明                         | 種類     |
|--------------------------|----------------------------|--------|
| <code>uuid</code>        | 仮想 GPU の種類の一意的識別子/オブジェクト参照 | 読み取り専用 |
| <code>vendor-name</code> | 仮想 GPU のベンダー名              | 読み取り専用 |

| パラメーター名                        | 説明                         | 種類     |
|--------------------------------|----------------------------|--------|
| <code>model-name</code>        | 仮想 GPU に関連付けられているモデル名      | 読み取り専用 |
| <code>freeze-frame</code>      | 仮想 GPU のフレームバッファサイズ (バイト数) | 読み取り専用 |
| <code>max-heads</code>         | 仮想 GPU でサポートされるディスプレイの最大数  | 読み取り専用 |
| <code>supported-on-PGUs</code> | この仮想 GPU をサポートする物理 GPU の一覧 | 読み取り専用 |
| <code>enabled-on-PGUs</code>   | この仮想 GPU が有効な物理 GPU の一覧    | 読み取り専用 |
| <code>VGPU-uuids</code>        | この種類の仮想 GPU の一覧            | 読み取り専用 |

## 仮想 GPU の操作

### `vgpu-create`

```
1 vgpu-create vm-uuid=uuid_of_vm gpu_group_uuid=uuid_of_gpu_group [vgpu-type-uuid=uuid_of_vgpu-type]
```

仮想 GPU を作成します。仮想マシンを指定した GPU グループに接続し、必要に応じて仮想 GPU の種類を指定します。仮想 GPU の種類を指定しない場合は、「パススルー」が割り当てられます。

### `vgpu-destroy`

```
1 vgpu-destroy uuid=uuid_of_vgpu
```

指定した仮想 GPU を破棄します。

## 仮想 GPU を持つ仮想マシンの VNC の無効化

```
1 xe vm-param-add uuid=uuid_of_vmparam-name=platform vgpu_vnc_enabled=true|false
```

`false` を指定すると、`disablevnc=1` がディスプレイエミュレーターに渡され、仮想マシンの VNC が無効になります。デフォルトでは、VNC は有効になっています。

## ホストコマンド

Citrix Hypervisor サーバー (host オブジェクト) を操作します。

Citrix Hypervisor サーバーとは、Citrix Hypervisor ソフトウェアを実行している物理サーバーを指します。これらのサーバー上では仮想マシンが実行され、コントロールドメインまたはドメイン 0 と呼ばれる特殊な権限を持つ仮想マシンにより制御されます。

Citrix Hypervisor サーバーオブジェクトは、次の標準的なオブジェクトリストコマンドでリストできます: `xe host-list`、`xe host-cpu-list`、`xe host-crashdump-list`。パラメーターは標準パラメーターコマンドで操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### host オブジェクトセレクター

ここで説明する多くのコマンドでは、1 つまたは複数の Citrix Hypervisor サーバーを操作対象として選択するための共通のメカニズムがあります。最も簡単なのは、引数 `host=uuid_or_name_label` を指定することです。また、すべての host オブジェクトのリストを、フィールドの値に基づいてフィルターして、Citrix Hypervisor を指定することもできます。たとえば、`enabled=true` と指定すると、`enabled` フィールドが `true` の Citrix Hypervisor サーバーがすべて操作対象として選択されます。複数の Citrix Hypervisor サーバーがフィルター条件に一致し、その複数の Citrix Hypervisor サーバーで操作を実行する場合は、`--multiple` を指定する必要があります。指定できるすべてのパラメーターの一覧は、次の表のとおりです。このコマンドのリストを取得するには、コマンド `xe host-list params=all` を実行します。Citrix Hypervisor サーバーを選択するパラメーターを指定しない場合、すべての Citrix Hypervisor サーバーに対してその操作が実行されます。

### host オブジェクトのパラメーター

Citrix Hypervisor サーバーには、次のパラメーターがあります：

| パラメーター名                       | 説明                                     | 種類        |
|-------------------------------|----------------------------------------|-----------|
| <code>uuid</code>             | Citrix Hypervisor サーバーの一意の識別子/オブジェクト参照 | 読み取り専用    |
| <code>name-label</code>       | Citrix Hypervisor サーバーの名前              | 読み取り/書き込み |
| <code>name-description</code> | Citrix Hypervisor サーバーの説明文字列           | 読み取り専用    |

| パラメーター名                           | 説明                                                                                                         | 種類                   |
|-----------------------------------|------------------------------------------------------------------------------------------------------------|----------------------|
| enabled                           | 無効になっている場合は <b>false</b> です。これにより、新しい仮想マシンがホスト上で起動するのを防ぎ、ホストのシャットダウンまたは再起動を準備します。ホストが有効な場合は <b>true</b> です | 読み取り専用               |
| API-version-major                 | メジャーバージョン番号                                                                                                | 読み取り専用               |
| API-version-minor                 | マイナーバージョン番号                                                                                                | 読み取り専用               |
| API-version-vendor                | API ベンダーの ID                                                                                               | 読み取り専用               |
| API-version-vendor-implementation | ベンダー実装の詳細                                                                                                  | 読み取り専用のマップパラメーター     |
| logging                           | ログ設定                                                                                                       | 読み取り/書き込み可のマップパラメーター |
| suspend-image-sr-uuid             | 一時停止状態のイメージが格納されるストレージリポジトリの一意的識別子/オブジェクトリファレンス                                                            | 読み取り/書き込み            |
| crash-dump-sr-uuid                | クラッシュダンプが格納されるストレージリポジトリの一意的識別子/オブジェクトリファレンス                                                               | 読み取り/書き込み            |
| software-version                  | バージョン管理パラメーターとその値のリスト                                                                                      | 読み取り専用のマップパラメーター     |
| capabilities                      | Citrix Hypervisor サーバーを実行できる Xen のバージョンのリスト                                                                | 読み取り専用のセットパラメーター     |
| other-config                      | Citrix Hypervisor サーバーの追加構成パラメーターを指定するキー/値ペアのリスト                                                           | 読み取り/書き込み可のマップパラメーター |
| chipset-info                      | チップセットの追加設定パラメーターを指定するキー/値ペアのリスト                                                                           | 読み取り専用のマップパラメーター     |
| hostname                          | Citrix Hypervisor サーバーのホスト名                                                                                | 読み取り専用               |
| address                           | Citrix Hypervisor サーバーの IP アドレス                                                                            | 読み取り専用               |

| パラメーター名                            | 説明                                                                                                                                       | 種類                   |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <code>license-server</code>        | ライセンスサーバーの情報を指定するキー/値ペアのリスト。Citrix 製品との通信では、デフォルトでポート 27000 が使用されます。競合が原因でポート番号を変更する場合の手順について詳しくは、「 <a href="#">ポート番号の変更</a> 」を参照してください。 | 読み取り専用のマップパラメーター     |
| <code>supported-bootloaders</code> | Citrix Hypervisor サーバーがサポートするブートローダーの一覧。<br><code>pygrub</code> 、 <code>eliloader</code> など                                              | 読み取り専用のセットパラメーター     |
| <code>memory-total</code>          | Citrix Hypervisor サーバー上の物理 RAM の量 (バイト数)                                                                                                 | 読み取り専用               |
| <code>memory-free</code>           | 仮想マシンに割り当てることができる物理 RAM の残量 (バイト数)                                                                                                       | 読み取り専用               |
| <code>host-metrics-live</code>     | このホストが動作可能な場合は <code>true</code>                                                                                                         | 読み取り専用               |
| <code>logging</code>               | <code>syslog_destination</code> キーでリモートの syslog サービスのホスト名を設定。                                                                            | 読み取り/書き込み可のマップパラメーター |
| <code>allowed-operations</code>    | 現在の状態で可能な操作のリスト。このリストは参考用で、クライアントがこのフィールドを読み取る時点でサーバーの状態が変更されている可能性もあります。                                                                | 読み取り専用のセットパラメーター     |
| <code>current-operations</code>    | 現在処理中の操作のリスト。このリストは参考用で、クライアントがこのフィールドを読み取る時点でサーバーの状態が変更されている可能性もあります。                                                                   | 読み取り専用のセットパラメーター     |
| <code>patches</code>               | ホストに対するパッチのセット                                                                                                                           | 読み取り専用のセットパラメーター     |
| <code>blobs</code>                 | バイナリデータストア                                                                                                                               | 読み取り専用               |
| <code>memory-free-computed</code>  | ホスト上の空きメモリ量 (少なくとも見積もった量)                                                                                                                | 読み取り専用               |

| パラメーター名                                  | 説明                                | 種類               |
|------------------------------------------|-----------------------------------|------------------|
| <code>ha-statefiles</code>               | 高可用性ステートファイルの UUID                | 読み取り専用           |
| <code>ha-network-peers</code>            | 障害発生時にこのホスト上の仮想マシンを実行できるホストの UUID | 読み取り専用           |
| <code>external-auth-type</code>          | 外部認証の種類 (Active Directory など)     | 読み取り専用           |
| <code>external-auth-service-name</code>  | 外部認証サービスの名前                       | 読み取り専用           |
| <code>external-auth-configuration</code> | 外部認証サービスの構成情報                     | 読み取り専用のマップパラメーター |

Citrix Hypervisor サーバーには、パラメーターリストを持つ以下のオブジェクトも含まれています。

Citrix Hypervisor サーバーの CPU には、次のパラメーターがあります：

| パラメーター名                  | 説明                                                   | 種類     |
|--------------------------|------------------------------------------------------|--------|
| <code>uuid</code>        | CPU の一意の識別子/オブジェクト参照                                 | 読み取り専用 |
| <code>number</code>      | Citrix Hypervisor サーバー内の物理 CPU コアの数                  | 読み取り専用 |
| <code>vendor</code>      | CPU 名のベンダー文字列                                        | 読み取り専用 |
| <code>speed</code>       | CPU のクロック速度 (Hz 数)                                   | 読み取り専用 |
| <code>modelname</code>   | CPU モデルのベンダー文字列。たとえば「Intel(R) Xeon(TM) CPU 3.00 GHz」 | 読み取り専用 |
| <code>stepping</code>    | CPU のリビジョン番号                                         | 読み取り専用 |
| <code>flags</code>       | 物理 CPU のフラグ (features フィールドのデコード版)                   | 読み取り専用 |
| <code>Utilisation</code> | 現在の CPU 使用率                                          | 読み取り専用 |
| <code>host-uuid</code>   | この CPU が動作するホストの UUID                                | 読み取り専用 |
| <code>model</code>       | 物理 CPU のモデル番号                                        | 読み取り専用 |

| パラメーター名             | 説明              | 種類     |
|---------------------|-----------------|--------|
| <code>family</code> | 物理 CPU のファミリー番号 | 読み取り専用 |

Citrix Hypervisor サーバーのクラッシュダンプ (crashdump オブジェクト) には、以下のパラメーターがあります:

| パラメーター名                | 説明                                                                                             | 種類     |
|------------------------|------------------------------------------------------------------------------------------------|--------|
| <code>uuid</code>      | クラッシュダンプの一意の識別子/オブジェクト参照                                                                       | 読み取り専用 |
| <code>host</code>      | クラッシュダンプが対応する Citrix Hypervisor サーバー                                                           | 読み取り専用 |
| <code>timestamp</code> | クラッシュダンプの日時。形式は <code>yyyymmdd-hhmmss-ABC</code> (ここで <code>ABC</code> は GMT などのタイムゾーンインジケーター) | 読み取り専用 |
| <code>size</code>      | クラッシュダンプのサイズ (バイト数)                                                                            | 読み取り専用 |

## host-all-editions

```
1 host-all-editions
```

利用可能なすべてのエディションのリストを取得します

## host-apply-edition

```
1 host-apply-edition [host-uuid=host_uuid] [edition=xenserver_edition="free" "per-socket" "xendesktop"]
```

特定エディションの Citrix Hypervisor ライセンスをホストサーバーに割り当てます。Citrix Hypervisor は、指定された種類のライセンスをライセンスサーバーに要求し、割り当て可能なライセンスがある場合はそれをライセンスサーバーからチェックアウトします。

Citrix Virtual Desktops の Citrix Hypervisor の場合、`"xendesktop"` を使用します。

初期ライセンス設定については、`license-server-address` および `license-server-port` も参照してください。

## host-backup

```
1 host-backup file-name=backup_filename host=host_name
```

このコマンドでは、指定した Citrix Hypervisor サーバーのコントロールドメインのバックアップを、コマンドの実行元マシンにダウンロードし、`file-name`のファイル名で保存します。

### 重要:

`xe host-backup` コマンドは、ローカルホスト上（つまり特定のホスト名を指定せずに）実行しても機能しますが、そのように使用しないでください。これを行うと、コントロールドメインのパーティションに大きなバックアップファイルが作成され、空きディスク容量が足りなくなります。このコマンドは、バックアップファイルを保持できるディスク領域があるリモートコンピューターからのみ使用してください。

## host-bugreport-upload

```
1 host-bugreport-upload [host-selector=host_selector_value...] [url=destination_url http-proxy=http_proxy_name]
```

このコマンドでは、新しいバグレポート（`xen-bugtool` を使って、すべてのオプションファイルを含めて）を生成し、サポート FTP サイトなどにアップロードします。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

オプションのパラメーターは、`http-proxy`: 使用する HTTP プロキシを指定する、および `url`: アップロード先を指定する URL です。これらのオプションパラメーターを使用しない場合、プロキシサーバーは特定されず、デフォルトのサポート FTP サイトにアップロードされます。

## host-call-plugin

```
1 host-call-plugin host-uuid=host_uuid plugin=plugin fn=function [args=args]
```

オプションの引数を指定して、指定されたホスト上のプラグイン内の関数を呼び出します。

## host-compute-free-memory

```
1 host-compute-free-memory
```

ホスト上の空きメモリの量を計算します。

## host-compute-memory-overhead

```
1 host-compute-memory-overhead
```

ホストの仮想化メモリアーヘッドを計算します。

## host-cpu-info

```
1 host-cpu-info [uuid=uuid]
```

ホストの物理 CPU に関する情報を一覧表示します。

## host-crashdump-destroy

```
1 host-crashdump-destroy uuid=crashdump_uuid
```

このコマンドでは、UUID で指定したクラッシュダンプを Citrix Hypervisor サーバーから削除します。

## host-crashdump-upload

```
1 host-crashdump-upload uuid=crashdump_uuid [url=destination_url] [http-proxy=http_proxy_name]
```

このコマンドでは、クラッシュダンプをサポート FTP サイトなどにアップロードします。これらのオプションパラメーターを使用しない場合、プロキシサーバーは特定されず、デフォルトのサポート FTP サイトにアップロードされます。オプションのパラメーターは、`http-proxy`: 使用する HTTP プロキシを指定する、および `url`: アップロード先を指定する URL です。

## host-declare-dead

```
1 host-declare-dead uuid=host_uuid
```

ホストが明示的に通信しておらず使用不可であることを宣言します。

**警告:**

この呼び出しは危険で、ホストが実際には使用可能な場合はデータを失う可能性があります。

## host-disable

```
1 host-disable [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーが無効になり、新しい仮想マシンがそのサーバー上で起動しなくなります。これにより、その Citrix Hypervisor サーバーがシャットダウンまたは再起動できる状態になります。

このコマンドの対象ホストを指定するには、host オブジェクトセレクターで説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

## host-disable-display

```
1 host-disable-display uuid=host_uuid
```

ホストの表示を無効にします。

## host-disable-local-storage-caching

```
1 host-disable-local-storage-caching
```

指定されたホスト上のローカルストレージキャッシュを無効にします。

## host-dmesg

```
1 host-dmesg [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーから Xen dmesg（カーネルリングバッファの出力）を取得します。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

## host-emergency-ha-disable

```
1 host-emergency-ha-disable [--force]
```

ローカルホスト上の高可用性を無効にします。破損した高可用性セットアップでプールを回復するためにのみ使用されます。

## host-emergency-management-reconfigure

```
1 host-emergency-management-reconfigure interface=
 uuid_of_management_interface_pif
```

このコマンドでは、この Citrix Hypervisor サーバーの管理インターフェイスを設定し直します。このコマンドは、Citrix Hypervisor サーバーが緊急モードの場合のみ使用します。緊急モードとは、あるリソースプール内のメンバーであるホストが、そのプールマスターへの接続を切断され、何度再試行しても接続できないことを意味します。

## host-enable

```
1 host-enable [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーが有効になり、新しい仮想マシンがそのサーバー上で起動可能になります。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

## host-enable-display

```
1 host-enable-display uuid=host_uuid
```

ホストの表示を有効にします。

## host-enable-local-storage-caching

```
1 host-enable-local-storage-caching sr-uuid=sr_uuid
```

指定されたホスト上のローカルストレージキャッシュを有効にします。

## host-evacuate

```
1 host-evacuate [host-selector=host_selector_value...]
```

このコマンドでは、指定したホスト上で実行されているすべての仮想マシンを、リソースプール内のほかの適切なホストに移行（ライブマイグレーション）します。最初に、`host-disable` コマンドを使用してホストを無効にします。

退避されたホストがプールマスターの場合、別のホストをプールマスターとして選択する必要があります。高可用性機能が無効なリソースプールでプールマスターを変更するには、`pool-designate-new-master` コマンドを使用します。詳しくは、「pool-designate-new-master」を参照してください。

高可用性機能が有効な場合は、そのホストをシャットダウンすれば、高可用性機能により任意のホストがプールマスターとして選出されます。詳しくは、「host-shutdown」を参照してください。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

## host-forget

```
1 host-forget uuid=host_uuid
```

このコマンドでは、指定した Citrix Hypervisor サーバーが XAPI エージェントから削除されて、その結果リソースプールから除外されます。

--force パラメーターを使用すると、確認のメッセージが表示されなくなります。

### 警告:

リソースプールの高可用性を有効にしたまま、このコマンドを使用しないでください。ホストを除外するには、事前に高可用性を無効にしておき、このコマンドを実行した後で高可用性を有効にします。

このコマンドは、「除外する」Citrix Hypervisor サーバーが使用不可の場合に役立ちます。ただし、Citrix Hypervisor サーバーが使用可能でプールの一部である場合は、代わりに `xe pool-eject` を使用します。

## host-get-cpu-features

```
1 host-get-cpu-features {
2 features=pool_master_cpu_features }
3 [uuid=host_uuid]
```

ホストの物理 CPU の機能を示す 16 進数値を出力します。

## host-get-server-certificate

```
1 host-get-server-certificate
```

インストールされているサーバーの SSL 証明書を取得します。

## host-get-sm-diagnostics

```
1 host-get-sm-diagnostics uuid=uuid
```

ホストごとの SM 診断情報を表示します。

## host-get-system-status

```
1 host-get-system-status filename=name_for_status_file [entries=
 comma_separated_list] [output=tar.bz2|zip] [host-selector=
 host_selector_value...]
```

システムのステータス情報を指定されたファイルにダウンロードします。オプションのパラメーター `entries` は、システム情報エントリのコンマ区切りのリストです。これらのエントリは、`host-get-system-status-capabilities` コマンドで返される XML フラグメントから指定します。詳しくは、「`host-get-system-status-capabilities`」を参照してください。このパラメーターを指定しない場合、すべてのシステム状態の情報がファイルに保存されます。パラメーター `output` は、`tar.bz2` (デフォルト) または `zip` である可能性があります。このパラメーターを指定しない場合、ファイルは `tar.bz2` 形式で保存されます。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。

## host-get-system-status-capabilities

```
1 host-get-system-status-capabilities [host-selector=host_selector_value
 ...]
```

このコマンドでは、指定したホストのシステム状態の情報を取得します。機能は、次の例のような XML フラグメントとして返されます：

```
1 <?xml version="1.0" ?>
2 <system-status-capabilities>
3 <capability content-type="text/plain" default-checked="yes" key="
4 xenserver-logs" \
5 max-size="150425200" max-time="-1" min-size="150425200" min-
6 time="-1" \
7 pii="maybe"/>
8 <capability content-type="text/plain" default-checked="yes" \
9 key="xenserver-install" max-size="51200" max-time="-1" min-size
 ="10240" \
 min-time="-1" pii="maybe"/>
10 ...
```

```
10 </system-status-capabilities>
```

各機能エンティティは、以下の属性を有することができます。

- **key**: 機能の一意の識別子。
- **content-type**: text/plain または application/data。人間が消費するエントリを UI がレンダリングできるかどうかを示します。
- **default-checked**: yes または no。ユーザーインターフェイスでこのエントリをデフォルトで選択するかどうかを示します。
- **min-size**、**max-size**: このエントリのサイズのおおよその範囲をバイト数で示します。-1 はサイズが重要でないことを示します。
- **min-time**、**max-time**: このエントリの収集時間のおおよその範囲を秒数で示します。-1 は時間が重要でないことを示します。
- **pii**: 個人を特定できる情報 (PII)。このエントリに、システムの所有者やネットワークポロジの詳細を特定できる情報があるかどうかを示します。この属性には、次の値のいずれかを指定できます:
  - **no**: エントリに機密性の高い情報がない
  - **yes**: エントリに機密性の高い情報がある、またはその可能性が高い
  - **maybe**: 機密性の高い情報があるかどうかを監査すべき
  - **if\_customized**: ファイルが変更されていない場合は、機密情報は含まれない。しかし、これらのファイルの編集が推奨されているため、このようなカスタマイズによって機密情報が導入された可能性がある。この値は特にコントロールドメインのネットワークスクリプトに使用される。

pii の値にかかわらず、いかなるバグレポートにもパスワードは含まれません。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。

## host-get-thread-diagnostics

```
1 host-get-thread-diagnostics uuid=uuid
```

ホストごとのスレッド診断情報を表示します。

## host-get-vms-which-prevent-evacuation

```
1 host-get-vms-which-prevent-evacuation uuid=uuid
```

特定のホストの退避を妨げる仮想マシンのリストを返し、それぞれの理由を表示します。

## host-is-in-emergency-mode

