

# H3C UIS HCI

## クイックスタートガイド

ドキュメントバージョン:5W100-20230727

---

Copyright©2023 New H3C Technologies Co.,Ltd. All rights reserved.

本マニュアルのいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または送信することはできません。

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者に帰属します。

このドキュメントの情報は、予告なしに変更されることがあります。

## 目次

UISについて .....	1
アーキテクチャー .....	1
ウェブページのレイアウト .....	2
ワークフロー .....	4
初期展開 .....	7
ステートフルフェイルオーバー環境を設定する .....	7
ライセンスを登録する .....	7
テンプレートプールを追加する .....	7
ポートプロファイルを追加する .....	8
OSイメージをアップロードする .....	10
VMを追加する .....	12
VMにオペレーティングシステムをインストールする .....	25
VMにCAStoolsをインストールする .....	29
制限事項とガイドライン .....	29
Windows または Linux オペレーティング システムに CAStools をインストールします .....	29
FreeBSD オペレーティング システム用の CAStools をインストールする .....	30
インストールを確認する .....	32
VMのIPアドレスを設定する .....	33
VMテンプレートを作成する .....	34
移行環境 .....	36
ソースデバイスを準備する .....	36
異機種間移行コンポーネントをインストールする .....	36
移行クライアントをインストールする .....	36
移行クライアントをダウンロード .....	36
移行クライアントをインストールする .....	37
宛先VMを準備する .....	40
PEイメージを取得する .....	40
宛先VMを作成する .....	40
TargetClient を構成する .....	41
移行を実行する .....	45
制限事項とガイドライン .....	45
移行タスクを作成する .....	45
ドライバーを構成する .....	48
宛先VMにアクセスする .....	50
VM IPv6アドレス管理を有効にする .....	53
VMのIPv6アドレスを指定する .....	53
DRX .....	55
DRXサービスを追加する .....	56
DRXサービス監視ポリシーを構成する .....	60
スケジュールされた拡張ポリシーを追加する .....	62
垂直拡張ポリシーを構成する .....	62
LB リソースコラボレーションを構成する .....	63
クラウドレインボー .....	65

ローカルおよびリモートのデータセンターを構成する .....	65
オンラインVM移行を実行する .....	67
<b>GPUリソースプールを構成する .....</b>	<b>68</b>
ホストのIOMMUを有効にする .....	68
GPUパススルーを構成する .....	69
VMIにGPUドライバーをインストールする .....	72
<b>vGPUリソースプールを構成する .....</b>	<b>73</b>
vGPUを追加する .....	74
vGPUリソースプールを構成する .....	75
Windows VMIにNVIDIAグラフィックドライバーをインストールする .....	79
Linux VMIにNVIDIAグラフィックドライバーをインストールする .....	80
サイトの災害復旧 .....	82
<b>ストレージの災害復旧を構成する .....</b>	<b>83</b>
設定手順 .....	83
サイトを構成する .....	83
ストレージの災害復旧を構成する .....	83
サイトの災害復旧を構成する .....	84
災害復旧シナリオ .....	84
復旧計画テスト .....	84
スケジュールされた回復 .....	85
障害回復 .....	86
リバースリカバリー .....	86
制限事項とガイドライン .....	87
<b>ネットワーク計画 .....</b>	<b>87</b>
サイトを追加 .....	88
ローカルサイトを追加する .....	88
リモートサイトを追加する .....	88
リモートサイトを追加する .....	89
ストレージの災害復旧を構成する .....	90
アドレスプールを追加する .....	90
ローカルアドレスプールの追加 .....	91
リモートアドレスプールを追加する .....	92
リモートデバイスを追加する .....	94
非同期レプリケーションペアを作成する .....	96
制限事項とガイドライン .....	96
手順 .....	96
ローカルサイトとリモートサイトにSRAを追加する .....	99
ローカルサイトのSRAを追加する .....	99
リモートサイトのSRAを追加する .....	100
ストレージレプリケーションペアを同期する .....	101
保護グループを構成する .....	102
回復計画を作成する .....	104
回復計画を実行する .....	105
復旧計画をテストする .....	105
復旧計画のテストを開始する .....	105
復旧計画のテストを完了する .....	106
スケジュールされたリカバリを実行する .....	108
リバースリカバリを実行する .....	110
障害回復を実行する .....	111
<b>ディスクバックアップベースの災害復旧を構成する .....</b>	<b>113</b>
アプリケーションシナリオ .....	113
構成環境 .....	113
メカニズム .....	113
設定手順 .....	114

災害復旧の準備 .....	114
DRMタスク.....	114
サイトを構成する.....	114
保護グループを構成する.....	114
復旧計画を構成する .....	115
災害復旧シナリオ.....	115
復旧計画テスト .....	115
スケジュールされた回復.....	116
障害回復.....	116
リバースリカバリ .....	117
バックアップデータの消去.....	117
ネットワーク図.....	117
CDPコンポーネントをインストールする.....	118
保護されたサイトを準備する.....	118
VM にディザスタリカバリ クライアントをインストールする(Windows クライアント).....	119
回復サイトを準備する.....	120
ディスクバックアップベースの災害復旧を構成する.....	121
復旧計画のテストを実行する.....	123
スケジュールされたリカバリを実行する.....	123
バックアップデータを消去.....	123
障害回復を実行する.....	124
<b>DPDKを構成する.....</b>	<b>125</b>
<b>ホストのDPDKを有効にする.....</b>	<b>125</b>
ブート設定を構成する.....	125
DPDK設定を構成する.....	126
(オプション) 割り込みアフィニティ設定を構成する.....	127
NICドライバーを編集する.....	128
DPDKを有効にしたvSwitchを追加する.....	128
VMのDPDK設定を構成する.....	129
<b>SR-IOV設定を構成する .....</b>	<b>133</b>
ホストのIOMMUを有効にする.....	134
物理NICのSR-IOVを構成する.....	134
VM の SR-IOV NIC を構成する.....	135
<b>分散仮想ファイアウォールを構成する.....</b>	<b>136</b>
仮想ファイアウォールを作成する.....	136
VMIに仮想ファイアウォールを接続する.....	138
<b>よくある質問.....</b>	<b>140</b>
インストール関連.....	140
UIS サーバーは VM に対してどのようなゲスト OS をサポートしていますか?.....	140
UIS マネージャーをアップグレードするにはどうすればよいですか?.....	140
UIS ライセンスには期限がありますか?.....	140
VM に複数のゲスト OS をインストールするにはどうすればよいですか?.....	140
構成関連.....	140
VM ディスクのフォーマットを raw または qcow2 に設定する必要がありますか?.....	140
VM のディスクを拡張するにはどうすればよいですか?.....	141
VM ディスクにはどのキャッシュ モードを選択すればよいですか?.....	141
最適な読み取りおよび書き込みパフォーマンスを得るには、VM ディスクをどのように構成すればよいですか? ...	142
VMware VM を UIS と互換性のある形式に変換するにはどうすればよいですか?.....	144
vDisk を複数の VM にマウントできますか?.....	146
パフォーマンス監視ページで VM のメモリ使用量が 100% のままになるのはなぜですか?.....	146
VM の MAC アドレスを変更するにはどうすればよいですか?.....	146
実行している UIS マネージャーのバージョンはどれですか?.....	146
実行している CVK カーネルのバージョンはどれですか?.....	147
実行している QEMU のバージョンはどれですか?.....	147

UIS マネージャーの障害は、管理対象の VM の操作に影響しますか? .....	147
UIS Manager のパスワードを回復するにはどうすればよいですか? .....	147
CVK ホストのルート パスワードを変更するにはどうすればよいですか? .....	148
ホストに障害が発生した後、UIS 管理ノードを回復するにはどうすればよいですか? .....	149
CVK サービス ホストのハードウェア障害にはどのように対処すればよいですか? .....	150
クラスターをスケーリングするにはどうすればよいですか? .....	151
UIS スーパーユーザー アカウント (管理者アカウント) のパスワードを変更するにはどうすればよいですか? .....	152
サービス計画関連 .....	152
アプリケーションを仮想化環境に移行するかどうかを決定する際に考慮すべき要素は何ですか? .....	152
物理サーバーに仮想デスクトップをいくつ展開できますか? .....	152
共有ストレージ デバイスにデプロイできる VM の数はいくつですか? .....	153
例外関連 .....	153
相互に ping できる 2 つの Linux VM 間でパケットを送信すると、ホストへのルートが存在しないというメッセージが表示されるのはなぜですか? .....	153
Windows Server 2008 R2 Datacenter x64 Edition のインストール時に受信した 0xc000035a エラーをどのように処理すればよいですか? .....	153
バックアップ ディスクに十分な容量があるにもかかわらず、CB バックアップを実行するときにディスク不足エラーが発生した場合、どうすれば対処できますか? .....	154
UIS クラスター内のノードへの管理 IP アドレスの割り当てには制限がありますか? .....	154
VM が暗号化ドングルを認識できない場合はどうすればよいですか? .....	155
ウイルス対策が有効になっている VM の移行後に、CAStools コマンドの実行や AISware フロントエンドドライバーのアンインストールが予期せず失敗するのを回避するには、どうすればよいですか? .....	155
ウイルス対策が有効になっている VM の実行中に CPU を追加した後に頻繁に応答しなくなったり、起動時にブルースクリーン (BSOD) が表示される問題が発生する場合、どうすれば対処できますか? .....	155
ウイルス対策が有効になっている VM で深刻な無応答の問題が発生したら、どうすれば解決できますか? .....	155
VM をシャットダウンせずに VM のウイルス対策機能を無効にできますか? .....	155
ウイルス対策が有効な VM OVF テンプレートから作成された VM でウイルス対策機能が無効になっているのはなぜですか? .....	155
VM を復元ポイントまたはバックアップに復元した後、VM のウイルス対策制御設定を再構成する必要がありますか? .....	156
<b>UIS パフォーマンス最適化のベストプラクティス .....</b>	<b>157</b>
ハードウェア .....	157
ストレージコントローラ .....	157
ストレージの展開 .....	157
ノードとディスク .....	158
I/O優先度を設定する .....	158
CPU動作モードを設定する .....	158
HugePagesを有効にする .....	159
VMディスクのプロビジョニングモードを設定する .....	160
ブロックデバイスをVMIにマウントする .....	161
VMディスクをフォーマットする .....	164
Windows を実行している VM でディスクをフォーマットする .....	164
Linux を実行している VM でディスクをフォーマットする .....	164
推奨されるサーバー構成 .....	165
ネットワーク計画 .....	166
ストレージディスクの種類 .....	166
推奨ディスク構成 .....	167
キャッシュ .....	167
メタデータディスク .....	167
ストレージデータディスク .....	168
データベースディスクタイプの計画 .....	168
データベースストレージボリュームの計画 .....	169
SQL Server データベースのストレージ ボリューム計画 .....	169
MySQL データベースのストレージ ボリューム計画 .....	169
Oracle データベースのストレージ ボリューム計画 .....	170
VM計画 .....	171

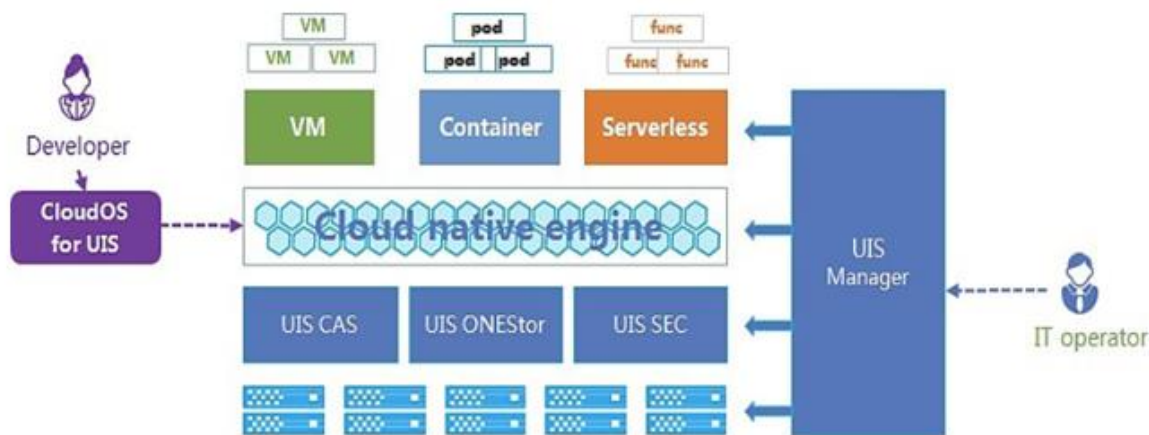
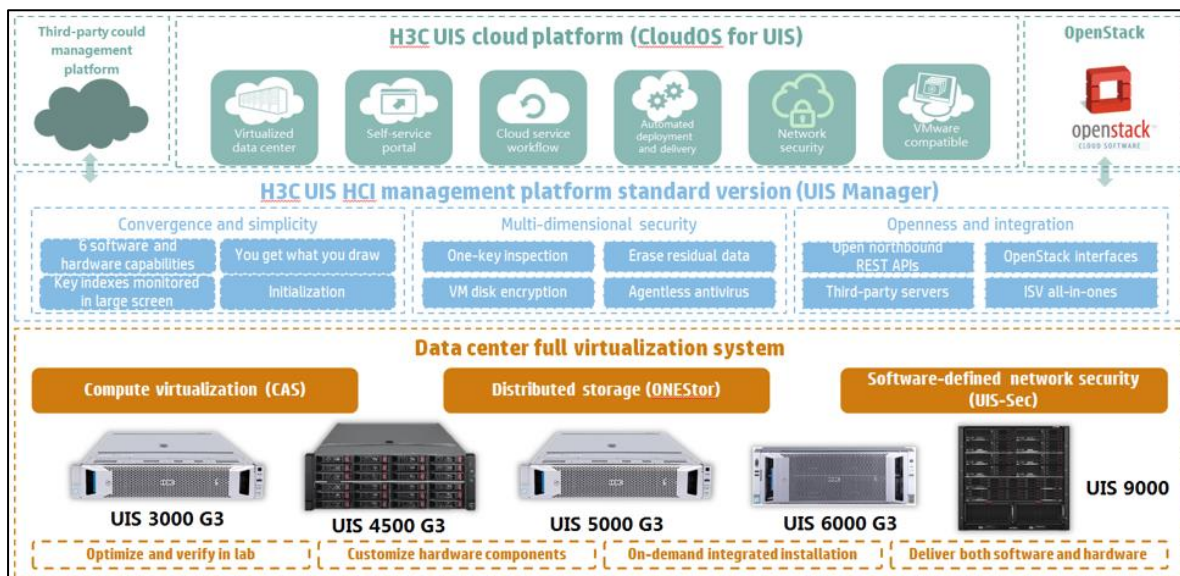
SQL Server VM 構成 .....	171
MySQL VM 構成 .....	172
Oracle VMの構成 .....	172
<b>ドキュメントおよびソフトウェア .....</b>	<b>174</b>
ドキュメント(英語版)はどこにありますか? .....	174
ドキュメント(日本語版)はどこにありますか? .....	176

# UISについて

H3C UIS HCI 製品は、**UIS-CAS** コンピューティング仮想化カーネル システム、**UIS-ONEStor** ストレージ仮想化カーネル システム、**UIS-Sec** ネットワーク セキュリティ仮想化カーネル システム、および UIS ハイパーコンバージド管理ソフトウェア (UIS Manager) を統合します。UIS は、簡素化された配信、セキュリティ コンプライアンス、通信レベルのカーネル、コンバージェンス管理、および使いやすいエクスペリエンスというコンセプトに基づいて設計されています。UIS は、ユーザーがサービスをオンラインに迅速に導入し、より安全なアーキテクチャーでサービスを実行し、より柔軟に操作できるように支援し、合理化された IT インフラストラクチャとクラウドへの容易なアクセスを実現します。

# アーキテクチャー

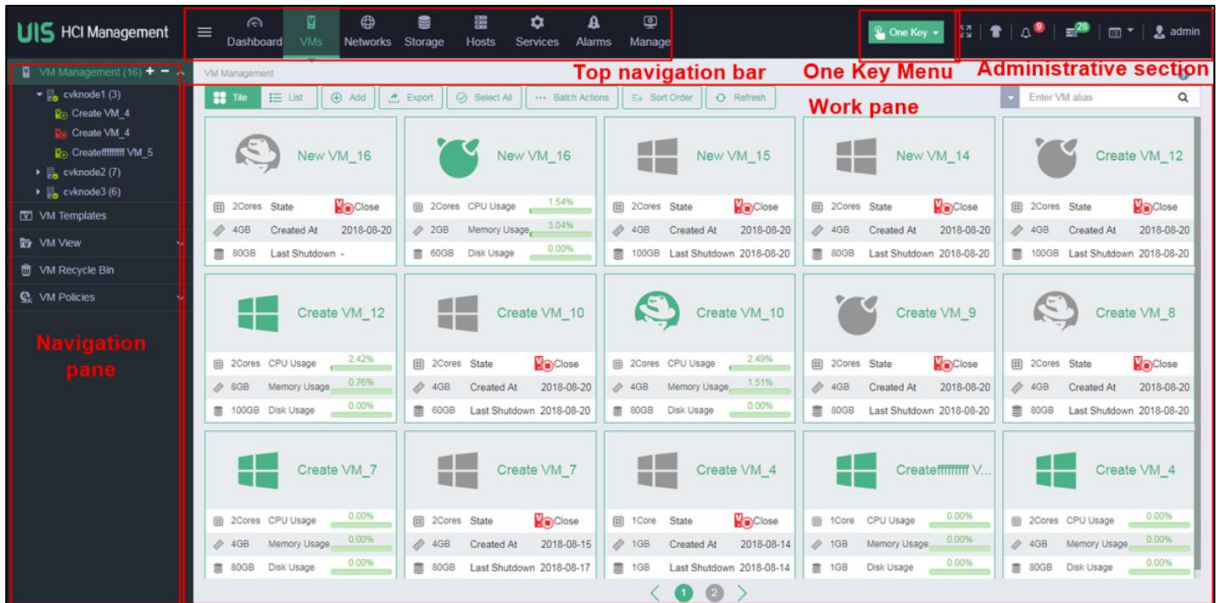
図1 H3C UIS アーキテクチャー



# ウェブページのレイアウト







図1 UIS マネージャーの Web ページ レイアウトを示します。

図 1 UIS マネージャーの Web ページ レイアウト



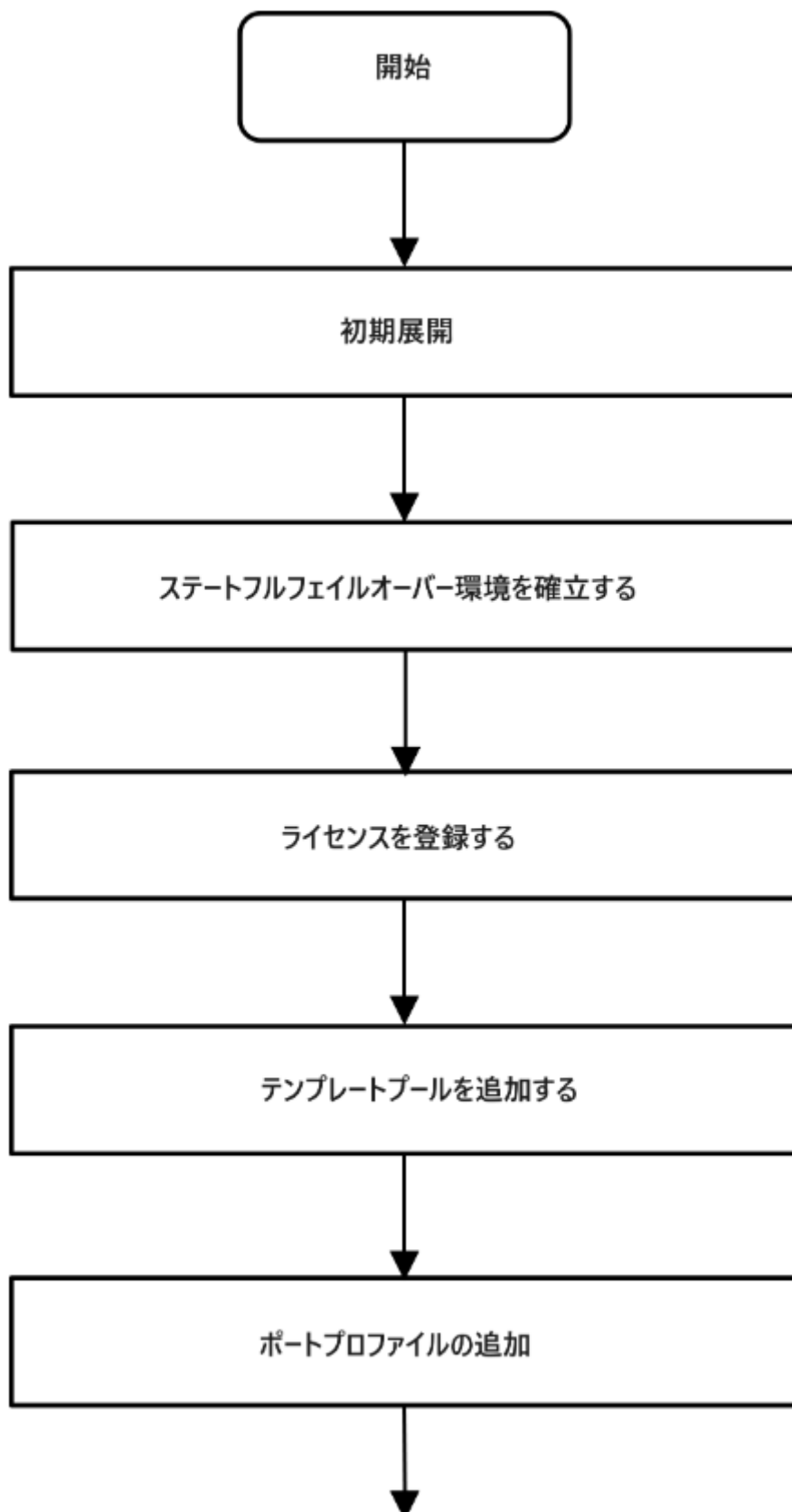
- **ナビゲーション ウィンドウ** - 上部のナビゲーション バーから選択したカテゴリのすべての機能のメニューが含まれています。1つのメニュー項目を選択すると、右側のパネルセクションにその項目の作業ウィンドウが表示されます。統計情報とグラフを表示するときに、ページの左上にあるハンバーガー ボタンをクリックすると、ナビゲーション ウィンドウが狭くなり、作業ウィンドウが拡張されます。
- **上部ナビゲーションバー** - 機能カテゴリが含まれます。カテゴリをクリックすると、ナビゲーション ウィンドウにそのカテゴリのすべての機能が表示されます。
  - **ダッシュボード** - UIS マネージャー、ホスト、VM、ストレージ クラスターのリソース割り当てと正常性状態の概要を取得できます。
  - **VMs** - VM の操作と管理、VM のリカバリのための VM スナップショットの構成、VM の簡単な作成のための VM テンプレートの構成、VM の展開を制御するための VM ポリシーの構成など、VM タスクを実行できます。
  - **ネットワーク** - ネットワークトポロジ、vSwitch、ポート プロファイルを管理できます。
  - **ストレージ** - 分散ストレージと共有ストレージを管理できます。
  - **ホスト** - ホストとホスト クラスターを管理できます。
  - **サービス** - 動的なリソース スケーリング、クラウド レインボー サービス、インテリジェント ソース スケジューリング、サイトの災害復旧を管理できます。
  - **アラーム** - HA センター、アラーム、監視レポート、リソース使用状況統計、および自己定義モニターを管理できます。



- システム - コンポーネント、セキュリティ、オペレーターとグループ、操作ログ、ログ収集、パラメーター、データ バックアップ、NTP サーバー、ステートフル フェイルオーバー、マルチ UIS システム管理、パッチ管理、ライセンスなど、システムを構成および管理できます。
- ワンキーメニュー - リソースの正常性状態のワンクリック検査、リソース使用状況の分析、ストレージのクリーンアップ、リソースのエクスポート、VM の復元、ゾンビ VM の操作、VM のシャットダウン、ハードウェアの交換などのタスクへのクイック アクセスが含まれます。
- 管理セクション:
  - : ページを全画面で表示します。
  - : スキンを変更します。
  - : アラームを確認します。
  - : タスクの軌跡を確認します。
  - : ヘルプ ファイルとバージョン情報を取得します。
  - : ログインアカウント情報を表示します。
- 作業ウィンドウナビゲーション ペインで選択したメニュー項目に応じて、システム、機能、およびサービスを管理、構成、監視するための領域を提供します。

# ワークフロー

このセクションでは、UIS が提供する基本的なサービスの使用方法を紹介します。



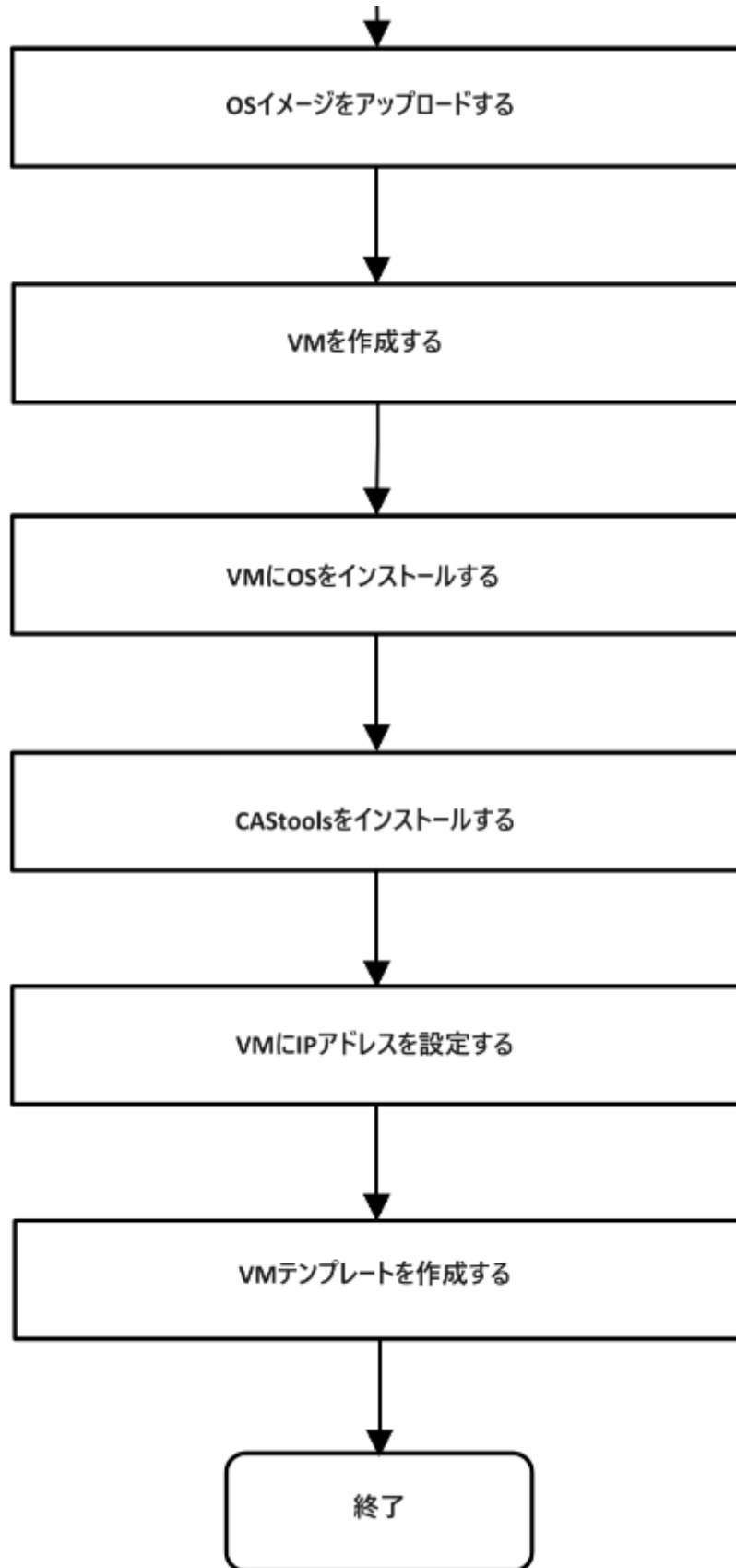


表1ワークフローの説明

操作	説明
初期展開	UIS ハイパーコンバージド クラスタが提供するサービスを使用する前に、初期展開を実行する必要があります。詳細については、 <b>H3C UIS マネージャー インストール ガイド</b> を参照してください。
ステートフルフェイルオーバー環境を確立する	オプション。 プライマリ ノードの障害時にプライマリ/バックアップ ノードの切り替えを実行してサービスの継続性を確保するために、管理ノードのステートフル フェイルオーバーを設定します。詳細については、 <b>H3C UIS マネージャ ステートフル フェイルオーバー設定ガイド</b> を参照してください。
ライセンスを登録する	UIS Manager は 90 日間の無料試用版を提供しています。試用版と正式版は同じ機能を提供します。試用期間終了後も UIS Manager を引き続き使用するには、フランチャイザーからライセンスを取得して、試用版を正式版にアップグレードしてください。詳細については、 <b>H3C UIS Manager 製品登録ガイド</b> を参照してください。
テンプレートプールを追加する	テンプレート プールは、VM テンプレートを保存する専用ディレクトリです。初期展開後、管理者は VM テンプレートを保存するためのテンプレート プールを構成できます。
ポートプロファイルの追加	ポート プロファイルは、VM の VLAN、ネットワーク優先度、およびトラフィック レート制限を設定するために使用されます。 管理者は、ネットワーク計画に基づいてポート プロファイルを作成し、作成時に VM のポート プロファイルを指定できます。
OSイメージをアップロードする	将来 VM にオペレーティング システムをインストールできるように、OS イメージを共有ストレージ プールにアップロードします。
VMを作成する	必要に応じて VM を作成します。
VMにOSをインストールする	サービス計画に従って VM にオペレーティング システムをインストールします。
CAStoolsをインストールする	VM にオペレーティング システムをインストールした後、CAStools をインストールして、VM の CPU、メモリ使用量、プロセス監視情報を取得し、VM の高速ディスクと高速 NIC に必要なドライブを提供します。CAStools を使用して、VM の IP アドレスを設定することもできます。
VMテンプレートを作成する	VM を使用して VM テンプレートを作成します。 VM テンプレートを使用すると、同じソフトウェアおよびハードウェア仕様を持つ複数の VM を一括してすばやく作成できるため、手動での VM 作成の構成の複雑さが軽減されます。

# 初期展開

UIS ハイパーコンバインド クラスターが提供するサービスを使用する前に、初期展開を実行する必要があります。詳細については、*H3C UIS マネージャー インストール ガイド*を参照してください。

## ステートフルフェイルオーバー環境を設定する

プライマリ ノードの障害時にプライマリ/バックアップの切り替えを実行してサービスの継続性を確保するには、管理ノードのステートフル フェイルオーバーを構成します。詳細については、*H3C UIS マネージャー ステートフル フェイルオーバー構成ガイド*を参照してください。

## ライセンスを登録する

UIS Manager は 90 日間の無料トライアルを提供しています。トライアル版と正式版は同じ機能を提供します。トライアル期間終了後も UIS Manager を引き続き使用するには、フランチャイザーからライセンスを取得して、トライアル版を正式版にアップグレードしてください。詳細については、*H3C UIS Manager ローカル ライセンス ガイド*を参照してください。

## テンプレートプールを追加する

1. 上部のナビゲーション バーで **VM** をクリックし、ナビゲーション ペインから **VM Templates** を選択します。
2. **Template Pool** をクリックします。
3. **Add Template Pool** をクリックします。

図 1 テンプレートプールを追加する

The screenshot shows a dialog box titled "Add Template Pool". It contains the following fields and options:

- Shared Storage \***: A dropdown menu with the selected value "defaultPool\_hdd".
- Storage Volume**: An empty text input field with a help icon (?) to its right.
- Name \***: An empty text input field.
- Target Path \***: A text input field containing the path "/vms/defaultPool\_hdd/".
- Type \***: A dropdown menu with the selected value "Shared Directory".