```
1 host-is-in-emergency-mode
```

このホストが緊急モードで動作しているかどうかを識別します。緊急モードの場合は**true**が出力され、それ以外は**false**が出力されます。このコマンドは、プールマスタが存在しなくてもメンバホストに直接実行できます。

## host-license-add

```
1 host-license-add [license-file=path/license_filename] [host-uuid=host_uuid]
```

無償版の Citrix Hypervisor で、ローカルのライセンスファイルを解析して、指定した Citrix Hypervisor サーバーにそのライセンスを追加します。

## host-license-remove

```
1 host-license-remove [host-uuid=host_uuid]
```

ホストに適用されているライセンスを削除します。

## host-license-view

```
1 host-license-view [host-uuid=host_uuid]
```

Citrix Hypervisor サーバーのライセンスの内容を表示します。

## host-logs-download

```
1 host-logs-download [file-name=logfile_name] [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーのログのコピーをダウンロードします。ログのコピーは、デフォルトで作成日時が記録された `hostname-yyyy-mm-dd T hh:mm:ssZ.tar.gz` という形式のファイル名で保存されます。オプションのパラメーター `file-name` を使用して、別のファイル名を指定できます。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

**重要:**

`xe host-logs-download` コマンドは、ローカルホスト上（つまり特定のホスト名を指定せずに）実行しても機能しますが、そのように使用しないでください。これを行うと、コントロールドメインのパーティションにログのコピーファイルが作成されてしまいます。このコマンドは、ログのコピーファイルを保持できるディスク領域があるリモートコンピュータからのみ使用してください。

## host-management-disable

```
1 host-management-disable
```

このコマンドでは、外部の管理ネットワークインターフェイス上のホストエージェントを無効にして、接続しているすべての API クライアント（XenCenter など）を切断します。このコマンドは、CLI が接続されている Citrix Hypervisor サーバーで直接操作します。Citrix Hypervisor サーバーのメンバーに適用された場合、コマンドはブールマスタに転送されません。

**警告:**

この CLI コマンドをリモートのホストに対して使用する場合は注意してください。このコマンドを実行すると、ネットワークを介してリモートでコントロールドメインに接続して、ホストエージェントを再度有効にすることができなくなります。

## host-management-reconfigure

```
1 host-management-reconfigure [interface=device] [pif-uuid=uuid]
```

このコマンドでは、Citrix Hypervisor サーバーが XenCenter に接続するための管理インターフェイスを再指定します。これにより、`/etc/xensource-inventory` の `MANAGEMENT_INTERFACE` キーが更新されます。

インターフェイス（IP アドレスが必要）のデバイス名を指定した場合、Citrix Hypervisor サーバーは直ちにバインドし直します。この場合、このコマンドは通常モードと緊急モードのいずれの場合でも機能します。

PIF オブジェクトの UUID を指定した場合、Citrix Hypervisor サーバーは再バインドすべき IP アドレスを自動的に判断します。この場合、緊急モードではこのコマンドを使用できません。

**警告:**

このコマンドをリモートのホストに対して使用する場合は、`xe pif-reconfigure` を使用して新しいインターフェイスでのネットワーク接続を設定しておいてください。これを行わないと、その Citrix Hypervisor サーバーに対して CLI コマンドを実行できなくなります。

## host-power-on

```
1 host-power-on [host=host_uuid]
```

このコマンドでは、ホストの電源投入機能が有効な Citrix Hypervisor サーバーの電源を投入します。このコマンドを使用する前に、対象のホストで `host-set-power-on` を有効にします。

## host-reboot

```
1 host-reboot [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーを再起動します。ここで指定するホストは、既に `xe host-disable` コマンドで無効になっている必要があります。ホストが有効になっていると、`HOST_IN_USE` というエラーメッセージが表示されます。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

指定した Citrix Hypervisor サーバーがプールのメンバーである場合、シャットダウン時に接続は失われますが、Citrix Hypervisor サーバーが元の接続状態に戻ると、プールに復帰します。他のメンバーとマスターは引き続き機能します。

マスターをシャットダウンすると、次のいずれかのアクションが発生するまでプールは機能しなくなります：

- メンバーの 1 人をマスターにする
- 元のマスターが再起動され、オンラインに戻る

マスターがオンラインに戻ると、メンバーは再接続してマスターと同期します。

## host-restore

```
1 host-restore [file-name=backup_filename] [host-selector=host_selector_value...]
```

このコマンドでは、`file-name` で指定した、Citrix Hypervisor サーバーコントロールソフトウェアのバックアップを復元します。このコマンドでの「復元」は通常の完全な復元ではなく、圧縮されたバックアップファイルがセカンダリパーティションに展開されるだけです。`xe host-restore` を実行した後は、インストール CD から起動して、[バックアップから復元] を選択する必要があります。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

## host-send-debug-keys

```
1 host-send-debug-keys host-uuid=host_uuid keys=keys
```

指定されたハイパーバイザーデバッグキーを、指定されたホストに送信します。

## host-set-hostname-live

```
1 host-set-hostname host-uuid=uuid_of_host hostname=new_hostname
```

`host-uuid`によって指定された Citrix Hypervisor サーバーのホスト名を変更します。これにより、コントロールドメインのデータベース内のホスト名レコードおよび Citrix Hypervisor サーバーの実際の Linux ホスト名が永続的に設定されます。`hostname`の値は`name_label`フィールドの値と同じではありません。

## host-set-power-on-mode

```
1 host-set-power-on-mode host=host_uuid power-on-mode={
2 "" | "wake-on-lan" | "iLO" | "DRAC" | "custom" }
3 \
4 [power-on-config:power_on_ip=ip-address power-on-config:
 power_on_user=user power-on-config:power_on_password_secret=
 secret-uuid]
```

電源管理ソリューションと互換性のある Citrix Hypervisor ホストのホスト電源投入機能を有効にします。`host-set-power-on`コマンドでは、ホストの電源管理ソリューションの種類を `power-on-mode` で指定する必要があります。次に、`power-on-config` 引数とそれに関連するキー/値ペアを使用して、構成オプションを指定します。

`"power_on_password_secret"`でキーを指定するには、事前にパスワードシークレットを作成しておく必要があります。詳しくは、「シークレット」を参照してください。

## host-shutdown

```
1 host-shutdown [host-selector=host_selector_value...]
```

このコマンドでは、指定した Citrix Hypervisor サーバーをシャットダウンします。ここで指定する Citrix Hypervisor サーバーは、既に`xe host-disable`コマンドで無効になっている必要があります。ホストが有効になっていると、`HOST_IN_USE`というエラーメッセージが表示されます。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

指定した Citrix Hypervisor サーバーがプールのメンバーである場合、シャットダウン時に接続は失われますが、Citrix Hypervisor サーバーが元の接続状態に戻ると、プールに復帰します。他のメンバーとマスターは引き続き機能します。

マスターをシャットダウンすると、次のいずれかのアクションが発生するまでプールは機能しなくなります：

- メンバーの 1 人をマスターにする
- 元のマスターが再起動され、オンラインに戻る

マスターがオンラインに戻ると、メンバーは再接続してマスターと同期します。

高可用性が有効なプールでは、任意のメンバーホストが自動的にプールマスターとして選出されます。高可用性が無効なプールでは、マスターが `pool-designate-new-master` コマンドを使用して、特定のサーバーを指定する必要があります。詳しくは、「`pool-designate-new-master`」を参照してください。

### host-sm-dp-destroy

```
1 host-sm-dp-destroy uuid=uuid dp=dp [allow-leak=true|false]
```

このコマンドは、ホスト上のストレージデータパスの破棄およびクリーンアップを試みます。完全にシャットダウンできない場合でも、`allow-leak=true` によってデータパスの記録をすべて削除します。

### host-sync-data

```
1 host-sync-data
```

プールマスターに格納されている非データベースのデータを、指定されたホストと同期させます。

### host-syslog-reconfigure

```
1 host-syslog-reconfigure [host-selector=host_selector_value...]
```

このコマンドは、指定した Citrix Hypervisor サーバー上の `syslog` デモンを再設定します。これにより、ホストの `logging` パラメーターで定義されている設定情報が適用されます。

このコマンドの対象ホストを指定するには、「host オブジェクトセレクター」で説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。

### host-data-source-list

```
1 host-data-source-list [host-selectors=host selector value...]
```

ホストで記録可能なデータソースのリストを出力します。

このコマンドの対象ホストを指定するには、`host` オブジェクトセレクターで説明されている標準的な方法を使用します。オプションの引数には、「`host` オブジェクトのパラメータ」から任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべてのホストに対してその操作が実行されます。

データソースには `standard` と `enabled` という 2 つのパラメーターがあります。このコマンドは、パラメーターの値を出力します：

- データソースの `enabled` パラメーターが `true` の場合、そのデータソースのメトリクス情報がパフォーマンスデータベースに記録中であることを示します。
- データソースの `standard` パラメーターが `true` の場合、そのデータソースのメトリクス情報がパフォーマンスデータベースにデフォルトで記録されることを示します。`enabled` の値は、このデータソースに対しても `true` に設定されます。
- データソースの `standard` パラメーターが `false` の場合、そのデータソースのメトリクス情報がパフォーマンスデータベースにデフォルトで記録されないことを示します。`enabled` の値は、このデータソースに対しても `false` に設定されます。

データソースメトリクスのパフォーマンスデータベースへの記録を開始するには、`host-data-source-record` コマンドを実行します。このコマンドは、`enabled` を `true` に設定します。停止するには、`host-data-source-forget` を実行します。このコマンドは、`enabled` を `false` に設定します。

## host-data-source-record

```
1 host-data-source-record data-source=name_description_of_data_source [
 host-selectors=host_selector_value...]
```

ホストで、指定したデータソースを記録します。

これにより、ホストの永続的なパフォーマンスメトリクスデータベースにデータソースからの情報が書き込まれます。このデータベースは、パフォーマンス上の理由から、通常のエージェントデータベースとは区別されます。

このコマンドの対象ホストを指定するには、`host` オブジェクトセレクターで説明されている標準的な方法を使用します。オプションの引数には、「`host` オブジェクトのパラメータ」から任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべてのホストに対してその操作が実行されます。

## host-data-source-forget

```
1 host-data-source-forget data-source=name_description_of_data_source [
 host-selectors=host_selector_value...]
```

ホストのデータソースを指定して記録を停止して、記録済みのすべてのデータを消去します。

このコマンドの対象ホストを指定するには、host オブジェクトセレクターで説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべてのホストに対してその操作が実行されます。

### host-data-source-query

```
1 host-data-source-query data-source=name_description_of_data_source [
 host-selectors=host_selector_value...]
```

ホストで、指定したデータソースを表示します。

このコマンドの対象ホストを指定するには、host オブジェクトセレクターで説明されている標準的な方法を使用します。オプションの引数には、「host オブジェクトのパラメータ」から任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべてのホストに対してその操作が実行されます。

### ログコマンド

ログ (log オブジェクト) を操作します。

### log-get

```
1 log-get
```

文字列ロガーに現在格納されているログを返します。

### log-get-keys

```
1 log-get-keys
```

ロガーの既知のキーを一覧表示します。

### log-reopen

```
1 log-reopen
```

すべてのロガーを再度開きます (ファイルのローテーションに使用します)。

## log-set-output

```
1 log-set-output output=output [key=key] [level=level]
```

すべてのロガーを指定した出力 (nil、stderr、string、file: *filename*、syslog: *something*) に設定します。

### メッセージコマンド

メッセージ (message オブジェクト) を操作します。message オブジェクトは、重要なイベントの発生をユーザーに通知するために作成され、XenCenter にアラートとして表示されます。

message オブジェクトのリストは、標準オブジェクトリストコマンド (`xe message-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### message オブジェクトのパラメーター

| パラメーター名                | 説明                           | 種類     |
|------------------------|------------------------------|--------|
| <code>uuid</code>      | メッセージの一意の識別子/オブジェクト参照        | 読み取り専用 |
| <code>name</code>      | メッセージの一意の名前                  | 読み取り専用 |
| <code>priority</code>  | メッセージの優先度。数値が大きいほど高い優先度を示します | 読み取り専用 |
| <code>class</code>     | メッセージのクラス (VM など)            | 読み取り専用 |
| <code>obj-uuid</code>  | 影響を受けるオブジェクトの UUID           | 読み取り専用 |
| <code>timestamp</code> | メッセージの生成時刻                   | 読み取り専用 |
| <code>body</code>      | メッセージの内容                     | 読み取り専用 |

### message-create

```
1 message-create name=message_name body=message_text [[host-uuid=
 uuid_of_host] | [sr-uuid=uuid_of_sr] | [vm-uuid=uuid_of_vm] | [pool-
 uuid=uuid_of_pool]]
```

メッセージを作成します。

## message-destroy

```
1 message-destroy [uuid=message_uuid]
```

既存のメッセージを破棄します。スクリプトを作成して、すべてのメッセージを破棄することもできます。次に例を示します：

```
1 # Dismiss all alerts \
2 IFS=","; for m in $(xe message-list params=uuid --minimal); do \
3 xe message-destroy uuid=$m \
4 done
```

## ネットワークコマンド

ネットワーク (network オブジェクト) を操作します。

network オブジェクトのリストは、標準オブジェクトリストコマンド (`xe network-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

## network オブジェクトのパラメーター

network オブジェクトには、以下のパラメーターがあります。

| パラメーター名                       | 説明                                                       | 種類               |
|-------------------------------|----------------------------------------------------------|------------------|
| <code>uuid</code>             | ネットワークの一意の識別子/オブジェクト参照                                   | 読み取り専用           |
| <code>name-label</code>       | ネットワークの名前                                                | 読み取り/書き込み        |
| <code>name-description</code> | ネットワークの説明文字列                                             | 読み取り/書き込み        |
| <code>VIF-uuids</code>        | 仮想マシンからこのネットワークに接続されている VIF の一意の識別子のリスト                  | 読み取り専用のセットパラメーター |
| <code>PIF-uuids</code>        | Citrix Hypervisor サーバーからこのネットワークに接続されている PIF の一意の識別子のリスト | 読み取り専用のセットパラメーター |
| <code>bridge</code>           | ローカル Citrix Hypervisor サーバー上のこのネットワークに対応するブリッジの名前        | 読み取り専用           |

| パラメーター名                                  | 説明                                                                                                                                                                                                                                                                                                                               | 種類        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <code>default-locking-mode</code>        | ARP フィルタを設定するときに VIF オブジェクトと一緒に使用するネットワークオブジェクト。VIF のすべてのフィルター規則を解除する場合は <code>unlocked</code> 、VIF のすべてのトラフィックをドロップする場合は <code>disabled</code> 。                                                                                                                                                                                | 読み取り/書き込み |
| <code>purpose</code>                     | Citrix Hypervisor サーバーがこのネットワークを使用するための目的セット。ネットワークを使用して NBD 接続を確立するには、 <code>nbd</code> に設定します。                                                                                                                                                                                                                                 | 読み取り/書き込み |
| <code>other-config:staticroutes</code>   | <code>subnet/netmask/gateway</code> 形式で指定する、サブネットへの通信路のコンマ区切りの一覧。たとえば、 <code>other-config:static-routes</code> に <code>172.16.0.0/15/192.168.0.3,172.18.0.0/16</code> を指定すると、 <code>172.16.0.0/15</code> へのトラフィックが <code>192.168.0.3</code> にルーティングされ、 <code>172.18.0.0/16</code> へのトラフィックが <code>192.168.0.4</code> にルーティングされます | 読み取り/書き込み |
| <code>other-config:ethtoolautoneg</code> | 物理インターフェイスまたはブリッジの自動ネゴシエーションを無効にする場合は <code>no</code> 。デフォルトは <code>yes</code> です。                                                                                                                                                                                                                                               | 読み取り/書き込み |
| <code>other-config:ethtool-rx</code>     | チェックサムの受信を有効にする場合は <code>on</code> 、無効にする場合は <code>off</code>                                                                                                                                                                                                                                                                    | 読み取り/書き込み |
| <code>other-config:ethtool-tx</code>     | チェックサムの転送を有効にする場合は <code>on</code> 、無効にする場合は <code>off</code>                                                                                                                                                                                                                                                                    | 読み取り/書き込み |
| <code>other-config:ethtool-sg</code>     | Scatter/Gather を有効にする場合は <code>on</code> 、無効にする場合は <code>off</code>                                                                                                                                                                                                                                                              | 読み取り/書き込み |
| <code>other-config:ethtool-tso</code>    | TCP セグメンテーションオフロードを有効にする場合は <code>on</code> 、無効にする場合は <code>off</code>                                                                                                                                                                                                                                                           | 読み取り/書き込み |

| パラメーター名                               | 説明                                           | 種類        |
|---------------------------------------|----------------------------------------------|-----------|
| <code>other-config:ethtool-ufo</code> | UDP フラグメンテーションオフロードを有効にする場合は on、無効にする場合は off | 読み取り/書き込み |
| <code>other-config:ethtool-gso</code> | 汎用セグメンテーションオフロードを有効にする場合は on、無効にする場合は off    | 読み取り/書き込み |
| <code>blobs</code>                    | バイナリデータストア                                   | 読み取り専用    |

## network-create

```
1 network-create name=label=name_for_network [name-description=descriptive_text]
```

ネットワークを作成します。

## network-destroy

```
1 network-destroy uuid=network_uuid
```

既存のネットワークを破棄します。

## SR-IOV コマンド

SR-IOV を操作するコマンドです。

`network-sriov` オブジェクトのリストは、標準オブジェクトリストコマンド (`xe network-sriov-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

## SR-IOV パラメーター

SR-IOV には次のパラメーターがあります。

| パラメーター名                   | 説明                 | 種類     |
|---------------------------|--------------------|--------|
| <code>physical-PIF</code> | SR-IOV を有効にする PIF。 | 読み取り専用 |

| パラメーター名                         | 説明                                                             | 種類     |
|---------------------------------|----------------------------------------------------------------|--------|
| <code>logical-pif</code>        | SR-IOV 論理 PIF。ユーザーはこれをパラメーターとして使用して、SR-IOV VLAN ネットワークを作成できます。 | 読み取り専用 |
| <code>requires-reboot</code>    | True に設定すると、ホストを再起動して SR-IOV を有効にするために使用されます。                  | 読み取り専用 |
| <code>remaining-capacity</code> | 残された使用可能な VF の数。                                               | 読み取り専用 |

### **network-sriov-create**

```
1 network-sriov-create network-uuid=network_uuid pif-uuid=
 physical_pif_uuid
```

特定の物理 PIF に対して SR-IOV ネットワークオブジェクトを作成し、物理 PIF 上で SR-IOV を有効にします。

### **network-sriov-destroy**

```
1 network-sriov-destroy uuid=network_sriov_uuid
```

SR-IOV ネットワークオブジェクトを削除し、物理 PIF 上で SR-IOV を無効にします。

### **SR-IOV VF** の割り当て

```
1 xe vif-create device=device_index mac=vf_mac_address network-uuid=
 sriov_network vm-uuid=vm_uuid
```

SR-IOV ネットワークから仮想マシンに VF を割り当てます。

### **SDN** コントローラーコマンド

SDN コントローラー (sdn-controller オブジェクト) を操作します。

### **sdn-controller-forget**

```
1 sdn-controller-introduce [address=address] [protocol=protocol] [tcp-
port=tcp_port]
```

SDN コントローラーを導入します。

### **sdn-controller-introduce**

```
1 sdn-controller-forget uuid=uuid
```

SDN コントローラーを削除します。

### トンネルコマンド

トンネル (tunnel オブジェクト) を操作します。

### **tunnel-create**

```
1 tunnel-create pif-uuid=pif_uuid network-uuid=network_uuid
```

ホスト上に新しいトンネルを作成します。

### **tunnel-destroy**

```
1 tunnel-destroy uuid=uuid
```

トンネルを破棄します。

### パッチコマンド

パッチ (patch オブジェクト) を操作します。

### **patch-apply**

```
1 patch-apply uuid=patch_uuid host-uuid=host_uuid
```

以前にアップロードしたパッチを指定されたホストに適用します。

### **patch-clean**

```
1 patch-clean uuid=uuid
```

以前にアップロードしたパッチファイルを削除します。

### **patch-destroy**

```
1 patch-destroy uuid=uuid
```

適用されていないパッチレコードとファイルをサーバーから削除します。

### **patch-pool-apply**

```
1 patch-pool-apply uuid=uuid
```

以前にアップロードしたパッチをプール内のすべてのホストに適用します。

### **patch-pool-clean**

```
1 patch-pool-clean uuid=uuid
```

プール内のすべてのホストで以前にアップロードしたパッチファイルを削除します。

### **patch-precheck**

```
1 patch-precheck uuid=uuid host-uuid=host_uuid
```

以前アップロードされたパッチに含まれている事前チェックを、指定したホストに対して実行します。

### **patch-upload**

```
1 patch-upload file-name=file_name
```

パッチファイルをサーバーにアップロードします。

**PBD** (物理ブロックデバイス) コマンド

PBD (pbd オブジェクト) を操作します。pbd オブジェクトは、Citrix Hypervisor サーバーがストレージリポジトリへのアクセスに使用するソフトウェアオブジェクトです。

pbd オブジェクトのリストは、標準オブジェクトリストコマンド (`xe pbd-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

**pbd** オブジェクトのパラメーター

pbd オブジェクトには、以下のパラメーターがあります。

| パラメーター名                         | 説明                                           | 種類                   |
|---------------------------------|----------------------------------------------|----------------------|
| <code>uuid</code>               | PBD の一意の識別子/オブジェクト参照                         | 読み取り専用               |
| <code>sr-uuid</code>            | PBD の接続先ストレージリポジトリ                           | 読み取り専用               |
| <code>device-config</code>      | ホストのストレージリポジトリバックエンドドライバーに提供される追加構成情報        | 読み取り専用のマップパラメーター     |
| <code>currently-attached</code> | ストレージリポジトリがこのホストに接続されている場合は true、それ以外は false | 読み取り専用               |
| <code>host-uuid</code>          | PBD が使用可能になっている物理マシンの UUID                   | 読み取り専用               |
| <code>host</code>               | このパラメーターは廃止。代わりに <code>host_uuid</code> を使用  | 読み取り専用               |
| <code>other-config</code>       | 追加の構成情報。                                     | 読み取り/書き込み可のマップパラメーター |

**pbd-create**

```
1 pbd-create host-uuid=uuid_of_host sr-uuid=uuid_of_sr [device-config:key
 =corresponding_value]
```

このコマンドでは、Citrix Hypervisor サーバー上に PBD を作成します。読み取り専用の `device-config` パラ

メーターは、作成時にのみ設定できます。

'path' から '/tmp' にマップを追加するには、コマンドで `device-config:path=/tmp` を指定します。

ストレージリポジトリの各種類でサポートされる `device-config` パラメーターのキー/値ペアについては、「[ストレージ](#)」を参照してください。

### **pbd-destroy**

```
1 pbd-destroy uuid=uuid_of_pbd
```

指定した PBD を破棄します。

### **pbd-plug**

```
1 pbd-plug uuid=uuid_of_pbd
```

このコマンドでは、PBD を Citrix Hypervisor サーバーにプラグします。成功すると、参照されているストレージリポジトリ（およびそれに含まれている VDI）が Citrix Hypervisor サーバーからアクセス可能になります。

### **pbd-unplug**

```
1 pbd-unplug uuid=uuid_of_pbd
```

このコマンドでは、PBD を Citrix Hypervisor サーバーからアンプラグします。

## **PIF（物理ネットワークインターフェイス）コマンド**

PIF（`pif` オブジェクト）を操作します。

`pif` オブジェクトのリストは、標準オブジェクトリストコマンド（`xe pif-list`）を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「[低レベルパラメーターコマンド](#)」を参照してください。

### **pif** オブジェクトのパラメーター

`pif` オブジェクトには、以下のパラメーターがあります。

| パラメーター名                              | 説明                                                                 | 種類                  |
|--------------------------------------|--------------------------------------------------------------------|---------------------|
| <code>uuid</code>                    | PIF の一意の識別子/オブジェクト参照                                               | 読み取り専用              |
| <code>device machine-readable</code> | インターフェイス名 (eth0 など)                                                | 読み取り専用              |
| <code>MAC</code>                     | PIF の MAC アドレス                                                     | 読み取り専用              |
| <code>other-config</code>            | 追加の PIF 構成 <code>name:value</code> ペア。                             | 読み取り/書き込み可のマップパラメータ |
| <code>physical</code>                | PIF が実際の物理ネットワークインターフェイスをポイントしている場合は <code>true</code>             | 読み取り専用              |
| <code>currently-attached</code>      | PIF が現在このホストに接続されているかどうか。 <code>true</code> または <code>false</code> | 読み取り専用              |
| <code>MTU</code>                     | PIF の MTU (Maximum Transmission Unit) バイト数。                        | 読み取り専用              |
| <code>VLAN</code>                    | この PIF を通過するすべてのトラフィックの VLAN タグ。 -1 は VLAN タグが割り当てられていないことを示す      | 読み取り専用              |
| <code>bond-master-of</code>          | この PIF がマスターになっているボンディングの UUID (該当する場合)                            | 読み取り専用              |
| <code>bond-slave-of</code>           | この PIF がスレーブになっているボンディングの UUID (該当する場合)                            | 読み取り専用              |
| <code>management</code>              | この PIF がコントロールドメインの管理インターフェイスとして指定されているかどうか                        | 読み取り専用              |
| <code>network-uuid</code>            | この PIF が接続されている仮想ネットワークの一意の識別子/オブジェクト参照                            | 読み取り専用              |
| <code>network-name-label</code>      | この PIF が接続している仮想ネットワークの名前                                          | 読み取り専用              |

| パラメーター名               | 説明                                                                           | 種類     |
|-----------------------|------------------------------------------------------------------------------|--------|
| host-uuid             | この PIF が接続している Citrix Hypervisor サーバーの一意識別子/オブジェクト参照                         | 読み取り専用 |
| host-name-label       | この PIF が接続している Citrix Hypervisor サーバーの名前                                     | 読み取り専用 |
| IP-configuration-mode | ネットワークアドレス設定の種類、DHCP または static                                              | 読み取り専用 |
| IP                    | PIF の IP アドレス。<br>IP-configuration-mode が static の場合はここで定義し、DHCP の場合は定義しない   | 読み取り専用 |
| netmask               | PIF のネットマスクアドレス。<br>IP-configuration-mode が static の場合はここで定義し、DHCP の場合は定義しない | 読み取り専用 |
| gateway               | PIF のゲートウェイアドレス。<br>IP-configuration-mode が static の場合はここで定義し、DHCP の場合は定義しない | 読み取り専用 |
| DNS                   | PIF の DNS アドレス。<br>IP-configuration-mode が static の場合はここで定義し、DHCP の場合は定義しない  | 読み取り専用 |
| io_read_kbs           | このデバイスの平均読み取り速度 (kB/秒)                                                       | 読み取り専用 |
| io_write_kbs          | このデバイスの平均書き込み速度 (kB/秒)                                                       | 読み取り専用 |
| carrier               | デバイスのリンク状態                                                                   | 読み取り専用 |
| vendor-id             | NIC ベンダーに割り当てられた ID                                                          | 読み取り専用 |
| vendor-name           | NIC ベンダーの名前                                                                  | 読み取り専用 |
| device-id             | ベンダーが NIC モデルに割り当てた ID                                                       | 読み取り専用 |
| device-name           | ベンダーが NIC モデルに割り当てた名前                                                        | 読み取り専用 |

| パラメーター名                                    | 説明                                                      | 種類        |
|--------------------------------------------|---------------------------------------------------------|-----------|
| <code>speed</code>                         | NIC のデータ転送レート                                           | 読み取り専用    |
| <code>duplex</code>                        | NIC の二重モード。full (全二重) または half (半二重)                    | 読み取り専用    |
| <code>pci-bus-path</code>                  | PCI バスパスのアドレス                                           | 読み取り専用    |
| <code>other-config: ethtool-speed</code>   | 接続速度 (Mbps) の設定                                         | 読み取り/書き込み |
| <code>other-config: ethtool-autoneg</code> | 物理インターフェイスまたはブリッジの自動ネゴシエーションを無効にする場合は no。デフォルトは yes です。 | 読み取り/書き込み |
| <code>other-config: ethtool-duplex</code>  | PIF のデュプレックス機能をフルまたはハーフに設定します。                          | 読み取り/書き込み |
| <code>other-config: ethtool-rx</code>      | チェックサムの受信を有効にする場合は on、無効にする場合は off                      | 読み取り/書き込み |
| <code>other-config: ethtool-tx</code>      | チェックサムの転送を有効にする場合は on、無効にする場合は off                      | 読み取り/書き込み |
| <code>other-config: ethtool-sg</code>      | Scatter/Gather を有効にする場合は on、無効にする場合は off                | 読み取り/書き込み |
| <code>other-config: ethtool-tso</code>     | TCP セグメンテーションオフロードを有効にする場合は on、無効にする場合は off             | 読み取り/書き込み |
| <code>other-config: ethtool-ufo</code>     | UDP フラグメンテーションオフロードを有効にする場合は on、無効にする場合は off            | 読み取り/書き込み |
| <code>other-config: ethtool-gso</code>     | 汎用セグメンテーションオフロードを有効にする場合は on、無効にする場合は off               | 読み取り/書き込み |
| <code>other-config: domain</code>          | DNS 検索パスの設定 (コンマ区切りの一覧)                                 | 読み取り/書き込み |
| <code>other-config: bondmiimon</code>      | リンクの状態チェック間隔 (ミリ秒)                                      | 読み取り/書き込み |

| パラメーター名                                      | 説明                                                                                                | 種類        |
|----------------------------------------------|---------------------------------------------------------------------------------------------------|-----------|
| <code>other-config:<br/>bonddowndelay</code> | リンクの切断が検出されてから切断リンクとして認識されるまでの待機時間（ミリ秒）。一時的な切断を許容するためのパラメーター                                      | 読み取り/書き込み |
| <code>other-config:<br/>bondupdelay</code>   | リンクの回復が検出されてから接続リンクとして認識されるまでの待機時間（ミリ秒）。一時的な回復を無視するための設定。指定された時間待機してからトラフィック転送が開始される（デフォルト値は31s）。 | 読み取り/書き込み |
| <code>disallow-unplug</code>                 | この PIF がストレージ専用 NIC の場合に true、それ以外は false                                                         | 読み取り/書き込み |

注:

PIF の `other-config` フィールドへの変更は、再起動後に有効になります。または、`xe pif-unplug` コマンドと `xe pif-plug` コマンドを使用して、PIF 設定が再書き込みされるようにすることもできます。

## **pif-forget**

```
1 pif-forget uuid=uuid_of_pif
```

特定のホスト上の指定した PIF を破棄します。

## **pif-introduce**

```
1 pif-introduce host-uuid=host_uuid mac=mac_address_for_pif device=
 interface_name
```

指定した Citrix Hypervisor サーバー上の物理インターフェイスを表す pif オブジェクトを作成します。

## **pif-plug**

```
1 pif-plug uuid=uuid_of_pif
```

指定した物理インターフェイスを起動します。

## pif-reconfigure-ip

```
1 pif-reconfigure-ip uuid=uuid_of_pif [mode=dhcp|mode=static] gateway=
 network_gateway_address IP=static_ip_for_this_pif netmask=
 netmask_for_this_pif [DNS=dns_address]
```

PIF の IP アドレスを変更します。静的アドレスを使用する場合は、`mode`パラメーターに**static**を設定し、`gateway`パラメーター、`IP`パラメーター、および`netmask`パラメーターに適切な値を設定します。DHCP を使用する場合は、`mode`パラメーターをDHCPに設定します。ほかのパラメーターを定義する必要はありません。

注:

STP Fast Link が無効な（またはサポートされていない）スイッチ上のポートにスパニングツリープロトコルで接続する物理ネットワークインターフェイスで静的 IP アドレスを使用すると、無トラフィック期間が発生します。

## pif-reconfigure-ipv6

```
1 pif-reconfigure-ipv6 uuid=uuid_of_pif mode=mode [gateway=
 network_gateway_address] [IPv6=static_ip_for_this_pif] [DNS=
 dns_address]
```

PIF の IPv6 アドレス設定を再構成します。

## pif-scan

```
1 pif-scan host-uuid=host_uuid
```

指定した Citrix Hypervisor サーバー上の新規物理インターフェイスを検出します。

## pif-set-primary-address-type

```
1 pif-set-primary-address-type uuid=uuid primary_address_type=
 address_type
```

この PIF で使用されるプライマリアドレスの種類を変更します。

## pif-unplug

```
1 pif-unplug uuid=uuid_of_pif
```

指定した物理インターフェイスを停止します。

## プールコマンド

リソースプール (pool オブジェクト) を操作します。リソースプールは、1 つまたは複数の Citrix Hypervisor サーバーの集合です。リソースプールでは 1 つ以上の共有ストレージリポジトリを使用して、プール内のあるホスト上で実行されている仮想マシンを、同じプール内の別のホストにほぼリアルタイムで移行できます。この移行は、仮想マシンをシャットダウンしたり再起動したりすることなく、仮想マシンの起動中に実行されます。各 Citrix Hypervisor サーバーは、それ自身がデフォルトでリソースプールを構成します。このプールにほかの Citrix Hypervisor サーバーを追加すると、追加したホストはメンバーホストとして動作し、元のホストがプールマスタになります。

シングルトンプールオブジェクトは、標準的なオブジェクトリストコマンド (`xe pool-list`) でリストできます。パラメーターは標準パラメーターコマンドで操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

## pool オブジェクトのパラメーター

pool オブジェクトには、以下のパラメータがあります。

| パラメーター名                       | 説明                                                   | 種類        |
|-------------------------------|------------------------------------------------------|-----------|
| <code>uuid</code>             | プールの一意の識別子/オブジェクト参照                                  | 読み取り専用    |
| <code>name-label</code>       | プールの名前                                               | 読み取り/書き込み |
| <code>name-description</code> | プールの説明文字列                                            | 読み取り/書き込み |
| <code>master</code>           | プールマスタとして動作する Citrix Hypervisor サーバーの一意の識別子/オブジェクト参照 | 読み取り専用    |
| <code>default-SR</code>       | プールのデフォルトストレージリポジトリの一意の識別子/オブジェクト参照                  | 読み取り/書き込み |
| <code>crash-dump-SR</code>    | メンバーホストのクラッシュダンブが格納されるストレージリポジトリの一意の識別子/オブジェクト参照     | 読み取り/書き込み |
| <code>metadata-vdis</code>    | プールの既知のメタデータ VDI                                     | 読み取り専用    |

| パラメーター名                      | 説明                                                                | 種類                    |
|------------------------------|-------------------------------------------------------------------|-----------------------|
| suspend-image-SR             | メンバーホスト上でサスペンド状態の仮想マシンが格納されるストレージリポジトリの一意的識別子/オブジェクト参照            | 読み取り/書き込み             |
| other-config                 | プールの追加構成パラメーターを指定するキー/値ペアのリスト                                     | 読み取り/書き込み可のマッピングパラメータ |
| supported-sr-types           | このプールで使用可能なストレージリポジトリの種類                                          | 読み取り専用                |
| ha-enabled                   | プールの高可用性が有効な場合に true、それ以外は false                                  | 読み取り専用                |
| ha-configuration             | 将来バージョン用に予約                                                       | 読み取り専用                |
| ha-statefiles                | 高可用性によりストレージの状態を検出するために使用される VDI の UUID リスト                       | 読み取り専用                |
| ha-host-failures-to-tolerate | システムアラートを送信せずに許容されるホスト障害数（フェイルオーバートレランス数）                         | 読み取り/書き込み             |
| ha-plan-exists-for           | 高可用性アルゴリズムにより算出される、対応可能なホスト障害数                                    | 読み取り専用                |
| ha-allow-overcommit          | プールがオーバーコミットできる場合は true、そうでない場合は false                            | 読み取り/書き込み             |
| ha-overcommitted             | プールがオーバーコミットされている場合に true                                         | 読み取り専用                |
| blobs                        | バイナリデータストア                                                        | 読み取り専用                |
| live-patching-disabled       | ライブパッチを有効にするには、false に設定します。ライブパッチを無効にするには、true に設定します。           | 読み取り/書き込み             |
| igmp-snooping-enabled        | IGMP スヌーピングを有効にするには、true に設定します。IGMP スヌーピングを無効にするには、false に設定します。 | 読み取り/書き込み             |

### **pool-apply-edition**

```
1 pool-apply-edition edition=edition [uuid=uuid] [license-server-address=address] [license-server-port=port]
```

プール全体にエディションを適用します。

### **pool-certificate-install**

```
1 pool-certificate-install filename=file_name
```

プール全体に SSL 証明書をインストールします。

### **pool-certificate-list**

```
1 pool-certificate-list
```

インストールされているすべての SSL 証明書をリストします。

### **pool-certificate-sync**

```
1 pool-certificate-sync
```

マスターからスレーブへの SSL 証明書と証明書失効一覧を同期します。

### **pool-certificate-uninstall**

```
1 pool-certificate-uninstall name=name
```

SSL 証明書をアンインストールします。

### **pool-crl-install**

```
1 pool-crl-install filename=file_name
```

プール全体に SSL 証明書失効一覧をインストールします。

### **pool-crl-list**

```
1 pool-crl-list
```

インストールされているすべての SSL 証明書失効一覧をリストします。

### **pool-crl-uninstall**

```
1 pool-crl-uninstall name=name
```

SSL 証明書失効一覧をアンインストールします。

### **pool-deconfigure-wlb**

```
1 pool-deconfigure-wlb
```

ワークロードバランスの設定を完全に削除します。

### **pool-designate-new-master**

```
1 pool-designate-new-master host-uuid=uuid_of_new_master
```

指定した Citrix Hypervisor サーバー（メンバーホスト）をプールマスタとして動作させます。このコマンドにより、プールマスタの役割をそのプール内の別のホストに正しく移譲できます。このコマンドは、現在のマスターがオンラインの場合にのみ機能します。これは以下に挙げられている緊急モードのコマンドに代わるものではありません。

### **pool-disable-external-auth**

```
1 pool-disable-external-auth [uuid=uuid] [config=config]
```

プール内のすべてのホストで外部認証を無効にします。

### **pool-disable-local-storage-caching**

```
1 pool-disable-local-storage-caching uuid=uuid
```

プール全体のローカルストレージキャッシュを無効にします。

### **pool-disable-redo-log**

```
1 pool-disable-redo-log
```

HA が有効になっていない限り、使用中は redo ログを無効にします。

### **pool-disable-ssl-legacy**

```
1 pool-disable-ssl-legacy [uuid=uuid]
```

各ホストで ssl-legacy を false に設定します。

### **pool-dump-database**

```
1 pool-dump-database file-name=filename_to_dump_database_into_(on_client)
```

プールデータベース全体のコピーをダウンロードして、クライアント上のファイルにバックアップします。

### **pool-enable-external-auth**

```
1 pool-enable-external-auth auth-type=auth_type service-name=
 service_name [uuid=uuid] [config:=config]
```

プール内のすべてのホストで外部認証を有効にします。auth-type の値によっては、特定の config: 値が必要になることに注意してください。

### **pool-enable-local-storage-caching**

```
1 pool-enable-local-storage-caching uuid=uuid
```

プール全体でローカルストレージキャッシュを有効にします。

### **pool-enable-redo-log**

```
1 pool-enable-redo-log sr-uuid=sr_uuid
```

HA が有効になっていない限り、使用中は指定されたストレージリポジトリの redo ログを有効にします。

### **pool-enable-ssl-legacy**

```
1 pool-enable-ssl-legacy [uuid=uuid]
```

各ホストで ssl-legacy を true に設定します。

### **pool-eject**

```
1 pool-eject host-uuid=uuid_of_host_to_eject
```

既存のリソースプールから指定した Citrix Hypervisor サーバーを除外します。

### **pool-emergency-reset-master**

```
1 pool-emergency-reset-master master-address=address_of_pool_master
```

スレーブメンバー Citrix Hypervisor サーバーが使用しているプールマスタのアドレスをリセットして、新しいアドレスのプールマスタに接続します。マスターホストでこのコマンドを実行しないでください。

### **pool-emergency-transition-to-master**

```
1 pool-emergency-transition-to-master
```

任意の Citrix Hypervisor サーバー（メンバーホスト）をプールマスタとして動作させます。Citrix Hypervisor サーバーは、ホストが緊急モードに移行してから、このコマンドを受け入れます。緊急モードとは、あるプール内のメンバーが、そのプールマスタへの接続を切断され、何度か再試行しても接続できないことを意味します。

ホストがプールに参加してからホストパスワードが変更された場合、このコマンドによってホストのパスワードがリセットされる可能性があります。詳しくは、「ユーザーコマンド」を参照してください。

### **pool-ha-enable**

```
1 pool-ha-enable heartbeat-sr-uuids=uuid_of_heartbeat_sr
```

指定したストレージリポジトリを中央ストレージハートビートリポジトリとして使用して、リソースプールの高可用性機能を有効にします。

### **pool-ha-disable**

```
1 pool-ha-disable
```

リソースプールの高可用性機能を無効にします。

### **pool-ha-compute-hypothetical-max-host-failures-to-tolerate**

現在のプール構成で許容されるホスト障害の最大数を計算します。

### **pool-ha-compute-max-host-failures-to-tolerate**

```
1 pool-ha-compute-hypothetical-max-host-failures-to-tolerate [vm-uuid=
vm_uuid] [restart-priority=restart_priority]
```

提供され、提案され、保護された仮想マシンで許容される最大ホスト障害数を計算します。

### **pool-initialize-wlb**

```
1 pool-initialize-wlb wlb_url=url wlb_username=wb_username wlb_password=
wlb_password xenserver_username=username xenserver_password=password
```

現在のプールのワークロードバランスをターゲット WLB サーバーで初期化します。

### **pool-join**

```
1 pool-join master-address=address master-username=username master-
password=password
```

Citrix Hypervisor サーバーを既存のリソースプールに追加します。

### **pool-management-reconfigure**

```
1 pool-management-reconfigure [network-uuid=network-uuid]
```

このコマンドでは、リソースプールのすべてのホストで XenCenter に接続するための管理インターフェイスを再指定します。これにより、すべてのホストで `/etc/xensource-inventory` の `MANAGEMENT_INTERFACE` キーが更新されます。

インターフェイス (IP アドレスが必要) のデバイス名を指定した場合、Citrix Hypervisor プールマスタは直ちにバインドし直します。この場合、このコマンドは通常モードと緊急モードのいずれの場合でも機能します。

指定されたネットワーク UUID から Citrix Hypervisor サーバーに割り当てられる PIF オブジェクトの UUID を特定し、これによって再バインドすべき IP アドレスを自動的に判断します。この場合、緊急モードではこのコマンドを使用できません。

**警告:**

このコマンドをリモートのホストに対して使用する場合は、`xe pif-reconfigure`を使用して新しいインターフェイスでのネットワーク接続を設定しておいてください。これを行わないと、その Citrix Hypervisor サーバーに対して CLI コマンドを実行できなくなります。

### **pool-recover-slaves**

```
1 pool-recover-slaves
```

プールマスタに対して、緊急モードで動作中のすべてのメンバーホストのプールマスターアドレスをリセットさせます。通常、`pool-emergency-transition-to-master`でメンバホストの1つを新しいプールマスタとして設定した後に、このコマンドを使用します。

### **pool-restore-database**