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

4. テンプレートプールのタイプを選択します。
  - **Shared Directory**を選択した場合は、共有ストレージを選択し、ストレージ ボリューム名とターゲットパスを入力します。このタイプは、管理ノードがサービス ノードとしても機能する管理ノード統合デプロイメント シナリオでのみ使用できます。
  - **Local File Directory**を選択した場合は、ターゲットパスを入力します。ターゲットパスは/vms/で始まる必要があります。この文字列で始まることのできるのは、ローカル ファイル ディレクトリのターゲットパスのみです。
  - **iSCSI Shared Directory**を選択した場合は、ターゲットパスと IP アドレスを入力し、LUN を選択します。
  - **FC Shared Directory**を選択した場合は、ターゲットパスを入力し、NAA を選択します。
  - **NFS Network File System**を選択した場合は、ターゲットパス、ソース ホスト IP、およびソースパスを入力します。
5. **Finish**をクリックします。

## ポートプロファイルを追加する

1. 上部のナビゲーション バーで、**Networks** をクリックし、ナビゲーション ペインからポートプロファイルを選択します。
2. **Add** をクリックします。
3. パラメーターを設定します。

図 1 プロファイルの基本設定を構成する

図 2 プロファイルのトラフィック設定を構成する

表 1 パラメーターの説明

パラメーター	説明
ACL	ポートプロファイルで使用される ACL を選択します。ACL 設定の詳細については、ユーザーガイドを参照してください。
VLAN ID	VLAN ID を入力します。VLAN ID は、NIC に接続された vSwitch 上のポート

	に適用されます。
Inbound Limit	<p>VM から vSwitch へのトラフィックを制限します。</p> <ul style="list-style-type: none"> <li>• <b>Avg. Bandwidth</b>—平均受信帯域幅を入力してください in Kbps.</li> <li>• <b>Burst Buffer</b>—受信バースト バッファを KByte 単位で入力します。</li> </ul>
Outbound Limit	<p>vSwitch から VM へのトラフィックを制限します。</p> <ul style="list-style-type: none"> <li>• <b>Avg. Bandwidth</b>—平均送信帯域幅を Kbps 単位で入力します。</li> <li>• <b>Burst Buffer</b>—送信バースト バッファを KByte 単位で入力します。</li> </ul>
Network Priority	ホストのトラフィックが大きい場合に VM 帯域幅の割り当てに使用する優先順位を選択します。

4. Finish をクリックします。

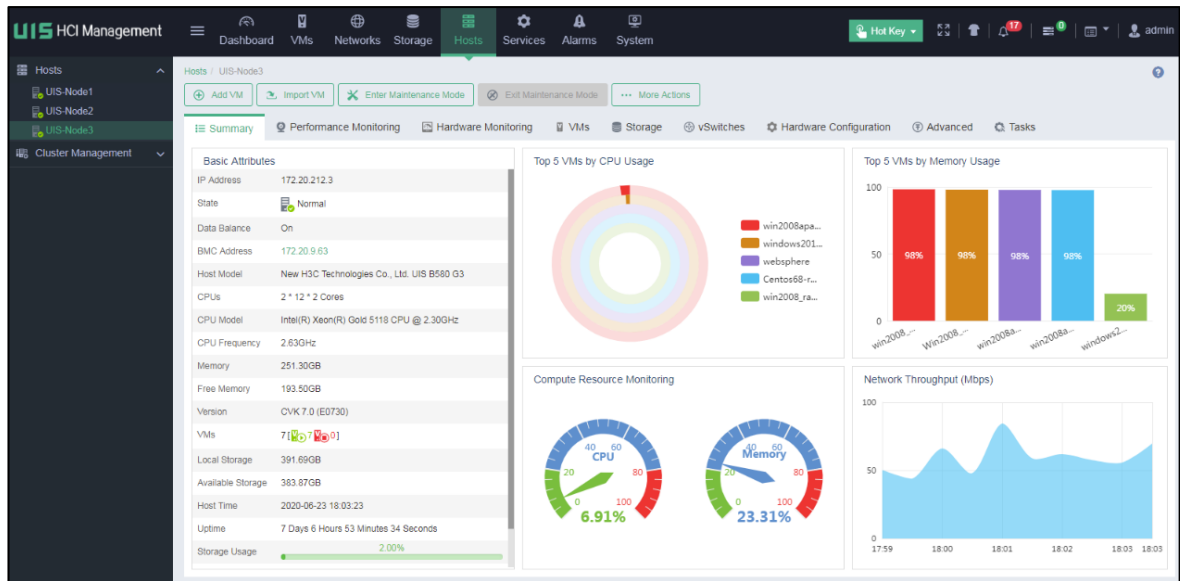
## OSイメージをアップロードする

ベスト プラクティスとして、オペレーティング システムの ISO イメージ ファイルを共有ストレージ プールにアップロードします。共有ストレージ プールをマウントした任意のホストで VM を作成する場合、オペレーターはイメージ ファイルを使用して VM のオペレーティング システムをインストールできます。ISO イメージ ファイルが **Local File Directory** タイプのストレージ プール (**defaultpool** や **isopool** など) にアップロードされている場合、このホスト上の VM のみが ISO イメージ ファイルを使用してオペレーティング システムをインストールできます。

1. 上部のナビゲーション バーで、**Hosts** をクリックします。
2. ターゲットホストを選択します。



図 1 ホスト概要ページ



3. Storage タブをクリックします。
4. ターゲット ストレージ プールを選択し、Upload File をクリックします。

図 2 ストレージプールの選択

The screenshot shows the 'Storage' section of the 'Hosts' overview page for 'UIS-Node3'. It contains two main tables:

**Storage Pools**

Alias	Type	Path	Total	Assigned	Available	State	Actions
muban	Shared File System	/vms/muban	200.00GB	0.00MB	63.98GB	Active	[Icons]
isopool	Local File Directory	/vms/isos	391.69GB	4.26GB	366.92GB	Active	[Icons]
data	Shared File System	/vms/data	1000.00GB	1000.06GB	752.28GB	Active	[Icons]
defaultPool_hdd	Shared File System	/vms/defaultPool_hdd	569.16GB	80.00GB	540.84GB	Active	[Icons]
ALL_HDD	Shared File System	/vms/ALL_HDD	1000.00GB	150.00GB	916.94GB	Active	[Icons]
defaultpool	Local File Directory	/vms/images	391.69GB	0.00MB	366.92GB	Active	[Icons]
ALL_SSD	Shared File System	/vms/ALL_SSD	750.00GB	920.00GB	177.68GB	Active	[Icons]

**Storage Volumes**

File Name	Size	Used	Type	Base Image File	User	Actions
<input type="checkbox"/> Auto_Dameng	40.00GB	70.51GB	qcow2		Auto_Dameng	[Icons]
<input type="checkbox"/> Auto_Dameng_2	100.00GB	2.57GB	qcow2		Auto_Dameng	[Icons]
<input type="checkbox"/> Auto_Dameng_3	64.00MB	3.00MB	qcow2		Auto_Dameng	[Icons]
<input type="checkbox"/> Centos68-rabbitmq	10.00GB	4.36GB	qcow2		Centos68-rabbitmq_7	[Icons]
<input type="checkbox"/> Centos68-rabbitmq-2	20.00GB	9.34GB	qcow2		Centos68-rabbitmq_7	[Icons]
<input type="checkbox"/> Centos68-rabbitmq-7	10.00GB	1.00MB	qcow2	/vms/data/Centos68-rabbitmq_7_image_1	Centos68-rabbitmq_7	[Icons]

Total 36 Items, Page 1/2

5. 破線のボックスをクリックしてファイルを選択し、Start をクリックします。

# VMを追加する

1. 上部のナビゲーションバーで、**VM** をクリックします。
2. 開いたページで、**Add** をクリックします。基本設定を構成した後、**Hardware** をクリックして詳細設定を構成するか、**Finish** をクリックして VM の作成を完了します。

図 1 VM の基本設定を構成する

The screenshot shows the 'Add VM' dialog box with two tabs: '1 Basic Info' (active) and '2 Hardware'. The 'Basic Info' tab contains the following fields and options:

- Alias\***: Text input field containing 'New VM\_30'.
- Description**: Text input field.
- Select Host**: Text input field with search, clear, and help icons.
- OS**: Radio buttons for 'Windows' (selected), 'Linux', and 'BSD'.
- Version**: Dropdown menu showing 'Microsoft Windows Server 2019 (64-bit)'.
- CPUs**: Spin box set to '2'.
- Memory**: Spin box set to '4' GB.
- Disk**: Spin box set to '80' GB.

At the bottom of the dialog are 'Hardware' and 'Finish' buttons. On the right side, a 'Details' panel shows a summary of the configuration:

- Alias: New VM\_30
- Description: (empty)
- Select Host: (empty)
- OS: Windows
- Version: Microsoft Windows Ser...
- CPUs: 2
- Memory: 4GB
- Disk: 80GB

表 1 基本設定

パラメーター	説明
Alias	VM のエイリアスを入力します。 VM を作成した後、エイリアスを編集できます。
Description	VM の説明を入力します。 同じ名前の VM を区別するために、異なる説明を指定できます。
Select Host	VM 展開用のホストを選択します。 ホストを選択しない場合、システムは、VM が最も少ない、メモリ使用量が最も少ない、CPU 使用量が最も少ないという基準に基づいて選択されたホストに VM を自動的に配置します。

OS and Version	SVM にインストールするゲスト OS を指定します。 実際にインストールする OS は、選択した OS とタイプおよびバージョンが同じである必要があります。
CPUs	vCPU の数を指定します。 VM の vCPU の数は、ホスト上の CPU の数を超えることはできません。
Memory	VM のメモリ容量を指定します。この設定はゲスト OS のメモリ サイズです。 VM で使用可能な最大メモリ サイズは、物理メモリ サイズによって異なります。
Disk	ディスクサイズを指定します。

3. 詳細設定で、**CPU** オプションを展開して CPU パラメーターを構成します。

図 2 VM の CPU パラメーターの設定

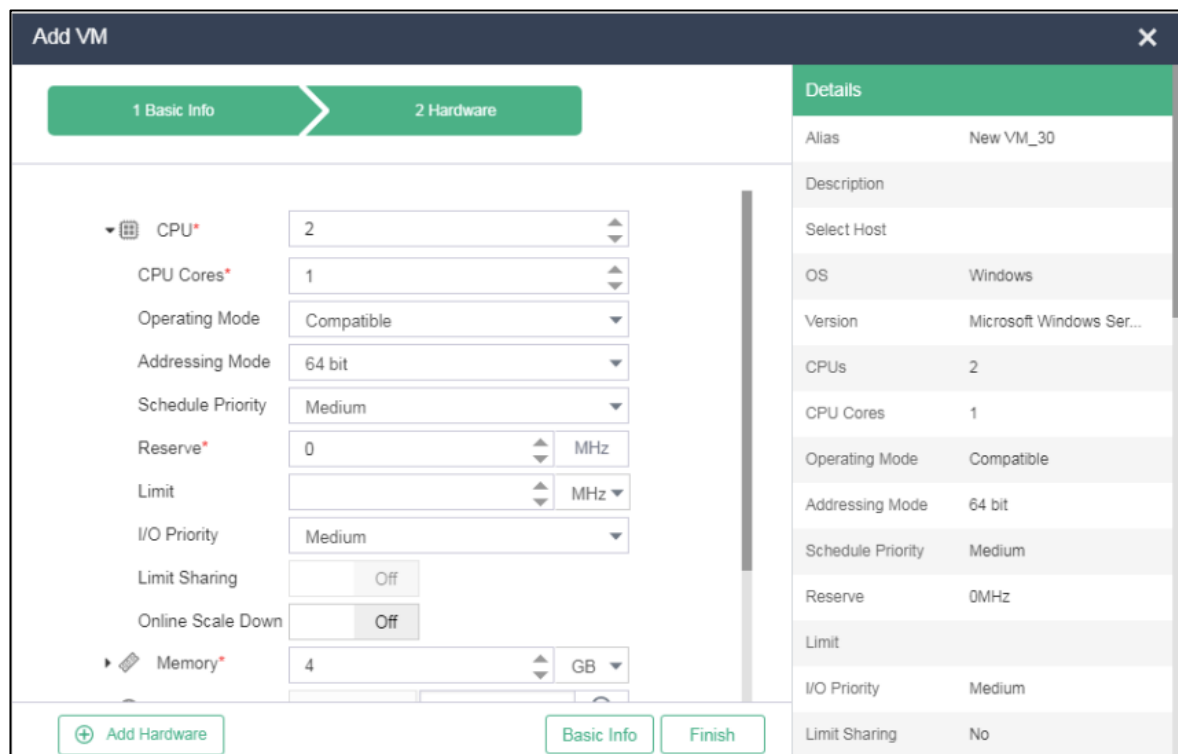


表 2 CPU パラメーター

パラメーター	説明
CPU	<p>vCPU の数を指定します。VM の vCPU の数はホスト上の CPU の数を超えることはできませんが、複数の VM の vCPU の合計数はホスト上の CPU の数を超えることができます。</p> <p>システムでは、VM はカーネル オペレーティング システム内のプロセスです。カーネルは、タイム スライスに基づいてプロセスをスケジュールします。プロセスのタイム スライスが CPU で使い果たされると、プロセスは一時停止され、CPU は次のプロセスに渡されます。したがって、VM に割り当てられる CPU の数が増えると、VM プロセスで使用できる CPU タイム スライスが増え、VM のパフォーマンスが向上します。</p>
CPU Cores	<p>CPU コア の数を指定します。デフォルト値は 1 です。</p> <p>VM の CPU コア の数はホストの CPU コア の数を超えることはできません。</p>
Bind Physical CPU	<p>VM の vCPU をホストの物理 CPU にバインドします。その後、VM はバインドされた物理 CPU のみを使用できます。このパラメーターは、複数の CPU 間でのプロセス切り替え時のキャッシュ ミスを減らすのに役立ちます。バインドにより VM の動作効率が向上しますが、システム全体のプロセス スケジューリングの観点からは、対称型マルチプロセッシング (SMP) の CPU 負荷分散に影響します。</p> <p>vCPU は、NUMA ノード間の物理 CPU にバインドできません。2 つのホスト間で VM 操作 (移行、クローン作成、復元、エクスポート操作など) を正常に実行するには、ソース ホストと宛先ホストが同じ NUMA アーキテクチャーを使用していることを確認する必要があります。このオプションは、ホストを選択した後にのみ使用できます。</p>
Operating Mode	<p>CPU の動作モードを選択します。オプションには、<b>Compatible</b> (デフォルト モード) と <b>Straight-Through</b> があります。</p> <ul style="list-style-type: none"> <li>• <b>Compatible</b>—異なるモデルの物理 CPU を同じモデルの vCPU に仮想化します。このモードでは、物理 CPU の違いがゲスト OS から保護されます。異なる CPU モデルを使用するホスト間で VM を移動するには、このモードを選択します。</li> <li>• <b>Straight-Through</b>—ゲスト OS が物理 CPU に直接アクセスできるようにします。このモードでは、互換モードよりも高いパフォーマンスが得られます。ただし、ソース ホストと宛先ホストが同じ CPU モデルを使用していることを確認する必要があります。</li> </ul>
Addressing Mode	<p>ゲスト OS に一致するアドレス指定モードを選択します。オプションには、64 bit (デフォルト) と 32 bit があります。64 ビット OS をインストー</p>

	<p>ルする場合は、<b>64 ビット モード</b>を選択する必要があります。64 ビット OS を使用する VM に <b>32 ビット モード</b>を選択すると、VM はシャットダウン後に起動できなくなります。</p>
Schedule Priority	<p>競合中に物理 CPU リソースを取得するために、VM 上のプロセスの優先順位を選択します。オプションには、<b>High</b>、<b>Medium</b>、<b>Low</b> があります。</p> <p>W 物理 CPU リソースが不十分な場合、High、Medium、Low の優先度を持つ VM は、CPU タイム スライスを 4:2:1 の割合で使用します。VM に割り当てられる優先度が高いほど、VM プロセスで使用できる物理 CPU タイム スライスが多くなり、VM のパフォーマンスが向上します。</p>
Reserve	<p>VM に保証される最小 CPU 周波数を入力します。</p>
Limit	<p>VM の最大クロック周波数を MHz または GHz で指定します。このパラメーターを空のままにすると、vCPU クロック周波数は制限されません。このパラメーターの値の範囲は 10 MHz から物理ホストの CPU 周波数までです。</p>
I/O Priority	<p>VM 上のプロセスがディスクの読み取り/書き込みを行うための I/O 優先度を選択します。オプションには、<b>Low</b>、<b>Medium</b>、<b>High</b> があります。</p> <p>ホスト上の複数の VM が同時にディスクの読み取りと書き込みを実行する場合、I/O 優先度の高い VM の方がパフォーマンスが向上します。</p>
Limit Sharing	<p>制限の共有をオンまたはオフにします。たとえば、4 つの CPU コアを持つ VM の制限の共有を有効にし、VM の 1 つの CPU コアが使用できる最大ホスト CPU 周波数を 2 GHz に設定した場合、VM と VM の 1 つの CPU コアの両方の最大ホスト CPU 周波数は 8 GHz になります。</p>
Online Scale Down	<p>CPU をオンラインで削減できるオンライン CPU スケールダウンをオンまたはオフにします。</p>

4. 詳細設定で、**Memory** オプションを展開して、メモリ パラメーターを構成します。

図 3 VM のメモリーパラメータの設定

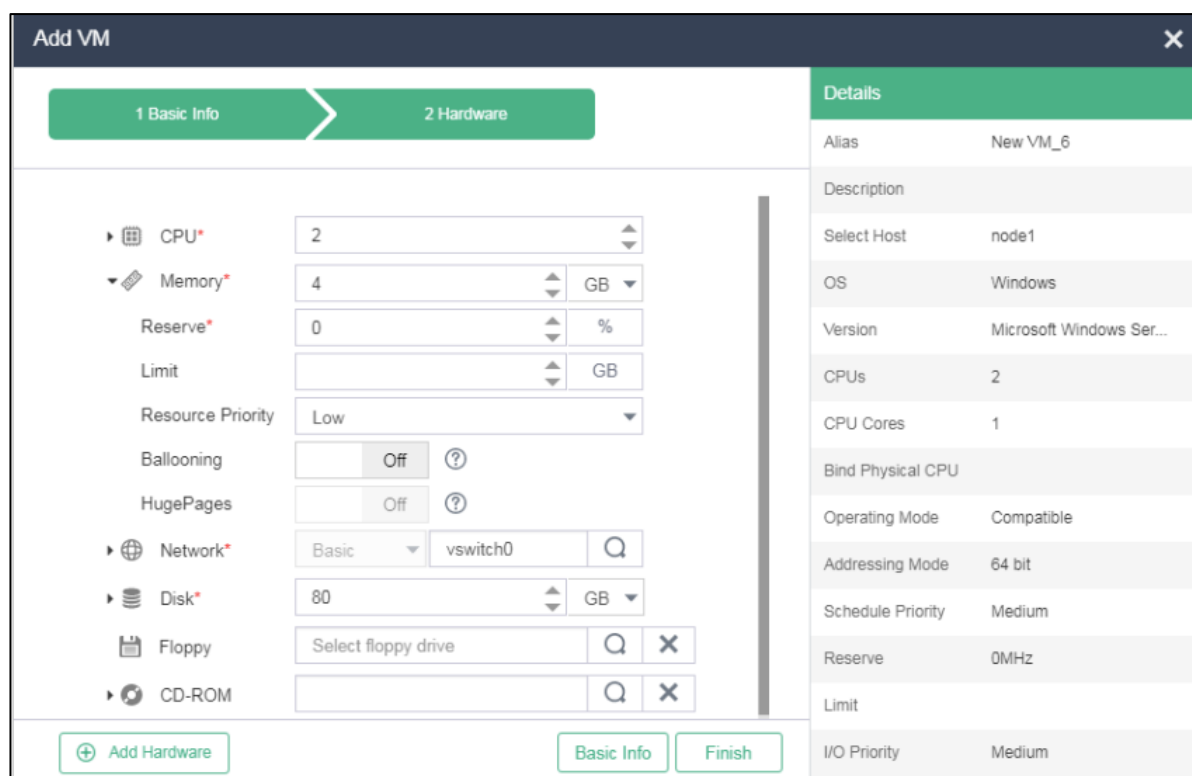


表 3 メモリーパラメータ

パラメーター	説明
Memory Size	<p>VM のオペレーティング システムの最大メモリ サイズを MB または GB 単位で指定します。このパラメーターの値の範囲は 512 MB からホストの最大メモリ サイズまでです。</p> <p>システムでは、メモリ リソースはオンデマンド ベースで VM に割り当てられません。そのため、ホスト上のすべての VM に指定するメモリの合計サイズは、ホストの物理メモリ サイズを超える可能性があります。ただし、DRS、HA、DPM、アフィニティ、またはアンチアフィニティ サービスが構成されている場合は冗長メモリ リソースが必要になるため、実際の運用環境ではメモリのオーバーコミットは推奨されません。</p> <p>VM のメモリ容量を指定します。この設定はゲスト OS のメモリ サイズです。VM で使用可能な最大メモリ サイズは物理メモリ サイズによって異なります。</p>
Reserve	<p>VM に予約するメモリを VM の最大メモリのパーセンテージで指定します。0 はメモリが予約されていないことを示します。VM の負荷が増加し、予約メモリがすべて使用されると、VM はアイドル状態であっても予約メモリを保持できます。</p> <p>ホストは、VM の実際のメモリ使用量に基づいて VM にメモリを割り当てます。</p>

	ホストのメモリが使い果たされた後に VM がさらにメモリを必要とする場合に備えて、VM 用にメモリを予約できます。
Limit	VM が使用できる最大ホスト メモリ容量を入力します。
Resource Priority	VM がメモリを要求するときの優先度を指定します。オプションには、 <b>Low</b> (デフォルト)、 <b>Medium</b> 、および <b>High</b> があります。VM が予約メモリよりも多くのメモリを要求すると、メモリ競合が発生した場合、ホストはリソースの優先度に基づいてメモリ割り当てを決定します。
Ballooning	メモリ競合が発生したときに VM をシャットダウンせずに VM 間でメモリを動的に分配するには、このオプションをオンにします。
HugePages	VM がホストの HugePages メモリを使用するように有効または無効にします。このオプションをオンにできるのは、ホストで HugePages 機能が有効になっていて、VM がシャットダウンされている場合のみです。また、この機能は、メモリ予約、メモリ制限、リソース優先度、バルーニングと相互に排他的です。

5. 詳細設定で、**network** オプションを展開して、ネットワーク パラメーターを構成します。

図 4 VM のネットワークパラメータの設定

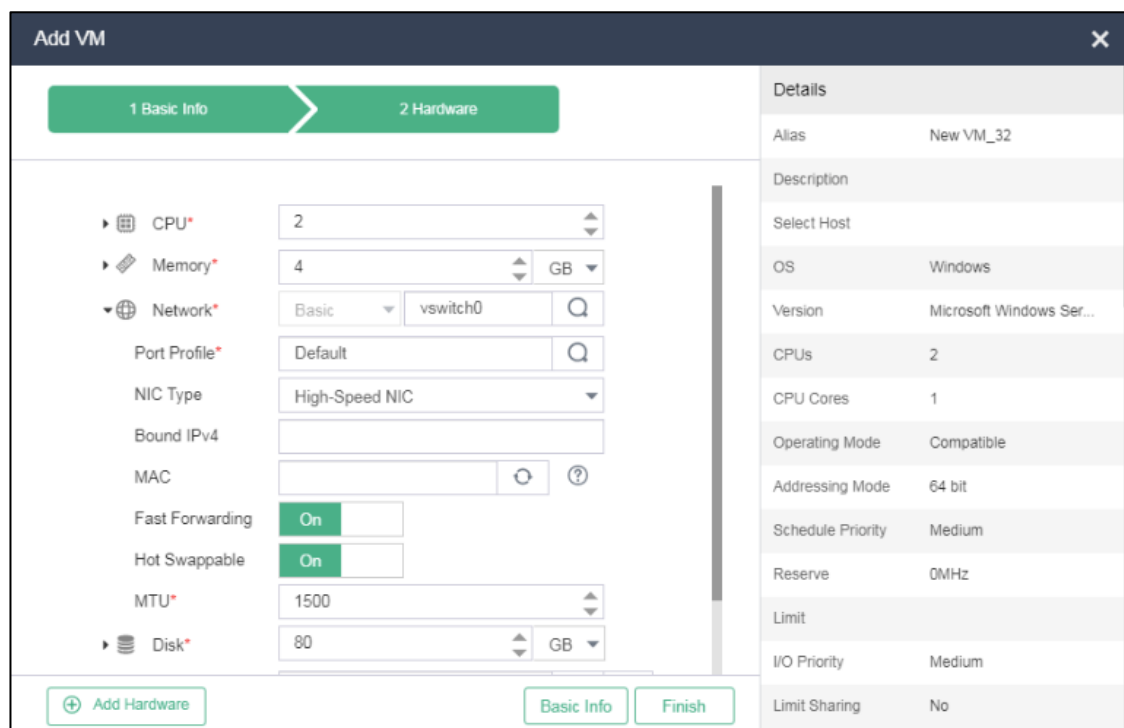


表 4 ネットワークパラメータ

パラメーター	説明
Network	VM の vSwitch を選択します。vSwitch は、ソフトウェア ベースの IP 転送および制御モジュールです。VM と外部ネットワーク間のすべてのトラフィックは、vSwitch を介して転送されます。
Port Profile	VM のネットワーク パラメーター (VLAN、ACL、ネットワーク帯域幅など) を指定します。
Virtual Firewall	VM の仮想ファイアウォールを選択します。VM の受信および送信データ パケットは、ファイアウォール ルールに基づいてフィルタリングされます。
NIC Type	<p>VM の NIC タイプを選択します。オプションには、<b>Common NIC</b>、<b>High-Speed NIC</b>、<b>Intel e1000 NIC</b>、および <b>SR-IOV Straight-Through NIC</b> があります。デフォルトの NIC タイプは高速 NIC です。</p> <ul style="list-style-type: none"> <li>• <b>Common NIC</b>—100 Mbps の伝送速度を提供します。</li> <li>• <b>Intel e1000 NIC</b>—1000 Mbps の伝送速度を提供します。</li> <li>• <b>High-Speed NIC</b>—P10000 Mbps の伝送速度を提供します。高速 NIC は CVK によって駆動されます。</li> <li>• <b>SR-IOV Straight-Through NIC</b>—VM は物理 NIC から仮想化された vNIC を使用します。SR-IOV ストレートスルー NIC は最高のパフォーマンスを提供しますが、物理 NIC と VM のサポートが必要です。このオプションは、VM のホストを選択した後にのみ使用できます。</li> </ul>
Driver Type	SR-IOV ストレートスルー NIC のドライバー タイプを選択します。選択できるのは <b>VFIO</b> のみです。このオプションは、NIC タイプが SR-IOV ストレートスルーの場合にのみ使用できます。
VLAN ID	VM の VLAN ID を設定します。このオプションは、NIC タイプが SR-IOV ストレートスルーの場合にのみ使用できます。
Bound IPv4/IPv6 Address	<p>VM の MAC アドレスにバインドされた IP アドレスを指定します。</p> <p>NIC が正しく通信するには、NIC に割り当てられた IP アドレスがバインドされた IP アドレスと同じであることを確認する必要があります。</p>
MAC	MAC アドレスを手動で指定します。フィールドを空のままにすると、システムによって VM に MAC アドレスが自動的に割り当てられます。



Fast Forwarding	高速転送を有効にすると、VM のネットワーク パフォーマンスが向上します。この機能は、高速 NIC でのみ使用できます。
Queue Number	VM NIC でデータ パケットを送受信するためのキューの数を設定します。デフォルト値は 1 です。キューの数を増やすと VM のネットワーク処理能力が向上しますが、CPU やメモリの消費など、パフォーマンスのオーバーヘッドも増加します。実際の状況に応じてこの設定を調整してください。キューの数を設定できるのは、高速転送が有効になっている場合のみです。
Hot Swappable	ENIC ホットスワップを有効または無効にします。このオプションは高速 NIC でのみ使用できます。
MTU	NIC の最大転送単位をバイト単位で指定します。デフォルトは 1500 です。このオプションは、共通、高速、および Intel e1000 NIC でのみ使用できます。