```
1 pool-restore-database file-name=filename_to_restore_from_on_client [dry-run=true|false]
```

データベースバックアップ (`pool-dump-database`で作成) をリソースプールにアップロードします。プールマスターがアップロードを受信すると、新しいデータベースを使用して再起動します。

`dry run` オプションも用意されており、実際の処理を実行しなくてもプールデータベースが復元可能かどうかを確認できます。`dry-run`のデフォルト値は `false` です。

### **pool-retrieve-wlb-configuration**

```
1 pool-retrieve-wlb-configuration
```

ワークロードバランスサーバーからプール最適化基準を取得します。

### **pool-retrieve-wlb-diagnostics**

```
1 pool-retrieve-wlb-diagnostics [filename=file_name]
```

ワークロードバランスサーバーから診断を取得します。

### **pool-retrieve-wlb-recommendations**

```
1 pool-retrieve-wlb-recommendations
```

ワークロードバランスサーバーからプールの仮想マシン移行推奨事項を取得します。

### **pool-retrieve-wlb-report**

```
1 pool-retrieve-wlb-report report=report [filename=file_name]
```

ワークロードバランスサーバーからレポートを取得します。

### **pool-send-test-post**

```
1 pool-send-test-post dest-host=destination_host dest-port=
 destination_port body=post_body
```

HTTPS を使用して、指定された本文を指定されたホストおよびポートに送信し、応答を出力します。これは、SSL レイヤーのデバッグに使用されます。

### **pool-send-wlb-configuration**

```
1 pool-send-wlb-configuration [config:=config]
```

ワークロードバランスサーバーのプール最適化基準を設定します。

### **pool-sync-database**

```
1 pool-sync-database
```

プールデータベースを、リソースプールのすべてのホストと強制的に同期します。データベースは定期的に自動複製されるため、このコマンドは通常の操作では不要です。しかしこのコマンドは、重要な CLI 操作の実行後、変更が迅速に複製されるようにするのに役立ちます。

プールを **igmp-snooping** に設定します

```
1 pool-param-set [uuid=pool-uuid] [igmp-snooping-enabled=true|false]
```

Citrix Hypervisor プールで IGMP スヌーピングを有効または無効にします。

## **PVS** アクセラレータコマンド

PVS アクセラレータを操作するためのコマンド。

### **pvs-cache-storage-create**

```
1 pvs-cache-storage-create sr-uuid=sr_uuid pvs-site-uuid=pvs_site_uuid
size=size
```

指定されたホストの特定のストレージリポジトリ上に PVS キャッシュを構成します。

### **pvs-cache-storage-destroy**

```
1 pvs-cache-storage-destroy uuid=uuid
```

PVS キャッシュを削除します。

### **pvs-proxy-create**

```
1 pvs-proxy-create pvs-site-uuid=pvs_site_uuid vif-uuid=vif_uuid
```

PVS プロキシを使用するように仮想マシン/仮想ネットワークインターフェイスを設定します。

### **pvs-proxy-destroy**

```
1 pvs-proxy-destroy uuid=uuid
```

この仮想ネットワークインターフェイス/仮想マシンの PVS プロキシを削除（またはスイッチオフ）します。

### **pvs-server-forget**

```
1 pvs-server-forget uuid=uuid
```

PVS サーバーを削除します。

### **pvs-server-introduce**

```
1 pvs-server-introduce addresses=addresses first-port=first_port last-port=
=last_port pvs-site-uuid=pvs_site_uuid
```

新しい PVS サーバーを導入します。

### **pvs-site-forget**

```
1 pvs-site-forget uuid=uuid
```

PVS サイトを削除します。

### **pvs-site-introduce**

```
1 pvs-site-introduce name-label=name_label [name-description=
name_description] [pvs-uuid=pvs_uuid]
```

新しい PVS サイトを導入します。

### ストレージマネージャコマンド

ストレージマネージャプラグイン (sm オブジェクト) を制御します。

ストレージマネージャオブジェクトは、標準的なオブジェクトリストコマンド (`xe sm-list`) でリストできます。パラメーターは標準パラメーターコマンドで操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### sm オブジェクトのパラメーター

sm オブジェクトには、以下のパラメーターがあります。

| パラメーター名                           | 説明                                          | 種類     |
|-----------------------------------|---------------------------------------------|--------|
| <code>uuid</code>                 | SM プラグインの一意の識別子/オブジェクトリファレンス                | 読み取り専用 |
| <code>name-label</code>           | SM プラグインの名前                                 | 読み取り専用 |
| <code>name-description</code>     | SM プラグインの説明文字列                              | 読み取り専用 |
| <code>type</code>                 | このプラグインが接続するストレージポジトリの種類                    | 読み取り専用 |
| <code>vendor</code>               | このプラグインを作成したベンダーの名前                         | 読み取り専用 |
| <code>copyright</code>            | SM プラグインの著作権声明                              | 読み取り専用 |
| <code>required-api-version</code> | Citrix Hypervisor サーバーで要求される最低 SM API バージョン | 読み取り専用 |
| <code>configuration</code>        | デバイス設定キーの名前と説明                              | 読み取り専用 |
| <code>capabilities</code>         | SM プラグインの機能                                 | 読み取り専用 |
| <code>driver-filename</code>      | SR ドライバーのファイル名。                             | 読み取り専用 |

## スナップショットコマンド

スナップショットを操作します。

### snapshot-clone

```
1 snapshot-clone new-name-label=name_label [uuid=uuid] [new-name-description=description]
```

既存のスナップショットを複製し、ストレージレベルの高速ディスククローン処理を行うことで、新しいテンプレートを作成します (サポートされる場合)。

### snapshot-copy

```
1 snapshot-copy new-name-label=name_label [uuid=uuid] [new-name-description=name_description] [sr-uuid=sr_uuid]
```

通常の方法で既存の仮想マシンを複製して新しいテンプレートを作成します（ストレージレベルの高速ディスククローン処理がサポートされる場合でもそれを使用しません）。複製された仮想マシンのディスクイメージは常に「フルイメージ」であり、CoWの一部ではありません。

### snapshot-destroy

```
1 snapshot-destroy [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

スナップショットを破棄します。そのスナップショットに関連付けられたストレージはそのまま残ります。ストレージも削除するには、`snapshot-uninstall` を使用します。

### snapshot-disk-list

```
1 snapshot-disk-list [uuid=uuid] [snapshot-uuid=snapshot_uuid] [vbd-params=vbd_params] [vdi-params=vdi_params]
```

選択した仮想マシン上のディスクを一覧表示します。

### snapshot-export-to-template

```
1 snapshot-export-to-template filename=file_name snapshot-uuid=snapshot_uuid [preserve-power-state=true|false]
```

スナップショットをファイル名にエクスポートします。

### snapshot-reset-powerstate

```
1 snapshot-reset-powerstate [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

管理ツールスタックデータベースでのみ、仮想マシンの電源を強制的に停止させます。このコマンドは、「一時停止」とマークされたスナップショットを回復するために使用されます。この操作は危険である可能性があります：メモリイメージが不要であることを確認する必要があります。スナップショットを再開できなくなります。

### snapshot-revert

```
1 snapshot-revert [uuid=uuid] [snapshot-uuid=snapshot_uuid]
```

既存の仮想マシンを以前のチェックポイント状態またはスナップショット状態に戻します。

## snapshot-uninstall

```
1 snapshot-uninstall [uuid=uuid] [snapshot-uuid=snapshot_uuid] [--force]
```

スナップショットをアンインストールします。この操作により、RW とマークされた、このスナップショットにのみ接続されている VDI を破棄します。VM レコードを単に破棄するには、`snapshot-destroy` を使用します。

### ストレージリポジトリコマンド

ストレージリポジトリ (sr オブジェクト) を制御するためのコマンド

sr オブジェクトのリストは、標準オブジェクトリストコマンド (`xe sr-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### sr オブジェクトのパラメーター

sr オブジェクトには、以下のパラメーターがあります。

| パラメーター名                         | 説明                                        | 種類               |
|---------------------------------|-------------------------------------------|------------------|
| <code>uuid</code>               | ストレージリポジトリの一意の識別子/オブジェクト参照                | 読み取り専用           |
| <code>name-label</code>         | ストレージリポジトリの名前                             | 読み取り/書き込み        |
| <code>name-description</code>   | ストレージリポジトリの説明文字列                          | 読み取り/書き込み        |
| <code>allowed-operations</code> | 現在の SR の状態で可能な操作のリスト                      | 読み取り専用のセットパラメーター |
| <code>current-operations</code> | このストレージリポジトリ上で現在処理中の操作のリスト                | 読み取り専用のセットパラメーター |
| <code>VDIs</code>               | このストレージリポジトリ内の仮想ディスクの一意の識別子/オブジェクト参照      | 読み取り専用のセットパラメーター |
| <code>PBDs</code>               | このストレージリポジトリに接続されている PBD の一意の識別子/オブジェクト参照 | 読み取り専用のセットパラメーター |

| パラメーター名                           | 説明                                                                                                                                                                                                  | 種類                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <code>physical-utilisation</code> | このストレージリポジトリ上で現在使用されている物理スペース (バイト数)。シンプロビジョニングの場合は、物理的な使用量が仮想割り当てより小さくなることがあります                                                                                                                    | 読み取り専用                |
| <code>physical-size</code>        | ストレージリポジトリの総物理サイズ (バイト数)                                                                                                                                                                            | 読み取り専用                |
| <code>type</code>                 | ストレージリポジトリの種類。使用するストレージリポジトリバックエンドドライバーを指定するために使用                                                                                                                                                   | 読み取り専用                |
| <code>introduced-by</code>        | ストレージリポジトリをイントロデュースした障害回復タスク (該当する場合)                                                                                                                                                               | 読み取り専用                |
| <code>content-type</code>         | SR の内容の種類。ISO ライブラリをほかの SR から区別するために使用されています。ISO のライブラリを格納するストレージリポジトリの <code>content-type</code> は <code>iso</code> である必要があります。そのほかのストレージリポジトリでは、このパラメーターを空白にするか <code>user</code> を指定することをお勧めします。 | 読み取り専用                |
| <code>shared</code>               | このストレージリポジトリを複数の Citrix Hypervisor サーバーで共有できる場合は <code>true</code> 。それ以外は <code>false</code>                                                                                                        | 読み取り/書き込み             |
| <code>other-config</code>         | ストレージリポジトリの追加構成パラメーターを指定するキー/値ペアのリスト                                                                                                                                                                | 読み取り/書き込み可のマッピングパラメータ |
| <code>host</code>                 | SR のホスト名                                                                                                                                                                                            | 読み取り専用                |
| <code>virtual-allocation</code>   | このストレージリポジトリの全 VDI の <code>virtual-size</code> 値の合計 (バイト数)                                                                                                                                          | 読み取り専用                |

| パラメーター名                | 説明          | 種類               |
|------------------------|-------------|------------------|
| <code>sm-config</code> | SM に依存するデータ | 読み取り専用のマップパラメーター |
| <code>blobs</code>     | バイナリデータストア  | 読み取り専用           |

## sr-create

```
1 sr-create name=label=name physical-size=size type=type content-type=
content_type device-config:config_name=value [host-uuid=host_uuid] [
shared=true | false]
```

ディスク上にストレージリポジトリを作成し、データベースにイントロデュースして、このストレージリポジトリを Citrix Hypervisor サーバーに接続するための PBD を作成します。 `shared` が `true` に設定されている場合、PBD はプールの Citrix Hypervisor サーバーそれぞれに作成されます。 `shared` が指定されていないか、 `false` に設定されている場合、PBD は `host-uuid` で指定された Citrix Hypervisor サーバーにのみ作成されます。

`device-config` パラメーターは、デバイスの `type` によって異なります。さまざまなストレージバックエンド用のパラメーターについては、「[ストレージ](#)」を参照してください。

## sr-data-source-forget

```
1 sr-data-source-forget data-source=data_source
```

ストレージリポジトリのデータソースを指定して記録を停止して、記録済みのすべてのデータを消去します。

## sr-data-source-list

```
1 sr-data-source-list"
```

ストレージリポジトリで、記録可能なデータソースのリストを出力します。

## sr-data-source-query

```
1 sr-data-source-query data-source=data_source
```

ストレージリポジトリのデータソースから最後に読み取った値を照会します。

### **sr-data-source-record**

```
1 sr-data-source-record data-source=data_source
```

ストレージリポジトリで、指定したデータソースを記録します。

### **sr-destroy**

```
1 sr-destroy uuid=sr_uuid
```

Citrix Hypervisor サーバー上の指定したストレージリポジトリを破棄します。

### **sr-enable-database-replication**

```
1 sr-enable-database-replication uuid=sr_uuid
```

指定した（共有）ストレージリポジトリへの XAPI データベースの複製を有効にします。

### **sr-disable-database-replication**

```
1 sr-disable-database-replication uuid=sr_uuid
```

指定したストレージリポジトリへの XAPI データベースの複製を無効にします。

### **sr-forget**

```
1 sr-forget uuid=sr_uuid
```

XAPI エージェントから、Citrix Hypervisor サーバーの指定されたストレージリポジトリを削除します。XAPI エージェントからストレージリポジトリが削除されると、ストレージリポジトリが切断され、その上の VDI にアクセスできなくなります。ただし、そのストレージリポジトリはソースメディア上に残ります（データは失われません）。

### **sr-introduce**

```
1 sr-introduce name=label=name physical-size=physical_size type=type
content-type=content_type uuid=sr_uuid
```

ストレージリポジトリのレコードをデータベースに配置するだけです。 `device-config` を使用して `device-config:parameter_key=parameter_value` の形式で追加パラメーターを指定します。例:

```
1 xe sr-introduce device-config:device=/dev/sdb1
```

注:

このコマンドは、通常の操作では使用しません。作成後のストレージリポジトリを共有用に再設定する必要がある場合や、さまざまな障害シナリオからの回復に使用できる、高度な操作です。

## sr-probe

```
1 sr-probe type=type [host-uuid=host_uuid] [device-config:config_name=value]
```

指定した `device-config` キーに基づいて、特定のバックエンドのスキャンを行います。 `device-config` で目的のストレージリポジトリバックエンドの設定パラメーターを指定すると、その値に一致するストレージリポジトリのリストが返されます。 `device-config` で一部のパラメーターのみを指定して特定バックエンドのスキャンを行うと、目的のストレージリポジトリを検出するために指定すべきほかの `device-config` パラメーターが返されます。スキャンの結果は、バックエンド固有の XML 形式で返され、CLI に出力されます。

`device-config` パラメーターは、デバイスの `type` によって異なります。さまざまなストレージバックエンド用のパラメーターについては、「[ストレージ](#)」を参照してください。

## sr-probe-ext

```
1 sr-probe-ext type=type [host-uuid=host_uuid] [device-config:=config] [sm-config:-sm_config]
```

ストレージプローブを実行します。 `device-config` パラメーターは、 `device-config:devs=/dev/sdb1` など指定できます。 `sr-probe` とは異なり、このコマンドはすべてのストレージリポジトリの種類に対して人間が判読可能な形式で結果を返します。

## sr-scan

```
1 sr-scan uuid=sr_uuid
```

ストレージリポジトリのスキャンを強制して、XAPI データベースを、そのストレージサブストレートに存在する VDI と同期します。

## **sr-update**

```
1 sr-update uuid=uuid
```

データベース内の sr オブジェクトのフィールドを更新します。

## **lvhd-enable-thin-provisioning**

```
1 lvhd-enable-thin-provisioning sr-uuid=sr_uuid initial-allocation=
initial_allocation allocation-quantum=allocation_quantum
```

LVHD ストレージリポジトリのシンプロビジョニングを有効にします。

サブジェクトコマンド

サブジェクトを操作します。

## **session-subject-identifier-list**

```
1 session-subject-identifier-list
```

外部で認証された既存のすべてのセッションのすべてのユーザーサブジェクト ID のリストを返します。

## **session-subject-identifier-logout**

```
1 session-subject-identifier-logout subject-identifier=subject_identifier
```

ユーザーのサブジェクト ID に関連付けられたすべての外部認証セッションをログアウトします。

## **session-subject-identifier-logout-all**

```
1 session-subject-identifier-logout-all
```

すべての外部認証セッションをログアウトします。

### **subject-add**

```
1 subject-add subject-name=subject_name
```

プールにアクセスできるサブジェクトのリストにサブジェクトを追加します。

### **subject-remove**

```
1 subject-remove subject-uuid=subject_uuid
```

プールにアクセスできるサブジェクトのリストからサブジェクトを削除します。

### **subject-role-add**

```
1 subject-role-add uuid=uuid [role-name=role_name] [role-uuid=role_uuid]
```

サブジェクトにロールを追加します。

### **subject-role-remove**

```
1 subject-role-remove uuid=uuid [role-name=role_name] [role-uuid=
 role_uuid]
```

サブジェクトからロールを削除します。

### **secret-create**

```
1 secret-create value=value
```

シークレットを作成します。

### **secret-destroy**

```
1 secret-destroy uuid=uuid
```

シークレットを破棄します。

## タスクコマンド

実行時間の長い非同期タスク (task オブジェクト) を操作します。非同期タスクとは、仮想マシンの起動、停止、一時停止などのタスクを指します。通常、これらのタスクは、要求された操作をまとめて実行するほかのアトミックサブタスクの集合からなります。

task オブジェクトのリストは、標準オブジェクトリストコマンド (`xe task-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### task オブジェクトのパラメーター

task オブジェクトには、以下のパラメーターがあります。

| パラメーター名                       | 説明                                                                                          | 種類     |
|-------------------------------|---------------------------------------------------------------------------------------------|--------|
| <code>uuid</code>             | タスクの一意の識別子/オブジェクトリファレンス                                                                     | 読み取り専用 |
| <code>name-label</code>       | タスクの名前                                                                                      | 読み取り専用 |
| <code>name-description</code> | タスクの説明文字列                                                                                   | 読み取り専用 |
| <code>resident-on</code>      | タスクを実行しているホストの一意の識別子/オブジェクトリファレンス                                                           | 読み取り専用 |
| <code>status</code>           | タスクの現在の状態                                                                                   | 読み取り専用 |
| <code>progress</code>         | タスクが保留中の場合はその処理の推定完了率 (0-1)。成功したかどうかに関係なく、完了すると値は 1。                                        | 読み取り専用 |
| <code>type</code>             | タスクが正常に完了した場合、このパラメーターにはエンコードされた結果のタイプが含まれる。タイプは、参照が結果フィールドにあるクラスの名前。それ以外の場合、このパラメーターの値は未定義 | 読み取り専用 |
| <code>result</code>           | タスクが正常に完了した場合は結果値 (Void またはオブジェクト参照)。それ以外は未定義                                               | 読み取り専用 |

| パラメーター名                         | 説明                                                                                          | 種類     |
|---------------------------------|---------------------------------------------------------------------------------------------|--------|
| <code>error_info</code>         | タスクが失敗した場合はそのタスクに関するエラー文字列。それ以外の場合、このパラメーターの値は未定義                                           | 読み取り専用 |
| <code>allowed_operations</code> | この状態で可能な操作のリスト                                                                              | 読み取り専用 |
| <code>created</code>            | タスクの作成時刻                                                                                    | 読み取り専用 |
| <code>finished</code>           | タスクが完了（成功または失敗）した時刻。 <code>task-status</code> が <code>pending</code> の場合、このフィールドの値は意味を持ちません | 読み取り専用 |
| <code>subtask_of</code>         | このサブタスクが参照するタスクの UUID                                                                       | 読み取り専用 |
| <code>subtasks</code>           | このタスクのすべてのサブタスクの UUID                                                                       | 読み取り専用 |

## task-cancel

```
1 task-cancel [uuid=task_uuid]
```

指定したタスクを取り消して戻します。

### テンプレートコマンド

仮想マシンテンプレート (template オブジェクト) を操作します。

基本的に、template オブジェクトは、`is-a-template` パラメーターが `true` に設定された vm オブジェクトです。テンプレートは、特定の仮想マシンをインスタント化するさまざまな設定を含む「ゴールドイメージ」です。Citrix Hypervisor にはテンプレートの基本セットが付属しており、これらを基に「未加工」の汎用仮想マシンを作成して、オペレーティングシステムベンダーのインストール CD から起動できます (RHEL、CentOS、SLES、Windows など)。仮想マシンを作成し、それを必要に応じて設定し、将来の展開用にそのコピーをテンプレートとして保存できます。

template オブジェクトのリストは、標準オブジェクトリストコマンド (`xe template-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

注:

`is-a-template`パラメーターを **false** に設定して、テンプレートを仮想マシンに直接変換することはできません。`is-a-template`パラメーターを **false** に設定することはサポートされておらず、仮想マシンを起動できなくなります。

## template オブジェクトのパラメーター

template オブジェクトには、以下のパラメータがあります。

- `uuid` (読み取り専用) テンプレートの一意の識別子/オブジェクト参照
- `name-label` (読み取り/書き込み) テンプレートの名前
- `name-description` (読み取り/書き込み) テンプレートの説明文字列
- `user-version` (読み取り/書き込み) バージョン情報に含める、仮想マシンおよびテンプレートの作成者用の文字列
- `is-a-template` (読み取り/書き込み) この VM がテンプレートの場合は true。  
テンプレート仮想マシンは起動できない仮想マシンであり、複製して別の仮想マシンを作成するためのものです。この値を true に設定すると、false にリセットすることはできません。このパラメーターを使用して、テンプレート仮想マシンを仮想マシンに変換することはできません。
- `is-control-domain` (読み取り専用) コントロールドメイン (ドメイン 0 またはドライバードメイン) の場合に true
- `power-state` (読み取り専用) 現在の電源状態。テンプレートの場合、この値は常に halted です。
- `memory-dynamic-max` (読み取り専用) 動的最大メモリ量 (バイト数)。  
現在使用されていないパラメーターですが、変更する場合は以下の制限があります: `memory_static_max >= memory_dynamic_max >= memory_dynamic_min >= memory_static_min`。
- `memory-dynamic-min` (読み取り/書き込み) 動的最小メモリ量 (バイト数)。  
現在、使用されていないパラメーターですが、変更する場合は `memory-dynamic-max` と同じ制限が適用されます。
- `memory-static-max` (読み取り/書き込み) 静的設定 (絶対) 最大値 (バイト数)。仮想マシンに割り当てるメモリ量を指定するためのパラメーターです。
- `memory-static-min` (読み取り/書き込み) 静的設定 (絶対) 最小値 (バイト数)。  
仮想マシンに割り当てる最少メモリ量。`memory-static-min`には`memory-static-max`よりも小さい値を指定します。  
通常では使用されないパラメーターですが、前述の制限が適用されます。
- `suspend-VDI-uuid` (読み取り専用) 一時停止イメージを格納する VDI (テンプレートの場合意味を持ちません)

- `VCPUs-params` (読み取り/書き込みマップパラメーター) 選択した vCPU ポリシーの構成パラメーター。

次のコマンドで、使用する vCPU を指定できます:

```
1 xe template-param-set uuid=<template_uuid> vCPUs-params:mask=1,2,3
```

これにより、このテンプレートから作成した仮想マシンは物理 CPU の 1、2、および 3 上でのみ動作します。

また、`cap` および `weight` パラメーターを使用して、vCPU の優先度 (xen scheduling) を指定できます。次に例を示します:

```
1 xe template-param-set uuid=<template_uuid> VCPUs-params:weight=512 xe template-param-set uuid=<template_uuid> VCPUs-params:cap=100
```

これにより、このテンプレートから作成した仮想マシン (`weight` は 512) は、そのホスト上のほかのドメイン (`weight` は 256) の 2 倍の CPU リソースを使用できます。`weight` に指定可能な値は 1 ~ 65535 で、デフォルト値は 256 です。

`cap` パラメーターを指定すると、Citrix Hypervisor サーバーの CPU にアイドルサイクルがある場合でも、このテンプレートから作成した仮想マシンが使用する CPU サイクルに上限を設定できます。`cap` には 1 つの物理 CPU のパーセンテージを指定します。つまり 100 は 1 つの物理 CPU、50 はその半分、400 は 4 つの物理 CPU を示します。デフォルト値は 0 で、これは上限を設定しないことを示します。

- `VCPUs-max` (読み取り/書き込み) vCPU の最大数
- `VCPUs-at-startup` (読み取り/書き込み) vCPU の起動数
- `actions-after-crash` (読み取り/書き込み) このテンプレートから作成した仮想マシンがクラッシュした後で実行する処理
- `console-uuids` (読み取り専用の設定パラメーター) 仮想コンソールデバイス
- `platform` (読み取り/書き込みマップパラメーター) プラットフォーム固有の構成

HVM ゲスト (Windows 仮想マシンなど) のパラレルポートのエミュレーションを無効にするには、次のコマンドを使用します。

```
1 xe vm-param-set uuid=<vm_uuid> platform:parallel=none
```

HVM ゲストのシリアルポートのエミュレーションを無効にするには、次のコマンドを使用します。

```
1 xe vm-param-set uuid=<vm_uuid> platform:hvm_serial=none
```

HVM ゲストの USB コントローラおよび USB タブレットデバイスのエミュレーションを無効にするには、次のコマンドを使用します。

```
1 xe vm-param-set uuid=<vm_uuid> platform:usb=false
2 xe vm-param-set uuid=<vm_uuid> platform:usb_tablet=false
```

- `allowed-operations` (読み取り専用の設定パラメーター) この状態で可能な操作のリスト
- `current-operations` (読み取り専用の設定パラメーター) このテンプレート上で現在処理中の操作のリスト
- `allowed-VBD-devices` (読み取り専用の設定パラメーター) 0 ~ 15 の整数で表した使用可能な VBD 識別子のリスト。このリストは参考情報であり、他のデバイスを使用することもできます (ただし機能しない場合があります)。
- `allowed-VIF-devices` (読み取り専用の設定パラメーター) 0 ~ 15 の整数で表した使用可能な VIF 識別子のリスト。このリストは参考情報であり、他のデバイスを使用することもできます (ただし機能しない場合があります)。
- `HVM-boot-policy` (読み取り/書き込み) HVM ゲストの起動ポリシー。BIOS の順序または空の文字列のいずれかです。
- `HVM-boot-params` (読み取り/書き込みマップパラメーター) `order` キーが HVM ゲストの起動順序を制御します: 起動順序は、`d` (CD/DVD)、`c` (ルートディスク)、および `n` (ネットワーク PXE ブート) の各文字で定義されます。デフォルトは `dc` です。
- `PV-kernel` (読み取り/書き込み) カーネルへのパス
- `PV-ramdisk` (読み取り/書き込み) `initrd` へのパス
- `PV-args` (読み取り/書き込み) カーネルコマンドライン引数の文字列
- `PV-legacy-args` (読み取り/書き込み) このテンプレートから作成した従来の仮想マシンを起動するための引数字列
- `PV-bootloader` (読み取り/書き込み) ブートローダーの名前またはパス
- `PV-bootloader-args` (読み取り/書き込み) ブートローダーの各種引数の文字列
- `last-boot-CPU-flags` (読み取り専用) このテンプレートから作成した仮想マシンを最後に起動したときの CPU フラグ。テンプレートに対しては指定されません
- `resident-on` (読み取り専用) このテンプレートから作成した仮想マシンが常駐する Citrix Hypervisor サーバー。テンプレートの場合は「`not in database`」と表示されます
- `affinity` (読み取り/書き込み) このテンプレートから作成した仮想マシンが優先的に実行される Citrix Hypervisor サーバー。`xe vm-start` コマンドによって使用され、仮想マシンを実行する場所を決定します
- `other-config` (読み取り/書き込みマップパラメーター) テンプレートの追加構成パラメーターを指定するキー/値ペアのリスト

- **start-time** (読み取り専用) このテンプレートから作成した仮想マシンのメトリクスが読み取られた日時。形式は`yyyymmddThh:mm:ss z`。ここで `z` は、1文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)。テンプレートの場合は `1 Jan 1970 Z` (Unix/POSIX エポックの基準日時) を設定します
- **install-time** (読み取り専用) このテンプレートから作成した仮想マシンのメトリクスが読み取られた日時。形式は`yyyymmddThh:mm:ss z`。ここで `z` は、1文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)。テンプレートの場合は `1 Jan 1970 Z` (Unix/POSIX エポックの基準日時) を設定します
- **memory-actual** (読み取り専用) このテンプレートから作成した仮想マシンが使用する実メモリ。テンプレートの場合は `0`
- **VCPUs-number** (読み取り専用) このテンプレートから作成した仮想マシンに割り当てられた仮想 CPU の数。テンプレートの場合は `0`
- **VCPUs-Utilization** (読み取り専用マップパラメーター) 仮想 CPU とその読み取り専用の `weight` マップパラメーターのリスト。 `os-version` はこのテンプレートから作成した仮想マシンのオペレーティングシステムのバージョン。テンプレートの場合は `not in database` と表示されます
- **PV-drivers-version** (読み取り専用マップパラメーター) このテンプレートから作成した仮想マシンの準仮想化ドライバーのバージョン。テンプレートの場合は `not in database` と表示されます
- **PV-drivers-detected** (読み取り専用) このテンプレートから作成した仮想マシンの準仮想化ドライバーの最新バージョンのフラグ。テンプレートの場合は `not in database` と表示されます
- **memory** (読み取り専用マップパラメーター) このテンプレートから作成した仮想マシンのエージェントによって報告されるメモリメトリック。テンプレートの場合は `not in database` と表示されます
- **disks** (読み取り専用マップパラメーター) このテンプレートから作成した仮想マシンのエージェントによって報告されるディスクメトリック。テンプレートの場合は `not in database` と表示されます
- **networks** (読み取り専用マップパラメーター) このテンプレートから作成した仮想マシンのエージェントによって報告されるネットワークメトリック。テンプレートの場合は `not in database` と表示されます
- **other** (読み取り専用マップパラメーター) このテンプレートから作成した仮想マシンのエージェントによって報告されるその他のメトリック。テンプレートの場合は `not in database` と表示されます
- **guest-metrics-last-updated** (読み取り専用) ゲスト内のエージェントがこれらのフィールドへ最後に書き込みを実行したときの日時。形式は`yyyymmddThh:mm:ss z`。ここで `z` は、1文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)
- **actions-after-shutdown** (読み取り/書き込み) 仮想マシンがシャットダウンした後で実行する処理
- **actions-after-reboot** (読み取り/書き込み) 仮想マシンが再起動した後で実行する処理
- **possible-hosts** (読み取り専用) この仮想マシンを実行可能なホストのリスト
- **HVM-shadow-multiplier** (読み取り/書き込み) ゲストで使用できるシャドウメモリ量に適用される乗数

- `dom-id` (読み取り専用) ドメイン ID (使用可能な場合。それ以外は-1)
- `recommendations` (読み取り専用) この仮想マシンのプロパティに対する推奨値と推奨範囲の XML 仕様
- `xenstore-data` (読み取り/書き込みマップパラメーター) 仮想マシンの作成後、`xenstore` ツリー (`/local/domain/*domid*/vmdata`) に挿入するデータ
- `is-a-snapshot` (読み取り専用) このテンプレートが仮想マシンスナップショットの場合は `true`
- `snapshot_of` (読み取り専用) このテンプレートのスナップショット元の仮想マシンの UUID
- `snapshots` (読み取り専用) このテンプレートから作成されたすべてのスナップショットの UUID
- `snapshot_time` (読み取り専用) 最新の仮想マシンスナップショットの作成日時
- `memory-target` (読み取り専用) このテンプレートに設定されているターゲットメモリ量
- `blocked-operations` (読み取り/書き込みマップパラメーター) このテンプレートで実行できない操作の一覧表示
- `last-boot-record` (読み取り専用) このテンプレートで最後に使用されたブートパラメーターのレコード (XML 形式)
- `ha-always-run` (読み取り/書き込み) このテンプレートのインスタンスがそのホストの障害時に常にほかのホストで再起動する場合は `true`。このパラメータは廃止されています。代わりに `ha-restartpriority` を使用します。
- `ha-restart-priority` (読み取り専用) 再起動またはベストエフォート型の読み取り/書き込み BLOB バイナリデータストア
- `live` (読み取り専用) 実行中の仮想マシンでのみ意味を持ちます。

## template-export

```
1 template-export template-uuid=uuid_of_existing_template filename=
 filename_for_new_template
```

指定したテンプレートのコピーを新規のファイル名でエクスポートします。

## template-uninstall

```
1 template-uninstall template-uuid=template_uuid [--force]
```

カスタムテンプレートをアンインストールします。この操作により、このテンプレートによって「所有」とマークされた VDI が破棄されます。

## アップデートコマンド

次のセクションには、Citrix Hypervisor サーバーのアップデートコマンドが含まれています。

アップデートオブジェクトのリストは、標準オブジェクトリストコマンド (`xe update-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

## アップデートパラメーター

Citrix Hypervisor サーバーのアップデートコマンドには、次のパラメーターがあります：

| パラメーター名                           | 説明                                  | 種類     |
|-----------------------------------|-------------------------------------|--------|
| <code>uuid</code>                 | アップデートの一意の識別子/オブジェクト参照              | 読み取り専用 |
| <code>host</code>                 | このアップデートが適用されるホストの一覧                | 読み取り専用 |
| <code>host-uuid</code>            | 照会する Citrix Hypervisor サーバーの一意の識別子  | 読み取り専用 |
| <code>name-label</code>           | アップデートの名前                           | 読み取り専用 |
| <code>name-description</code>     | アップデートの説明文字列                        | 読み取り専用 |
| <code>applied</code>              | このアップデートが適用されているかどうか。true または false | 読み取り専用 |
| <code>installation-size</code>    | アップデートのサイズ (バイト数)                   | 読み取り専用 |
| <code>after-apply-guidance</code> | XAPI ツールスタックまたはホストの再起動が必要かどうか       | 読み取り専用 |
| <code>version</code>              | アップデートのバージョン                        | 読み取り専用 |

## update-upload

```
1 update-upload file-name=update_filename
```

指定したアップデートファイルを Citrix Hypervisor サーバーにアップロードします。このコマンドでアップデートを適用できる状態になります。アップロードに成功すると、アップデートファイルの UUID が返されます。同じアップデートが既にアップロードされている場合、`UPDATE_ALREADY_EXISTS`エラーが返され、これはアップロードされません。

### **update-precheck**

```
1 update-precheck uuid=update_uuid host-uuid=host_uuid
```

指定したアップデートに含まれている事前チェックを、指定した Citrix Hypervisor サーバーに対して実行します。

### **update-destroy**

```
1 update-destroy uuid=update_file_uuid
```

適用されていないアップデートファイルをプールから削除します。ホストに適用できないアップデートファイルの削除に使用できます。

### **update-apply**

```
1 update-apply host-uuid=host_uuid uuid=update_file_uuid
```

指定したアップデートファイルを適用します。

### **update-pool-apply**

```
1 update-pool-apply uuid=update_uuid
```

指定したアップデートをリソースプール内のすべての Citrix Hypervisor サーバーに適用します。

### **update-introduce**

```
1 update-introduce vdi-uuid=vdi_uuid
```

更新 VDI を導入します。

### **update-pool-clean**

```
1 update-pool-clean uuid=uuid
```

プール内のすべてのホストからアップデートファイルを削除します。

## ユーザーコマンド

**user-password-change**

```
1 user-password-change old=old_password new=new_password
```

ログインしているユーザーのパスワードを変更します。このコマンドを実行するにはスーパーバイザー権限が必要なため、変更前のパスワードフィールドはチェックされません。

**VBD**（仮想ブロックデバイス）コマンド

VBD (vbd オブジェクト) を操作します。

vbd オブジェクトは、仮想マシンを VDI に接続するソフトウェアオブジェクトで、仮想ディスクの内容を示します。VBD (vbd オブジェクト) には VDI を仮想マシンに関連付ける属性（起動の可否、読み取り/書き込みメトリックなど）があります。vdi オブジェクトには仮想ディスクの物理属性に関する情報（ストレージリポジトリの種類、ディスクの共有の可否、メディアが読み取り/書き込み可能か読み取り専用かなど）があります。

vbd オブジェクトのリストは、標準オブジェクトリストコマンド (`xe vbd-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

**vbd** オブジェクトのパラメーター

vbd オブジェクトには、以下のパラメーターがあります。

| パラメーター名                     | 説明                                    | 種類     |
|-----------------------------|---------------------------------------|--------|
| <code>uuid</code>           | VBD の一意の識別子/オブジェクト参照                  | 読み取り専用 |
| <code>vm-uuid</code>        | この VBD が接続されている仮想マシンの一意の識別子/オブジェクト参照  | 読み取り専用 |
| <code>vm-name-label</code>  | この VBD が接続されている仮想マシンの名前               | 読み取り専用 |
| <code>vdi-uuid</code>       | この VBD がマップされている VDI の一意の識別子/オブジェクト参照 | 読み取り専用 |
| <code>vdi-name-label</code> | この VBD がマップされている VDI の名前              | 読み取り専用 |
| <code>empty</code>          | 空のドライブの場合に <code>true</code>          | 読み取り専用 |

| パラメーター名                               | 説明                                                                                                                                | 種類                    |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <code>device</code>                   | ゲストから見たデバイス。たとえば <code>hda</code>                                                                                                 | 読み取り専用                |
| <code>userdevice</code>               | <code>vbd-create</code> のときに <code>device</code> パラメーターによって指定されるデバイス番号。 <code>hda</code> の場合は 0、 <code>hdb</code> の場合は 1 のようになります | 読み取り/書き込み             |
| <code>bootable</code>                 | この VBD が起動可能な場合に <code>true</code>                                                                                                | 読み取り/書き込み             |
| <code>mode</code>                     | VBD のマウントに使用すべきモード                                                                                                                | 読み取り/書き込み             |
| <code>type</code>                     | 仮想マシンに VBD が表示される方法。ディスクや CD などです                                                                                                 | 読み取り/書き込み             |
| <code>currently-attached</code>       | VBD がこのホストに接続されている場合は <code>true</code> 。それ以外は <code>false</code>                                                                 | 読み取り専用                |
| <code>storage-lock</code>             | ストレージレベルのロックが取得された場合は <code>true</code>                                                                                           | 読み取り専用                |
| <code>status-code</code>              | 最後の接続操作に関連するエラー/成功コード                                                                                                             | 読み取り専用                |
| <code>status-detail</code>            | 最後の接続操作の状態に関連するエラー/成功コード                                                                                                          | 読み取り専用                |
| <code>qos_algorithm_type</code>       | 使用する QoS アルゴリズム                                                                                                                   | 読み取り/書き込み             |
| <code>qos_algorithm_params</code>     | 選択した QoS アルゴリズムのパラメーター                                                                                                            | 読み取り/書き込み可のマッピングパラメータ |
| <code>qos_supported_algorithms</code> | この VBD でサポートされる QoS アルゴリズム                                                                                                        | 読み取り専用のセットパラメータ       |
| <code>io_read_kbs</code>              | この VBD の平均読み取り速度 (kB/秒)                                                                                                           | 読み取り専用                |
| <code>io_write_kbs</code>             | この VBD の平均書き込み速度 (kB/秒)                                                                                                           | 読み取り専用                |
| <code>allowed-operations</code>       | 現在の状態で可能な操作のリスト。このリストは参考用で、クライアントがこのフィールドを読み取る時点でサーバーの状態が変更されている可能性もあります                                                          | 読み取り専用のセットパラメータ       |

| パラメーター名                         | 説明                                                                                    | 種類                  |
|---------------------------------|---------------------------------------------------------------------------------------|---------------------|
| <code>current-operations</code> | 実行中の各タスクのリンク。タスクの性質を表す<br><code>current_operation</code> enum に対して、このオブジェクトを参照して使用する。 | 読み取り専用のセットパラメータ     |
| <code>unpluggable</code>        | この VBD がホットアンプラグをサポートする場合は <code>true</code>                                          | 読み取り/書き込み           |
| <code>attachable</code>         | デバイスが接続できる場合は <code>true</code>                                                       | 読み取り専用              |
| <code>other-config</code>       | 追加の構成                                                                                 | 読み取り/書き込み可のマップパラメータ |

## vbd-create

```
1 vbd-create vm-uuid=uuid_of_the_vm device=device_value vdi-uuid=
 uuid_of_vdi_to_connect_to [bootable=true] [type=Disk|CD] [mode=RW|RO
]
```

仮想マシン上に VBD を作成します。

`device` フィールドに指定可能な値は 0 ~ 15 の整数で、数値は仮想マシンごとに一意である必要があります。現在指定可能な値は、指定した仮想マシンの `allowed-VBD-devices` パラメーターで確認できます。これは `vbd` パラメーターに `userdevice` として表示されます。

`type` が `Disk` の場合、`vdi-uuid` は必須です。Disk の `mode` パラメーターには `RO` または `RW` を指定できます。

`type` が `CD` の場合、`vdi-uuid` は任意です。VDI を指定しない場合は、空の VBD が CD 用に作成されます。CD の `mode` パラメーターは `RO` である必要があります。

## vbd-destroy

```
1 vbd-destroy uuid=uuid_of_vbd
```

指定した VBD を破棄します。

その VBD の `other-config:owner` パラメーターが `true` の場合、関連付けられている VDI も破棄されます。

## vbd-eject

```
1 vbd-eject uuid=uuid_of_vbd
```

指定した VBD のドライブからメディアを取り除きます。このコマンドが機能するのは、メディアの種類が取り外し可能 (物理 CD または ISO) な場合のみです。それ以外の場合は、エラーメッセージ `VBD_NOT_REMOVABLE_MEDIA` が返されます。

### **vbd-insert**

```
1 vbd-insert uuid=uuid_of_vbd vdi-uuid=uuid_of_vdi_containing_media
```

指定した VBD のドライブに新しいメディアを挿入します。このコマンドが機能するのは、メディアの種類が取り外し可能 (物理 CD または ISO) な場合のみです。それ以外の場合は、エラーメッセージ `VBD_NOT_REMOVABLE_MEDIA` が返されます。

### **vbd-plug**

```
1 vbd-plug uuid=uuid_of_vbd
```

仮想マシンが実行状態のときに VBD の接続を試みます。

### **vbd-unplug**