6. 詳細設定で、Disk オプションを展開して、ディスク パラメーターを構成します。

図 5 VM のディスクパラメータの設定

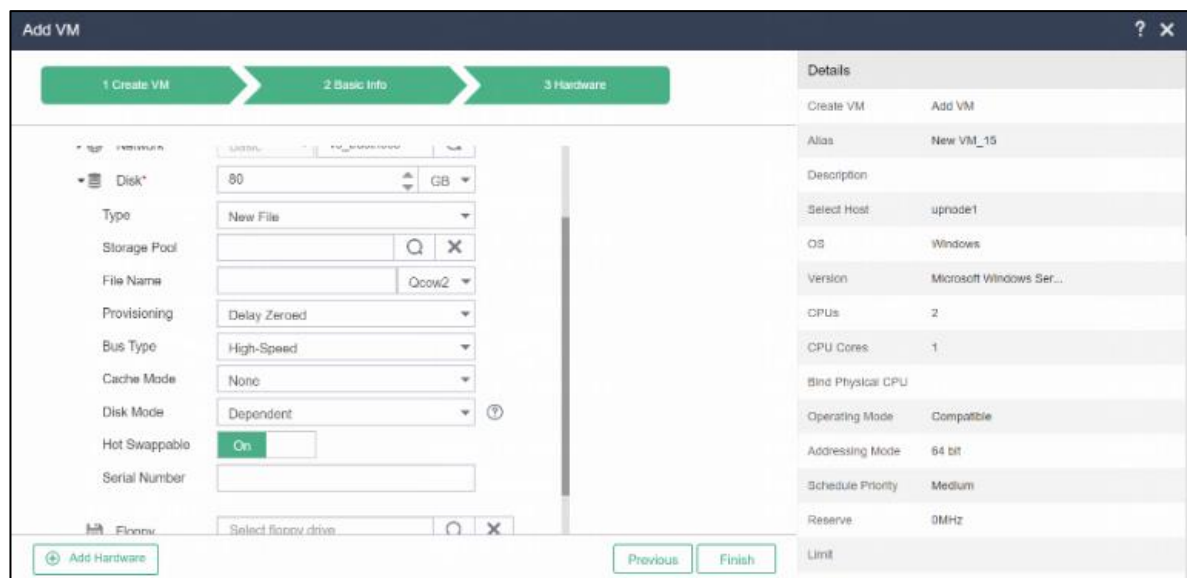


表 5 ディスクパラメータ

パラメーター	説明
Disk	ディスクサイズを指定します。
Type	<p>ディスクのストレージ サービス タイプを指定します。ファイル ストレージまたはブロック ストレージを指定できます。ファイル 保存のオプションには、New File または Existing File があります。ファイル ストレージのオプションには、新しいファイル または 既存のファイルがあります。デフォルトでは、VM のディスクとして新しいファイルが作成されます。ディスク タイプのオプションは、VM の作成時にホストが選択されている場合にのみ使用できます。ホストが選択されていない場合、このオプションの値は New File のみになります。</p> <ul style="list-style-type: none"> <li>• <b>New Block Device</b>—このオプションを選択した場合は、RBD ストレージ プールに VM のディスクとして RBD を作成します。</li> <li>• <b>Existing Block Device</b>—ブロック デバイスは、IP SAN または FC SAN 上のストレージ LUN など、ファイル システムを持たないデバイスであり、raw デバイスとも呼ばれます。ブロック デバイスは通常、高性能、データベース、および高性能 I/O コンピューティングを必要とする仮想化環境で使用されます。</li> <li>• <b>New File</b>—ファイルは VM にディスクとして提示され、ブロック デバイスよりも管理が容易になります。このオプションを選択すると、VM のディスクとして空のファイルが作成されます。</li> <li>• <b>Existing File</b>—このオプションを選択した場合は、他の VM で使用されていない既存のストレージ ファイルを VM のディスクとして指定します。</li> </ul>
Storage Pool	新しいディスクを作成するストレージ プールを選択します。
File Name	<p>新しいファイルをディスクとして使用する場合は、ディスクのファイル名を入力します。 ディスクのフォーマット モードを選択します。 <b>High Speed</b> と <b>Intelligent</b> (デフォルト) を選択できます。</p> <ul style="list-style-type: none"> <li>• <b>High Speed</b>—ディスクは RAW 形式です。RAW 形式では I/O 効率が高くなりますが、内部スナップショットはサポートされません。</li> <li>• <b>Intelligent</b>—ディスクは qcow2 形式です。</li> </ul>
Provisioning	<p>ボリュームプロビジョニングモードを選択します。 オプションには、<b>Thin</b> (デフォルト)、<b>Delay Zeroed</b>、および <b>Zeroed</b> があります。</p> <ul style="list-style-type: none"> <li>• <b>Thin</b>—ボリュームの作成時に、ボリュームの初期操作に必要なストレージ スペースのみを割り当てます。後でボリュームにさらにストレージ スペースが必要になった場合は、最大ストレ</li> </ul>

	<p>ージ サイズを超えない限り、ボリュームに必要なだけのストレージ スペースを割り当てることができます。このモードでは、メタデータ I/O コストが高いため、パフォーマンスは最も低くなります。</p> <ul style="list-style-type: none"> <li>• <b>Delay Zeroed</b>—ボリュームの作成時に、指定された最大ストレージ サイズをボリュームに割り当てます。物理デバイスに残っているデータは作成中に消去されませんが、VM からの最初の書き込み時にゼロで消去されます。このモードではパフォーマンスが低下し、書き込み増幅の問題が発生します。ファイルシステムの最小データ管理単位は 1 MB です。4 KB のデータのみが書き込まれると、残りの 1020 KB のデータがクリアされ、コストが高くなります。</li> <li>• <b>Zeroed</b>—ボリュームの作成時に、指定された最大ストレージ サイズをボリュームに割り当てます。物理デバイスに残っているデータは、作成中にゼロに設定されます。このモードでボリュームを作成すると、他のモードでボリュームを作成する場合よりも時間がかかる場合があります。このモードでは最高のパフォーマンスが得られますが、オンデマンドでリソースが割り当てられないため、仮想化シナリオでリソースが無駄になります。</li> </ul>
Bus Type	<p>バス タイプを選択します。オプションには、IDE、USB、High-Speed (デフォルト)、High-Speed SCSI があります。</p> <ul style="list-style-type: none"> <li>• <b>IDE</b>—CD-ROM ドライブなどの IDE デバイスに適用されます。このバス タイプはパフォーマンスが低くなります。</li> <li>• <b>USB</b>—USB 周辺機器に適用可能です。</li> <li>• <b>High-Speed</b>—最高のパフォーマンスを提供し、最も一般的に使用されます。</li> <li>• <b>High-Speed SCSI</b>—システム占有率が低く、転送速度が速くなります。特殊な SCSI 命令や頻繁な SCSI 命令を処理する場合は、このタイプを選択します。</li> </ul>
Cache Mode	<p>VM のデータ キャッシュ モードを選択します。オプションには、Directsync (デフォルト)、Writethrough、Writeback、None があります。キャッシュ モードが異なると、読み取り/書き込みのパフォーマンスも異なります。</p> <ul style="list-style-type: none"> <li>• <b>Directsync</b>—データは物理ディスクに書き込まれ、その後 VM のディスク ファイルに同期されます。これにより、データのセキュリティは向上しますが、効率は低下します。VM がローカルディスクを使用する場合は、このモードを選択してデータのセキュリティを確保します。</li> <li>• <b>Writethrough</b>—データはホスト キャッシュから読み取られ、ホスト キャッシュに書き込まれ、その後物理ディスクに書き込まれます。このモードでは、書き込みパフォーマンスは最も低くなりますが、データのセキュリティは最も高くなります。</li> <li>• <b>Writeback</b>—データは VM キャッシュに書き込まれ、次</li> </ul>

	<p>にホスト キャッシュに書き込まれ、最後に物理ディスクに書き込まれます。データがホスト キャッシュに書き込まれるとすぐに書き込み操作が完了します。このモードでは、効率是最も高くなりますが、データのセキュリティは最も低くなります。</p> <ul style="list-style-type: none"> <li>• <b>None</b>—データは VM キャッシュに書き込まれ、その後物理ディスクに書き込まれます。このモードでは、セキュリティとパフォーマンスの面で全体的に最高のパフォーマンスが実現されません。</li> </ul>
Disk Mode	<p>VM のディスクを外部スナップショットに含めるかどうかを選択します。このパラメーターは、VM がファイル タイプ ディスクを使用している場合にのみ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>Dependent</b>—外部スナップショットにディスクを含めません。外部スナップショットを使用して VM を復元すると、ディスクも復元されます。</li> <li>• <b>Independent-Persistent</b>—外部スナップショットにディスクは含まれません。外部スナップショットを使用して VM を復元する場合、ディスクは復元されません。</li> </ul>
Hot Swappable	<p>ディスクのホットスワップを有効または無効にします。このオプションは高速バスタイプでのみ使用できます。</p>
Serial Number	<p>ゲスト OS 内のディスクのシリアル番号。シリアル番号は仮想ディスクを一意に識別します。ディスクのシリアル番号はカスタマイズできます。不明なエラーを回避するには、VM 上の複数の仮想ディスクに同じシリアル番号を割り当てないでください。また、クラスター内またはホスト上の複数の VM 仮想ディスクに同じシリアル番号を割り当てないでください。</p>

7. 詳細設定でフロッピードライブを選択し、CD-ROM オプションを展開して CD-ROM ドライブのパラメーターを構成します。

図 6 VM のフロッピーおよび CD-ROM ドライブのパラメーターを構成する

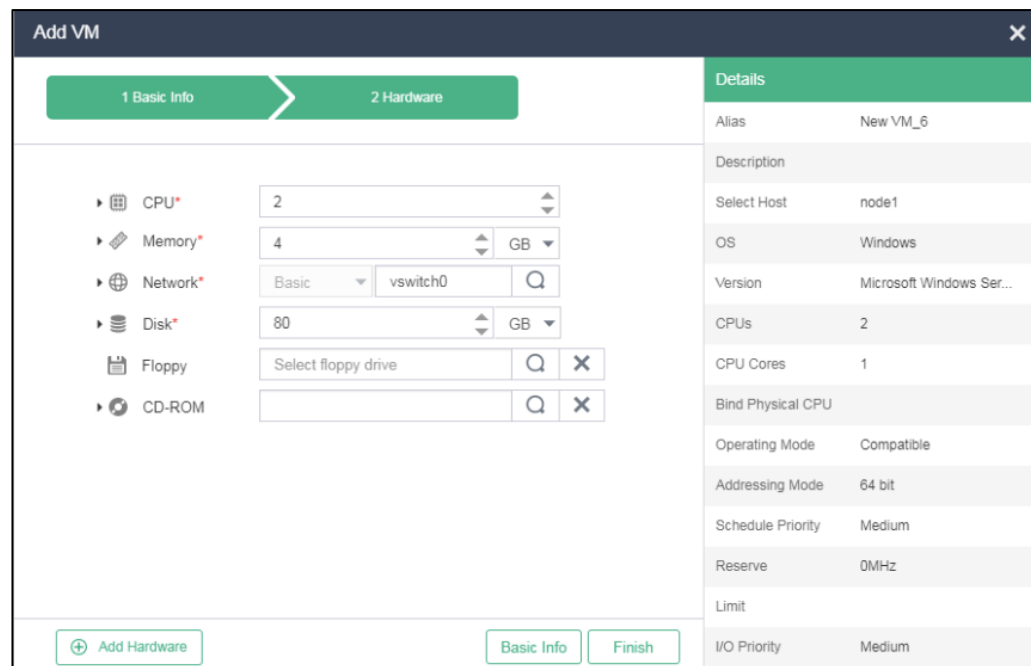


表 6 フロッピーおよび CD-ROM ドライブのパラメーター

パラメーター	説明
Floppy	フロッピー ドライブ イメージを選択します。システムは、選択したオペレーティング システムのバージョンと互換性のある高速ドライバーを自動的にロードします。
CD-ROM	CD-ROM ドライブ イメージを選択します。 VM にオペレーティング システムをインストールするための ISO イメージ ファイルを選択できます。
Connection Mode	接続モードを選択します。オプションには、 <b>CD/DVD</b> と <b>イメージ ファイル</b> (デフォルト) があります。

8. VM に追加するハードウェア オプションを選択するには、**Add Hardware** をクリックします。オプションには、**NIC**、**Disk**、**CD-ROM**、**Floppy disk**、**GPU Device**、**USB Device**、**Remote USB Device**、**PCI**、**vTPM Device**、および **Watchdog** があります。

図 7 ハードウェアの追加

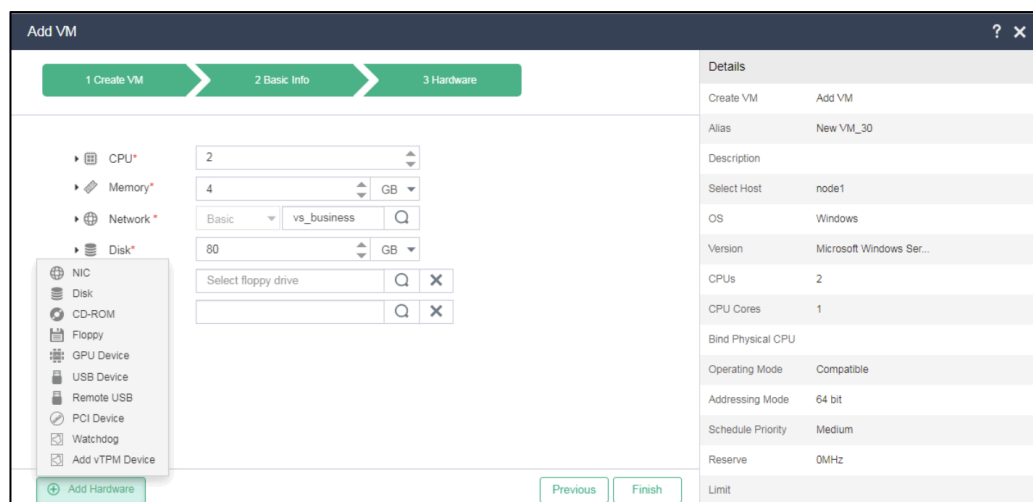


表 7 ハードウェアパラメータ

ハードウェア	パラメータ	説明
GPU Device	Resource Pool	クラスター内で使用可能なすべての GPU を含むリソース プールを選択します。
	Service Template	サービス テンプレートを選択します。サービス テンプレートは、VM がリソース (GPU や HBA など) にアクセスする優先順位を定義します。リソースが不足している場合、ホストは VM の優先順位に基づいて VM にリソースを割り当てます。
	Driver Type	GPU ドライバーの種類を設定します。VFIO ドライバーのみがサポートされています。
USB Device	Connection Mode	USB 接続規格を設定します。オプションには、 <b>USB 1.0</b> 、 <b>USB 2.0</b> 、 <b>USB 3.0</b> (デフォルト) があります。 このオプションは、VM の作成時にホストを選択した場合にのみ使用できません。
Remote USB	Connection Mode	ネットワーク USB 接続規格を設定します。オプションには、 <b>USB 1.0</b> 、 <b>USB 2.0</b> 、 <b>USB 3.0</b> (デフォルト) があります。 このオプションは、VM の作成時にホストを選択した場合にのみ使用できません。
PCI Device	Driver Type	PCI デバイス ドライバーの種類を設定します。オプションには <b>KVM</b> と <b>VFIO</b> (デフォルト) があります。 このオプションは、VM の作成時にホストを選択した場合にのみ使用できま

	す。
Watchdog	VM にウォッチドッグを追加します。割り込みオプションには、再起動 (デフォルト)、電源オフ、移行 があります。

9. **Finish** をクリックします。

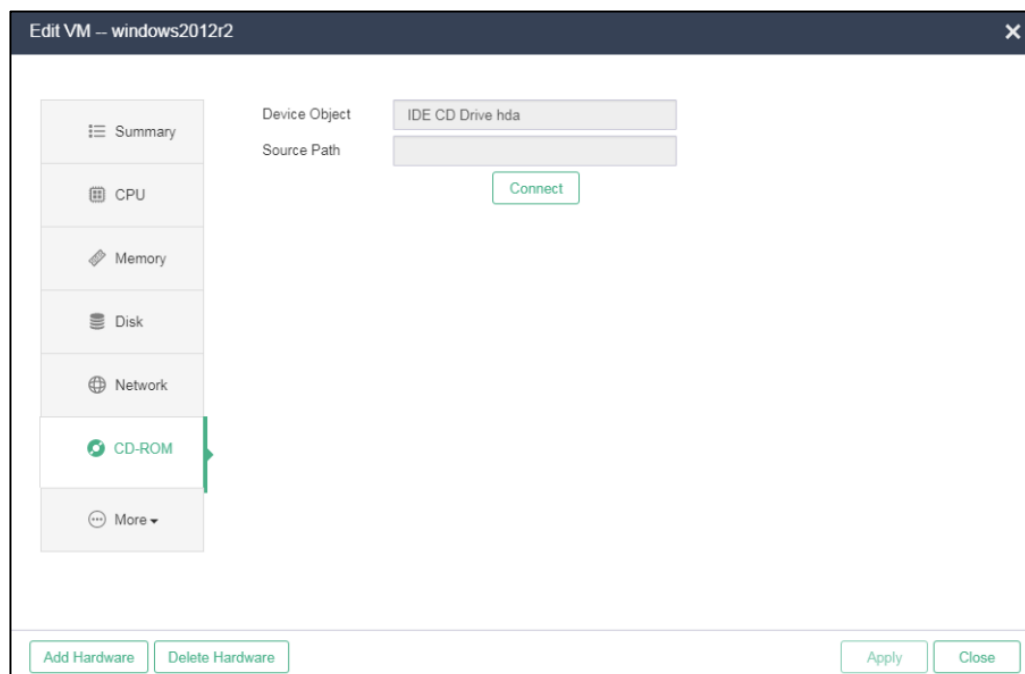
## VMにオペレーティングシステムをインストールする

### OSイメージをVMのCD-ROMにマウントする

作成時に ISO イメージ ファイルを VM にマウントした場合は、このタスクをスキップできます。

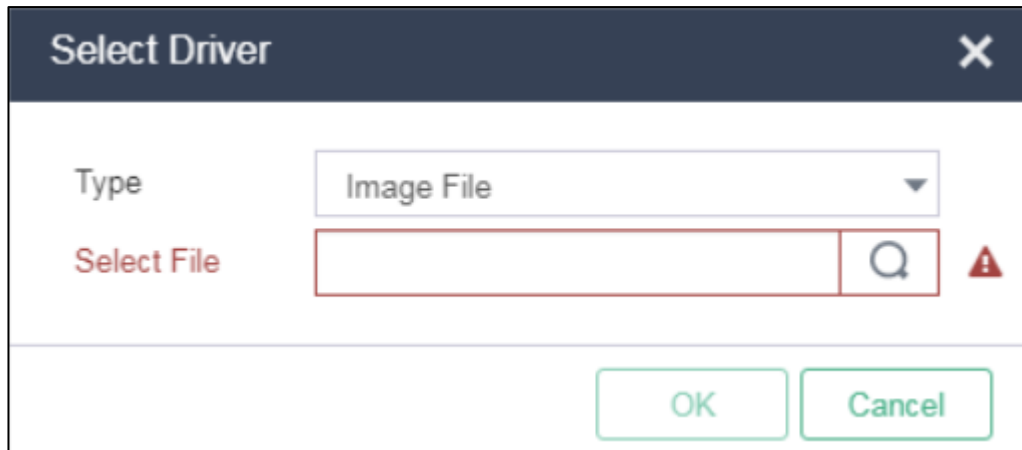
1. 上部のナビゲーション バーで、VM をクリックします。
2. ナビゲーション ペインから VM を選択します。
3. Edit をクリックします。
4. CD-ROM タブをクリックします。

図 1 VM の編集



5. **Connect** をクリックします。

図 2 ドライバーの選択



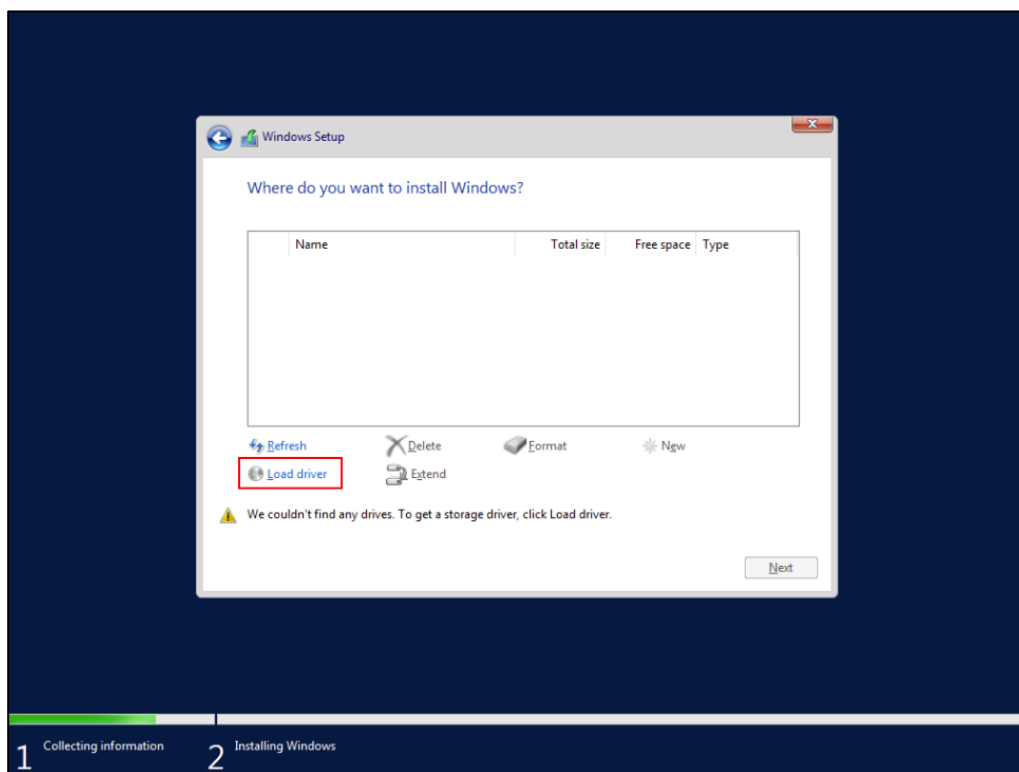
6. Select File フィールドをクリックします。
7. "OS イメージをアップロードする"でアップロードした ISO イメージ ファイルを選択します。
8. OK をクリックします。

## オペレーティング システムをインストールする

1. VM の概要情報ページで、**Start** をクリックします。
2. VM の概要情報ページで、VM の **Console** をクリックします。
3. 管理者がインストール ウィザードに従って VM にオペレーティング システムをインストールできるように、オペレーティング システムのインストール ページが自動的に開きます。
4. デフォルトでは、UIS システムは VM を作成するときに高速ディスクを使用します。Windows オペレーティング システムは、インストール ディスクにドライバーが含まれていないため、ディスク情報を取得できません。Windows オペレーティング システムを使用している場合は、次のタスクを実行してください。:
  - a. Load Driver をクリックします。

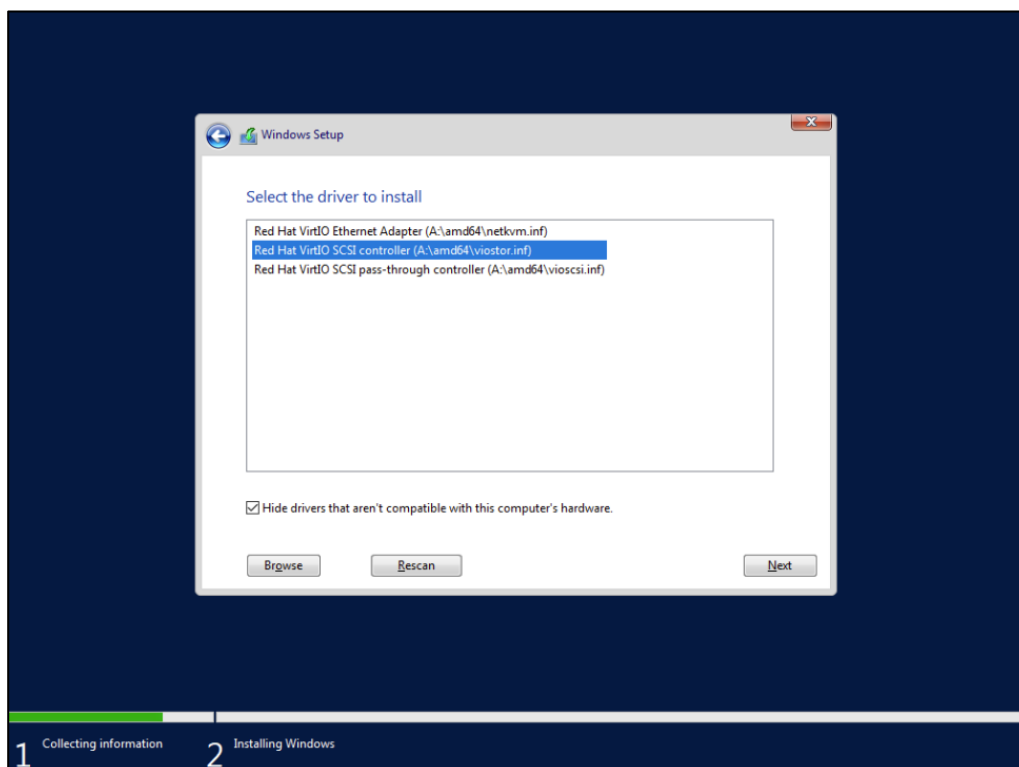


図 3 ドライバーの読み込み



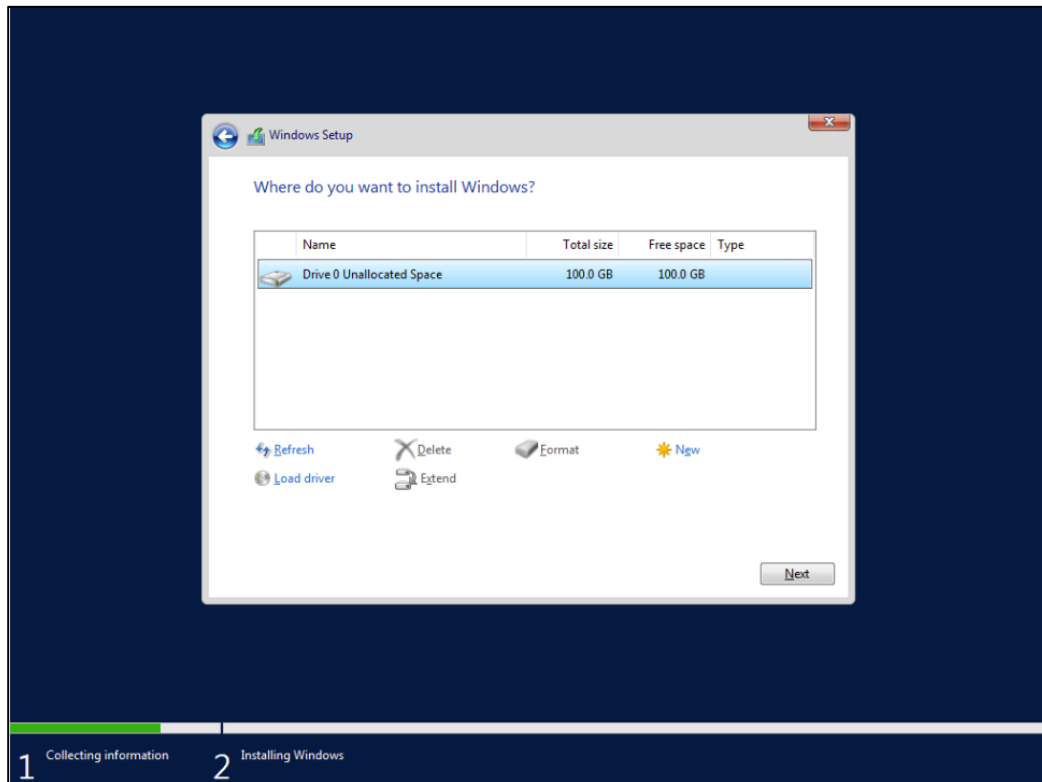
b. Red Hat VirtIO SCSI controller を選択します。

図 4 VirtIO SCSI Controller で Red H を選択します。



- c. 高速ディスクドライバーが読み込まれると、インストール ウィンドウに高速ディスクの情報が表示されます。

図 5 高速ディスク情報



- d. インストール ウィザードに従って、オペレーティング システムのインストールを完了します。

# VMにCAStoolsをインストールする

CAStools とオペレーティング システム間の互換性については、H3C UIS サーバー仮想化ソフトウェアとハードウェアの互換性を参照してください。

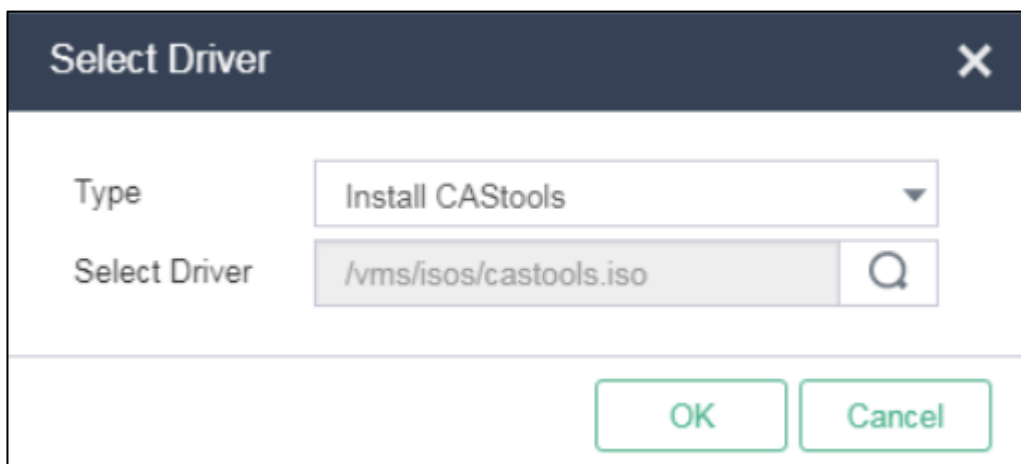
## 制限事項とガイドライン

- FreeBSD VM 用の CAStools のインストール中に pkg bootstrap コマンドが失敗した場合は、適切なイメージ ソースまたはリポジトリを使用します。たとえば、FreeBSD 12.3 の場合は、12.1 または 12.2 のイメージ ソースを使用します。
- CAStool タイプが Virtio である FreeBSD VM に CAStools をインストールした後、VM の Edit をクリックし、VM 概要ページの詳細設定で CAStool タイプを共通シリアル ポートに変更します。

## Windows または Linux オペレーティング システム に CAStools をインストールします

1. UIS にログインし、ターゲット VM を選択して、Edit をクリックします。
2. CD-ROM タブをクリックし、Connect をクリックします。
3. Type リストから **Install CAStools** を選択し、OK をクリックします。

図 1 CAStools のインストール



4. オペレーティング システムの種類に応じて CAStools をインストールします。インストールが完了したら、VM を再起動します。
  - オペレーティング システムの種類が Windows の場合は、コンソールから VM にログインし、CAS\_tools\_setup インストール プログラムをダブルクリックし、インストール ウィザードに従って CAStools のインストールを完了します。
  - オペレーティングシステムの種類が Linux の場合は、root ユーザーとしてオペレーティングシステムにログインし、次のコマンドを実行します。:

ルート パスワードは、オペレーティング システムのインストール時に指定したものです。

```
[root@localhost~]# mount /dev/cdrom /media
mount: /dev/sr0 is write-protected, mounting read-only
[root@localhost~]# cd /media
[root@localhost media]# ls
CAS_tools_setup.exe CAS_tools_upgrade.js linux query.bat readme.txt
[root@localhost media]# cd linux
[root@localhost linux]# sh ./CAS_tools_install.sh
Preparing... #####[100%]
Updating / installing...
 1:qemu-ga-6.0.2.0-1 #####[100%]
Non-SUSE
Created symlink from /etc/systemd/system/multi-user.target.wants/qemu-ga.service to
/usr/lib/systemd/system/qemu-ga.service.
```