```
1 vbd-unplug uuid=uuid_of_vbd
```

仮想マシンが実行状態のときに VBD の接続解除を試みます。

## **VDI (仮想ディスクイメージ) コマンド**

VDI (vdi オブジェクト) を操作します。

vdi オブジェクトはソフトウェアオブジェクトで、仮想マシンに表示される仮想ディスクの内容を示します。これは、仮想マシンを VDI に結び付けるオブジェクトである vbd オブジェクトとは異なります。vdi オブジェクトには仮想ディスクの物理属性に関する情報 (ストレージリポジトリの種類、ディスクの共有の可否、メディアが読み取り/書き込み可能か読み取り専用かなど) があります。VBD (vbd オブジェクト) には VDI を仮想マシンに関連付ける属性 (起動の可否、読み取り/書き込みメトリックなど) があります。

vdi オブジェクトのリストは、標準オブジェクトリストコマンド (`xe vdi-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

**vdi** オブジェクトのパラメーター

vdi オブジェクトには、以下のパラメーターがあります。

| パラメーター名                           | 説明                                                              | 種類               |
|-----------------------------------|-----------------------------------------------------------------|------------------|
| <code>uuid</code>                 | VDI の一意の識別子/オブジェクト参照                                            | 読み取り専用           |
| <code>name-label</code>           | VDI の名前                                                         | 読み取り/書き込み        |
| <code>name-description</code>     | VDI の説明文字列                                                      | 読み取り/書き込み        |
| <code>allowed-operations</code>   | この状態で可能な操作のリスト                                                  | 読み取り専用のセットパラメーター |
| <code>current-operations</code>   | この VDI で現在処理中の操作のリスト                                            | 読み取り専用のセットパラメーター |
| <code>sr-uuid</code>              | VDI を格納するストレージリポジトリ                                             | 読み取り専用           |
| <code>vbd-uuids</code>            | この VDI を参照する VBD のリスト                                           | 読み取り専用のセットパラメーター |
| <code>crashdump-uuids</code>      | この VDI を参照するクラッシュダンプのリスト                                        | 読み取り専用のセットパラメーター |
| <code>virtual-size</code>         | 仮想マシンで表示されるディスクのサイズ (バイト数)。ストレージバックエンドの種類によっては、正確に表示されない場合があります | 読み取り専用           |
| <code>physical-utilisation</code> | ストレージリポジトリ上での VDI の物理スペース (バイト数)                                | 読み取り専用           |
| <code>type</code>                 | VDI の種類。たとえば System または User                                    | 読み取り専用           |
| <code>sharable</code>             | VDI が共有可能な場合は true                                              | 読み取り専用           |
| <code>read-only</code>            | VDI を読み取り専用のみでマウントする場合は true                                    | 読み取り専用           |
| <code>storage-lock</code>         | VDI がストレージレベルでロックされている場合は true                                  | 読み取り専用           |
| <code>parent</code>               | VDI がチェーンの一部である場合は、親 VDI への参照                                   | 読み取り専用           |

| パラメーター名                       | 説明                                                                                                                                                      | 種類                    |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <code>missing</code>          | ストレージリポジトリのスキャン操作によりこの VDI がディスク上に存在しないと認識された場合は <code>true</code>                                                                                      | 読み取り専用                |
| <code>other-config</code>     | VDI の追加構成情報                                                                                                                                             | 読み取り/書き込み可のマッピングパラメータ |
| <code>sr-name-label</code>    | ストレージリポジトリの名前                                                                                                                                           | 読み取り専用                |
| <code>location</code>         | 場所情報                                                                                                                                                    | 読み取り専用                |
| <code>managed</code>          | VDI が管理されている場合は <code>true</code>                                                                                                                       | 読み取り専用                |
| <code>xenstore-data</code>    | VDI の接続後、xenstore ツリー ( <code>/local/domain/0/backend/vbd/domid/device-id/smdata</code> ) に挿入するデータ。SM バックエンドは通常このフィールドを <code>vdi_attach</code> に設定します。 | 読み取り専用のマッピングパラメータ     |
| <code>sm-config</code>        | SM に依存するデータ                                                                                                                                             | 読み取り専用のマッピングパラメータ     |
| <code>is-a-snapshot</code>    | この VDI が仮想マシンストレージスナップショットの場合は <code>true</code>                                                                                                        | 読み取り専用                |
| <code>snapshot_of</code>      | この VDI のスナップショット元のストレージの UUID                                                                                                                           | 読み取り専用                |
| <code>snapshots</code>        | この VDI のすべてのスナップショットの UUID                                                                                                                              | 読み取り専用                |
| <code>snapshot_time</code>    | この VDI を作成したスナップショット操作の日時                                                                                                                               | 読み取り専用                |
| <code>metadata-of-pool</code> | この VDI を作成したプールの UUID                                                                                                                                   | 読み取り専用                |
| <code>metadata-latest</code>  | VDI がプールの最新のメタデータを含んでいることを示すフラグ                                                                                                                         | 読み取り専用                |
| <code>cbt-enabled</code>      | 変更ブロック追跡が VDI で有効になっていることを示すフラグ                                                                                                                         | 読み取り/書き込み             |

## **vdi-clone**

```
1 vdi-clone uuid=uuid_of_the_vdi [driver-params:key=value]
```

直接使用できる、指定された VDI の書き込み可能なコピーを新規作成します。このコマンドがサポートされる場合、`vdi-copy`よりも高速にイメージを複製できます。

オプションの`driver-params`マップパラメーターを使用して、ベンダー固有の追加構成情報を、その VDI のバックエンドストレージドライバーに渡すことができます。詳しくは、ストレージベンダードライバーのドキュメントを参照してください。

## **vdi-copy**

```
1 vdi-copy uuid=uuid_of_the_vdi sr-uuid=uuid_of_the_destination_sr
```

VDI を指定したストレージリポジトリにコピーします。

## **vdi-create**

```
1 vdi-create sr-uuid=uuid_of_sr_to_create_vdi_on name=label=
name_for_the_vdi type=system|user|suspend|crashdump virtual-size=
size_of_virtual_disk sm-config-*=storage_specific_configuration_data
```

VDI を作成します。

`virtual-size`パラメーターは、バイト単位または IEC 標準の KiB、MiB、GiB、および TiB を使用して指定できます。

### 注:

ディスクのシンプロビジョニングをサポートする種類のストレージリポジトリ（ローカル VHD や NFS）では、ディスクの仮想割り当てが強制されません。このため、ストレージリポジトリ上で仮想ディスクを過剰に割り当てる場合には注意が必要です。過剰に割り当てたストレージリポジトリに空き領域がなくなった場合、そのターゲットサブストレートを使うか、またはそのストレージリポジトリ上の不要な VDI を削除して、ディスク領域を確保する必要があります。

ストレージリポジトリの種類によっては、設定したブロックサイズで分割できるように`virtual-size`の値が切り上げられる可能性があります。

## **vdi-data-destroy**

```
1 vdi-data-destroy uuid=uuid_of_vdi
```

指定された VDI に関連付けられたデータを破棄しますが、変更ブロック追跡のメタデータは保持します。

注:

VDI の増分バックアップを作成するために変更ブロック追跡を使用する場合、スナップショットを削除しながらメタデータを保持するには、`vdi-data-destroy` コマンドを使用するようにしてください。変更ブロック追跡が有効になった VDI のスナップショットで `vdi-destroy` を使用しないでください。

## **vdi-destroy**

```
1 vdi-destroy uuid=uuid_of_vdi
```

指定した VDI を破棄します。

注:

VDI の増分バックアップを作成するために変更ブロック追跡を使用する場合、スナップショットを削除しながらメタデータを保持するには、`vdi-data-destroy` コマンドを使用するようにしてください。変更ブロック追跡が有効になった VDI のスナップショットで `vdi-destroy` を使用しないでください。

ローカル VHD および NFS のストレージリポジトリでは、`vdi-destroy` により即時にディスク領域が解放されるのではなく、ストレージリポジトリのスキャン時に定期的に解放されます。VDI の破棄後のディスク領域を強制的に解放するには、手動で `[sr-scan](#sr-scan)` を実行します。

## **vdi-disable-cbt**

```
1 vdi-disable-cbt uuid=uuid_of_vdi
```

VDI の変更ブロック追跡を無効にします。

## **vdi-enable-cbt**

```
1 vdi-enable-cbt uuid=uuid_of_vdi
```

VDI の変更ブロック追跡を有効にします。

注:

変更ブロック追跡は、ライセンスが適用された Citrix Hypervisor Premium Edition インスタンスでのみ有効にできます。

## **vdi-export**

```
1 vdi-export uuid=uuid_of_vdi filename=filename_to_export_to [format=
 format] [base=uuid_of_base_vdi] [--progress]
```

指定したファイル名に VDI をエクスポートします。VDI は、次のいずれかの形式でエクスポートできます：

- raw
- vhd

VHD 形式はスパースである場合があります。VDI 内に割り当てられていないブロックがある場合、これらのブロックは VHD ファイルから省略され、VHD ファイルが小さくなる可能性があります。サポートされているすべての VHD ベースのストレージタイプ（EXT、NFS）から VHD 形式にエクスポートできます。

base パラメーターを指定する場合、このコマンドにより、エクスポートされた VDI とベース VDI の間で変更されたブロックのみがエクスポートされます。

### vdi-forget

```
1 vdi-forget uuid=uuid_of_vdi
```

ストレージから VDI を削除せずに、データベースから VDI レコードだけを削除します。通常は、[vdi-destroy](#vdi-destroy) を使用します。

### vdi-import

```
1 vdi-import uuid=uuid_of_vdi filename=filename_to_import_from [format=
 format] [--progress]
```

VDI をインポートします。VDI は、次のいずれかの形式でインポートできます：

- raw
- vhd

### vdi-introduce

```
1 vdi-introduce uuid=uuid_of_vdi sr-uuid=uuid_of_sr name-label=
 name_of_new_vdi type=system|user|suspend|crashdump location=
 device_location_(varies_by_storage_type) [name-description=
 description_of_vdi] [sharable=yes|no] [read-only=yes|no] [other-
 config=map_to_store_misc_user_specific_data] [xenstore-data=
 map_to_of_additional_xenstore_keys] [sm-config=
 storage_specific_configuration_data]
```

ストレージを実際に変更したり作成したりせずに、既存のストレージデバイスの vdi オブジェクトを作成します。このコマンドは、ホットプラグされたストレージデバイスを自動的にイントロデュースするために、主に内部で使用されます。

### **vdi-list-changed-blocks**

```
1 vdi-list-changed-blocks vdi-from-uuid=first-vdi-uuid vdi-to-uuid=second
-vdi-uuid
```

2 つの VDI を比較し、変更されたブロックの一覧を BASE64 でエンコードされた文字列として返します。このコマンドは、変更ブロック追跡を有効にした VDI に対してのみ機能します。

詳しくは、「[変更ブロック追跡](#)」を参照してください。

### **vdi-pool-migrate**

```
1 vdi-pool-migrate uuid=VDI_uuid sr-uuid=destination-sr-uuid
```

VDI を指定したストレージリポジトリに移行し、VDI を実行中のゲストに接続します。(ストレージライブマイグレーション)

詳しくは、「[仮想マシンの移行](#)」を参照してください。

### **vdi-resize**

```
1 vdi-resize uuid=vdi_uuid disk-size=new_size_for_disk
```

UUID で指定した VDI のサイズを変更します。

### **vdi-snapshot**

```
1 vdi-snapshot uuid=uuid_of_the_vdi [driver-params=params]
```

バックアップまたはテンプレートの作成時、またはその両方の作成時に参照できる、読み書き可能な VDI を作成します。バックアップを行う場合、仮想マシン内でバックアップソフトウェアをインストールして実行する代わりに、スナップショットを使ってバックアップを作成できます。仮想マシンの外部でバックアップソフトウェアがスナップショットの内容をバックアップメディアに保存している間も、仮想マシンを停止する必要はありません。同様に、スナップショットはテンプレートの基になる「ゴールドイメージ」として使用することもできます。テンプレートは、いずれの VDI からも作成できます。

オプションの `driver-params` マップパラメーターを使用して、VDI の基盤となるバックエンドストレージドライバーに追加のベンダー固有の構成情報を渡します。詳しくは、ストレージベンダードライバーのドキュメントを参照してください。

スナップショットの複製は、常に書き込み可能な VDI を作成します。

## **vdi-unlock**

```
1 vdi-unlock uuid=uuid_of_vdi_to_unlock [force=true]
```

指定した VDI のロック解除を試みます。 `force=true` を指定すると、強制的にロックを解除します。

## **vdi-update**

```
1 vdi-update uuid=uuid
```

データベース内の vdi オブジェクトのフィールドを更新します。

## **VIF** (仮想ネットワークインターフェイス) コマンド

VIF (vif オブジェクト) を操作します。

vif オブジェクトのリストは、標準オブジェクトリストコマンド (`xe vif-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### **vif** オブジェクトのパラメーター

vif オブジェクトには、以下のパラメーターがあります。

- `uuid` (読み取り専用) VIF の一意の識別子/オブジェクト参照
- `vm-uuid` (読み取り専用) この VIF が存在する仮想マシンの一意の識別子/オブジェクト参照
- `vm-name-label` (読み取り専用) VIF が存在する仮想マシンの名前
- `allowed-operations` (読み取り専用の設定パラメーター) この状態で可能な操作のリスト
- `current-operations` (読み取り専用の設定パラメーター) この VIF で現在処理中の操作のリスト
- `device` (読み取り専用) VIF バックエンドの作成順を示す、VIF の整数ラベル
- `MAC` (読み取り専用) 仮想マシンに提供される、VIF の MAC アドレス

- **MTU** (読み取り専用) VIF の MTU (Maximum Transmission Unit) バイト数。

このパラメーターは読み取り専用ですが、`other-config` マップパラメーターの `mtu` キーでこの MTU 設定よりも優先される値を指定できます。たとえば、ジャンボフレームを使用するように仮想 NIC の MTU をリセットするには次のコマンドを実行します：

```
1 xe vif-param-set \
2 uuid=<vif_uuid> \
3 other-config:mtu=9000
```

- `currently-attached` (読み取り専用) デバイスが接続されている場合は `true`
- `qos_algorithm_type` (読み取り/書き込み) 使用する QoS アルゴリズム
- `qos_algorithm_params` (読み取り/書き込みマップパラメーター) 選択した QoS アルゴリズムのパラメーター
- `qos_supported_algorithms` (読み取り専用の設定パラメーター) この VIF でサポートされる QoS アルゴリズム
- `MAC-autogenerated` (読み取り専用) VIF の MAC アドレスが自動生成の場合に `true`
- `other-config` (読み取り/書き込みマップパラメーター) 追加構成の `key:value` ペア
- `other-config:ethtoolrx` (読み取り/書き込み) チェックサムの受信を有効にする場合は `on`、無効にする場合は `off`
- `other-config:ethtooltx` (読み取り/書き込み) チェックサムの転送を有効にする場合は `on`、無効にする場合は `off`
- `other-config:ethtoolsg` (読み取り/書き込み) Scatter/Gather を有効にする場合は `on`、無効にする場合は `off`
- `other-config:ethtooltso` (読み取り/書き込み) TCP セグメンテーションオフロードを有効にする場合は `on`、無効にする場合は `off`
- `other-config:ethtoolufo` (読み取り/書き込み) UDP フラグメンテーションオフロードを有効にする場合は `on`、無効にする場合は `off`
- `other-config:ethtoolgso` (読み取り/書き込み) 汎用セグメンテーションオフロードを有効にする場合は `on`、無効にする場合は `off`
- `other-config:promiscuous` (読み取り/書き込み) VIF がブリッジ上で無作為検出 (ブリッジ上のすべてのトラフィックを検出) を行う場合に `true`。侵入検知システム (IDS) などを仮想マシンで実行するのに便利です。
- `network-uuid` (読み取り専用) この VIF が接続されている仮想ネットワークの一意の識別子/オブジェクト参照
- `network-name-label` (読み取り専用) この VIF が接続されている仮想ネットワークの名前

- `io_read_kbs` (読み取り専用) この VIF の平均読み取り速度 (kB/秒)
- `io_write_kbs` (読み取り専用) この VIF の平均書き込み速度 (kB/秒)
- `locking_mode` (読み取り専用) VIF で送受信されるトラフィックを MAC アドレスや IP アドレスでフィルターするためのロックモード。追加のパラメーターが必要です。
- `locking_mode:default` (読み取り専用) ネットワークのロックモードが VIF に適用されます。

ネットワークの `default-locking-mode` が `disabled` の場合、Citrix Hypervisor によってそのネットワークが接続する VIF ですべての送受信トラフィックがドロップされます。`default-lockingmode` が `unlocked` の場合、Citrix Hypervisor によってそのネットワークが接続する VIF ですべての送受信トラフィックが許可されます。詳しくは、「ネットワークコマンド」を参照してください。

- `locking_mode:locked` (読み取り/書き込み) VIF で特定の MAC アドレスおよび IP アドレスで送受信されるトラフィックのみが許可されます。IP アドレスが指定されていない場合、トラフィックは許可されません。
- `locking_mode:unlocked` (読み取り/書き込み) VIF で送受信されるトラフィックにいかなるフィルターも適用されません。
- `locking_mode:disabled` (読み取り/書き込み) Citrix Hypervisor により VIF ですべての送受信トラフィックがドロップされます。

## vif-create

```
1 vif-create vm-uuid=uuid_of_the_vm device=see below network-uuid=
 uuid_of_network_to_connect_to [mac=mac_address]
```

仮想マシンに VIF を作成します。

`device` フィールドに指定可能な値は、指定した仮想マシンのパラメーター `allowed-VIF-devices` にリストされます。VIF が存在しない仮想マシンで指定可能な値は 0 ~ 15 の整数です。

`mac` パラメーターは、`aa:bb:cc:dd:ee:ff` 形式の標準 MAC アドレスです。指定しない場合、ランダムな MAC アドレスが作成されます。`mac=random` を指定することで、ランダムな MAC アドレス作成を明示的に設定することもできます。

## vif-destroy

```
1 vif-destroy uuid=uuid_of_vif
```

VIF を破棄します。

### **vif-move**

```
1 vif-move uuid=uuid network-uuid=network_uuid
```

VIF を別のネットワークに移動します。

### **vif-plug**

```
1 vif-plug uuid=uuid_of_vif
```

仮想マシンが実行状態のときに VIF の接続を試みます。

### **vif-unplug**

```
1 vif-unplug uuid=uuid_of_vif
```

仮想マシンが実行状態のときに VIF の接続解除を試みます。

### **vif-configure-ipv4**

この仮想インターフェイスで IPv4 設定を構成します。以下のように、IPv4 設定を設定します。

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=static address=CIDR_address
 gateway=gateway_address
```

次に例を示します：

```
1 VIF.configure_ipv4(vifObject,"static", " 192.168.1.10/24", "
 192.168.1.1")
```

以下のように、IPv4 設定を削除します。

```
1 vif-configure-ipv4 uuid=uuid_of_vif mode=none
```

### **vif-configure-ipv6**

この仮想インターフェイスで IPv6 設定を構成します。以下のように、IPv6 設定を設定します。

```
1 vif-configure-ipv6 uuid=uuid_of_vif mode=static address=IP_address
 gateway=gateway_address
```

次に例を示します：

```
1 VIF.configure_ipv6(vifObject,"static", "fd06:7768:b9e5:8b00::5001/64",
"fd06:7768:b9e5:8b00::1")
```

以下のように、IPv6 設定を削除します。

```
1 vif-configure-ipv6 uuid=uuid_of_vif mode=none
```

## VLAN（仮想ネットワーク）コマンド

VLAN（仮想ネットワーク）を操作します。仮想インターフェイスの一覧を出力して編集するには、PIF コマンドを使用します。このコマンドには、関連付けられた仮想ネットワークがあることを示す VLAN パラメーターがあります。詳しくは、「PIF（物理ネットワークインターフェイス）コマンド」を参照してください。たとえば、VLAN を一覧表示するには `xe pif-list` を使用します。

### vlan-create

```
1 vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
 uuid_of_network
```

Citrix Hypervisor サーバー上に VLAN を作成します。

### pool-vlan-create

```
1 pool-vlan-create pif-uuid=uuid_of_pif vlan=vlan_number network-uuid=
 uuid_of_network
```

リソースプール内のすべてのホストについて、指定されたネットワークが接続されているインターフェイス（eth0など）を識別し、新しい PIF オブジェクトを作成およびプラグして、VLAN を作成します。

### vlan-destroy

```
1 vlan-destroy uuid=uuid_of_pif_mapped_to_vlan
```

VLAN を破棄します。VLAN にマップされた PIF の UUID を指定する必要があります。

## 仮想マシンコマンド

仮想マシン（vm オブジェクト）とその属性を操作します。

## vm オブジェクトセレクター

ここで説明する多くのコマンドでは、以下の標準的な方法で1つまたは複数の仮想マシンを操作対象として指定します。最も簡単な方法は、引数`vm=name_or_uuid`を指定することです。実際の仮想マシンの `uuid` は、`xe vm-list power-state=running`などを実行して簡単に取得できます（指定できるフィールドの一覧を取得するには、コマンド`xe vm-list params=all`を使用します）。たとえば、`power-state=halted`を指定することで仮想マシンを選択します。その仮想マシンの`power-state`パラメーターは`halted`と同等です。複数の仮想マシンがフィルター条件に一致し、そのすべてのオブジェクトに対してコマンドを実行する場合は、オプション`--multiple`を指定します。指定できるすべてのパラメーターの一覧は、次の表のとおりです。

vm オブジェクトのリストは、標準オブジェクトリストコマンド (`xe vm-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

## vm オブジェクトのパラメーター

vm オブジェクトには、以下のパラメーターがあります。

### 注:

書き込み可能な vm パラメーターの値は、対象の仮想マシンが実行中であっても変更できます。ただし、その変更は動的には適用されず、仮想マシンを再起動するまで反映されません。

- `appliance`（読み取り/書き込み）仮想マシンを含んでいる仮想アプライアンス/vApp
- `uuid`（読み取り専用）仮想マシンの一意の識別子/オブジェクト参照
- `name-label`（読み取り/書き込み）仮想マシンの名前
- `name-description`（読み取り/書き込み）仮想マシンの説明文字列
- `order start order`（読み取り/書き込み）vApp の起動/シャットダウン時や高可用性での仮想マシンの起動順序
- `version`（読み取り専用）この仮想マシンが復元された回数。新しい仮想マシンを古いバージョンで上書きする場合は、`vm-recover`を呼び出します
- `user-version`（読み取り/書き込み）バージョン情報に含める、仮想マシンおよびテンプレートの作成者用の文字列
- `is-a-template`（読み取り/書き込み）この仮想マシンがテンプレートでない場合は `false`。テンプレート仮想マシンは起動できないものであり、複製して仮想マシンを作成するためのものです。この値を `true` に設定すると、その後 `false` にリセットすることはできません。このパラメーターを使用して、テンプレート仮想マシンを仮想マシンに変換することはできません。
- `is-control-domain`（読み取り専用）コントロールドメイン（ドメイン 0 またはドライバードメイン）の場合に `true`

- `power-state` (読み取り専用) 現在の電源状態
- `start-delay` (読み取り/書き込み) 仮想マシンの起動コールが返るまでの待機時間
- `shutdown-delay` (読み取り/書き込み) 仮想マシンのシャットダウンコールが返るまでの待機時間
- `memory-dynamic-max` (読み取り/書き込み) 動的最大メモリ量 (バイト数)
- `memory-dynamic-min` (読み取り/書き込み) 動的最小メモリ量 (バイト数)
- `memory-static-max` (読み取り/書き込み) 静的設定 (絶対) 最大値 (バイト数)。この値を変更する場合は、仮想マシンをシャットダウンする必要があります。
- `memory-static-min` (読み取り/書き込み) 静的設定 (絶対) 最小値 (バイト数)。この値を変更する場合は、仮想マシンをシャットダウンする必要があります。
- `suspend-VDI-uuid` (読み取り専用) 一時停止イメージを格納する VDI
- `VCPUs-params` (読み取り/書き込みマップパラメーター) 選択した vCPU ポリシーの構成パラメーター。

次のコマンドで、使用する vCPU を指定できます

```
1 xe vm-param-set uuid=<vm_uuid> VCPUs-params:mask=1,2,3
```

これにより、この仮想マシンは物理 CPU の 1、2、および 3 上でのみ動作します。

また、`cap` および `weight` パラメーターを使用して、vCPU の優先度 (xen scheduling) を指定できます。次に例を示します:

```
1 xe vm-param-set uuid=<vm_uuid> VCPUs-params:weight=512 xe vm-param-set uuid=<vm_uuid> VCPUs-params:cap=100
```

これにより、この仮想マシン (`weight` は 512) は、その Citrix Hypervisor サーバー上のほかのドメイン (`weight` は 256) の 2 倍の CPU リソースを使用できます。`weight` に指定可能な値は 1 ~ 65535 で、デフォルト値は 256 です。`cap` パラメーターを指定すると、Citrix Hypervisor サーバーの CPU にアイドルサイクルがある場合でも、この仮想マシンが使用する CPU サイクルに上限を設定できます。`cap` には 1 つの物理 CPU のパーセンテージを指定します。つまり 100 は 1 つの物理 CPU、50 はその半分、400 は 4 つの物理 CPU を示します。デフォルト値は 0 で、これは上限を設定しないことを示します。

- `VCPUs-max` (読み取り/書き込み) vCPU の最大数。
- `VCPUs-at-startup` (読み取り/書き込み) vCPU の起動数
- `actions-after-crash` (読み取り/書き込み) 仮想マシンがクラッシュしたときに実行する処理。PV ゲーストの場合、有効なパラメーターは次のとおりです:
  - `preserve` (分析用のみ)
  - `coredump_and_restart` (コアダンプを記録して、仮想マシンを再起動する)
  - `coredump_and_destroy` (コアダンプを記録して、仮想マシンを停止状態のままにする)
  - `restart` (コアダンプを記録せずに、仮想マシンを再起動する)

- `destroy` (コアダンプを記録せずに、仮想マシンを停止状態のままにする)
- `console-uuids` (読み取り専用の設定パラメーター) 仮想コンソールデバイス
- `platform` (読み取り/書き込みマップパラメーター) プラットフォーム固有の構成

VDA を無効にして Windows 10 をタブレットモードに切り替えるには:

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=0
```

VDA を有効にして Windows 10 をタブレットモードに切り替えるには:

```
1 xe vm-param-set uuid=<vm_uuid> platform:acpi_laptop_slate=1
```

現在の状態を確認するには:

```
1 xe vm-param-get uuid=<vm_uuid> param-name=platform param-key=acpi_laptop_slate
```

- `allowed-operations` (読み取り専用の設定パラメーター) この状態で可能な操作のリスト
- `current-operations` (読み取り専用の設定パラメーター) 仮想マシン上で現在処理中の操作のリスト
- `allowed-VBD-devices` (読み取り専用の設定パラメーター) 0 ~ 15 の整数で表した使用可能な VBD 識別子のリスト。このリストは参考情報であり、他のデバイスを使用することもできます (ただし機能しない場合があります)。
- `allowed-VIF-devices` (読み取り専用の設定パラメーター) 0 ~ 15 の整数で表した使用可能な VIF 識別子のリスト。このリストは参考情報であり、他のデバイスを使用することもできます (ただし機能しない場合があります)。
- `HVM-boot-policy` (読み取り/書き込み) HVM ゲストの起動ポリシー。BIOS の順序または空の文字列のいずれかです。
- `HVM-boot-params` (読み取り/書き込みマップパラメーター) `order` キーが HVM ゲストの起動順序を制御します: 起動順序は、d (CD/DVD)、c (ルートディスク)、および n (ネットワーク PXE ブート) の各文字で定義されます。デフォルトは dc です。
- `HVM-shadow-multiplier` (読み取り/書き込み) 仮想マシンに許可するシャドウメモリオーバーヘッドの量を制御する浮動小数点値。デフォルトは 1.0 (最小値) で、この値は上級ユーザーのみが変更するようにしてください。
- `PV-kernel` (読み取り/書き込み) カーネルへのパス
- `PV-ramdisk` (読み取り/書き込み) `initrd` へのパス
- `PV-args` (読み取り/書き込み) カーネルコマンドライン引数の文字列
- `PV-legacy-args` (読み取り/書き込み) 従来の仮想マシンを起動するための引数文字列

- `PV-bootloader` (読み取り/書き込み) ブートローダーの名前またはパス
- `PV-bootloader-args` (読み取り/書き込み) ブートローダーの各種引数の文字列
- `last-boot-CPU-flags` (読み取り専用) 仮想マシンが最後に起動した CPU フラグの説明
- `resident-on` (読み取り専用) 仮想マシンが常駐する Citrix Hypervisor サーバー
- `affinity` (読み取り/書き込み) 仮想マシンが優先的に実行される Citrix Hypervisor サーバー。 `xe vm-start` コマンドによって使用され、仮想マシンを実行する場所を決定します
- `other-config` (読み取り/書き込みマップパラメーター) 仮想マシンの追加構成パラメーターを指定するキー/値ペアのリスト `other-config` パラメーターがキーと値のペア `auto_poweron: true` を含む場合、その仮想マシンはホストの起動時に自動的に開始されます。
- `start-time` (読み取り専用) 仮想マシンのメトリックが読み取られた日時のタイムスタンプ。このタイムスタンプの形式は `yyyymmddThh:mm:ss z`。ここで `z` は、1 文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)
- `install-time` (読み取り専用) 仮想マシンのメトリックが読み取られた日時のタイムスタンプ。このタイムスタンプの形式は `yyyymmddThh:mm:ss z`。ここで `z` は、1 文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)
- `memory-actual` (読み取り専用) 仮想マシンが使用する実メモリ
- `VCPUs-number` (読み取り専用) Linux 仮想マシンの場合、仮想マシンに割り当てられている仮想 CPU の数。この値が `VCPUS-max` と異なっていても構いません。また、`vm-vcpu-hotplug` コマンドを使用すると、仮想マシンを再起動せずに値を変更できます。詳しくは、「`[vm-vcpu-hotplug](#vm-vcpu-hotplug)`」を参照してください。Windows 仮想マシンの場合、常に `VCPUSmax` に設定された数の仮想 CPU を使用します。この値を変更した場合、仮想マシンの再起動が必要です。Citrix Hypervisor サーバー上の物理 CPU の数より大きい値を `VCPUS-number` に設定すると、パフォーマンスが著しく低下します。
- `VCPUs-Utilization` (読み取り専用マップパラメーター) 仮想 CPU とその優先度 (weight) のリスト
- `os-version` (読み取り専用マップパラメーター) 仮想マシンのオペレーティングシステムのバージョン
- `PV-drivers-version` (読み取り専用マップパラメーター) 仮想マシンの準仮想化ドライバーのバージョン
- `PV-drivers-detected` (読み取り専用) 仮想マシンの準仮想化ドライバーの最新バージョンのフラグ
- `memory` (読み取り専用マップパラメーター) 仮想マシンのエージェントによって報告されるメモリメトリック
- `disks` (読み取り専用マップパラメーター) 仮想マシンのエージェントによって報告されるディスクメトリック。
- `networks` (読み取り専用マップパラメーター) 仮想マシンのエージェントによって報告されるネットワークメトリック。

- `other` (読み取り専用マップパラメーター) 仮想マシンのエージェントによって報告されるその他のメトリック
- `guest-metrics-lastupdated` (読み取り専用) ゲスト内のエージェントがこれらのフィールドへ最後に書き込みを実行したときの日時。このタイムスタンプの形式は `yyyymmddThh:mm:ss z`。ここで `z` は、1文字の軍用タイムゾーンインジケーターで、たとえば `Z` は UTC (GMT)
- `actions-after-shutdown` (読み取り/書き込み) 仮想マシンがシャットダウンした後で実行する処理
- `actions-after-reboot` (読み取り/書き込み) 仮想マシンが再起動した後で実行する処理
- `possible-hosts` この読み取り専用仮想マシンを実行可能なホスト
- `dom-id` (読み取り専用) ドメイン ID (使用可能な場合。それ以外は-1)
- `recommendations` (読み取り専用) この仮想マシンのプロパティに対する推奨値と推奨範囲の XML 仕様
- `xenstore-data` (読み取り/書き込みマップパラメーター) 仮想マシンの作成後、`xenstore` ツリー (`/local/domain/domid/vm-data`) に挿入するデータ
- `is-a-snapshot` (読み取り専用) この仮想マシンがスナップショットの場合は `true`
- `snapshot_of` (読み取り専用) このスナップショット元の仮想マシンの UUID
- `snapshots` (読み取り専用) この仮想マシンのすべてのスナップショットの UUID
- `snapshot_time` (読み取り専用) この仮想マシンスナップショットの作成日時
- `memory-target` (読み取り専用) この仮想マシンに設定されているターゲットメモリ量
- `blocked-operations` (読み取り/書き込みマップパラメーター) この仮想マシンで実行できない操作の一覧表示
- `last-boot-record` (読み取り専用) このテンプレートで最後に使用されたブートパラメーターのレコード (XML 形式)
- `ha-always-run` (読み取り/書き込み) この仮想マシンがそのホストの障害時に常にほかのホストで再起動する場合は `true`。このパラメータは廃止されています。代わりに `ha-restart-priority` を使用します。
- `ha-restart-priority` (読み取り/書き込み) 再起動またはベストエフォート
- `blobs` (読み取り専用) バイナリデータストア
- `live` (読み取り専用) 仮想マシンが実行中の場合は `true`。高可用性機能により仮想マシンが実行されていないと認識される場合は `false`。

## **vm-assert-can-be-recovered**

```
1 vm-assert-can-be-recovered uuid [database] vdi-uuid
```

特定の仮想マシンを回復するためにストレージを使用できるかどうかをテストします。

## vm-call-plugin

```
1 vm-call-plugin vm-uuid=vm_uuid plugin=plugin fn=function [args:key=
 value]
```

オプションの引数 (args:key=value) を指定して、指定された仮想マシン上のプラグイン内の関数を呼び出します。特殊文字 (たとえば改行) を含む「value」文字列を渡すには、構文 args:key:file=local\_file を代わりに使用して、local\_file の内容を取得し、全体として「key」に割り当てます。

## vm-cd-add

```
1 vm-cd-add cd-name=name_of_new_cd device=
 integer_value_of_an_available_vbd [vm-selector=vm_selector_value...]
```

選択した仮想マシンに新しい仮想 CD を追加します。deviceパラメーターは、仮想マシンのallowed-VBD-devicesパラメーターの値から選択する必要があります。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-cd-eject

```
1 vm-cd-eject [vm-selector=vm_selector_value...]
```

仮想 CD ドライブから CD をイジェクトします。このコマンドは、仮想マシンに設定されている CD が1つのみの場合に機能します。複数の CD がある場合は、xe vbd-ejectコマンドを使用し、VBD の UUID を指定します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-cd-insert

```
1 vm-cd-insert cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

仮想 CD ドライブに CD を挿入します。このコマンドは、仮想マシンに設定されている CD が1つのみで、そのデバイスが空である場合に機能します。空の CD デバイスが複数ある場合は、xe vbd-insertコマンドを使用し、VBD と挿入する VDI の UUID を指定します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-cd-list

```
1 vm-cd-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

指定した仮想マシンに接続されている CD のリストを出力します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

対象の VBD パラメーターと VDI パラメーターも指定できます。

## vm-cd-remove

```
1 vm-cd-remove cd-name=name_of_cd [vm-selector=vm_selector_value...]
```

指定した仮想マシンから仮想 CD を削除します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-checkpoint

```
1 vm-checkpoint new-name-label=name_label [new-name-description=description]
```

ストレージレベルの高速ディスクスナップショット処理により、既存の仮想マシンをチェックポイントします（サポートされる場合）。

## vm-clone

```
1 vm-clone new-name-label=name_for_clone [new-name-description=description_for_clone] [vm-selector=vm_selector_value...]
```

既存の仮想マシンを複製し、ストレージレベルの高速ディスククローン処理を行います（サポートされる場合）。**new-name-label** 引数と **new-name-description** 引数を使用して、複製後の仮想マシンの名前と説明（オプション）を指定します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-compute-maximum-memory

```
1 vm-compute-maximum-memory total=
 amount_of_available_physical_ram_in_bytes [approximate=add overhead
 memory for additional vCPUS? true|false] [vm-selector=
 vm_selector_value...]
```

物理 RAM の合計量を上限値として、既存の仮想マシンに割り当てることが可能な静的メモリの最大量を計算します。オプションのパラメーター `approximate` を使用すると、仮想マシンに仮想 CPU を後から追加する場合を考慮して、十分な量の余分なメモリを予約できます。

次に例を示します：

```
1 xe vm-compute-maximum-memory vm=testvm total='xe host-list params=
 memory-free --minimal'
```

このコマンドでは、`xe host-list` が返した `memory-free` パラメーターの値を使用して、仮想マシン `testvm` の最大メモリ量を設定します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-compute-memory-overhead

```
1 vm-compute-memory-overhead
```

仮想マシンの仮想化メモリオーバーヘッドを計算します。

## vm-copy

```
1 vm-copy new-name-label=name_for_copy [new-name-description=
 description_for_copy] [sr-uuid=uuid_of_sr] [vm-selector=
 vm_selector_value...]
```

通常の方法で既存の仮想マシンを複製します（ストレージレベルの高速ディスククローン処理がサポートされる場合でもそれを使用しません）。複製された仮想マシンのディスクイメージは常にフルイメージであり、コピーオンライト (CoW) の一部ではありません。

`new-name-label` 引数と `new-name-description` 引数を使用して、複製後の仮想マシンの名前と説明（オプション）を指定します。

`sr-uuid` では、複製後の仮想マシンを格納するストレージリポジトリを指定します。このパラメータを指定しない場合、元の仮想マシンと同じストレージリポジトリに格納されます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

### vm-copy-bios-strings

```
1 vm-copy-bios-strings host-uuid=host_uuid
```

指定されたホストの BIOS 文字列を仮想マシンにコピーします。

### vm-crashdump-list

```
1 vm-crashdump-list [vm-selector=vm selector value...]
```

指定した仮想マシンに関するクラッシュダンプのリストを出力します。

オプションの引数 `params` を使用して特定のパラメーター値を持つオブジェクトだけを出力する（つまりリストをフィルターする）場合は、そのオブジェクトのパラメーターのリストを含む文字列を値として指定します。または、キーワード `all` を指定してすべてのパラメーターのリストを出力することもできます。 `params` を使用しない場合、使用可能なすべてのパラメーターのうち、デフォルトのサブセットが出力されます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

### vm-data-source-list

```
1 vm-data-source-list [vm-selector=vm selector value...]
```

仮想マシンで、記録可能なデータソースのリストを出力します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべての仮想マシンに対してその操作が実行されます。

データソースには、パラメーターとして `standard` および `enabled` があり、このコマンドの出力で確認できます。データソースの `enabled` パラメーターが `true` の場合、そのデータソースのメトリクス情報がパフォーマンスデータベースに記録中であることを示します。 `standard` パラメーターが `true` のデータソースでは、デフォルトでメトリクス情報がパフォーマンスデータベースに記録されます（`enabled` パラメーターに `true` が設定されます）。データソースの `standard` パラメーターが `false` の場合、そのデータソースのメトリクス情報がパフォーマンスデータベースにデフォルトで記録されないことを示します（`enabled` パラメーターに `false` が設定されます）。

データソースメトリクスのパフォーマンスデータベースへの記録を開始するには、`vm-data-source-record` コマンドを実行します。このコマンドは、`enabled` を `true` に設定します。停止するには、`vm-data-source-forget` を実行します。このコマンドは、`enabled` を `false` に設定します。

## vm-data-source-record

```
1 vm-data-source-record data-source=name_description_of_data-source [vm-selector=vm selector value...]
```

仮想マシンで、指定したデータソースを記録します。

これにより、仮想マシンの永続的なパフォーマンスメトリクスデータベースにデータソースからの情報が書き込まれます。このデータベースは、パフォーマンス上の理由から、通常のエージェントデータベースとは区別されます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべての仮想マシンに対してその操作が実行されます。

## vm-data-source-forget

```
1 vm-data-source-forget data-source=name_description_of_data-source [vm-selector=vm selector value...]
```

仮想マシンのデータソースを指定して記録を停止して、記録済みのすべてのデータを消去します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべての仮想マシンに対してその操作が実行されます。

## vm-data-source-query

```
1 vm-data-source-query data-source=name_description_of_data-source [vm-selector=vm_selector_value...]
```

仮想マシンで、指定したデータソースを表示します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。ホストを選択するパラメーターを指定しない場合、すべての仮想マシンに対してその操作が実行されます。

## vm-destroy

```
1 vm-destroy uuid=uuid_of_vm
```

指定した仮想マシンを破棄します。その仮想マシンに関連付けられたストレージはそのまま残ります。ストレージも削除するには、`xe vm-uninstall`を使用します。

## vm-disk-add

```
1 vm-disk-add disk-size=size_of_disk_to_add device=uuid_of_device [vm-selector=vm_selector_value...]
```

指定した仮想マシンにディスクを追加します。`device`パラメーターは、仮想マシンの`allowed-VBD-devices`パラメーターの値から選択します。

`disk-size`パラメーターは、バイト単位または IEC 標準の KiB、MiB、GiB、および TiB を使用して指定できます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-disk-list

```
1 vm-disk-list [vbd-params] [vdi-params] [vm-selector=vm_selector_value...]
```

指定した仮想マシンに接続されているディスクのリストを出力します。`vbd-params`および`vdi-params`パラメーターは、それぞれのオブジェクトのフィールドを制御して出力します。この2つのパラメーターをコンマ区切りリストとして指定するか、完全なリストの場合は特殊キー`all`を指定します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-disk-remove

```
1 vm-disk-remove device=integer_label_of_disk [vm-selector=vm_selector_value...]
```

指定した仮想マシンからディスクを削除して、そのディスクを破棄します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-export

```
1 vm-export filename=export_filename [metadata=true|false] [vm-selector=vm_selector_value...]
```

指定された仮想マシン（ディスクイメージを含む）を、ローカルマシン上のファイルにエクスポートします。仮想マシンのエクスポート先のファイル名を、`filename`パラメーターで指定します。ファイル名の拡張子として、`.xva`を指定する必要があります。

`metadata`パラメーターが**true**の場合、ディスクはエクスポートされません。仮想マシンメタデータのみが出力ファイルに書き込まれます。このパラメーターを使用することで、仮想マシンのストレージをほかの方法で移動して、仮想マシン情報を再作成できるようになります。詳しくは、「`vm-import`」を参照してください。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「`vm` オブジェクトセレクター」を参照してください。オプションの引数には、`vm` オブジェクトのパラメーターから任意の数を指定できます。

## vm-import

```
1 vm-import filename=export_filename [metadata=true|false] [preserve=true|false] [sr-uuid=destination_sr_uuid]
```

以前にエクスポートしたファイルから仮想マシンをインポートします。`preserve`を**true**に設定すると、元の仮想マシンの MAC アドレスが保持されます。`sr-uuid`によって、仮想マシンのインポート先のストレージリポジトリを決定します。このパラメーターが指定されていない場合、デフォルトのストレージリポジトリが使用されます。

`metadata`を**true**に設定すると、エクスポート済みのメタデータを、それに関連付けられているディスクブロックを除外してインポートできます。このメタデータのみインポートは、VDIが見つからない場合（ストレージリポジトリと`VDI.location`により指定）に失敗します。この場合、`--force`オプションを指定して強制的にインポートできます。ディスクのミラーまたは移動が可能な場合、メタデータのインポート/エクスポートは、異なるリソースプール間で仮想マシンをすばやく移動するための手段になります（障害復旧時など）。

注:

複数の仮想マシンをインポートする場合は、同時に実行するよりも順番に実行した方が早く完了します。

## vm-install

```
1 vm-install new-name-label=name [template-uuid=uuid_of_desired_template] [template=template_uuid_or_name] [sr-uuid=sr_uuid | sr-name-label=name_of_sr] [copy-bios-strings-from=host_uuid]
```

テンプレートから仮想マシンをインストールまたは複製します。`template-uuid`引数または`template`引数のいずれかを使用して、テンプレート名を指定します。`sr-uuid`引数または`sr-name-label`引数のいずれかを使用して、ストレージリポジトリを指定します。BIOS で特定ホスト用にロックされたメディアからインストールする場合は、`copy-bios-strings-from`引数を指定します。

注:

既存のディスクを持つテンプレートからインストールする場合は、デフォルトでそのディスクと同じストレージリポジトリ上に新しいディスクが作成されます。ストレージリポジトリがサポートする場合は、これらのディスクの高速複製が実行されます。ほかのストレージリポジトリをコマンドで指定した場合は、新しいディスクがそのストレージリポジトリ上に作成されます。この場合、高速複製は不可能であり、完全コピーが実行されます。

既存のディスクを持たないテンプレートからのインストールでは、指定したストレージリポジトリ、またはプールのデフォルトストレージリポジトリ（ストレージリポジトリを指定しない場合）上に新しいディスクが作成されます。

### **vm-is-bios-customized**