## FreeBSD オペレーティング システム用の CAStools をインストールする

1. オペレーティング システムに root ユーザーとしてログインします。

ルート パスワードは、オペレーティング システムのインストール時に指定したものです。
2. FreeBSD ISO イメージ ファイルに基づいて、次のコマンドを実行して pkg と python をインストールします:

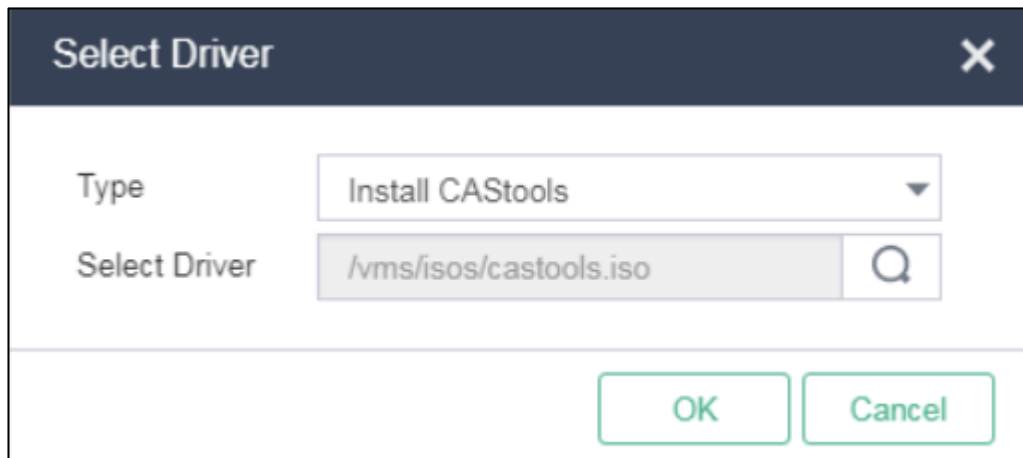
```
root@:~ # mkdir /dist
root@:~ # mount -t cd9660 /dev/cd0 /dist
root@:~ # setenv REPOS_DIR /dist/packages/repos
root@:~ # pkg bootstrap
```

```
The package management tool is not yet installed on your system.
Do you want to fetch and install it now? [y/n]:y
Bootstrapping pkg from file:///dist/packages/FreeBSD:11:amd64, please wait...
Installing pkg-1.8.7_1...
Extracting pkg-1.8.7_1:100%
root@:~ # pkg install python
Updating FreeBSD_install_cdrom repository catalogue...
Fetching meta.tzx:100% 260 B 0.3KB/s 00:01
Fetching packagesite.tzx:100% 244 KiB 249.9Kb/s 00:01
Processing entries:100%
FreeBSD_install_cdrom repository update completed.1075 packages processed.
Updating database digests format:100%
Checking intergrity...done(0 conflicting)
The following 7 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  python:2.7_2,2
  python27:2.7.12
  libffi:3.2.1
  indexinfo:0.2.4
  readline:6.3.8
  gettext-runtime:0.19.8.1
  python2:2_3
Number of packages to be installed:7
The process will require 69 MiB more space.
Proceed with this action?[y/n]:y
```

3. UIS にログインし、VM を選択して、Edit をクリックします。
4. CD-ROM タブをクリックし、Connect をクリックします。
5. Type リストから Install CAStools を選択し、OK をクリックします。

図 2 CAStools のインストール



6. VM のコンソールを開き、次のコマンドを実行します:

```
root@:~ # mount -t cd9660 /dev/cd0 /media/
```

```
root@:~ # cd /media/linux/
```

```
root@:~ # ./CAS_tools_install.sh
```

```
Installing qemu-ga-6.0.2.0-amd64...
```

```
Extracting qemu-ga-6.0.2.0-amd64: 100%
```

```
Message from qemu-ga-6.0.2.0-amd64:
```

```
Qemu-ga has been installed successfully, Use 'service qemu-ga start' to start!
```

## インストールを確認する

1. VM の summary information ページに入ります。
2. CAStools 状態が実行中であることを確認します。

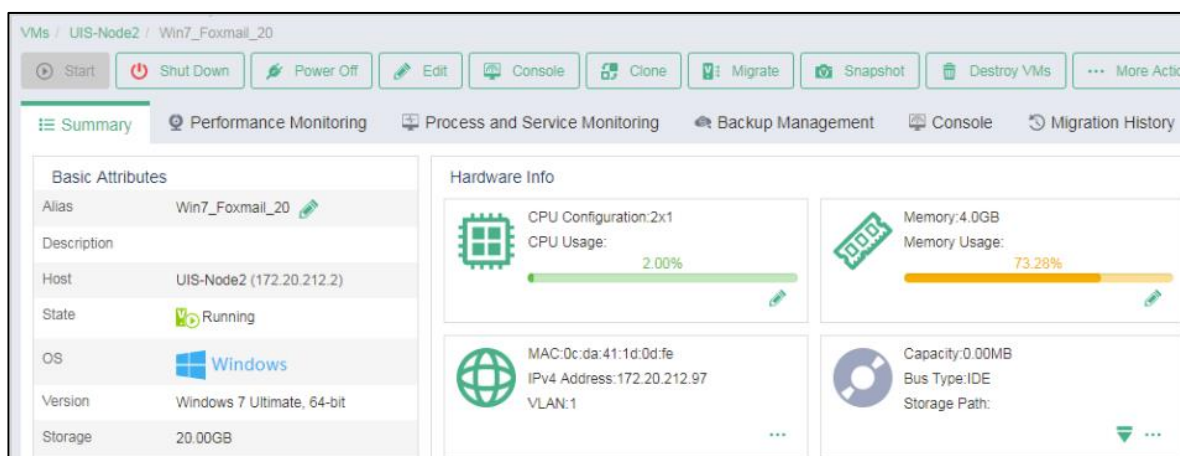
# VMのIPアドレスを設定する

インストールされた VM には、デフォルトでは IP アドレスがありません。CAStools を使用して、UIS Manager で VM に IP アドレスを割り当てることができます。

VMのIPアドレスを設定するには:

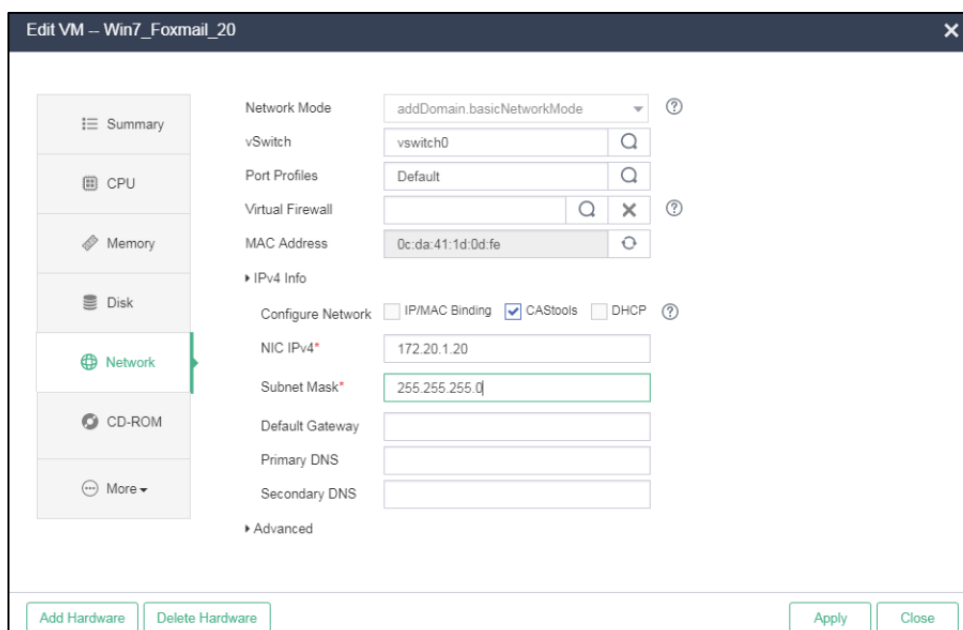
1. VM の概要情報ページで、Edit をクリックします。

図 1 VM summary ページ



2. **Network** タブをクリックします。
3. **Configure Network** で **CAStools** を選択します。

図 2 ネットワーク CAStools の設定



4. VM の IP アドレス情報を指定し、**Apply** をクリックします。  
設定された IP アドレスは、VM の概要情報ページに表示されます。
5. VM のオペレーティング システムにログインし、**ipconfig** コマンド (Windows) または **ifconfig** コマンド (Linux) を使用して、構成された IP アドレスを確認します。

## VMテンプレートを作成する

VM テンプレートは VM から複製または変換されます。

- **Clone to template**—元の VM をそのまま残しながら、VM のテンプレート コピーを作成します。
- **Convert to template**—シャットダウン状態の VM をテンプレートに変換します。変換された VM はテンプレートとしてのみ使用でき、削除されます。

VMテンプレートを複製するには:

1. 上部のナビゲーション バーで、VM をクリックします。
2. ナビゲーション ペインから VM を選択します。
3. **More Actions** をクリックし、**Clone to Template** を選択します。
4. VM テンプレート情報を指定し、テンプレートを保存するパスを選択します。
5. OK をクリックします。

## 異機種移行を構成する

異機種移行では、物理 x86 サーバー、UIS マネージャーによって管理される VM、および別のプラットフォームによって管理される VM 上のディスク データを UIS マネージャー プラットフォーム上の宛先 VM に移行できます。ソース デバイスにクライアントをインストールする必要があります。

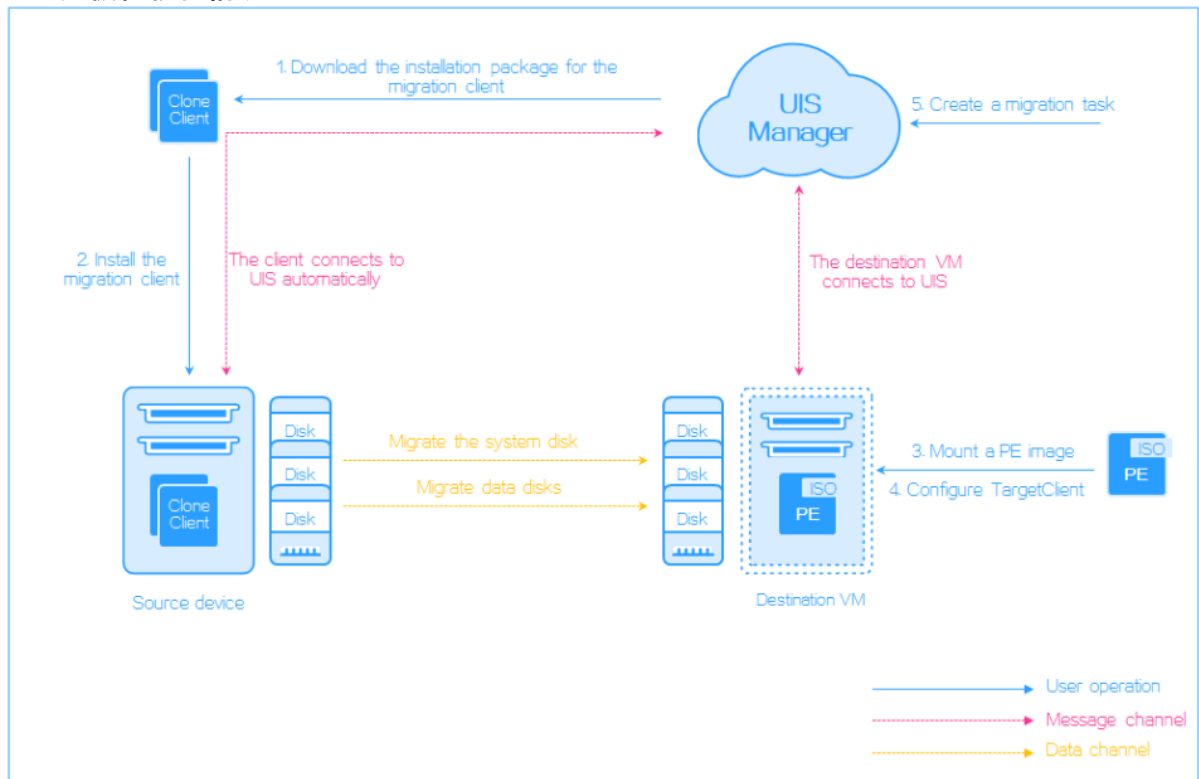
## 制限事項とガイドライン

- ディスクまたはボリューム上で増分移行またはバックアップを実行するには、次の要件が満たされていることを確認してください。
  - ボリュームまたはディスクの容量は 128 TB 以下です。最高のオンライン移行パフォーマンスを得るためのベスト プラクティスとして、ボリュームまたはディスクの容量を 32 TB 以内に抑えます。
  - 増分間隔で増分されるデータは 1 TB 以下です。
- EXT2/EXT3/EXT4 ファイル システムで差分移行またはバックアップを実行するには、ファイル システムの容量が 64 TB 未満であることを確認してください。
- その他の制限とガイドラインについては、対応するリリースの使用ガイドラインを参照するか、テクニカル サポートにお問い合わせください。



# 構成ワークフロー

図1 異機種移行構成ワークフロー

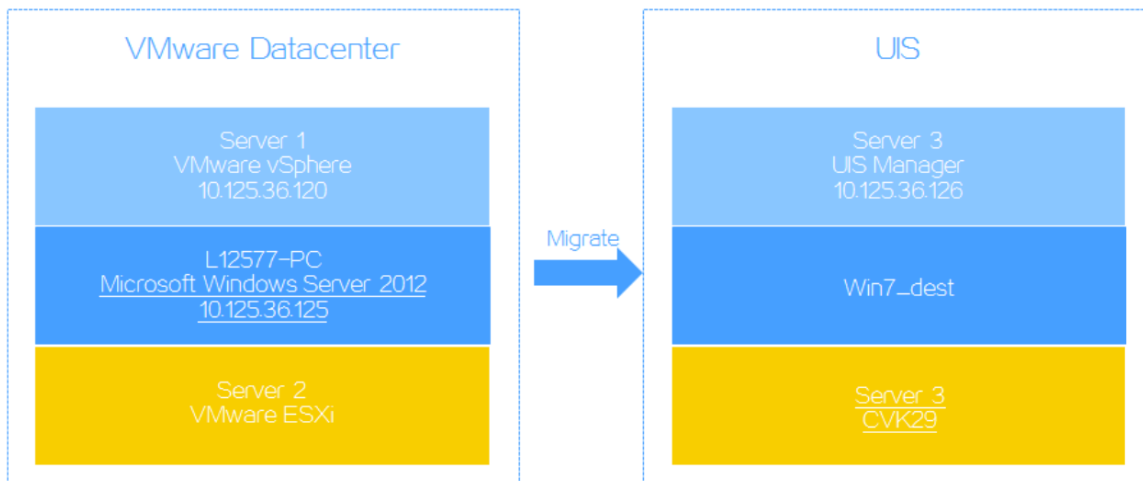


異機種間の移行を実行するには、次のタスクを実行する必要があります。

1. UIS マネージャーからソース デバイス (物理サーバーまたは VM) に移行クライアントをダウンロードします。
2. 移行クライアントをインストールし、ソース デバイスを UIS マネージャーに接続します。すると、移行クライアントはソース デバイスのステータスを UIS マネージャーに報告します。
3. PE イメージを宛先 VM にマウントし、TargetClient を構成して、TargetClient を UIS Manager に接続します。次に、TargetClient は宛先 VM のステータスを UIS Manager に報告します。
4. 移行タスクを作成して開始します。移行クライアントは移行コマンドを受信し、システム ディスクとデータ ディスクの移行を開始します。

# 移行環境

図 1 移行環境



## ソースデバイスを準備する

### 異機種間移行コンポーネントをインストールする

1. movesure.tar.gz パッケージをターゲット ホスト上の任意のフォルダーにアップグレードします。
2. tar -zxvf movesure.tar.gz コマンドを実行して、パッケージを現在のフォルダーに解凍します。
3. movesure フォルダーで sh install\_en.sh コマンドを実行して、異種移行コンポーネントをインストールします。

異種移行コンポーネントをアンインストールするには、sh uninstall.sh コマンドを実行します。

## 移行クライアントをインストールする

### 移行クライアントをダウンロード

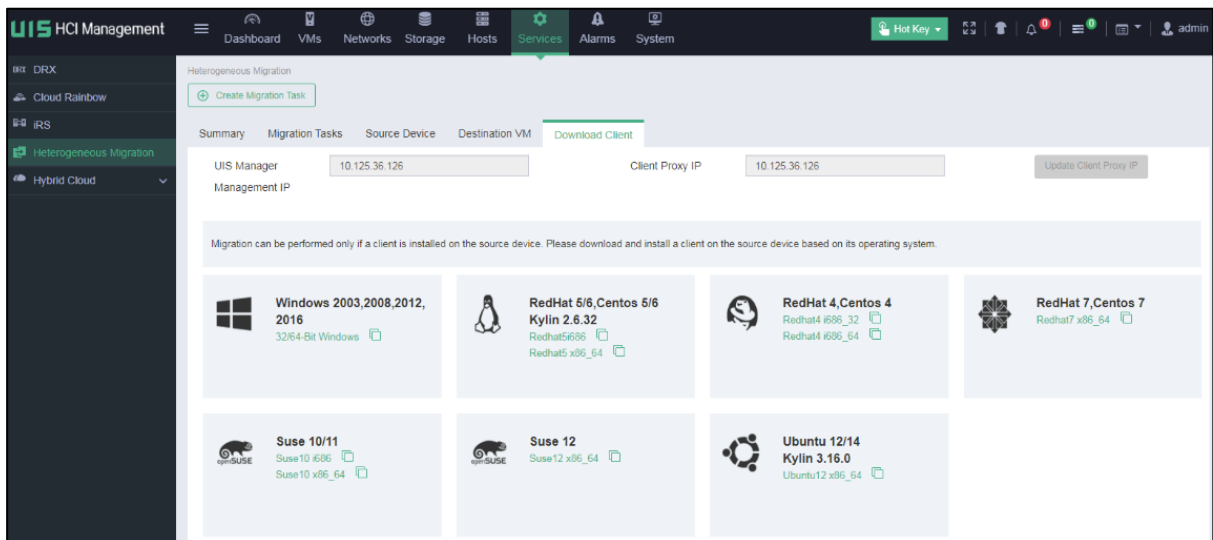
1. UIS マネージャーにログインします。
2. 上部のナビゲーション バーで、Services をクリックします。
3. 左側のナビゲーション ペインから、Heterogeneous Migration を選択します。

4. DownloadClient タブをクリックします。デフォルトでは、クライアント プロキシ IP アドレスは UIS マネージャーの管理 IP アドレスです。

クライアント プロキシ IP アドレスが正しいことを確認します。IP アドレスが実際のアドレスと異なる場合は、Update Client Proxy IP をクリックします。これは、移行ライセンスがアクティブ化された後にのみ使用できます。移行ライセンスを登録するには、ライセンス ページの機能ライセンス タブにアクセスします。

5. 以下の方法を使用して、対象のインストールパッケージをダウンロードします：
  - 対象 OS 名をクリックします。システムは、Clone\_Client\_xxx.zip という名前の .zip ファイルでインストール パッケージをダウンロードします (例: Clone\_Client\_Redhat5x86\_64.zip)。次に、ファイルを解凍し、解凍したインストール パッケージを FTP 経由でソース デバイスにアップロードする必要があります。
  - 対象クライアント エディションの アイコンをクリックして、ダウンロード用の URL を取得します。次に、ソース デバイスのリモート コンソールにアクセスし、URL を使用してインストール パッケージをダウンロードします。

図 1 移行クライアントのダウンロード

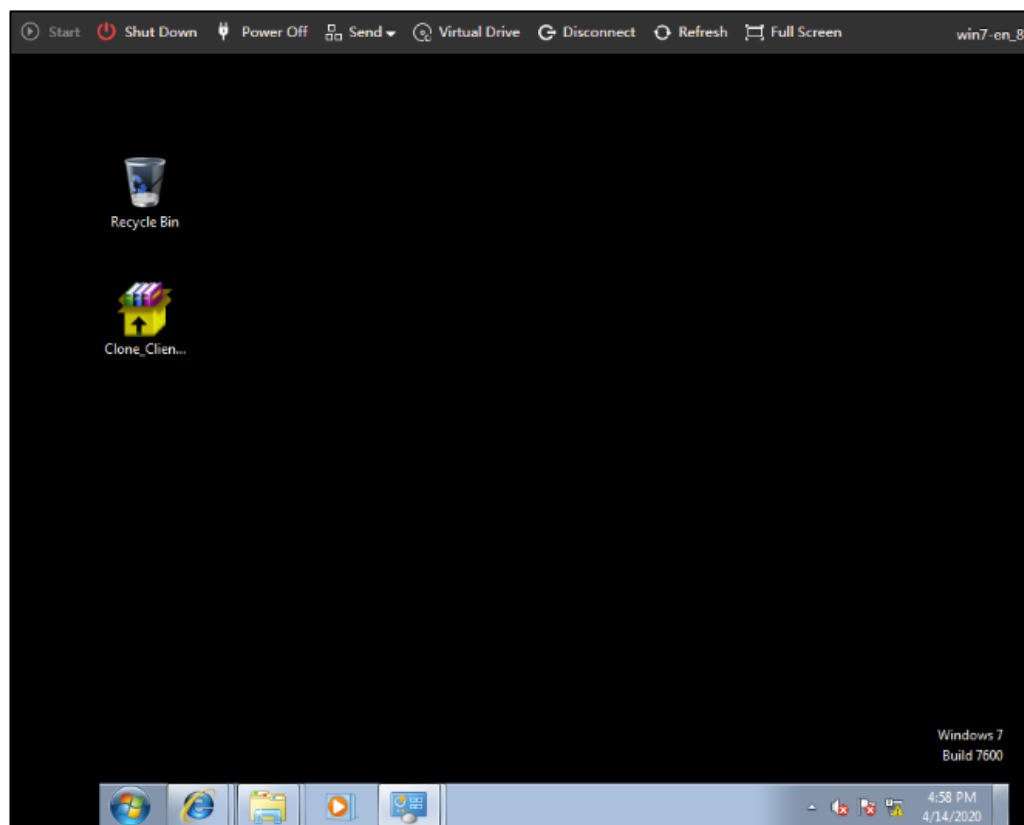


## 移行クライアントをインストールする

UIS 管理ネットワークの IP アドレスが変更された場合は、Update Client Proxy IP をクリックして、サーバー IP アドレスを新しい管理ネットワーク IP アドレスに更新します。インストールの失敗を回避するには、ソース デバイスのファイアウォールとセキュリティ ポリシー設定を無効にします。ソース デバイスが VM の場合は、ソース デバイスで移行ツールのポートが有効になっていることを確認します。

1. ソースデバイスのリモート コンソールにアクセスします。

図 2 ソースデバイスのリモートコンソールにアクセスする



2. Clone\_Client\_Win.exe をダブルクリックします。開いたウィンドウでインストール言語を選択し、OK をクリックします。
3. インストール契約に同意し、インストール ディレクトリを選択して、インストール プロセスを開始します。
4. CDP ドライバー プログラムをインストールするには、プロンプトで Y をクリックします。
5. インストール後、インストールしたクライアントを有効にするには、ソース デバイスを再起動します。

ソースデバイスが Windows オペレーティングシステムを使用している場合、再起動操作によってサービスが中断されます。影響を最小限に抑えるには、ソースデバイスがビジーでないときに再起動してください。

図 3 ソースデバイスの再起動



再起動後、Services> Heterogeneous Migration > Source Device ページにアクセスして、ソース デバイスがソース リストに追加されたことを確認できます。

デフォルトでは、システムはソースデバイスにオペレーティングシステムのコンピュータ名で名前を付けます。

図 4 ソースデバイスリスト

Name	IP Address	Device Description	Device State	Migration State	Licensed	Destination Device	Destination Device ID	Actions
localhost.localdomain	10.125.36.127		Online	To Finish	Yes	p2v-dest	10.125.36.128	
L12577-PC	10.125.36.125		Online		No			

# 宛先VMを準備する

## PEイメージを取得する

UIS は、Windows OS と Linux OS での移行用にそれぞれ Win10PE と Centos7PE イメージを提供します。PE イメージは UIS バージョン イメージとともにリリースされます。ターゲット VM に正しい PE イメージがマウントされている場合にのみ、TargetClient を構成できます。VM を構成する前に PE イメージ ファイルを取得し、UIS マネージャーに PE イメージ ファイルをアップロードします。

## 宛先VMを作成する

宛先 VM の使用可能なディスク サイズと合計ディスク サイズの両方が、ソース デバイスのディスク サイズ以上であることを確認します。

ソース デバイスが Suse10 OS を使用している場合は、宛先 VM を作成するときにバス タイプを IDE に設定します。

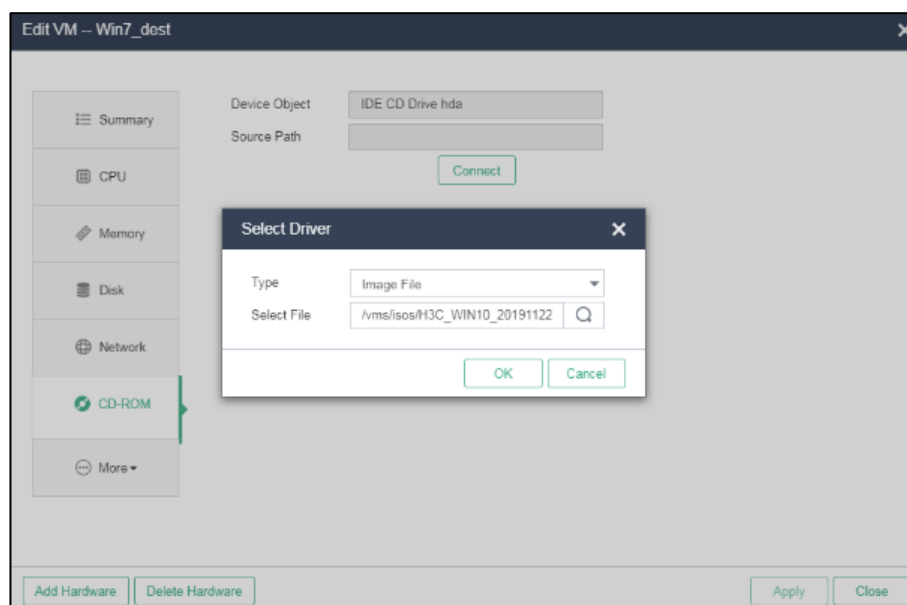
図 1 宛先 VM の作成

Details	
Alias	Win7_dest
Description	
Select Host	cvknode1
OS	Windows
Version	Microsoft Windows Ser...
CPUs	2
Memory	4GB
Disk	80GB

# TargetClient を構成する

1. PE イメージを宛先 VM にマウントします。

図 2 PE イメージを宛先 VM にマウントする



2. 宛先 VM を起動し、VM コンソールにアクセスします。VM は PE イメージから起動し、ターゲットクライアントを実行して H3C コンバーター プラットフォームにアクセスします。

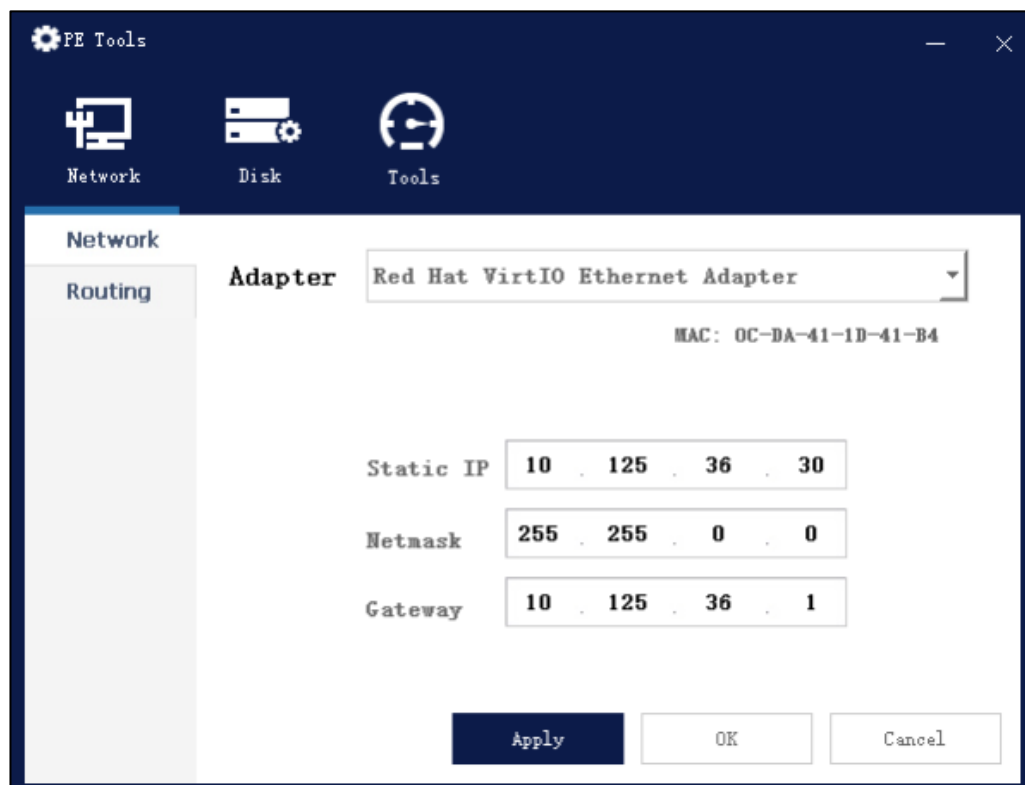
図 3 H3C コンバーター プラットフォーム



3. Tools をクリックし、VM が UIS マネージャーと通信するためのネットワーク設定を構成します。

この手順で構成されたネットワーク設定は、VM の再起動後に失われます。移行後、必要に応じて VM のネットワーク設定を再構成できます。

図 4 ネットワーク設定の構成



4. UIS マネージャーの IP アドレスを入力し、VM のホスト名を指定して、矢印をクリックします。

ローカル IP アドレス フィールドはオプションです。デフォルトでは、移行プラットフォームにアクセスするために宛先 VM が使用するデフォルトの IP アドレスが使用されます。UIS マネージャーがパブリック IP アドレスを使用する場合、または 2 つのホストがステートフル フェイルオーバーを提供する場合は、ローカル IP アドレスを指定する必要があります。そうしないと、ソース デバイスは宛先 VM に接続できません。

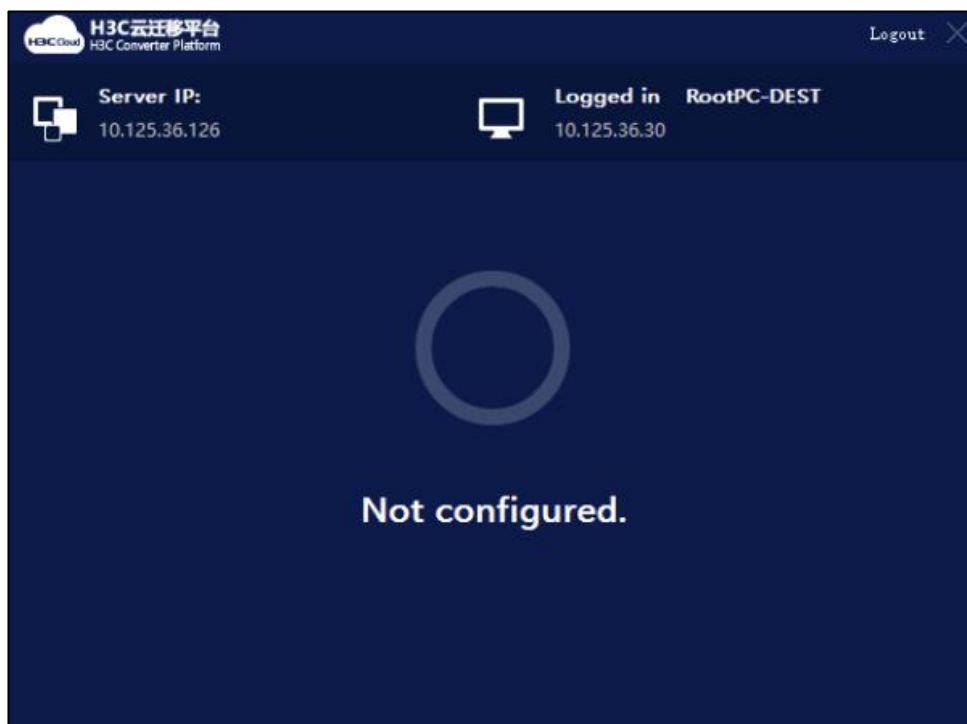


図 5 TargetClient パラメータの設定



開いたページには、TargetClient と宛先 VM が UIS Manager に接続されていることが示されます。

図 6 ターゲットクライアント接続



5. Services > Heterogeneous Migration > Destination VM ページにアクセスし、宛先 VM が宛先 VM ページに追加され、VM ステータスがオンラインになっていることを確認します。

移行タスクをサポートするのは、オンラインの宛先 VM のみです。オンラインの宛先 VM の移行操作が失敗した場合は、ネットワークアドレスの競合がないことを確認してください。

図 7 宛先 VM リスト

Name	IP Address	Device Description	Device State	Migration State	Source Device Name	Source Device IP	Actions
p2v-dest	10.125.36.128		Online	To Finish	localhost.localdomain	10.125.36.127	
RootPC-DEST	10.125.36.30		Online	Not Configured			

# 移行を実行する

## 制限事項とガイドライン

移行プロセスはネットワーク帯域幅を占有し、ソース デバイスのコンピューティング パフォーマンスに影響を及ぼし、移行中はサービスが中断されます。ベスト プラクティスとして、オフピーク時にデータ移行を実行し、サービス切り替え時間を適切に調整します。

移行の失敗やその他の互換性の問題を回避するには、プラットフォームがソース デバイスのオペレーティング システムと互換性があり、宛先デバイスに十分なハードウェア リソースがあることを確認します。

移行後、一部のハードウェアのドライバーを再ロードまたは更新する必要がある場合があります。NIC の MAC アドレスやハード ドライブ文字などの一部のハードウェア設定が変更される場合があります。ハードウェアにバインドされたアプリケーションがある場合は、それに応じてアプリケーションを編集する必要があります。

## 移行タスクを作成する

1. 上部のナビゲーション バーで、Services をクリックします。
2. 左側のナビゲーション ペインから、Heterogeneous Migration を選択します。
3. Create Migration Task をクリックします。
4. I have read the restrictions and guidelines を選択し、Next をクリックします。
5. ソースデバイスと宛先 VM を指定します。

図 1 ソースデバイスと宛先 VM の指定

Create Migration Task

1 Restrictions and Guidelines | 2 Destination Match | 3 Task Settings | Licenses (Available/Total) 19/20

1. The system identifies whether the source device driver matches the destination VM hardware. If the system prompts incompatibility risks, you must export incompatible hardware information, prepare a driver file, and import the file to the system. Then, you can import the destination driver to the destination VM after migration.

2. The data on the destination disk, including the partition table will be erased. After migration, all the data on the source disk will be migrated to the target disk.

Source Device \* L12577-PC

Destination VM \* RootPC-DEST

Disk Selection and Match \* label,C:

Add Migration Task Previous Next Cancel

6. ソース ディスクとターゲット ディスクを選択します。デフォルトでは、システムは各ソース デバイス ディスクをターゲット デバイス ディスクにマップします。ソース ディスクをターゲット ディスクに手動でマップする場合は、ターゲット ディスクのサイズがソース ディスクと同じかそれより大きいことを確認してください。動的ソース ディスクの場合、ターゲット ディスクとソース ディスクのサイズは同じである必要があります。

・移行できるのはシステム ディスクとデータ ディスクのみです。

・パーティション テーブルを含む宛先ディスク上のデータは消去されます。移行後、ソース ディスク上のすべてのデータがターゲット ディスクに移行されます。

LVM ディスクは論理ボリュームなので、移行先ディスクを選択する必要はありませんが、システムは LVM データも移行します。

7. 必要に応じてタスク パラメーターを構成します。移行タスクをすぐに開始するには、Start をクリックします。移行タスクを保存するには、Save をクリックします。後で移行タスク リストにアクセスして、保存したタスクを開始できます。

- ・ 移行タスクを構成する前に、タスクで指定するソース デバイスのライセンスを取得する必要があります。移行タスクを複数回実行し、複数の移行タスクで同じソース デバイスを指定できます。

- ・ 移行タスクが保存または実行されると、移行ライセンスがソース デバイスに即時発行されます。システムが移行タスクの作成に失敗しても、発行されたライセンスは再利用できません。このような場合は、失敗の原因を特定し、別の移行タスクを作成してください。

図 2 タスクパラメーターの設定

Create Migration Task

1 Restrictions and Guidelines 2 Destination Match 3 Task Settings licenses (Available/Total) 19/20

Data compression can reduce requirements on migration bandwidth but will increase resource consumption of the source device and might affect service operation.

Automatic Incremental Migration Interval 30 Minutes

Migration Speed Limit 50 MBps

Migration Method Full Simple

Data Compression Off

Previous Save Start Cancel

8. 移行タスク リストを表示するには、Migration Tasks タブをクリックします。システムは移行タスクにソースデバイス名で名前を付け、30 秒ごとにリストを更新します。

移行タスクには、デフォルトでソース デバイス名が付けられます。

図 3 移行タスクリスト

Source Device Name	Source Device IP	Source Device Description	Migration State	Migration Progress	Estimated Time	Destination Device	Destination Device IP	Actions
localhost.localdomain	10.125.36.127		To Finish	100%	00:00:01	q2v-dest	10.125.36.128	[Stop] [Refresh] [Delete]
L12577-PC	10.125.36.125		In Progress	0.00%	24:00:00	RootPC-DEBT	10.125.36.30	[Pause] [Refresh] [Delete]

9. 移行タスクの詳細情報を表示するには、ソース デバイス名をクリックします。詳細情報ページには、移行プロセス、デバイス情報、およびログが表示されます。

システムは、定期的にデータをサンプリングして、移行タスクの実行進行状況を計算します。多数のディスクを移行する場合、システムは実行進行状況をリアルタイムで更新しないことがあります。これは移行には影響しません。各ディスクの移行状態の移行進行状況を確認できます。

図 4 移行タスクの詳細情報の表示

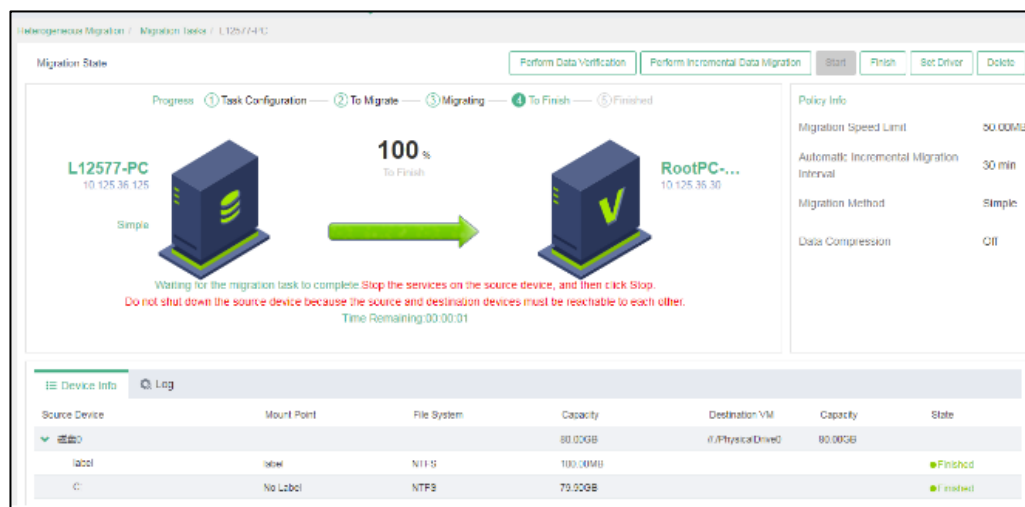
Source Device	Mount Point	File System	Capacity	Destination VM	Capacity	State
物理0	label	NTFS	100.00GB	\\PhysicalDrive0	80.00GB	Finished
C:	No Label	NTFS	70.00GB			0.00%

10. 移行タスクを手動で完了しない場合、システムは増分移行間隔で定期的に移行タスクを実行します。移行タスクを手動で完了するには、Finish をクリックします。

タスクを手動で終了する前に、デバイスが新しいデータを生成しないように、ソース デバイス上のサービスを停止する必要があります。

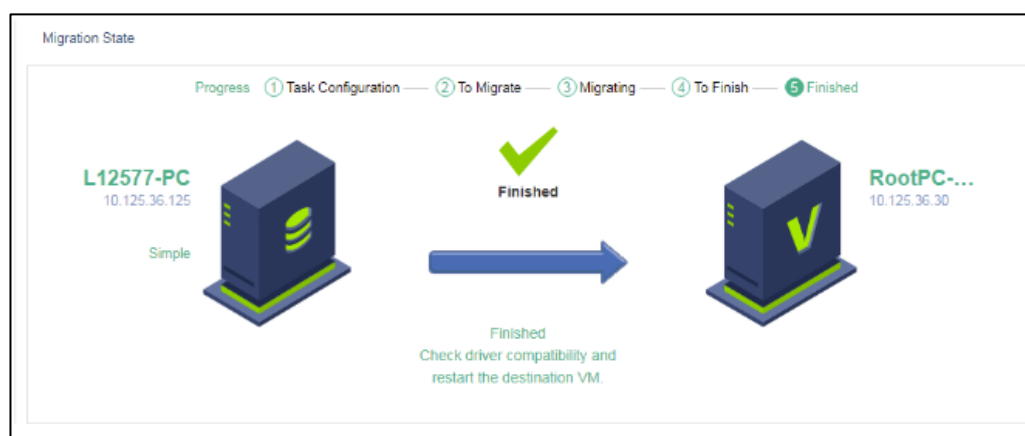
最初の実行後に完了していない移行タスクに対して、手動で増分データ移行を実行できます。増分移行では、前回の移行以降に変更されたデータまたは新しいデータのみがコピーされます。最初の実行後に完了していない移行タスクに対して、データの整合性を検証し、データを復元できます。

図 5 移行タスクの終了



タスクを完了すると、タスクは Finished 状態になります。

図 6 移行完了



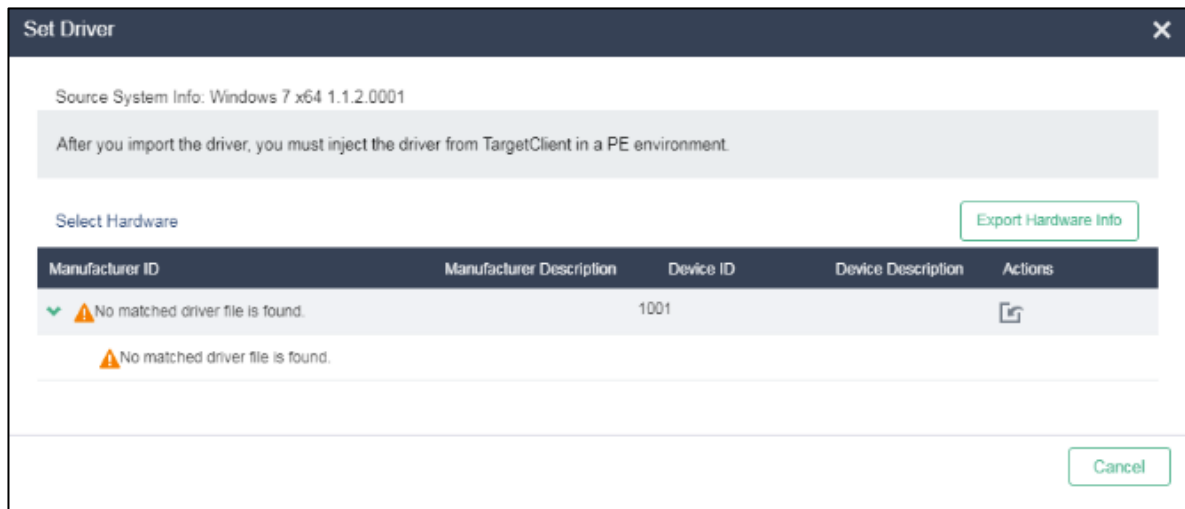
## ドライバーを構成する

ベスト プラクティスとして、カーネル バージョンが 2.6.25 以上 (たとえば、redhat 5.2) の場合は Linux OS 用の Virtio ドライバーを使用し、カーネル バージョンが 2.6.25 以外の場合は IDE ドライバーを使用します。

システムは、移行タスクのディスクドライバーの非互換性リスクを検出できます。ドライバーの非互換性の問題がある可能性のあるハードウェアに関する情報をエクスポートし、そのハードウェアのドライバーを移行先 VM にインポートできます。

1. 移行タスクの詳細ページで、Driver の設定 をクリックします。

図 7 Configuring a driver

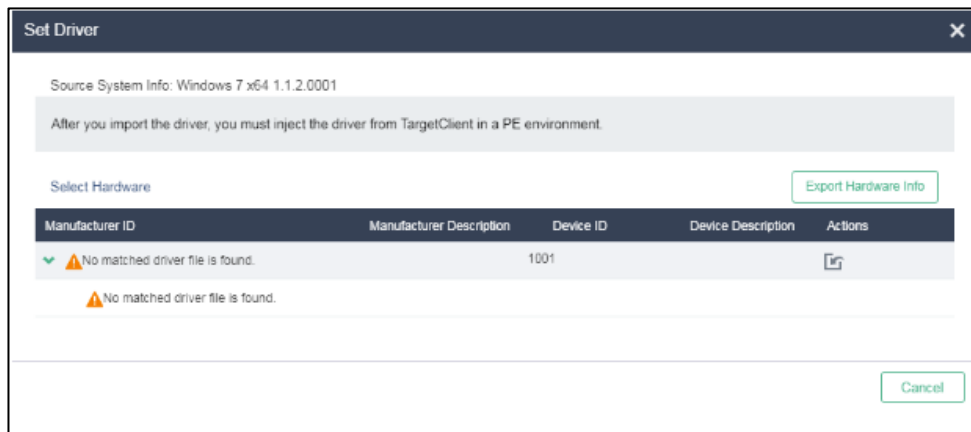


2. Export Hardware Info をクリックします。システムは、宛先 VM のディスクに関するハードウェア情報を TXT 形式でエクスポートします。
3. ダウンロードしたファイルを開いて、必要なドライバーに関する情報を表示します。ファイル名は *Destination\_VM\_name* Driver Hardware Info.txt です。
4. アップロードするドライバー ファイルを .zip ファイルに圧縮し、圧縮ファイルに *mptspi.zip* という名前を付けます。

通常、ドライバー ファイルは、Windows の場合は .sys または .inf ファイル、Linux の場合は .ko ファイルです。

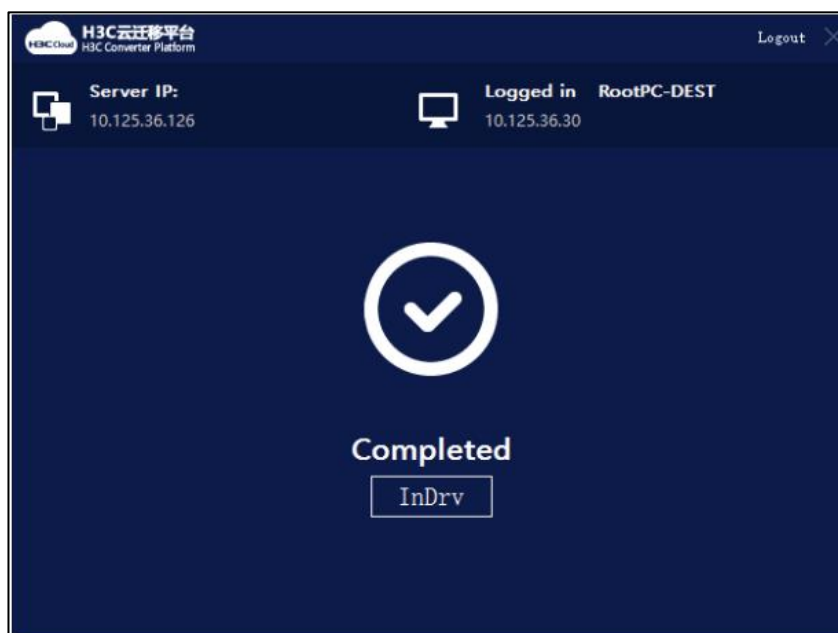
圧縮ファイルに多層フォルダーが含まれていないことを確認してください。
5. 詳細なタスク情報ページで、インポート ボタンをクリックして、圧縮ファイルを UIS マネージャーにインポートします。

図 8 圧縮ファイルを UIS マネージャーにインポートする



6. TargetClient で InDrv をクリックして、宛先 VM にドライバーをインストールします。

図 9 ドライバーのインストール



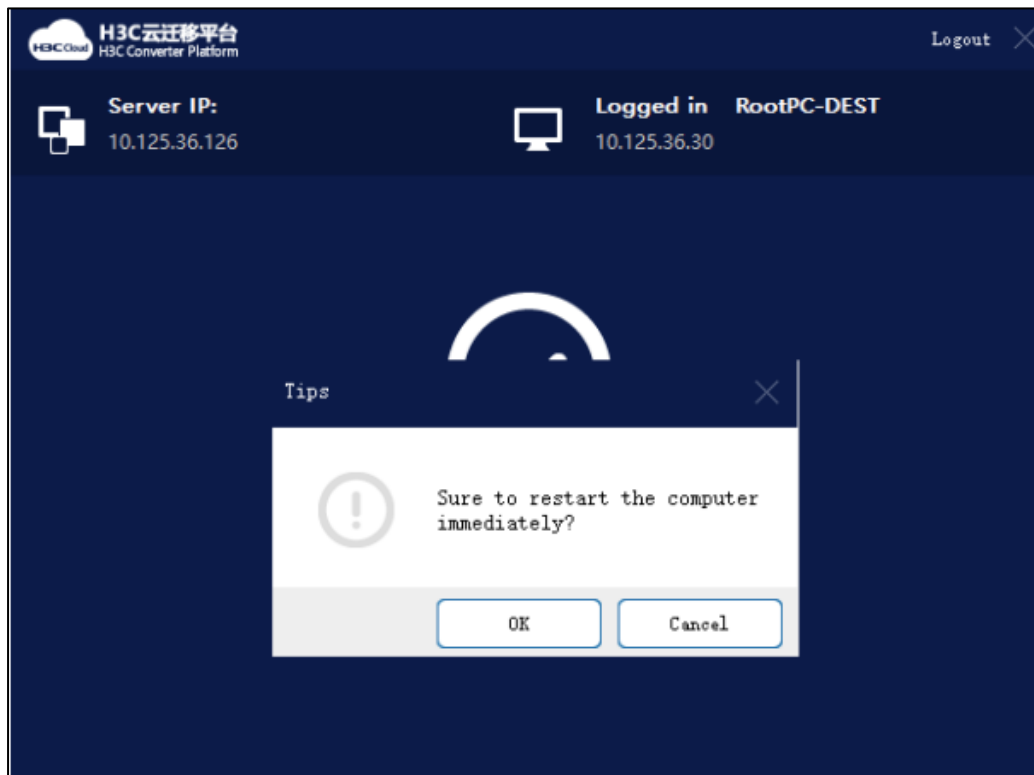
## 宛先VMにアクセスする

1. 宛先 VM のコンソールにアクセスし、H3C コンバーター プラットフォームを終了します。
2. プロンプトで OK をクリックして、宛先 VM を再起動します。

VM のオペレーティング システムにアクセスできない場合、またはシステムからパーティションまたはディスクが見つからないというメッセージが表示される場合は、VM の電源をオフにして、VM を再起動し、CAS からの起動を選択します。



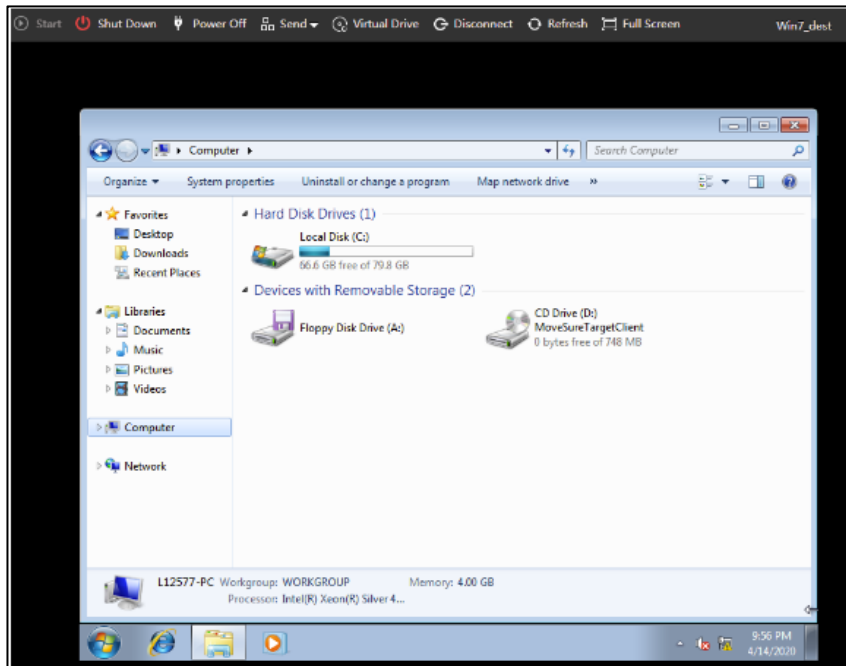
図 10 宛先 VM の再起動



3. ユーザー名とパスワードを入力して、宛先 VM にアクセスします。ソース デバイスのすべてのデータが宛先 VM に移行されていることを確認します。

デフォルトでは、宛先 VM はソース デバイスと同じユーザー名とパスワードを使用します。

図 11 宛先 VM 上のデータの検証



## IPv6設定

サービス ネットワークの IPv6 設定を構成します。サービス ネットワークにより、VM はサービスを提供できるようになります。

図1 IPv6設定フローチャート

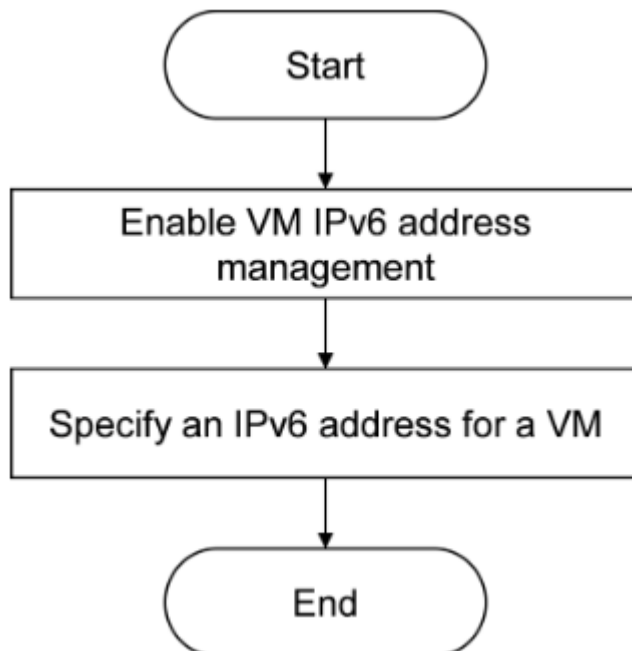


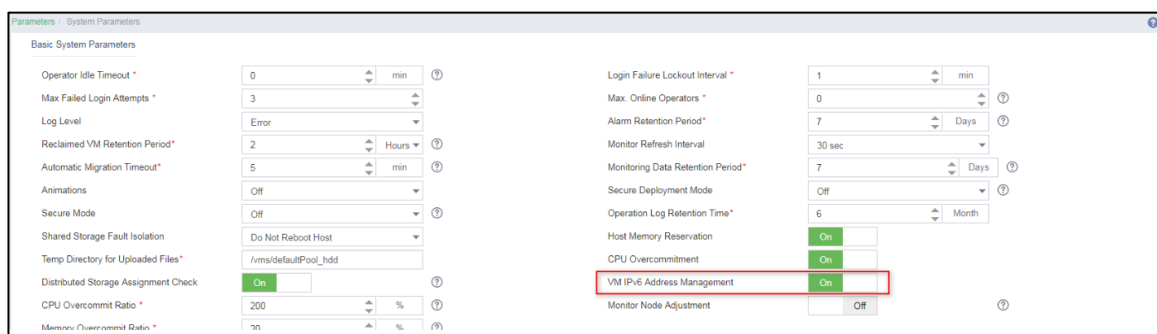
表1 IPv6設定ワークフロー

手順	備考
VM IPv6アドレス管理を有効にする	必須。 VM の IPv6 アドレスを指定するには、このタスクを実行して VM IPv6 アドレス管理を有効にする必要があります。
VMのIPv6アドレスを指定する	必須。 ユーザーが IPv6 ネットワーク経路で VM によって提供されるサービスにアクセスできるように、VM の IPv6 アドレスを指定するには、このタスクを実行します。

## VM IPv6アドレス管理を有効にする

1. 上部のナビゲーション バーで、**System** をクリックし、ナビゲーション ペインから **Parameter > System Parameters** を選択します。
2. VM IPv6 アドレス管理を有効にし、**Save** をクリックします。

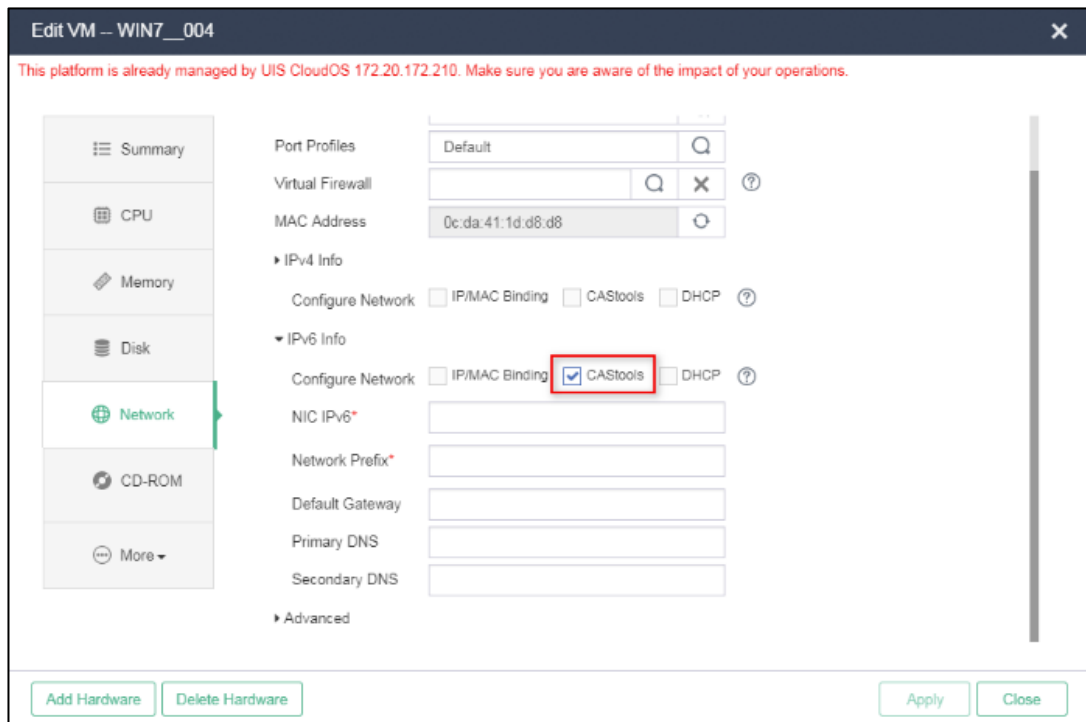
図 1 VM IPv6 アドレス管理の有効化



## VMのIPv6アドレスを指定する

1. 上部のナビゲーション バーで、VM をクリックします。
2. VM を選択し、Edit をクリックします。
3. Network タブをクリックします。
4. CAStools を選択し、VM の IPv6 設定を構成します。