```
1 vm-is-bios-customized
```

仮想マシンの BIOS 文字列がカスタマイズされているかどうかを示します。

### **vm-memory-balloon**

```
1 vm-memory-balloon target=target
```

実行中の仮想マシンのメモリターゲットを設定します。指定された値は、仮想マシンの `memory_dynamic_min` の値および `memory_dynamic_max` の値で定義された範囲内でなければなりません。

### **vm-memory-dynamic-range-set**

```
1 vm-memory-dynamic-range-set min=min max=max
```

仮想マシンのダイナミックメモリ範囲を設定します。ダイナミックメモリ範囲は、仮想マシンのメモリのソフト下限と上限を定義します。仮想マシンが実行中または停止中にこれらのフィールドを変更することは可能です。ダイナミックレンジは静的範囲内に収まる必要があります。

### **vm-memory-limits-set**

```
1 vm-memory-limits-set static-min=static_min static-max=static_max
dynamic-min=dynamic_min dynamic-max=dynamic_max
```

仮想マシンのメモリ制限を構成します。

## vm-memory-set

```
1 vm-memory-set memory=memory
```

仮想マシンのメモリ割り当てを設定します。

## vm-memory-shadow-multiplier-set

```
1 vm-memory-shadow-multiplier-set [vm-selector=vm_selector_value...] [
 multiplier=float_memory_multiplier]
```

指定した仮想マシンのシャドウメモリ乗数を設定します。

これは、ハードウェア支援型仮想マシンに割り当てられるシャドウメモリの量を変更するための高度なオプションです。

Citrix Virtual Apps などの特化したアプリケーションの処理負荷で最高のパフォーマンスを得るには、追加のシャドウメモリが必要です。

このメモリは、オーバーヘッドとして考えることができます。シャドウメモリは、仮想マシン用の通常のメモリとは別に計算されます。このコマンドを実行すると、その乗数に応じてホスト上の空きメモリ量が減り、`HVM_shadow_multiplier` フィールドが仮想マシンに割り当てられた値でアップデートされます。Citrix Hypervisor サーバーの空きメモリ量が足りない場合は、エラーが返されます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。

## vm-memory-static-range-set

```
1 vm-memory-static-range-set min=min max=max
```

仮想マシンの静的メモリ範囲を設定します。静的メモリ範囲は、仮想マシンのメモリのハード下限と上限を定義します。仮想マシンの停止中にのみ、これらのフィールドを変更できます。ダイナミックレンジは静的範囲内に収まる必要があります。

## vm-memory-target-set

```
1 vm-memory-target-set target=target
```

停止中または実行中の仮想マシンのメモリターゲットを設定します。指定された値は、仮想マシンの `memory_static_min` の値および `memory_static_max` の値で定義された範囲内でなければなりません。

**vm-memory-target-wait**

```
1 vm-memory-target-wait
```

実行中の仮想マシンが現在のメモリターゲットに達するまで待機します。

**vm-migrate**

```
1 vm-migrate [copy=true|false] [host-uuid=destination_host_uuid] [host=
 name_or_uuid_of_destination_host] [force=true|false] [live=true|
 false] [vm-selector=vm_selector_value...] [remote-master=
 destination_pool_master_uuid] [remote-username=
 destination_pool_username] [remote-password=
 destination_pool_password] [remote-network=
 destination_pool_network_uuid] [vif:=vif_uuid] [vdi=vdi_uuid]
```

このコマンドでは、指定した仮想マシンを物理ホスト間で移行します。hostパラメーターには、Citrix Hypervisor サーバーの名前か UUID を指定できます。たとえば、2つのホストが共有しているストレージに仮想マシンのディスクがあるプール内でその別のホストに仮想マシンを移行するには、次のコマンドを実行します：

```
1 xe vm-migrate uuid=vm_uuid host-uuid=host_uuid
```

ストレージを共有していない同一プール内のホスト間で仮想マシンを移動する（ストレージライブマイグレーション）には、次のコマンドを実行します：

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78 \
2 remote-username=username remote-password=password \
3 host-uuid=destination_host_uuid vdi=vdi_uuid
```

各 VDI が格納されているストレージリポジトリは、次のようにして選択できます。

```
1 xe vm-migrate uuid=vm_uuid host-uuid=destination_host_uuid \
2 vdi1:vdi_1_uuid=destination_sr_uuid \
3 vdi2:vdi_2_uuid=destination_sr2_uuid \
4 vdi3:vdi_3_uuid=destination_sr3_uuid
```

また、移行後に仮想マシンに接続するネットワークは、次のようにして選択できます。

```
1 xe vm-migrate uuid=vm_uuid \
2 vdi1:vdi_1_uuid=destination_sr_uuid \
3 vdi2:vdi_2_uuid=destination_sr2_uuid \
4 vdi3:vdi_3_uuid=destination_sr3_uuid \
5 vif:vif_uuid=network_uuid
```

プール間の移行の場合は、次のコマンドを実行します。

```
1 xe vm-migrate uuid=vm_uuid remote-master=12.34.56.78
2 remote-username=username remote-password=password \
3 host-uuid=desination_host_uuid vdi=vdi_uuid
```

ストレージライブマイグレーション、ライブマイグレーション、ライブ VDI マイグレーションの詳細については、「[仮想マシンの移行](#)」を参照してください。

デフォルトでは、仮想マシンが一時停止し、移行後に別のホスト上で再開します。`live`パラメーターは、ライブマイグレーションを選択します。ライブマイグレーションは仮想マシンを実行したまま移行できます。したがって、このときの仮想マシンのダウンタイムは1秒未満です。仮想マシンでメモリ負荷の高い処理を実行中など、状況によってはライブマイグレーション機能が無効になります。この場合、仮想マシンを一時停止してからメモリ転送が行われます。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「[vm オブジェクトセレクター](#)」を参照してください。オプションの引数には、`vm` オブジェクトのパラメーターから任意の数を指定できます。

### **vm-pause**

```
1 vm-pause
```

実行中の VM を一時停止します。この操作では、関連するメモリは解放されません (`vm-suspend`を参照)。

### **vm-query-services**

```
1 vm-query-services
```

特定の VM によって提供されるシステムサービスを照会します。

### **vm-reboot**

```
1 vm-reboot [vm-selector=vm_selector_value...] [force=true]
```

指定した仮想マシンを再起動します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「[vm オブジェクトセレクター](#)」を参照してください。オプションの引数には、`vm` オブジェクトのパラメーターから任意の数を指定できます。

強制的な再起動を引き起こすには、`force`引数を使用します。これは、物理サーバーの電源ケーブルをコンセントから抜くことに相当する操作です。

## vm-recover

```
1 vm-recover vm-uuid [database] [vdi-uuid] [force]
```

指定した VDI のデータベースから仮想マシンを回復します。

## vm-reset-powerstate

```
1 vm-reset-powerstate [vm-selector=vm_selector_value...] {
2 force=true }
```

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

これは、プール内のメンバホストがダウンしたときのみ使用する、高度なコマンドです。このコマンドを使用して、プールマスターに強制的に VM の電源の状態を `halted` にリセットさせることができます。基本的に、このコマンドにより仮想マシンとそのディスクが強制的にロックされるため、その仮想マシンをプール内の別のホスト上で起動できます。このコマンドでは `force` 引数の指定が必須で、これを指定しないと失敗します。

## vm-resume

```
1 vm-resume [vm-selector=vm_selector_value...] [force=true|false] [on=
 host_uuid]
```

指定した仮想マシンを再開します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

仮想マシンがリソースプールの共有ストレージリポジトリ上にある場合は、起動するプールメンバーを `on` 引数で指定します。デフォルトでは、システムにより適切な任意のホストが決定されます。

## vm-retrieve-wlb-recommendations

```
1 vm-retrieve-wlb-recommendations
```

選択された仮想マシンのワークロードバランス推奨事項を取得します。

## vm-shutdown

```
1 vm-shutdown [vm-selector=vm_selector_value...] [force=true|false]
```

指定した仮想マシンをシャットダウンします。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

仮想マシンを強制的にシャットダウンするには、`force`引数を使用します。これは、物理サーバーの電源ケーブルをコンセントから抜くことに相当する操作です。

## vm-snapshot

```
1 vm-snapshot new-name-label=name_label [new-name-description+
 name_description]
```

ストレージレベルの高速ディスクスナップショット処理により、既存の仮想マシンをスナップショットします（サポートされる場合）。

## vm-start

```
1 vm-start [vm-selector=vm_selector_value...] [force=true|false] [on=
 host_uuid] [--multiple]
```

指定した仮想マシンを起動します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

仮想マシンがリソースプールの共有ストレージリポジトリ上にある場合は、その仮想マシンを起動するプールメンバーを`on`引数で指定します。デフォルトでは、システムにより適切な任意のホストが決定されます。

## vm-suspend

```
1 vm-suspend [vm-selector=vm_selector_value...]
```

指定した仮想マシンをサスペンドします。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-uninstall

```
1 vm-uninstall [vm-selector=vm_selector_value...] [force=true|false]
```

仮想マシンをアンインストールし、そのディスク（RW とマークされ、この仮想マシンにのみ接続されている VDI）とそのメタデータレコードを破棄します。仮想マシンのメタデータだけを破棄するには、`xe vm-destroy` を使用します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

## vm-unpause

```
1 vm-unpause
```

一時停止した仮想マシンの一時停止を解除します。

## vm-vcpu-hotplug

```
1 vm-vcpu-hotplug new-vcpus=new_vcpu_count [vm-selector=vm_selector_value ...]
```

実行中の Linux 仮想マシンで使用可能な vCPU の数を動的に調整します。vCPU の数は、パラメーター `VCPUs-max` によって制限されます。Windows 仮想マシンの場合、常に `VCPUs-max` に設定された数の仮想 CPU を使用します。この値を変更した場合、仮想マシンの再起動が必要です。

このコマンドの対象 Linux 仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

注:

Citrix VM Tools をインストールせずに Linux 仮想マシンを実行する場合、仮想マシンで以下のコマンドを `root` として実行し、新しくホットプラグされた vCPU が確実に使用されるようにする必要があります: 

```
for i in /sys/devices/system/cpu/cpu[1-9]*/online; do if ["$(cat $i)" = 0]; then echo 1 > $i; fi; done
```

## vm-vif-list

```
1 vm-vif-list [vm-selector=vm_selector_value...]
```

指定した仮想マシンの VIF のリストを出力します。

このコマンドの対象仮想マシンを指定するには、標準的な方法を使用します。詳しくは、「vm オブジェクトセレクター」を参照してください。VIF ではなく仮想マシンがフィルターの対象になることに注意してください。オプションの引数には、vm オブジェクトのパラメーターから任意の数を指定できます。

### スケジュールされたスナップショット

仮想マシンのスケジュールされたスナップショットとその属性を操作します。

vmss オブジェクトのリストは、標準オブジェクトリストコマンド (`xe vmss-list`) を使用して出力でき、パラメーターは標準パラメーターコマンドを使用して操作できます。詳しくは、「低レベルパラメーターコマンド」を参照してください。

### vmss-create

```
1 vmss-create enabled=True/False name=label=name type=type frequency=
 frequency retained-snapshots=value name-description=description
 schedule:schedule
```

プールのスナップショットスケジュールを作成。

次に例を示します：

```
1 xe vmss-create retained-snapshots=9 enabled=true frequency=daily \
2 name-description=sample name=label=samplepolicy type=snapshot \
3 schedule:hour=10 schedule:min=30
```

スナップショットスケジュールには次のパラメーターがあります。

| パラメーター名                         | 説明                          | 種類        |
|---------------------------------|-----------------------------|-----------|
| <code>name-<b>label</b></code>  | スナップショットスケジュールの名前。          | 読み取り/書き込み |
| <code>name-description</code>   | スナップショットスケジュールの説明。          | 読み取り/書き込み |
| <code>type</code>               | ディスクスナップショットまたはメモリスナップショット。 | 読み取り/書き込み |
| <code>frequency</code>          | 毎時、毎日、毎週                    | 読み取り/書き込み |
| <code>retained-snapshots</code> | 保持するスナップショット範囲：1 ~ 10。      | 読み取り/書き込み |

| パラメーター名               | 説明                                                                                                                   | 種類        |
|-----------------------|----------------------------------------------------------------------------------------------------------------------|-----------|
| <code>schedule</code> | <code>schedule:days</code> (月曜日～日曜日)、 <code>schedule:hours</code> (0～23)、 <code>schedule:minutes</code> (0、15、30、45) | 読み取り/書き込み |

---

## **vmss-destroy**

```
1 vmss-destroy uuid=uuid
```

プールのスナップショットスケジュールを破棄。

## **USB** パススルー

**USB** パススルーの有効化/無効化

```
1 pusb-param-set uuid=pusb_uuid passthrough-enabled=true/false
```

USB パススルーを有効/無効にします。

## **pusb-scan**

```
1 pusb-scan host-uuid=host_uuid
```

PUSB をスキャンして更新します。

## **vusb-create**

```
1 vusb-create usb-group-uuid=usb_group_uuid vm-uuid=vm_uuid
```

プールに仮想 USB を作成します。仮想マシンを起動して、USB を仮想マシンにパススルーします。

## **vusb-unplug**

```
1 vusb-unplug uuid=vusb_uuid
```

仮想マシンから USB を接続解除します。

## vusb-destroy

```
1 vusb-destroy uuid=vusb_uuid
```

仮想マシンから仮想 USB 一覧を削除します。

## SDK および API

December 30, 2019

以下の Citrix Hypervisor 開発者向けドキュメントは、<https://developer-docs.citrix.com/>で参照できます。

- [Management API Guide \(英語\)](#)
- [ソフトウェア開発キットガイド](#)
- [Changed Block Tracking Guide \(英語\)](#)
- [Supplemental Packs and the DDK Guide \(英語\)](#)
- [Citrix XenCenter プラグイン仕様ガイド](#)

## データガバナンス

December 30, 2019

この記事では、Citrix Hypervisor によるログの収集、保存、保持に関する情報を提供します。

Citrix Hypervisor は、仮想マシンの展開をユーザーが作成および管理できるサーバー仮想化プラットフォームです。XenCenter は、Citrix Hypervisor の管理ユーザーインターフェイスです。Citrix Hypervisor および XenCenter は、次の機能を提供する一環としてユーザーデータを収集および保存できます：

- **ヘルスチェック** - ヘルスチェックサービスは XenCenter マシン上で実行され、サービスに登録されている Citrix Hypervisor サーバーおよびプールのサーバーステータスレポートを生成します。情報は収集され、ユーザーが定義したスケジュールで Citrix Insight Services に自動的にアップロードされます。詳しくは、「[ヘルスチェック](#)」を参照してください。
- **サーバーの状態レポート** - サーバーの状態レポートはオンデマンドでも生成でき、Citrix Insight Services にアップロードするか、シトリックスサポートに提供することができます。サーバーの状態レポートには、ユーザーの環境における問題の診断に役立つ情報が含まれています。
- **管理エージェントの自動更新** - 管理エージェントは、Citrix Hypervisor サーバーまたはプールでホストされている仮想マシン内で実行されます。サーバーまたはプールにライセンスが付与されている場合、管理エージェントは更新を確認して、それ自体および仮想マシン内の I/O ドライバーに更新を適用できます。更新の確認

の一環として、自動アップデート機能は、管理エージェントが実行されている仮想マシンを識別できる Web リクエストをシトリックスに送信します。

- **XenCenter** のアップデートの確認 - この機能により、XenCenter が管理する Citrix Hypervisor サーバーおよびプールで修正プログラム、累積更新プログラム、または新しいリリースを利用できるかどうかが決まります。更新の確認の一環として、この機能は、利用統計情報を含む Web 要求をシトリックスに送信します。この利用統計情報はユーザー固有ではなく、世界中の XenCenter インスタンスの総数を推定するために使用されます。
- **XenCenter** のメール通知 - XenCenter は、通知のしきい値を超えたときにメール通知を送信するように構成できます。これらのメール通知を送信するために、XenCenter はターゲットのメールアドレスを収集して保存します。

### データ所在地

Citrix Hypervisor 診断ログは、Citrix Hypervisor をインストールしたサーバー上にあります。

Citrix Insight Services にアップロードされたサーバーの状態レポートは、米国にある Amazon S3 環境に保存されます。

管理エージェントの自動アップデート機能および XenCenter のアップデートの確認機能によって行われたリクエストから取得された Web ログは、米国の Microsoft Azure クラウド環境にあります。その後、これらのログのコピーが英国のログ管理サーバーに作成されます。

メール通知の送信に XenCenter が使用するメールアドレスは、XenCenter をインストールしたマシンに保存されます。

### データ収集

Citrix Hypervisor および XenCenter は、次のデータソースから情報を収集します：

- XenCenter
- Citrix Hypervisor サーバーとプール
- ホストされた VM

### データ送信

XenCenter およびヘルスチェックサービスは、サーバーステータスレポートを Citrix Insight Services に安全に送信します。

管理エージェントの自動アップデート機能および XenCenter のアップデートの確認機能による Web リクエストは、HTTPS 経由で行われます。Web ログファイルは、ログ管理サーバーに安全に送信されます。

### データ管理

Citrix Hypervisor サーバーとプールは、MyCitrix アカウントを使用して収集および保存されるデータをオプトインすることにより、ヘルスチェックに登録する必要があります。これらのサーバーとプールは、いつでもヘルスチェックから登録解除できます。

ヘルスチェックデータとサーバーステータスレポートに含めるデータアイテムを選択できます。Citrix Insight Services の MyCitrix アカウントにアップロードされたヘルスチェックデータまたはサーバーステータスレポートを削除することもできます。

仮想マシンが管理エージェントの自動アップデート機能を使用するかどうかを選択できます。管理エージェントの自動アップデート機能の使用を選択した場合、Web 要求に仮想マシン ID 情報を含めるかどうかも選択できます。

XenCenter のアップデートの確認機能はデフォルトで有効になっています。この機能を無効にすることもできます。

XenCenter で構成されたメール通知を削除して、保存されているメール情報を削除できます。

### データ保持

Citrix Insight Services は、ヘルスチェックサービスによって収集された、またはユーザーがアップロードしたサーバーの状態レポートの自動データ保持を実装していません。そのため、ユーザーがデータ保持ポリシーを決定します。Citrix Insight Services の MyCitrix アカウントにアップロードされたヘルスチェックデータまたはサーバーステータスレポートを削除できます。

Citrix Insight Services のデータ処理について詳しくは、Citrix Insight Services Web サイトの [についてのデータの収集とプライバシー](#) の声明を参照してください。

管理エージェントの自動アップデート機能および XenCenter のアップデートの確認機能によって作成された Web リクエストからの情報を含む Web ログは、無期限に保持できます。

XenCenter は、メール通知の有効期間中にメール通知を提供するために使用されるメール情報を保持します。設定済みのメール通知を削除すると、データは削除されます。

### データ収集契約

ヘルスチェックによって Citrix Insight Services にアップロードされる情報は、トラブルシューティングや診断サポート、および [Citrix Insight Services ポリシー](#) と [Citrix プライバシーポリシー](#) で必要な製品の品質、信頼性、パフォーマンスの向上を目的として使用されます。

シトリックスが受信した情報は常に、[Citrix プライバシーポリシー](#) に従って扱われます。

### 付録：収集されたデータ

- サーバーの状態レポート

- 管理エージェントの自動アップデート Web ログ
- Web ログのアップデートの確認
- XenCenter のメール通知

#### サーバーの状態レポート

サーバーの状態レポートには、次のログファイルを含めることができます：

| ログの種類               | PII が含まれているか |
|---------------------|--------------|
| xapi-debug          | 可能性あり        |
| xen-info            | 可能性あり        |
| conntest            | いいえ          |
| xha-liveset         | 可能性あり        |
| high-availability   | 可能性あり        |
| firstboot           | はい           |
| xenserver-databases | はい           |
| multipath           | 可能性あり        |
| disk-info           | 可能性あり        |
| xenserver-logs      | 可能性あり        |
| xenserver-install   | 可能性あり        |
| process-list        | はい           |
| blobs               | いいえ          |
| xapi                | はい           |
| host-crashdump-logs | 可能性あり        |
| xapi-subprocess     | いいえ          |
| pam                 | いいえ          |
| control-slice       | 可能性あり        |
| tapdisk-logs        | いいえ          |
| kernel-info         | 可能性あり        |
| xenserver-config    | 可能性あり        |
| xenserver-domains   | いいえ          |
| device-model        | はい           |

| ログの種類                | PII が含まれているか  |
|----------------------|---------------|
| hardware-info        | 可能性あり         |
| xenopsd              | 可能性あり         |
| loopback-devices     | 可能性あり         |
| system-services      | いいえ           |
| system-logs          | 可能性あり         |
| network-status       | はい            |
| v6d                  | 可能性あり         |
| CVSM                 | いいえ           |
| message-switch       | 可能性あり         |
| VM-snapshot-schedule | いいえ           |
| xcp-rrdd-plugins     | 可能性あり         |
| yum                  | カスタマイズされている場合 |
| fcoe                 | はい            |
| xapi-clusterd        | 可能性あり         |
| network-config       | カスタマイズされている場合 |
| boot-loader          | いいえ           |

#### 管理エージェントの自動アップデート **Web** ログ

管理エージェントの自動更新 **Web** 要求には、次のデータポイントを含めることができます：

- 管理エージェントがインストールされている仮想マシンの IP アドレス
- 仮想マシンの UUID

#### **XenCenter** のアップデート **Web** ログの確認

アップデート機能のチェック **Web** 要求には、次のデータポイントが含まれています：

- XenCenter ホストマシンの IP アドレス
- XenCenter バージョン
- UUID

### **XenCenter** のメール通知

メールアラートを提供するには、XenCenter は次のデータポイントを保存します：

- メールアドレス
- SMTP サーバー



#### **Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).