図 1 CAStools を使用して VM の IPv6 アドレスを指定する



VM に CAStools がインストールされ、正常に動作している場合にのみ、VM の IP アドレスを構成できます。

# DRX

図1 DRX構成フローチャート

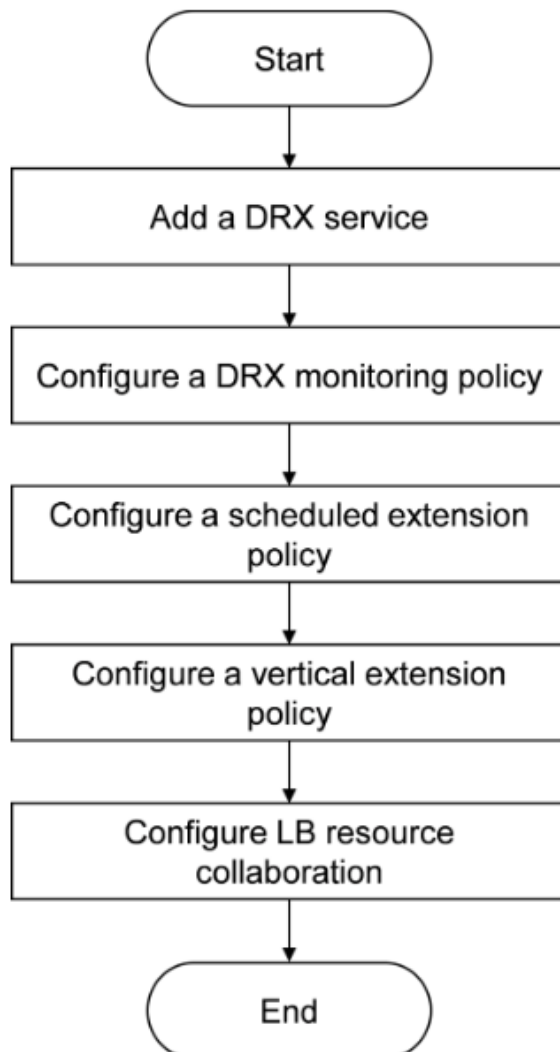


表1 DRX設定手順

タスク	説明
DRXサービスを追加する	DRX は、同じクラスター内で同じサービスを提供する VM を VM グループに追加します。グループ内の VM の接続数、平均 CPU 使用率、平均メモリ使用率を定期的にチェックし、DRX ポリシーとリソース拒否モード、リソース再利用ポリシーと再利用モードに基づいて、グループ内の VM の数を動的に調整します。
DRXサービス監視ポリシーを構成する	オプション。 拡張監視ポリシーで、VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続数、ネットワークトラフィック、ディスク I/O、および IOPS がしきい値を複数回超えると、システムは VM グループ内に VM を自動的に作成します。 VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続数、ネットワークトラフィック、ディスク I/O、および IOPS が、リソース再利用監視ポリシーのしきい値を複数回下回ると、システムは VM グループ内の VM を自動的に再利用します。
スケジュールされた拡張ポリシーを追加する	オプション。 スケジュールされた拡張ポリシーは、サービス サージが定期的に発生するアプ

タスク	説明
	リケーション システムで特定の時点で VM を作成するために使用されます。
垂直拡張ポリシーを構成する	オプション。 DRX サービスに垂直拡張ポリシーが設定されている場合、CPU 使用率またはメモリ使用率が垂直拡張ポリシーで設定されたしきい値を超えると、システムは VM に CPU またはメモリを追加します。
LB リソースコラボレーションを構成する	オプション。 DRX と LB の連携により、弾力性のあるサービス リソース プールが提供されます。

## DRXサービスを追加する

1. 上部のナビゲーション バーで、**Services**をクリックします。
2. **Add DRX Service**をクリックします。
3. 必要に応じて DRX サービス パラメーターを設定します。ロード バランサーは後でバインドできます。

パラメーター	説明
Cluster	DRX サービスのクラスターを選択します。
Storage	自動的に作成される VM の共有ストレージ プールを指定します。
Backup Cluster	DRX サービスを実行するバックアップ クラスターを指定します。現在のクラスターが DRX 要件を満たすことができない場合、バックアップ クラスターに VM が作成されます。バックアップ クラスターに VM を作成するには、リソースのインポートタイプが <b>Fast Clone</b> に設定されているときに、クラスターとそのバックアップ クラスターが同じ共有ストレージを使用する必要があります。
VM	DRX サービスでサポートされる VM の最大数を指定します。これは、VM グループで許可される VM の最大数です。
Effective	DRX サービスを有効にする方法を選択します。オプションには、 <b>Now</b> 、 <b>Custom</b> 、と <b>No</b> があります。 <ul style="list-style-type: none"> <li>• <b>Now</b> - DRX サービスは、作成後すぐに有効になります。</li> <li>• <b>Custom</b> - DRX サービスは指定された時間範囲で有効になります。</li> <li>• <b>No</b> - DRX サービスは有効になりません。</li> </ul>
Start Time	DRX サービスが有効になる開始時刻を指定します。このフィールドは、 <b>Effective</b> リストから <b>Custom</b> を選択した場合に必須です。開始時刻のみを設定すると、DRX サービスは常にこの時刻から有効になります。

パラメーター	説明
End Time	DRX サービスが有効になる終了時刻を指定します。このフィールドは、EffectiveリストからCustomを選択した場合は必須です。終了時刻のみを設定すると、DRX サービスは現在の時刻から終了時刻まで有効になります。
Bind Load Balance	ロードバランサーを DRX サービスにバインドするかどうかを構成します。

4. **Next**をクリックし、期間と検出間隔を設定します。

パラメーター	説明
Duration	拡張監視ポリシーで VM グループ内の VM の平均 CPU 使用率とメモリ使用量、および接続数がしきい値を複数回超える時間、または再利用監視ポリシーでしきい値を複数回下回る時間を指定します。
Detection Interval	VM グループ内の VM の CPU 使用率、メモリ使用量、接続を検出する間隔を指定します。

5. **Resource Import Settings**をクリックし、**Edit** アイコンをクリックして 必要に応じて設定を編集します。

パラメーター	説明
--------	----





パラメーター	説明
Resource Import Settings	拡張機能監視ポリシーで、VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続数、ネットワークトラフィック、ディスク I/O、および IOPS がしきい値を複数回超えると、VM グループ内に VM が自動的に作成されます。
Import Mode	DRX サービスに対応する VM グループに VM を作成するモードを選択します。オプションには、 <b>Fast Deployment</b> と <b>Fast Clone</b> があります。 <ul style="list-style-type: none"> <li>• <b>Fast Deployment</b> -選択した VM テンプレートを通じて VM グループ内に VM が作成されます。</li> <li>• <b>Fast Clone</b> -クローンする VM を選択することで、VM グループ内に VM が作成されます。</li> </ul>
VMs to Create	1 つの DRX タスクに対して作成する VM の数を指定します。

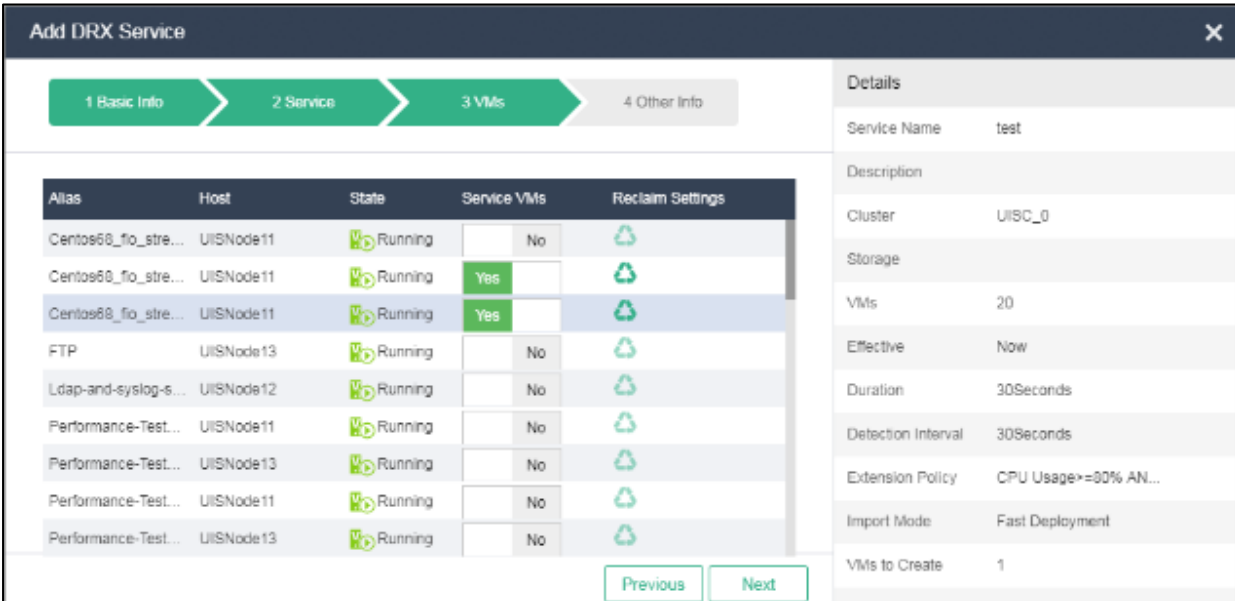
6. **Resource Reclaim Settings**をクリックし、**Edit**アイコンをクリックして 必要に応じて設定を構成し、**Next**.をクリックします。










パラメーター	説明
Resource Reclaim Settings	VM グループ内の VM の平均 CPU 使用率、平均メモリ使用量、接続数、ネットワークトラフィック、ディスク I/O、および IOPS が、リソース再利用監視ポリシーのしきい値を複数回下回ると、VM グループ内の VM は自動的に再利用されます。
Reclaim Type	回収タイプを選択します。オプションには、 <b>Reclaim Now</b> と <b>Slow-Offline</b> があります。 <ul style="list-style-type: none"> <li>• <b>Reclaim Now</b> -再利用条件が満たされている限り、VM は再利用されません。</li> <li>• <b>Slow-Offline</b> -再利用条件が満たされると、システムは VM が TCP パケットを受信するのを阻止し、VM によって送信されたパケットの数が 10 秒ごとにしきい値より小さいかどうかを識別します。数がしきい値より小さい場合、システムは VM を直ちに再利用します。数がしきい値より小さくない場合、システムは数がしきい値より小さくなるかタイムアウトに達するまで VM を再利用しません。</li> </ul>
Threshold	低速オフライン VM 再利用をトリガーできる VM によって送信されるパケットの最大数を指定します。このフィールドは、再利用タイプとして <b>Slow-Offline</b> を選択した場合にのみ必須です。



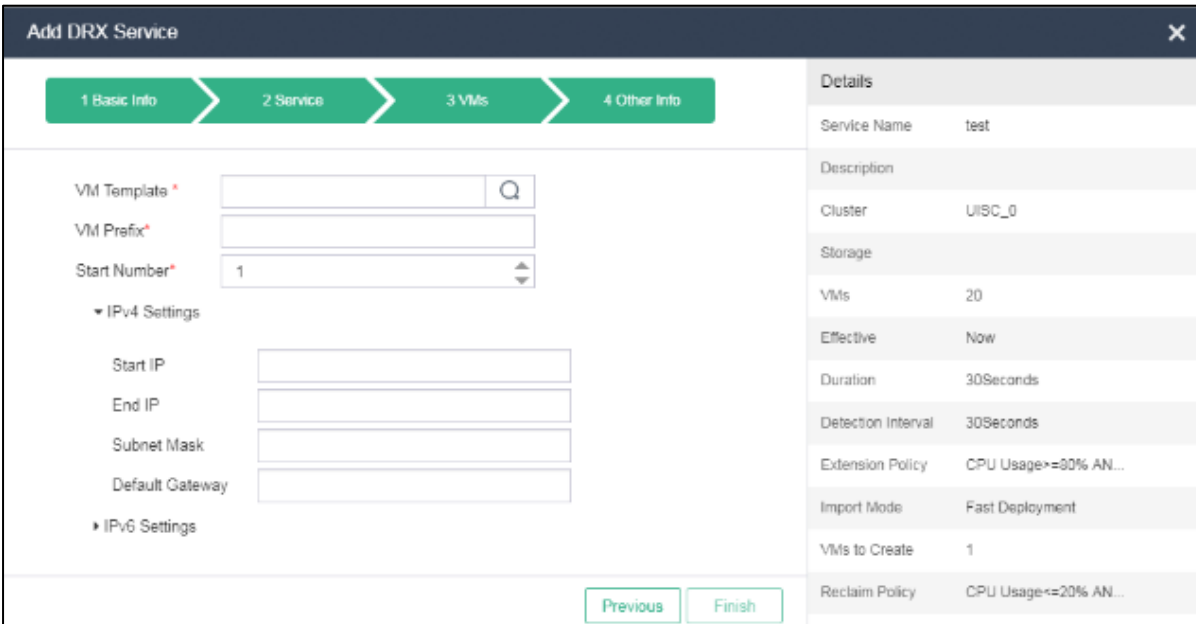
パラメーター	説明
Timeout	低速オフライン VM 再利用をトリガーできるタイムアウトを指定します。このフィールドは、再利用タイプとして <b>Slow-Offline</b> を選択した場合にのみ必要です。
Reclaim Mode	VM を再利用するモードを選択します。オプションには、 <b>Shut Down VM</b> 、 <b>Delete VM</b> と <b>Put VM to Sleep</b> などがあります。 <ul style="list-style-type: none"> <li>• <b>Shut Down VM</b> - VM の電源をオフにします。</li> <li>• <b>Delete VM</b> - VM を削除します。</li> <li>• <b>Put VM to Sleep</b> - VM を休止状態にします。</li> </ul>
Min. Running VMs	リソース再利用タスクで実行状態にある必要がある VM の最小数を指定します。

7. 同じサービスを実行する VM を VM グループに追加し、 または  アイコンをクリックして、必要に応じて VM を自動的に再利用するかどうかを構成します。 は VM を自動的に再利用することを示し、 は VM を自動的に再利用しないことを示します。



Alias	Host	State	Service VMs	Reclaim Settings
Centos68_fo_stre...	UISNode11	Running	No	
Centos68_fo_stre...	UISNode11	Running	Yes	
Centos68_fo_stre...	UISNode11	Running	Yes	
FTP	UISNode13	Running	No	
Ldap-and-syslog-s...	UISNode12	Running	No	
Performance-Test...	UISNode11	Running	No	
Performance-Test...	UISNode13	Running	No	
Performance-Test...	UISNode11	Running	No	
Performance-Test...	UISNode13	Running	No	

8. **Next**をクリックし、必要に応じて拡張機能の設定を構成し、**Finish**をクリックします。



パラメーター	説明
VM Template	高速展開用の VM テンプレートを選択します。このパラメーターは、リソースのインポートタイプとして <b>Fast Deployment</b> を選択した場合にのみ必要です。
VM to Clone	クローンする VM を選択します。このパラメーターは、リソースのインポートタイプとして高速クローンを選択した場合にのみ必要です。クローンする VM は、選択した VM グループからのみ選択でき、VM は次の要件を満たしている必要があります。 <ul style="list-style-type: none"> <li>• イメージファイルは共有ストレージプールにあります。</li> <li>• VM 上に USB、PCI、SR-IOV、または TPM デバイスが存在しません。</li> <li>• VM は NUMA ノードまたは物理 CPU にバインドされていません。</li> <li>• VM のストレージタイプはインテリジェントです。</li> </ul>
VM Prefix	VM グループに作成する VM のプレフィックスを入力します。
Start Number	VM の開始番号を入力します。この番号は VM プレフィックスの後に表示されません。作成された VM の数が増えると、最大数に達するまで番号も増加します。
IPv4 Configuration	<ul style="list-style-type: none"> <li>• 開始 IP : VM の開始 IPv4 アドレスを指定します。</li> <li>• 終了 IP : VM の終了 IPv4 アドレスを指定します。IP 割り当てに十分な IPv4 アドレスを予約します。</li> <li>• サブネットマスク: VM のサブネットマスクを指定します。</li> <li>• デフォルト ゲートウェイ: VM のデフォルト ゲートウェイを指定します。</li> </ul>
IPv6 Configuration	<ul style="list-style-type: none"> <li>• 開始 IP: VM の開始 IPv6 アドレスを指定します。</li> <li>• 終了 IP: VM の終了 IPv6 アドレスを指定します。IP 割り当てに十分な IPv6 アドレスを予約します。</li> <li>• ネットワークプレフィックス: IPv6 アドレスのプレフィックスの長さを指定します。</li> <li>• デフォルト ゲートウェイ: VM のデフォルト ゲートウェイを指定します。</li> </ul>

## DRXサービス監視ポリシーを構成する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**DRX > DRX service name**を選択します。
2. **Resource Monitoring**をクリックします。
3. 必要に応じてサービス監視設定を編集します。

## Service Monitor Settings



Configure the load monitoring parameters and schedule policies for the DRX service. The system automatically creates VMs when the threshold and duration set in the extension policy are reached and automatically reclaims VMs when conditions set in the reclaim policy are matched.

Duration\*  Seconds

Interval\*  Seconds

Extension Policy\* CPU Usage $\geq$ 80% AND Memory Usag...

Reclaim Policy\* CPU Usage $\leq$ 20% AND Memory Usag...

OK

Cancel

## スケジュールされた拡張ポリシーを追加する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**DRX > DRX service name**を選択します。
2. **Scheduled Extension Policy**をクリックします。
3. **Add**をクリックします。

The screenshot shows a dialog box titled "Add Scheduled Extension Policy". It contains the following fields and controls:

- Name\***: Text input field.
- Description**: Text input field.
- VMs to Create\***: Dropdown menu.
- Frequency**: Dropdown menu with "Monthly" selected.
- Date\***: Spinners for "1" and "Day".
- Start Time\***: Spinners for "Hour" and "Min".
- End Time\***: Spinners for "Hour" and "Min".
- Now**: A checkbox with the label "Off".

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

4. 必要に応じてポリシー パラメーターを設定し、**OK**をクリックします。
  - 頻度を **Daily**に設定し、開始時刻を UIS マネージャーの現在のシステム時刻よりも早く設定すると、スケジュールされた拡張タスクは翌日に有効になります。
  - スケジュールされた拡張のデフォルトのポーリング間隔は 10 分です。指定された期間中は DRX は実行されません。
  - スケジュールされた拡張ポリシーで指定されていない期間中、ポリシーを使用して作成された VM は、リソース再利用ポリシーを満たしている場合に再利用されます。

## 垂直拡張ポリシーを構成する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから **DRX > DRX service name**を選択します。
2. **Vertical Extension Policy**をクリックします。
3. CPU とメモリのパラメーターを設定し、**OK**をクリックします。

Vertical Extension Policy
✕

A DRX service can adjust the CPU and memory resources in a VM group based on the extension policy.

Configure CPU

CPU Usage >\*  %

CPUs to Add\*  Sockets

Limit\*  Cores

Configure Memory

Memory Usage >\*  %

Memory to Add\*  GB

Limit\*  GB

パラメーター	説明
Configure CPU	CPU 使用率による垂直拡張ポリシーを有効にするには、このオプションを選択します。
CPU Usage	CPU 使用率のしきい値を指定します。このしきい値に達すると、システムは VM に CPU を追加します。
CPUs to Add	VM に追加する CPU の数を指定します。
Limit	VM に追加できる CPU の最大数を指定します。
Configure Memory	メモリ使用量による垂直拡張ポリシーを有効にするには、このオプションを選択します。
Memory Usage	メモリ使用量のしきい値を指定します。このしきい値に達すると、システムは VM にメモリを追加します。
Memory to Add	VM に追加するメモリ サイズを指定します。
Limit	VM に追加できる最大メモリ サイズを指定します。

## LB リソースコラボレーションを構成する

1. 上部のナビゲーション バーで **Services** をクリックし、ナビゲーション ペインから **DRX > DRX service name** を選択します。
2. **Load Balancing** をクリックします。
3. 必要に応じて LB パラメーターを設定し、**OK** をクリックします。

Load Balancing
✕

1 IP Settings
2 Basic Info
3 VMs

▼ IPv4 Settings

Start IP

End IP

Subnet Mask

Default Gateway

▶ IPv6 Settings

Details

Bound IP Type IPv4

Load Balancer

Virtual Server

Virtual Server Type

Virtual Server IP Address

Virtual Server Port

Real Server Farm

Real Server Farm Scheduling Algorithm

Real Server Farm Health Check

Next

パラメーター	説明
Start IP	VM の開始 IP アドレスを入力します。
End IP	VM の終了 IP アドレスを入力します。開始 IP と終了 IP を指定するときは、割り当てるアドレスが十分にあることを確認してください。
Load Balancer	ロード バランサーを選択します。ロード バランサーはトラフィックを実際のサーバーに分散します。
Virtual Server	仮想サーバーを選択します。仮想サーバーは仮想 IP を提供します。仮想サーバーはユーザー要求を受信し、ロード バランサーは要求に応答する実際のサーバーを選択します。
Real Server Farm	サービスを提供する VM を含む実際のサーバー ファームを選択します。
VM Port	サービス ポートを入力します。サービス ポートによって提供されるサービスが異なります。
Scheduling Algorithm	スケジューリング アルゴリズムを選択します。ロード バランサーは、スケジューリング アルゴリズムに基づいて実サーバーを選択します。
Health Check Method	ヘルス チェック方法を選択します。ロード バランサーは、実サーバー ファーム内の実サーバーのヘルス状態をチェックします。実サーバーが使用不可であることが検出された場合、ロード バランサーは実サーバーにユーザー要求を分散しません。実サーバーが回復すると、ロード バランサーは実サーバーにユーザー要求を分散し続けます。このプロセスはユーザーには透過的です。

# クラウドレインボー

Cloud Rainbow は、サービス中断なしでデータセンター間で UIS リソース共有と手動 VM 移行を提供します。

図1クラウドレインボー構成フローチャート

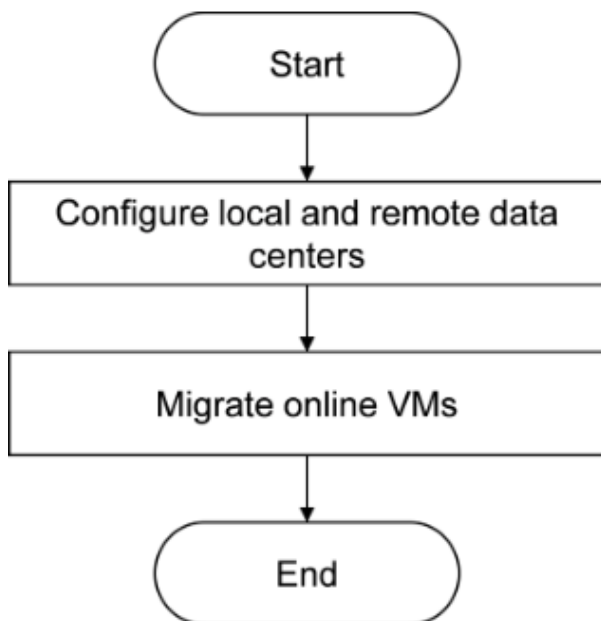
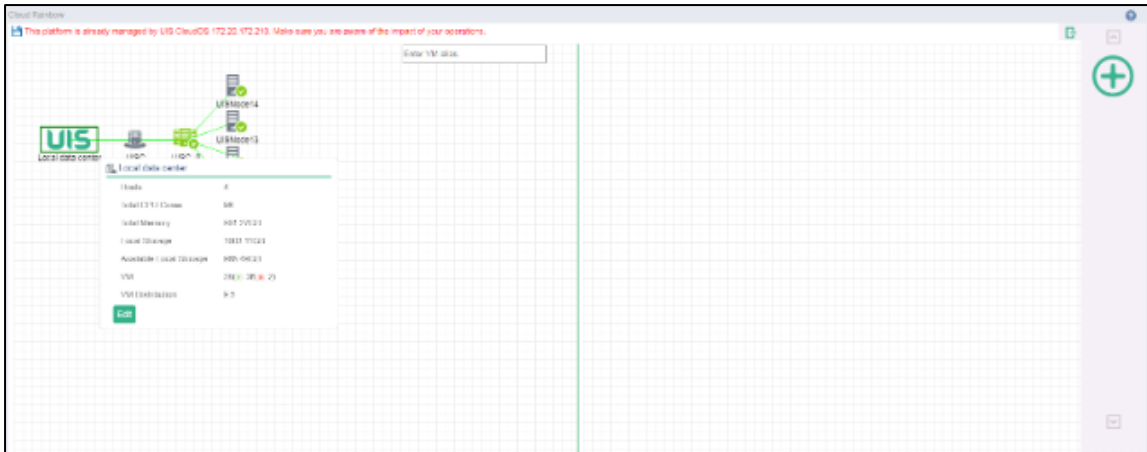


表1クラウドレインボー構成ワークフロー

手順	備考
ローカルおよびリモートのデータセンターを構成する	必須。 ローカルおよびリモート データ センターの IP アドレス、ログイン モード、ユーザー名、およびパスワードを構成するには、このタスクを実行します。
オンラインVM移行を実行する	必須。 2 つのデータセンター間でオンライン VM を移行するには、このタスクを実行します。

## ローカルおよびリモートのデータセンターを構成する

1. 上部のナビゲーション バーで **Services**をクリックし、ナビゲーション ペインから**Cloud Rainbow**を選択します。
2. ローカル データ センター アイコンをクリックし、開いたダイアログ ボックスで**Edit Data Center** をクリックします。



- UIS マネージャーのデータセンター名と管理 IP アドレスを入力し、**OK**をクリックします。

### Configure Local Data Center ✕

Name\*

IP Address\*

Login Mode\* HTTP ✓ HTTPS

Port\*

OK
Cancel

- Add**アイコンをクリックします。開いたダイアログボックスで、ローカル データ センターのパラメーターを構成し、**OK**をクリックします。

### Add Data Center ✕

Name\*

Description

IP Address\*

Login Mode\* HTTP ✓ HTTPS

Port\*

Username\*

Password\*

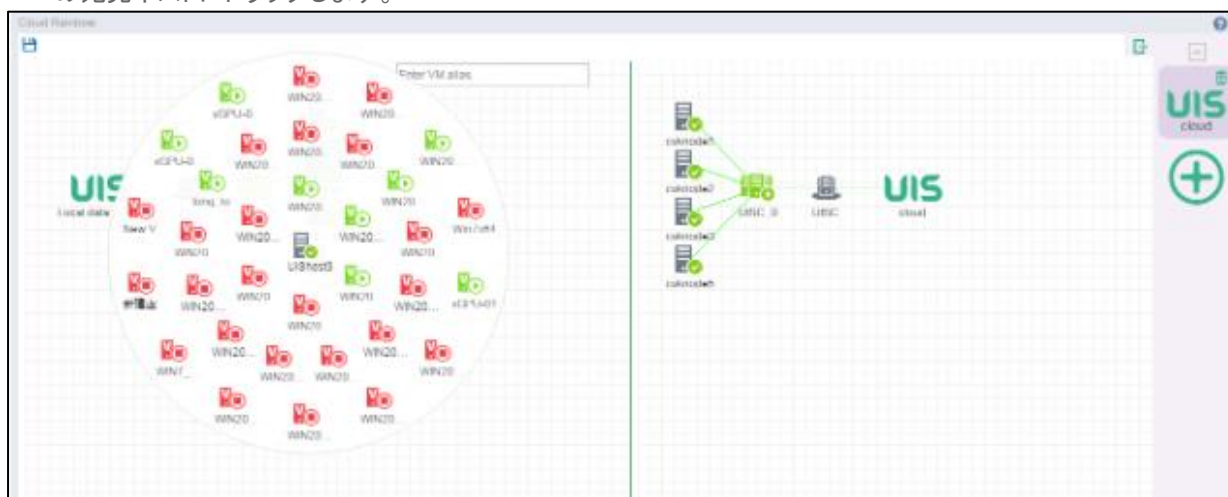
OK
Cancel



パラメーター	説明
Name	データセンターの名前を指定します。中国語または英語で最大 36 文字。必須。
Description	データセンターの説明を指定します。中国語または英語で最大 120 文字。オプション。
IP Address	データセンターの IP アドレスを入力します。ドット付き 10 進表記の IPv4 アドレスである必要があります。必須です。
Login Mode	データセンターにログインする方法を選択します。必須。
Port	データセンターにアクセスするためのポート番号を入力します。HTTP を使用する場合、デフォルトのポート番号は 8080 です。HTTPS を使用する場合、デフォルトのポート番号は 8443 です。必須です。
Username	データセンターにアクセスするためのユーザー名を入力します。必須です。
Password	データセンターにアクセスするためのパスワードを入力します。最大 32 文字の中国語または英語。必須。

## オンラインVM移行を実行する

1. ホストをダブルクリックしてホスト上のすべての VM を表示し、ターゲット VM をリモート UIS マネージャー上の宛先ホストにドラッグします。



2. 必要に応じてパラメーターを設定し、**Next**をクリックします。

パラメーター	説明
Timeout	実行中の VM を移行するための移行タイムアウトを入力します。タイムアウト タイマーが期限切れになる前に VM を移行できない場合、システムは VM を一時停止し、移行後に VM を復元します。
Compress	送信するデータを圧縮するには、このオプションを選択します。

3. 宛先ストレージ プールを選択し、**Finish**をクリックします。
4. タスク コンソールを開いて、VM 移行の進行状況を表示します。

# GPUリソースプールを構成する

図1 GPUリソースプールの構成フローチャート

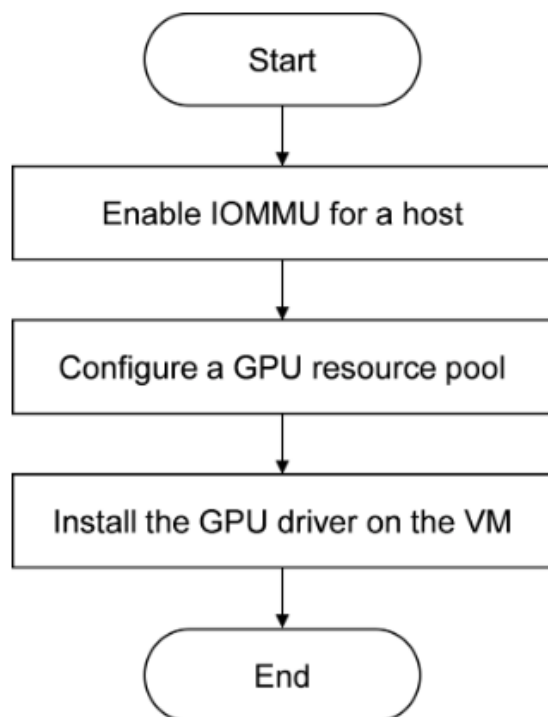
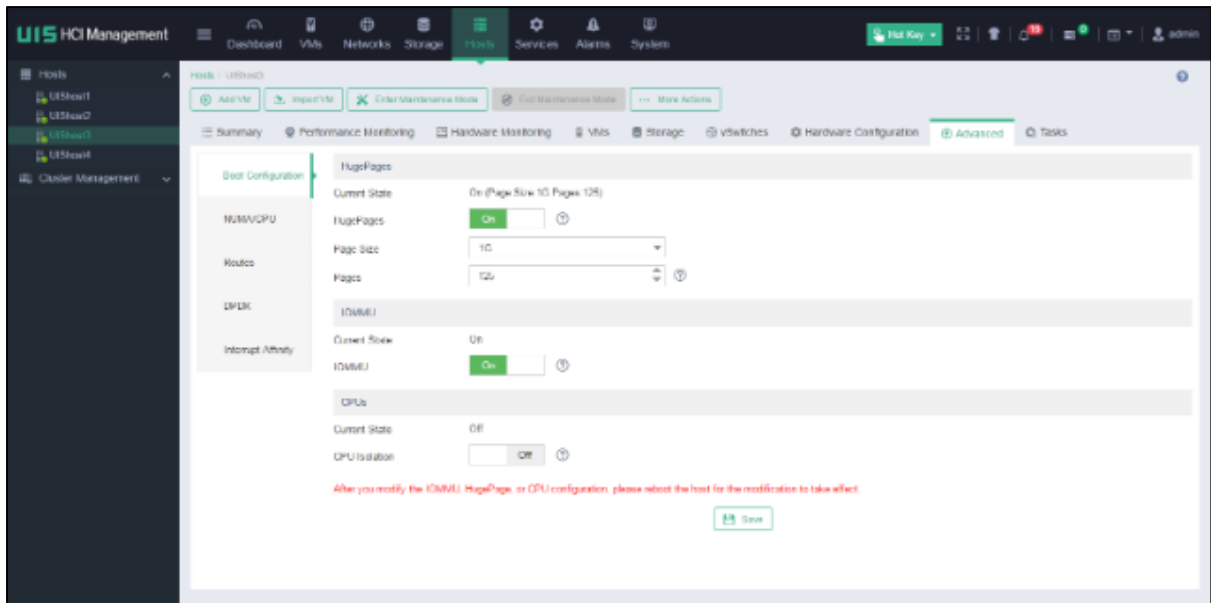


表1 GPUリソースプールの構成ワークフロー

手順	備考
ホストのIOMMUを有効にする	必須。 ホストで GPU パススルーを構成する前に、このタスクを実行してホストの IOMMU を有効にする必要があります。構成を有効にするには、ホストを再起動する必要があります。
GPUパススルーを構成する	必須。 このタスクを実行して、同じクラスター内の異なるホスト上の GPU パススルー用の物理 GPU を GPU リソース プールに追加し、GPU パススルーを使用する VM を VM グループに追加します。 システムは、VM グループ内の VM が起動または再起動すると、GPU リソースプールのリソース使用量と VM の優先度に基づいて VM に GPU を割り当てます。
VMにGPUドライバーをインストールする	必須。 VM が GPU を識別できるように、VM に GPU ドライバーをインストールするには、このタスクを実行します。

## ホストのIOMMUを有効にする

1. 上部のナビゲーション バーで、**Hosts**をクリックします。
2. GPU が搭載されたホストを選択します。
3. **Advanced**タブをクリックし、**Boot Configuration**をクリックします。
4. IOMMU を有効にし、**Save**をクリックします。

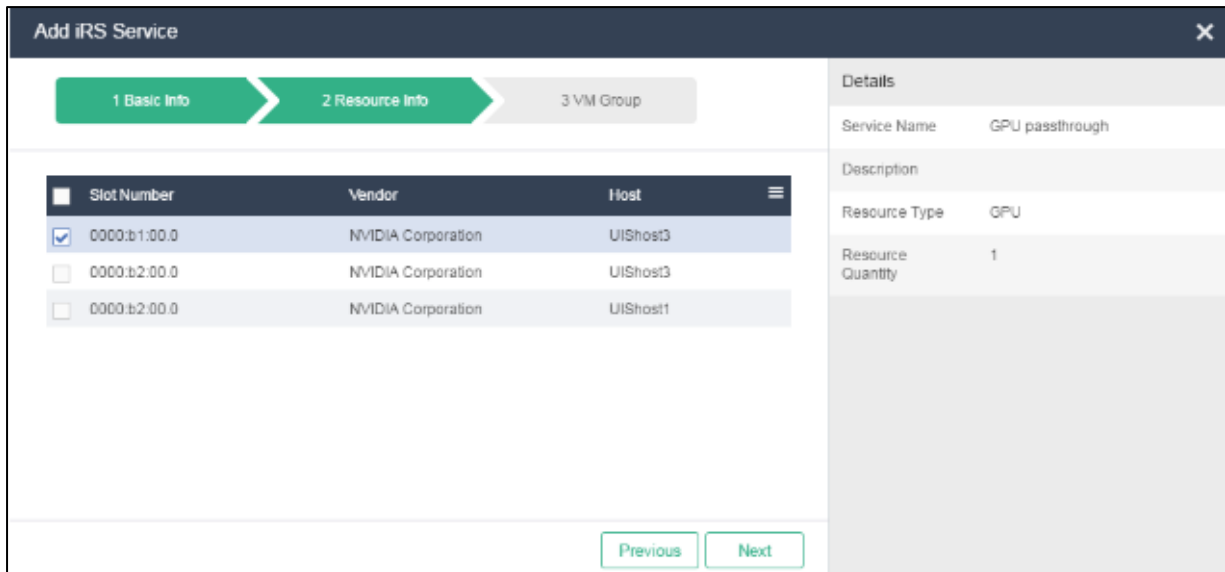


5. Enter Maintenance Mode をクリックします。
6. More Actions をクリックし、Restart Host を選択します。
7. ホストが再起動したら、Exit Maintenance Mode をクリックします。

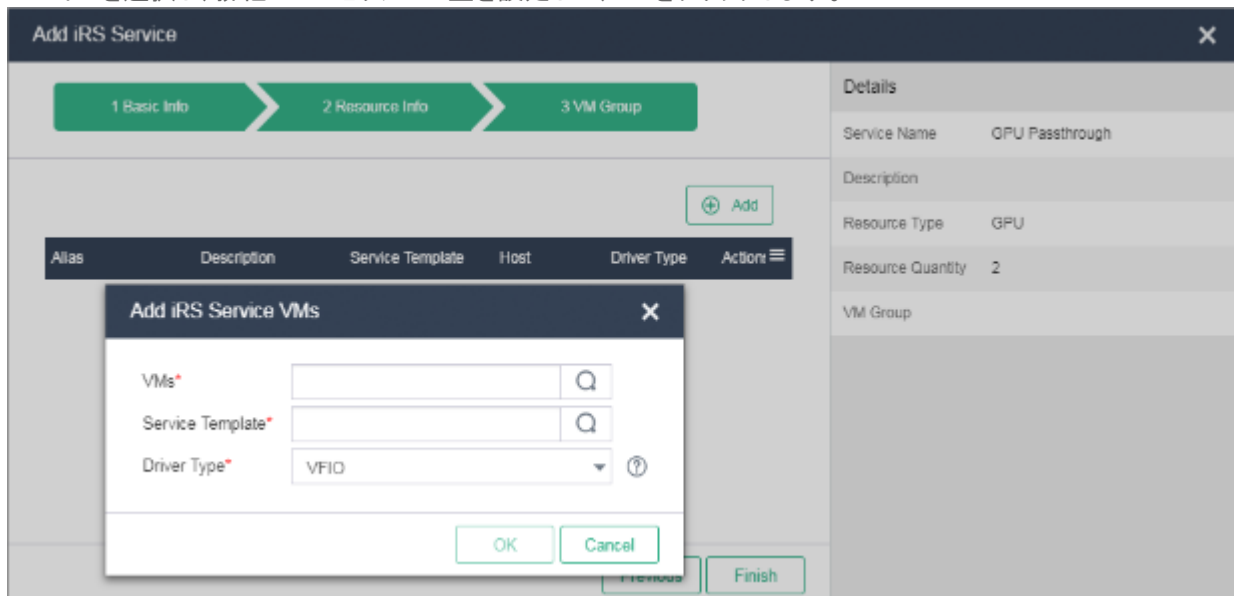
## GPUパススルーを構成する

1. 上部のナビゲーション バーで Services をクリックし、ナビゲーション ペインから iRS を選択します。
2. Add iRS Service をクリックし、サービス名を入力して、Resource Type リストから GPU を選択し、Next. をクリックします。

3. GPU を選択し、Next. をクリックします。



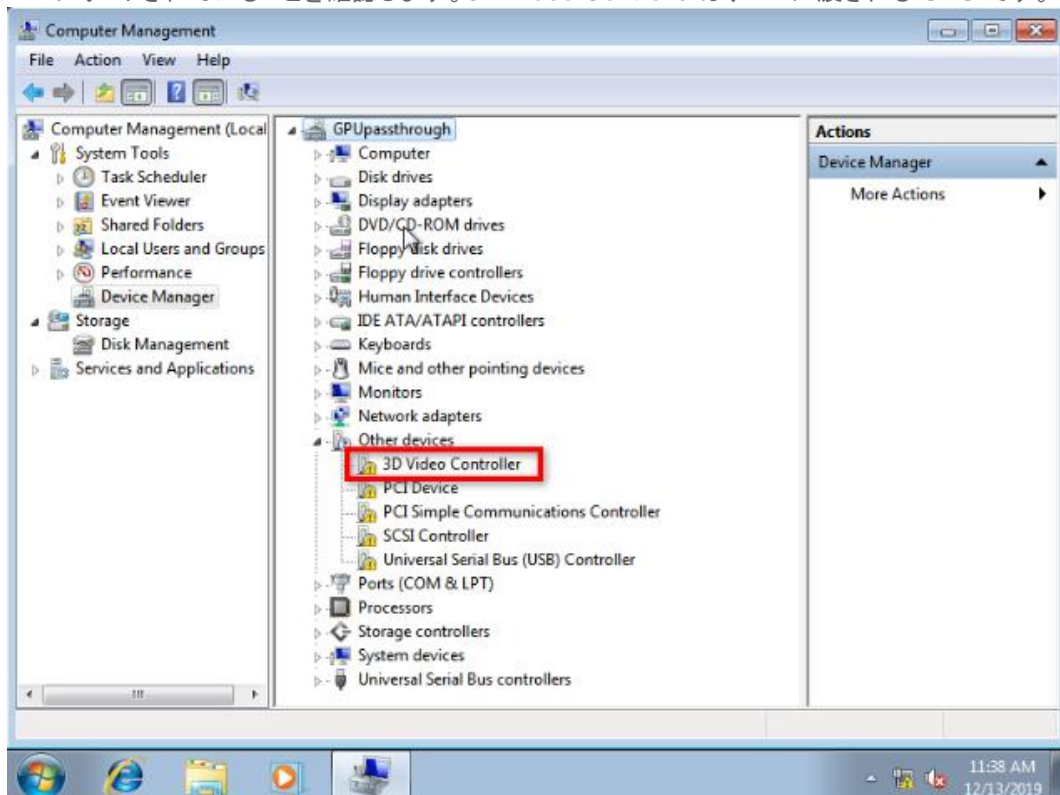
4. VM グループに VM を追加するには、**Add**をクリックします。VM、サービス テンプレート、**VFIO**ドライバー タイプを選択し、排他モードとリソース量を設定して、**OK**をクリックします。



パラメーター	説明
VMs	シャットダウン状態の 1 つまたは複数の VM を選択します。複数の VM を選択した場合、それらの VM は同じサービスを提供する VM グループに割り当てられます。
Service Template	<p>サービス テンプレートを選択します。</p> <p>サービス テンプレートは、サービス テンプレートを使用して物理リソースを使用する VM の優先順位と、サービス テンプレートを使用するすべての VM が使用できるリソースの合計比率を定義します。VM ごとにサービス テンプレートを指定する必要があります。</p> <p>GPU リソースの使用時に VM に高い優先度を割り当てるには、VM に対して優先度の高いサービス テンプレートを選択します。</p> <p>UIS マネージャーは、次のルールに従って GPU リソースを割り当てます。</p> <ul style="list-style-type: none"> <li>VM が同じ優先度のサービス テンプレートを使用する場合、VM ブートシーケンスで GPU リソースを割り当てます。</li> <li>アイドル状態の GPU が起動する VM より少ない場合は、優先順位に従</li> </ul>

パラメーター	説明
	<p>って GPU リソースを割り当てます。</p> <ul style="list-style-type: none"> <li>• 次の条件が満たされた場合、一部の低優先度 VM から GPU リソースを再利用し、高優先度 VM に GPU リソースを割り当てます。</li> <li>○ アイドル状態の GPU は、起動する優先度の高い VM よりも少なくなります。</li> <li>○ 同じ低優先度サービス テンプレートを使用する VM は、サービス テンプレートで指定されたリソース比率よりも多くのリソースを占有します。</li> </ul>
Driver Type	VM で使用されるドライバーのタイプ。VFIO のみが使用可能です。
Exclusive Mode	VM が指定された GPU/vGPU リソースを排他的に使用できるかどうかを選択します。[はい]を選択した場合、GPU/vGPU リソースは他の VM では使用できません。この機能は、選択した GPU リソース プールに追加された使用可能な GPU/vGPU リソースがホストにある場合にのみ使用できます。この機能が有効になっているときに VM を移行するには、ターゲット ホストで十分な GPU/vGPU リソースが使用可能であり、VM がパワーオフになっていることを確認してください。
Resource Count	<p>VM で使用できる GPU/vGPU リソースの最大数を設定します。値は、リソース プールのタイプと排他モード機能の状態によって異なります。</p> <ul style="list-style-type: none"> <li>• vGPU リソース プールを選択した場合、使用できるのは 1 つだけです。</li> <li>• GPU リソース プールを選択し、排他モードが無効になっている場合、値はリソース プール内の単一ホスト上の GPU の最大数になります。たとえば、リソース プールに 3 つのホストがあり、ホストにそれぞれ 3、2、2 個の GPU がある場合、値は 3 になります。</li> <li>• GPU リソース プールを選択し、排他モードが有効になっている場合、値は VM に接続されているホスト上で使用可能な GPU の数になります。</li> </ul>

5. **Finish**をクリックします。
6. ナビゲーション ペインから**GPU**を選択します。作成された VM を右クリックし、**Start**を選択します。
7. VM のコンソールにアクセスします。**Device Manager**を開き、**3D Video Controller**が**Other devices**の下にリストされていることを確認します。3D Video Controllerは、VM に渡される GPU です。

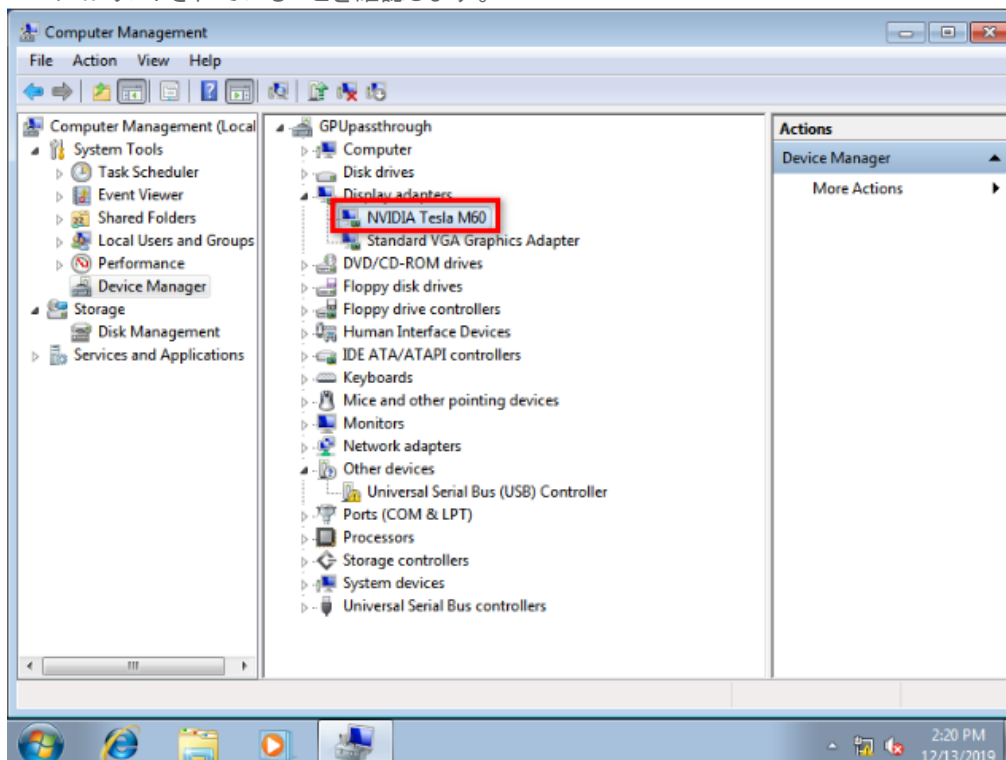


# VMにGPUドライバーをインストールする

1. 互換性のあるNVIDIA GPU ドライバーを VM にアップロードします。
2. GPU ドライバーをインストールします。



3. ドライバーがインストールされたら、**Device Manager**を開き、**Display adapters**の下に正しい GPU モデルがリストされていることを確認します。



# vGPUリソースプールを構成する

図 1 vGPU リソース プールの構成フローチャート

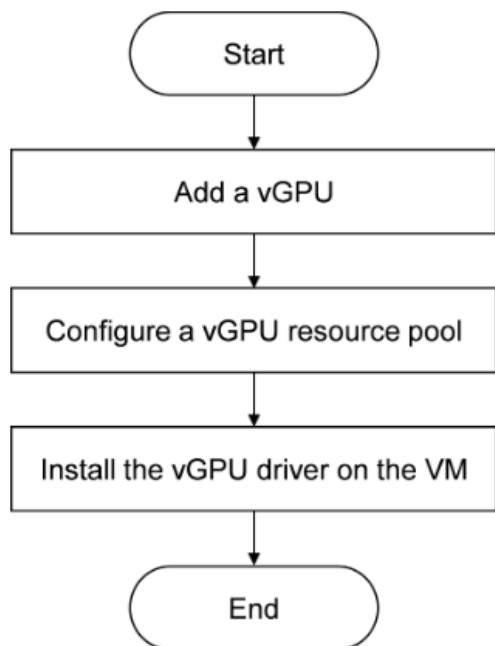
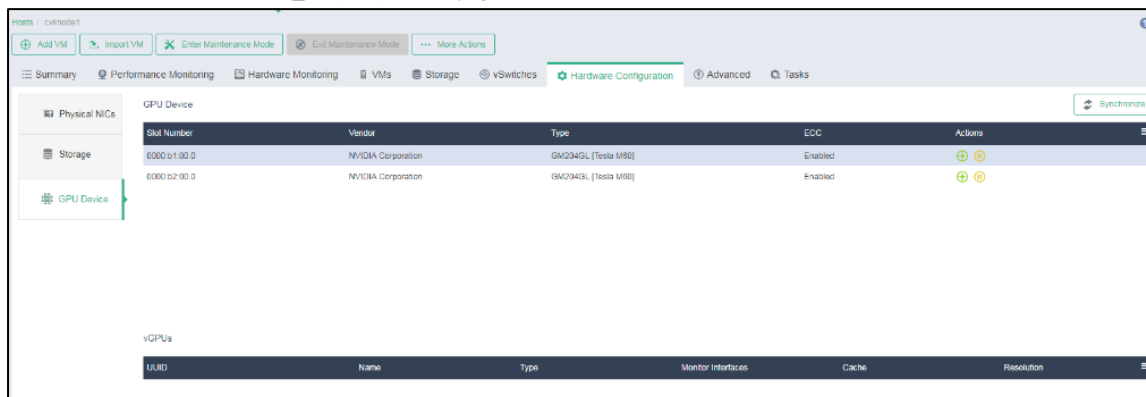


表 1 vGPU リソース プールの構成ワークフロー

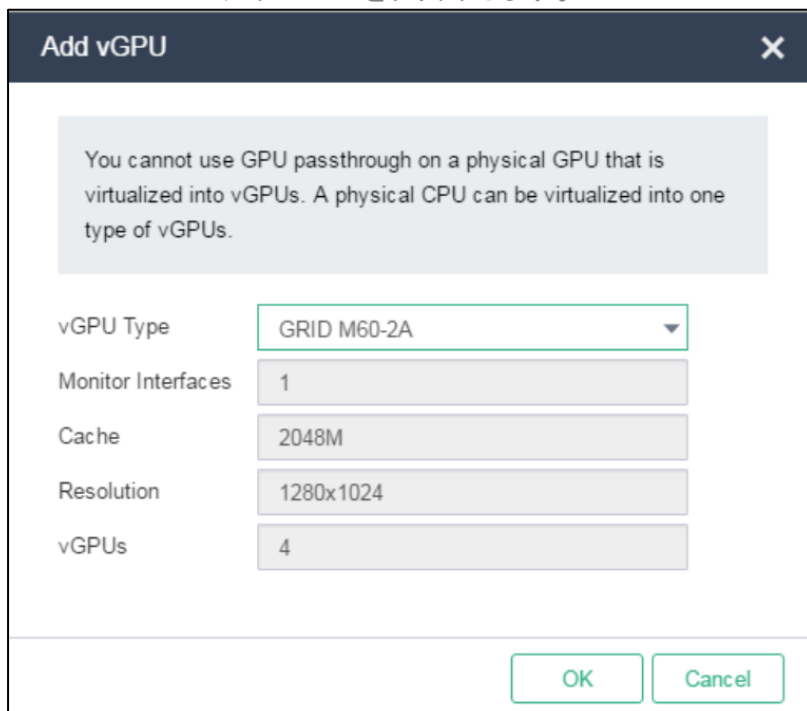
手順	備考
vGPUを追加する	必須。 UIS Manager は、NVIDIA 仮想 GPU テクノロジーを統合して、VM ユーザーに GPU 仮想化サービスを提供します。 vGPU を作成する前に、ホストに NVIDIA GRID vGPU をサポートする GPU がインストールされていることを確認してください。
vGPUリソースプールを構成する	必須。 このタスクを実行して、同じクラスター内の異なるホスト上の vGPU を vGPU リソースプールに追加し、vGPU を使用する VM を VM グループに追加します。 システムは、VM グループ内の VM が起動または再起動すると、vGPU リソースプールのリソース使用量と VM の優先度に基づいて、VM に vGPU を割り当てます。詳細については、「vGPU リソース プール」を参照してください。
<ul style="list-style-type: none"><li>Windows VM にNVIDIAグラフィックスドライバーをインストールする</li><li>Linux VMに NVIDIAグラフィックスドライバーをインストールする</li></ul>	必須。 VM が vGPU を識別できるように、VM に NVIDIA グラフィックスドライバーをインストールするには、このタスクを実行します。

## vGPUを追加する

1. 上部のナビゲーションバーで、**Hosts**をクリックします。
2. ターゲットホストを選択し、タブをクリックします。
3. **GPU Devices**タブをクリックします。



4. GPUのAddアイコン をクリックします。



5. vGPUタイプを選択し、**OK**をクリックします。



## vGPUリソースプールを構成する

1. 上部のナビゲーションバーで**Services**をクリックし、ナビゲーションペインから**iRS**を選択します。
2. **Add iRS Service** をクリックし、サービス名と説明を入力し、**Resource Type**リストから**vGPU**を選択して、**Next**をクリックします。

The screenshot shows the 'Add iRS Service' dialog box with the 'Basic Info' step active. The 'Service Name' field is filled with 'vGPU M60-2A', and the 'Resource Type' dropdown is set to 'vGPU'. A 'Next' button is located at the bottom right of the dialog.

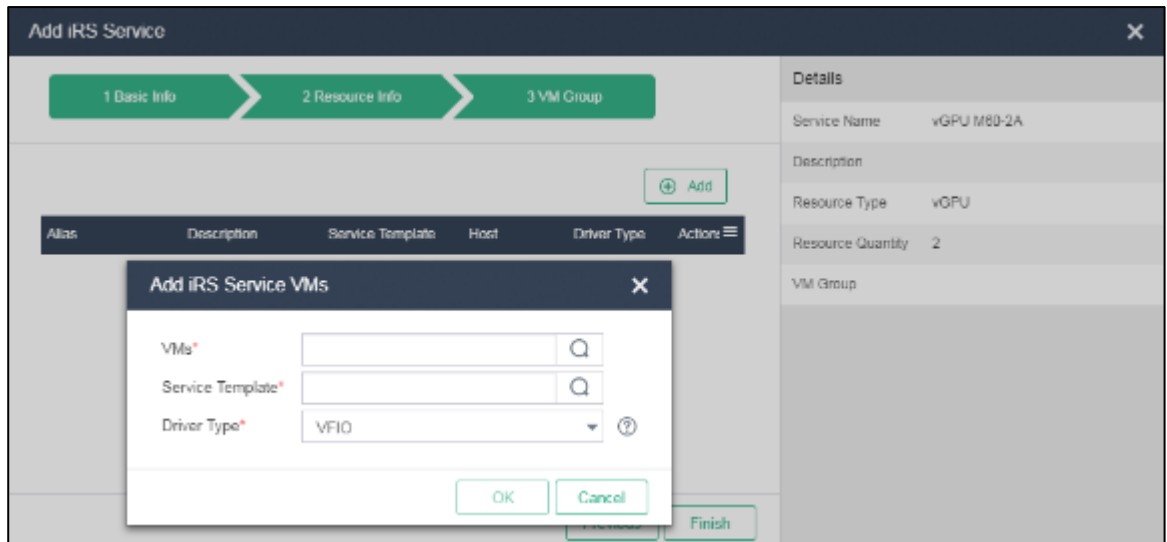
3. 対象の vGPU プール名を選択し、vGPU プールに割り当てる vGPU を選択して、**Next**をクリックします。

1 つの GPU リソース プールに追加できるのは、同じモデルの vGPU のみです。

The screenshot shows the 'Add iRS Service' dialog box with the 'Resource Info' step active. A table lists vGPU resources with columns for UUID, Name, Host, and Slot Number. Two resources are selected. The 'vGPU Name' dropdown is set to 'GRID M60-2A'. 'Add vGPU', 'Previous', and 'Next' buttons are at the bottom.



UUID	Name	Host	Slot Number
<input checked="" type="checkbox"/> 032c2f44-b200-5ce9-0015-1f...	GRID M60-2A	UIShost3	0000 b2-00.0
<input checked="" type="checkbox"/> 56a6b11e-b200-5723-b9fb-c...	GRID M60-2A	UIShost3	0000 b2-00.0
<input type="checkbox"/> c4a70b5fb200-5e05-a77b-0...	GRID M60-2A	UIShost3	0000 b2-00.0
<input type="checkbox"/> e7281c3e-b200-5b4e-8938-b...	GRID M60-2A	UIShost3	0000 b2-00.0

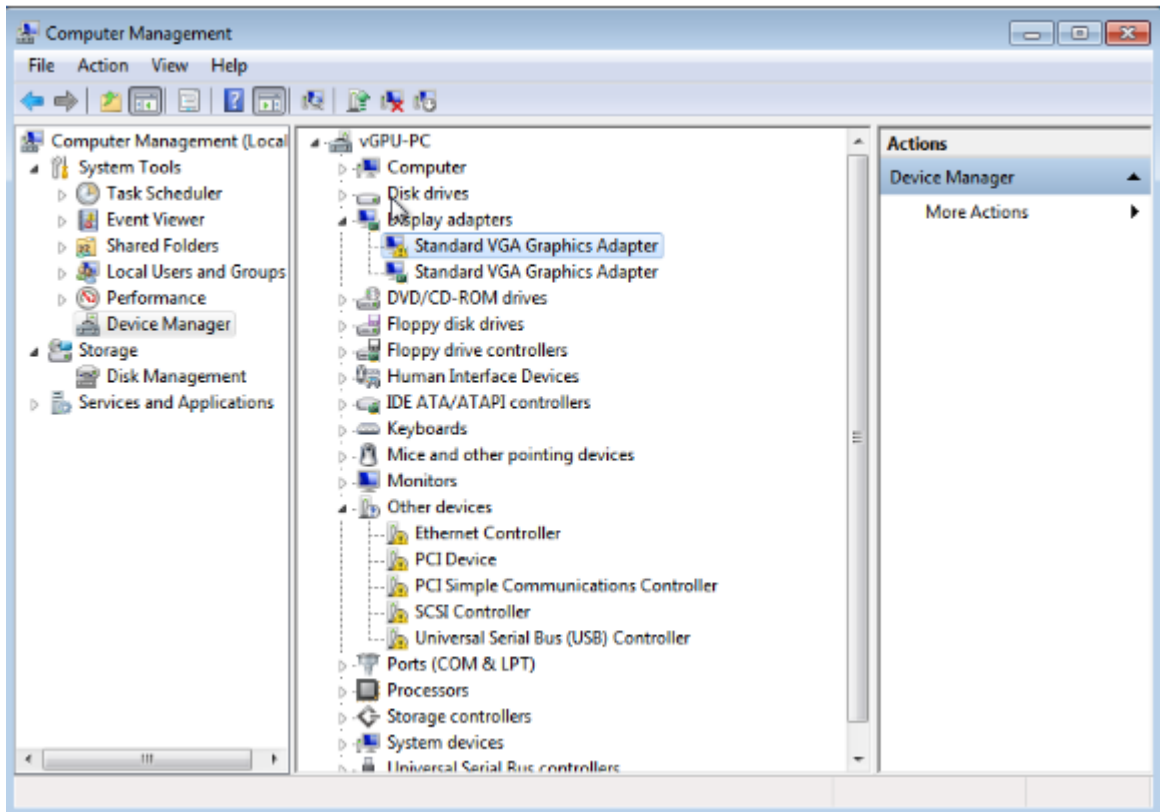
4. サービス VM を追加するには、**Add**をクリックします。



パラメーター	説明
VM	シャットダウン状態の 1 つまたは複数の VM を選択します。複数の VM を選択した場合、それらの VM は同じサービスを提供する VM グループに割り当てられます。
Service Template	<p>サービス テンプレートを選択します。</p> <p>サービス テンプレートは、サービス テンプレートを使用して物理リソースを使用する VM の優先順位と、サービス テンプレートを使用するすべての VM が使用できるリソースの合計比率を定義します。VM ごとにサービス テンプレートを指定する必要があります。</p> <p>vGPU リソースを使用する際に VM に高い優先度を割り当てるには、VM に対して優先度の高いサービス テンプレートを選択します。</p> <p>UIS マネージャーは、次のルールに従って vGPU リソースを割り当てます。</p> <ul style="list-style-type: none"> <li>• VM が同じ優先度のサービス テンプレートを使用する場合、VM ブートシーケンスで vGPU リソースを割り当てます。</li> <li>• アイドル状態の vGPU が起動する VM より少ない場合は、vGPU リソースを優先順位に従って割り当てます。</li> <li>• 次の条件が満たされた場合、一部の低優先度 VM から vGPU リソースを再利用し、高優先度 VM に vGPU リソースを割り当てます。 <ul style="list-style-type: none"> <li>○ アイドル状態の vGPU は、起動する優先度の高い VM よりも少なくなります。</li> <li>○ 同じ低優先度サービス テンプレートを使用する VM は、サービス テンプレートで指定されたリソース比率よりも多くのリソースを占有します。</li> </ul> </li> </ul>
Driver Type	VM で使用されるドライバーのタイプ。VFIO のみが使用可能です。
Exclusive Mode	VM が指定された GPU/vGPU リソースを排他的に使用できるかどうかを選択します。[はい]を選択した場合、GPU/vGPU リソースは他の VM では使用できません。この機能は、選択した GPU リソース プールに追加された使用可能な GPU/vGPU リソースがホストにある場合にのみ使用できます。この機能が有効になっているときに VM を移行するには、ターゲットホストで十分な GPU/vGPU リソースが使用可能であり、VM がパワーオフになっていることを確認してください。

パラメーター	説明
Resource Count	<p>VM で使用できる GPU/vGPU リソースの最大数を設定します。値は、リソース プールのタイプと排他モード機能の状態によって異なります。</p> <ul style="list-style-type: none"> <li>• vGPU リソース プールを選択した場合、使用できるのは 1 つだけです。</li> <li>• GPU リソース プールを選択し、排他モードが無効になっている場合、値はリソース プール内の単一ホスト上の GPU の最大数になります。たとえば、リソース プールに 3 つのホストがあり、ホストにそれぞれ 3、2、2 個の GPU がある場合、値は 3 になります。</li> <li>• GPU リソース プールを選択し、排他モードが有効になっている場合、値は VM に接続されているホスト上で使用可能な GPU の数になります。</li> </ul>

5. **VM**フィールドのアイコン  をクリックし、サービス VM を選択して、**OK**をクリックします。  
 選択した VM はシャットダウン状態である必要があります。複数のサービス VM を選択した場合、同じサービス テンプレートと優先順位が割り当てられます。追加操作を再度実行して、別のサービス テンプレートを別のグループのサービス VM に割り当てることができます。
6. **Service Template**フィールドのアイコン  をクリックし、サービス テンプレートを選択して、**OK**をクリックします。  
 デフォルトでは、定義済みのノンリニア編集サービス テンプレートとトランスコーディング サービス テンプレートがシステムに存在します。必要に応じてサービス テンプレートを追加できますが、デフォルトのテンプレートを含むすべてのサービス テンプレートのリソース割り当て比率の合計が 100% を超えないようにする必要があります。
7. **Finish**をクリックします。
8. 左側のナビゲーション ペインから、追加した vGPU プールを選択します。
9. **VM**タブで、起動する VM を選択し、VM リストを右クリックして**Start**を選択し、開いたダイアログ ボックスで **OK**をクリックします。
10. VM を右クリックし、ショートカット メニューから**Console**を選択して、VM が起動するまで待ちます。
11. VM でデバイス マネージャーを開き、**Display adapters**選択して、vGPU が VM に接続されていることを確認します。

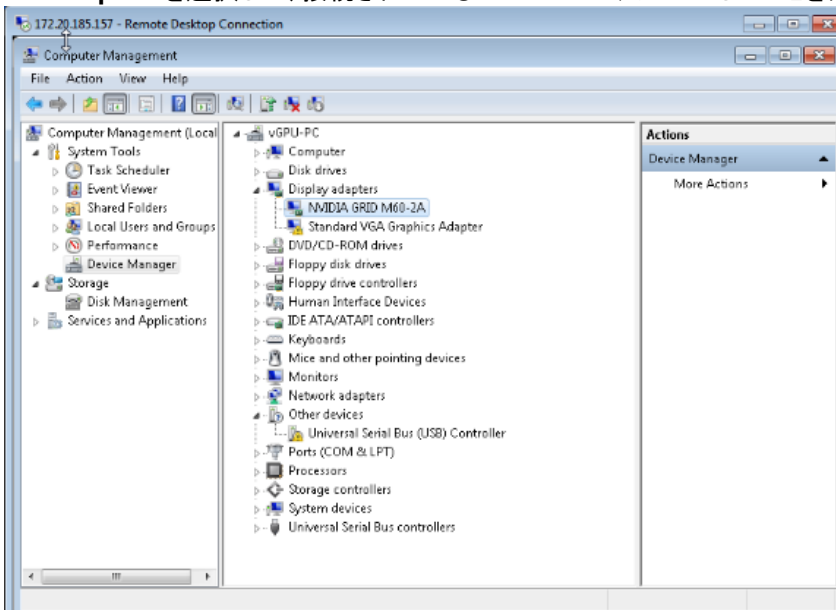


# Windows VMにNVIDIAグラフィックドライバーをインストールする

1. 一致する NVIDIA グラフィックドライバーをダウンロードし、VM にアップロードします。
2. ドライバーインストーラーをダブルクリックし、セットアップウィザードに従ってドライバーをインストールします。



3. VM を再起動します。  
NVIDIA グラフィックドライバーをインストールすると、VNC コンソールは使用できなくなります。RGS や Mstsc などのリモート デスクトップ ソフトウェアを使用して VM にアクセスしてください。
4. リモート デスクトップ ソフトウェアを使用して VM にログインします。デバイス マネージャーを開き、**Display adapters**を選択して、接続されている vGPU のモデルが正しいことを確認します。



# Linux VMにNVIDIAグラフィックドライバーをインストールする

## 制限事項とガイドライン

- Linux VM は、タイプ A を除くすべての vGPU タイプをサポートします。詳細については、NVIDIA Web サイトにアクセスしてください。タイプ A の vGPU は、ドライバーをインストールしても使用できません。
- 一部の Linux オペレーティング システム バージョンのみが vGPU をサポートしています。詳細については、NVIDIA Web サイトを参照してください。
- vGPUドライバーのバージョンは、ホスト上の GPU ドライバーのバージョンによって異なります。たとえば、ホスト GPU ドライバーのバージョンが 440.53 の場合、vGPU ドライバーのバージョンは 440.56 になります。詳細については、NVIDIA Web サイトを参照してください。

表-1ドライバーバージョン対応表(例)

ドライバータイプ	vGPU ソフトウェア	vGPU マネージャー	VM ドライバー (Linux)	VM ドライバー (Windows)
ドライバーバージョン	10.1	440.53	440.56	442.06

## 手順

1. `lspci` コマンドを実行して、vGPU の読み込み状態を表示します。コマンド出力に文字列 **NVIDIA** が含まれている場合、vGPU の状態は正常です。コマンド出力に文字列 **NVIDIA** が含まれていない場合は、テクニカル サポートにお問い合わせください。

図1 vGPUのロード状態

```
[root@localhost ~]# lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 823715B PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 823715B PIIX3 IDE [Natoma/Triton II]
00:01.2 USB controller: Intel Corporation 823715B PIIX3 USB [Natoma/Triton II] (rev 01)
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 03)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Red Hat, Inc Virtio network device
00:04.0 USB controller: Intel Corporation 82801DB/DBM (ICH4/ICH4-M) USB2 EHCI Controller (rev 10)
00:05.0 USB controller: NEC Corporation uPD720200 USB 3.0 Host Controller (rev 03)
00:06.0 SCSI storage controller: Red Hat, Inc Virtio SCSI
00:07.0 Communication controller: Red Hat, Inc Virtio console
00:08.0 SCSI storage controller: Red Hat, Inc Virtio block device
00:09.0 Unclassified device [08ff]: Red Hat, Inc Virtio memory balloon
00:0a.0 VGA compatible controller: NVIDIA Corporation Device 1b38 (rev a1)
```

1. FTP を使用して、NVIDIA Web サイトから取得したドライバーを VM にアップロードします。

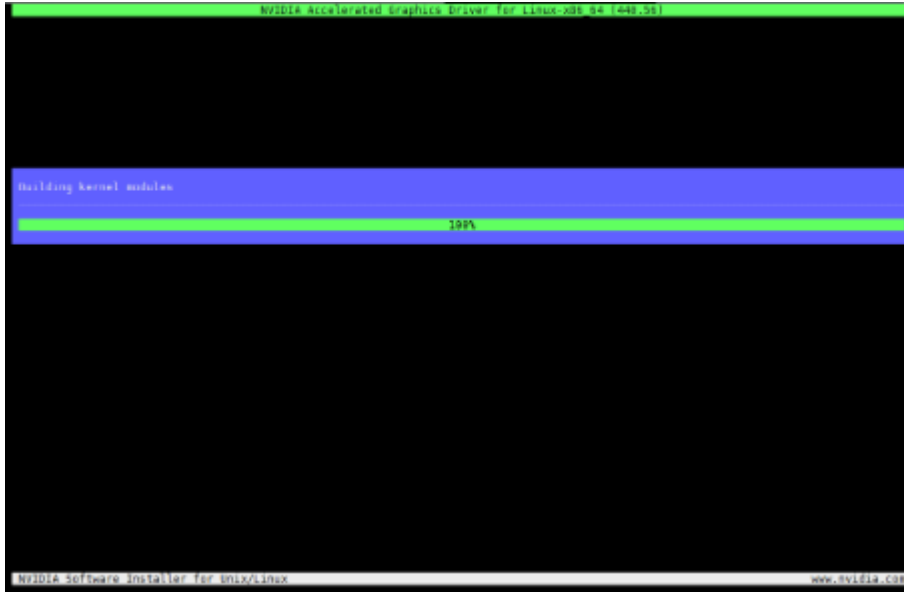
図2 ドライバーのアップロード

```
[root@localhost ~]# ll
total 159352
-rw----- 1 root root 1388 Sep 26 00:13 anaconda-ks.cfg
-rw-r--r-- 1 root root 79640 Sep 26 06:25 dkms-2.8.3-2.el7.noarch.rpm
-rw-r--r-- 1 root root 1609 Sep 26 00:35 initial-setup-ks.cfg
-rwxr-xr-x 1 root root 147691119 Sep 26 00:50 NVIDIA-Linux-x86_64-440.56-grid.run
-rw-r--r-- 1 root root 15389956 Sep 26 00:51 nvidia-vgpu-0.1-1.el7.x86_64.rpm
```

2. VM にドライバーをインストールします。インストールを完了するには、次のコマンドを順番に実行します。

```
[root@localhost ~]# chmod +x NVIDIA-Linux-x86_64-440.56-grid.run
[root@localhost ~]# init 3
[root@localhost ~]# ./NVIDIA-Linux-x86_64-440.56-grid.run
```

図3 インストール完了



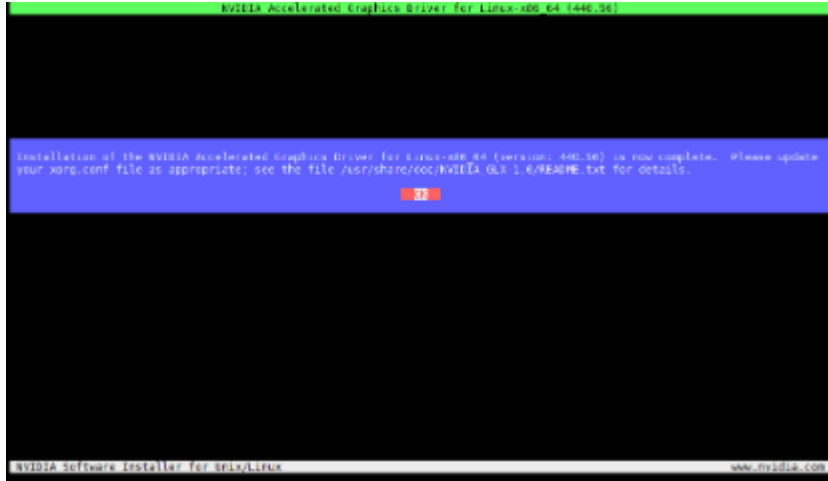
次のエラーが発生した場合は、次のタスクを実行してインストールを完了してください。

図4 インストールエラー



- A 次のコマンドを実行します。  
[root@localhost ~]# sh NVIDIA-Linux-x86\_64-440.56-grid.run -k \$(uname -r)  
インストーラーのプロンプトに次のように応答します。
- EULAに同意する
  - 32ビットバイナリのインストールは避ける
  - x.orgファイルの変更は禁止
- B 図6に示すような結果が返されることを確認します。

図5 実行結果



4. インストール後、`nvidia-smi`コマンドを実行してvGPU 情報を表示します。その後、vGPU を正しく使用できるようになります。

図6 vGPU情報の表示

```
[root@localhost ~]# nvidia-smi
Thu Oct 1 01:04:21 2020
+-----+
| NVIDIA-SMI 440.56      Driver Version: 440.56      CUDA Version: 10.2     |
+-----+-----+-----+-----+-----+-----+
| GPU  Name            Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp            Perf         Pwr:Usage/Cap|      Memory-Usage | GPU-Util  Compute M. |
+-----+-----+-----+-----+-----+-----+
|   0   GRID P40-6C         On          | 00000000:00:0A.0 Off  |      0%      Default  |
|N/A   N/A             P8          N/A /  N/A  |  816MiB /  6144MiB |           |                    |
+-----+-----+-----+-----+-----+-----+
| Processes:                                                       GPU Memory |
|  GPU       PID    Type   Process name                     Usage      |
+-----+-----+-----+-----+-----+
| No running processes found                                     |
+-----+-----+-----+-----+-----+-----+-----+
```

## サイトの災害復旧

災害復旧システムには、地理的に分散したサイトに展開された 2 つ以上の同一のサービス システムが含まれます。災害復旧システムはサービス システムを監視し、サービス システム間のデータの一貫性を維持します。1 つのサービス システムに障害が発生すると、そのサービスは別のサイトにフェールオーバーされ、サービスの継続性が確保されます。UIS は、ストレージ レプリケーション ベースの災害復旧とディスク バックアップ ベースの災害復旧をサポートします。

SRM as a Service を使用すると、UIS で作成された CloudOS VM に対してストレージ レプリケーション ベースのディザスタリカバリを実行できます。SRM as a Service の構成は、ストレージ レプリケーション ベースのディザスタリカバリの構成と似ています。SRM as a Service を使用するには、保護グループを作成するときに、サービス タイプとして SRM as a Service を選択します。

## 特徴

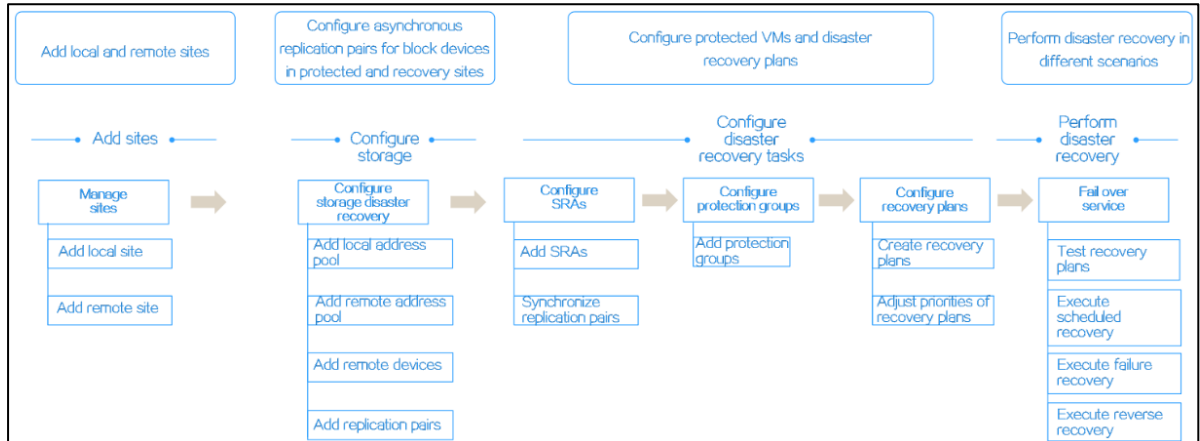
- ストレージの災害復旧を構成する
- ディスクバックアップベースの災害復旧を構成する



# ストレージの災害復旧を構成する

## 設定手順

図1 UIS災害復旧構成手順



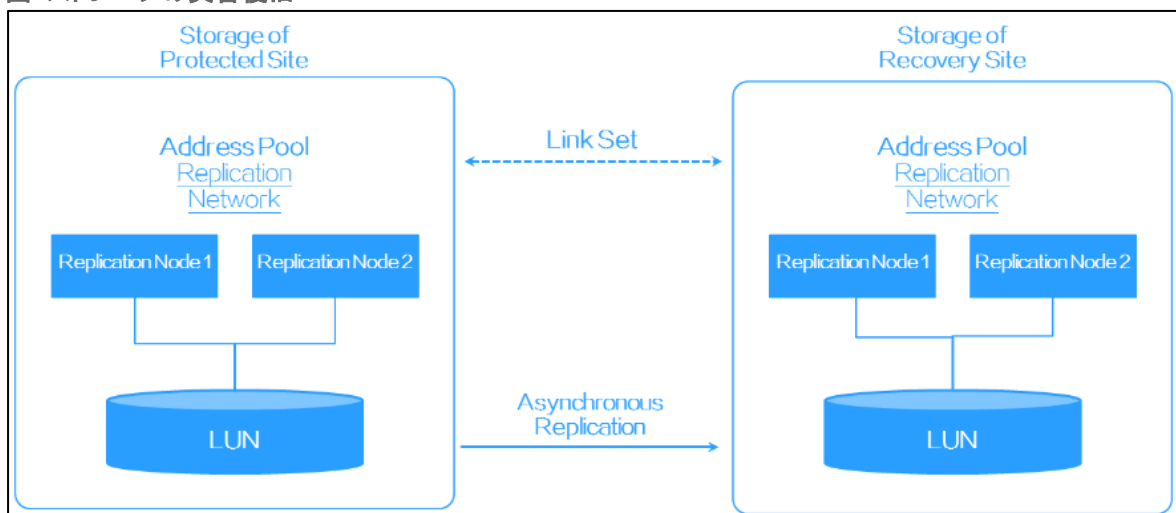
## サイトを構成する

保護サイトとリカバリ サイト (それぞれローカル サイトとリモート サイト) を構成します。ストレージ ディザスタリカバリを構成した後、サイトに SRA を追加し、ブロック デバイス間で非同期レプリケーション ペアを同期します。

## ストレージの災害復旧を構成する

ストレージ障害復旧を実装するには、保護サイトと復旧サイトのブロック デバイス (LUN) 間のマッピングである非同期レプリケーション ペアを作成する必要があります。ブロック デバイスは、サイトのアドレス プール間に確立されたリンクを介して、データ同期ポリシーに基づいてデータを同期します。リンク セットはリモート デバイスと呼ばれます。

図2ストレージの災害復旧

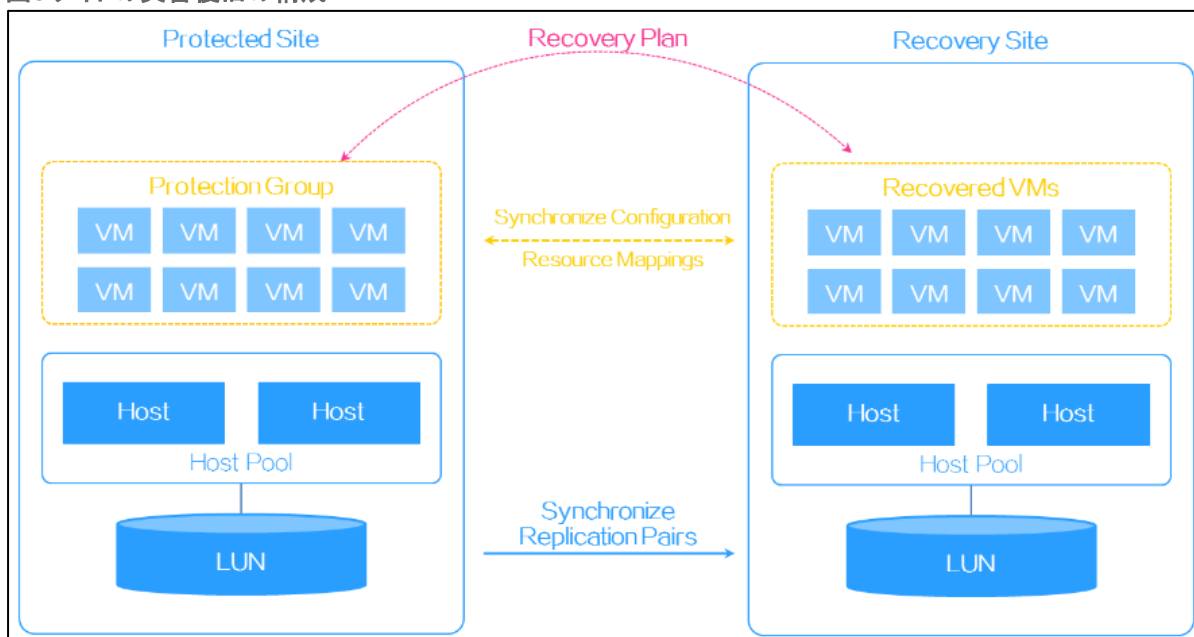


# サイトの災害復旧を構成する

サイトの災害復旧を構成するには、次の手順を実行します。

1. 同じストレージプール (ストレージ アレイ内の 1 つまたは複数の LUN) に接続された VM を保護グループに割り当て、保護サイトとリカバリ サイトの vSwitch、ポート プロファイル、およびストレージ間のマッピングを作成します。
2. 保護グループの回復計画を構成します。

図3サイトの災害復旧の構成

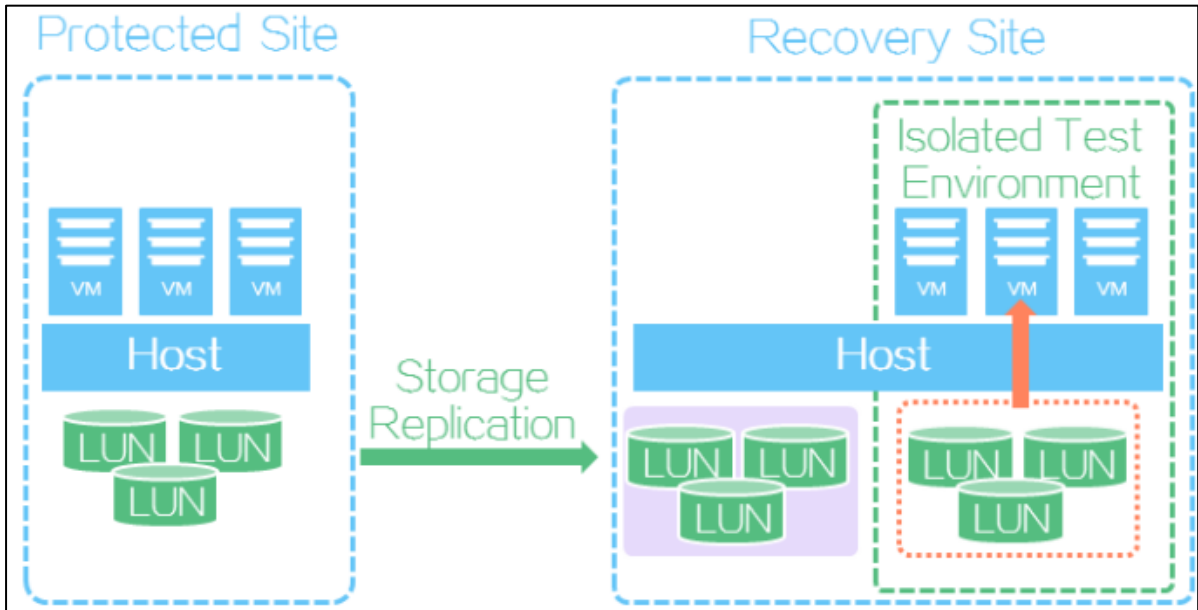


## 災害復旧シナリオ

### 復旧計画テスト

SRM を使用すると、サービスを中断することなく、リカバリ プランに基づいて VM をリカバリ サイトの分離されたテスト環境にフェイルオーバーすることで、リカバリ プランが正しく動作するかどうかをテストできます。リカバリ プラン テストでは、VM はリカバリ サイトの LUN に接続されます。環境をクリアし、リカバリ プランの状態を準備完了に復元するには、リカバリ プラン テストを手動で終了する必要があります。

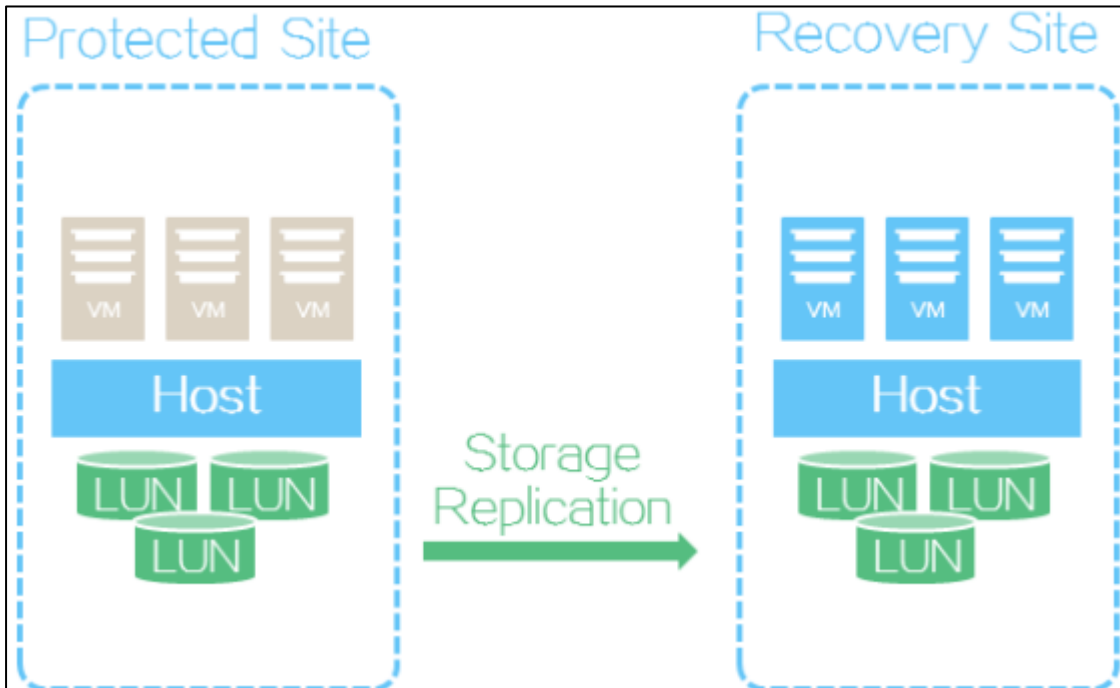
図4復旧計画テスト



## スケジュールされた回復

スケジュールされたリカバリでは、保護されたサイトの VM がシャットダウンされ、保護されたサイトの定期的なメンテナンスのためにスケジュールに従ってリカバリ サイトで VM が再開されます。スケジュールされたリカバリでは、データレプリケーションがトリガーされます。SRM は、保護されたすべてのデータをリカバリ サイトにコピーし終えた後にのみ、リカバリ サイトで VM を再開します。異機種環境では、SRM は保護された VM をシャットダウンしません。保護されたサイトで手動でシャットダウンする必要があります。

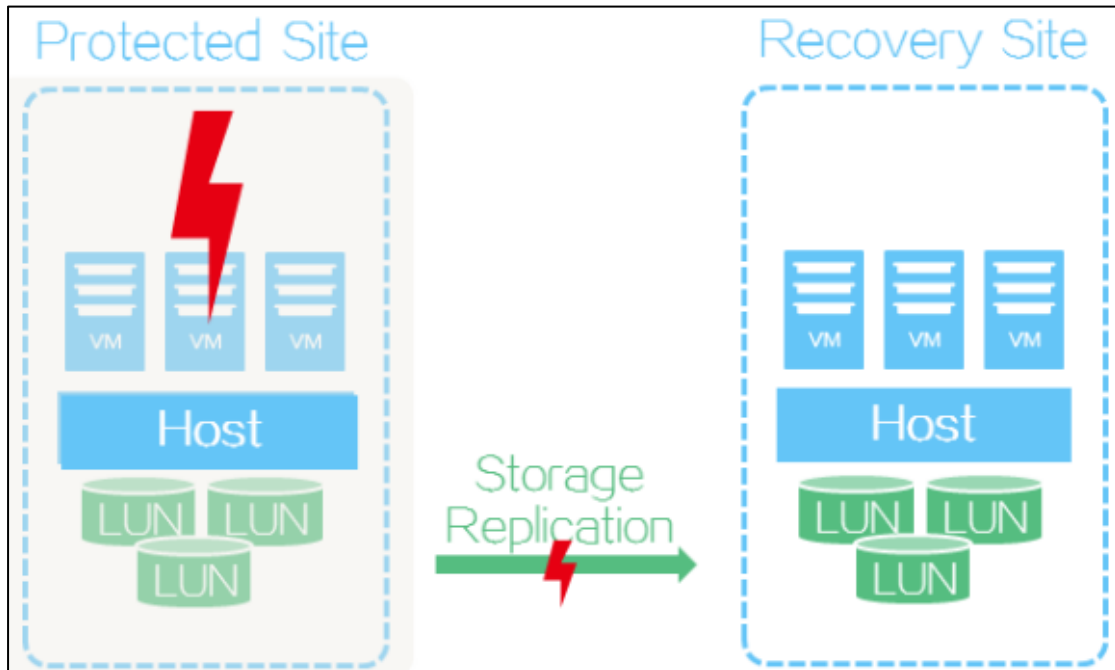
図5スケジュールされた回復



## 障害回復

障害復旧では、復旧計画に基づいて復旧サイトで VM を復元し、保護されたサイトに障害が発生した場合のサービス中断時間を短縮します。

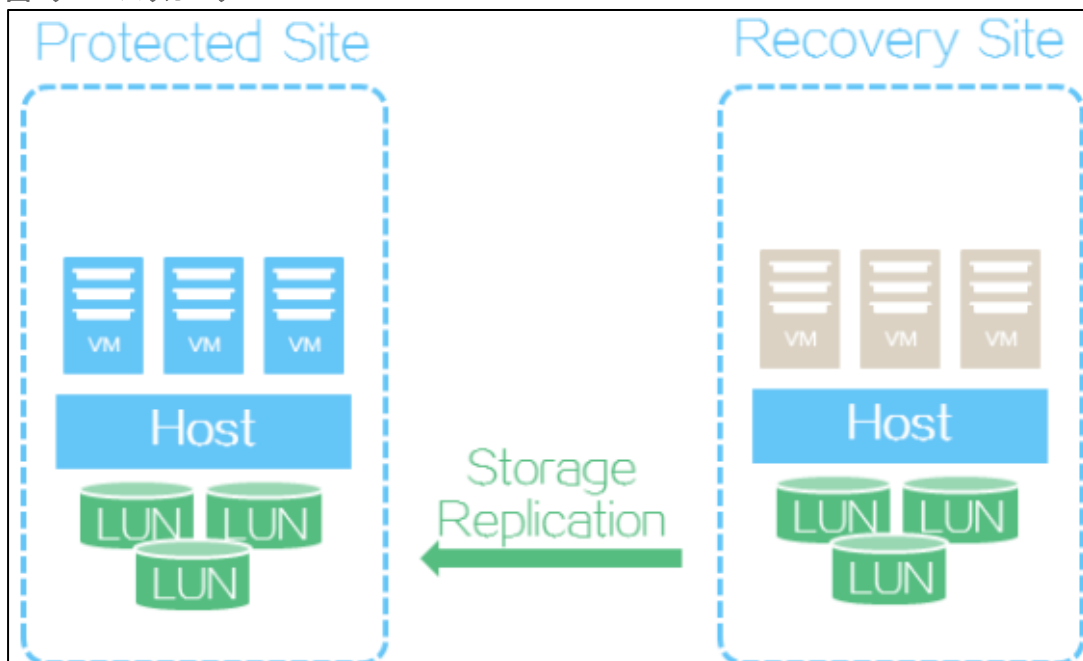
図6障害回復



## リバースリカバリー

リバースリカバリでは、保護されたサイトが障害から回復したときに、VM をリカバリ サイトから保護されたサイトにフォールバックします。

図7リバースリカバリー



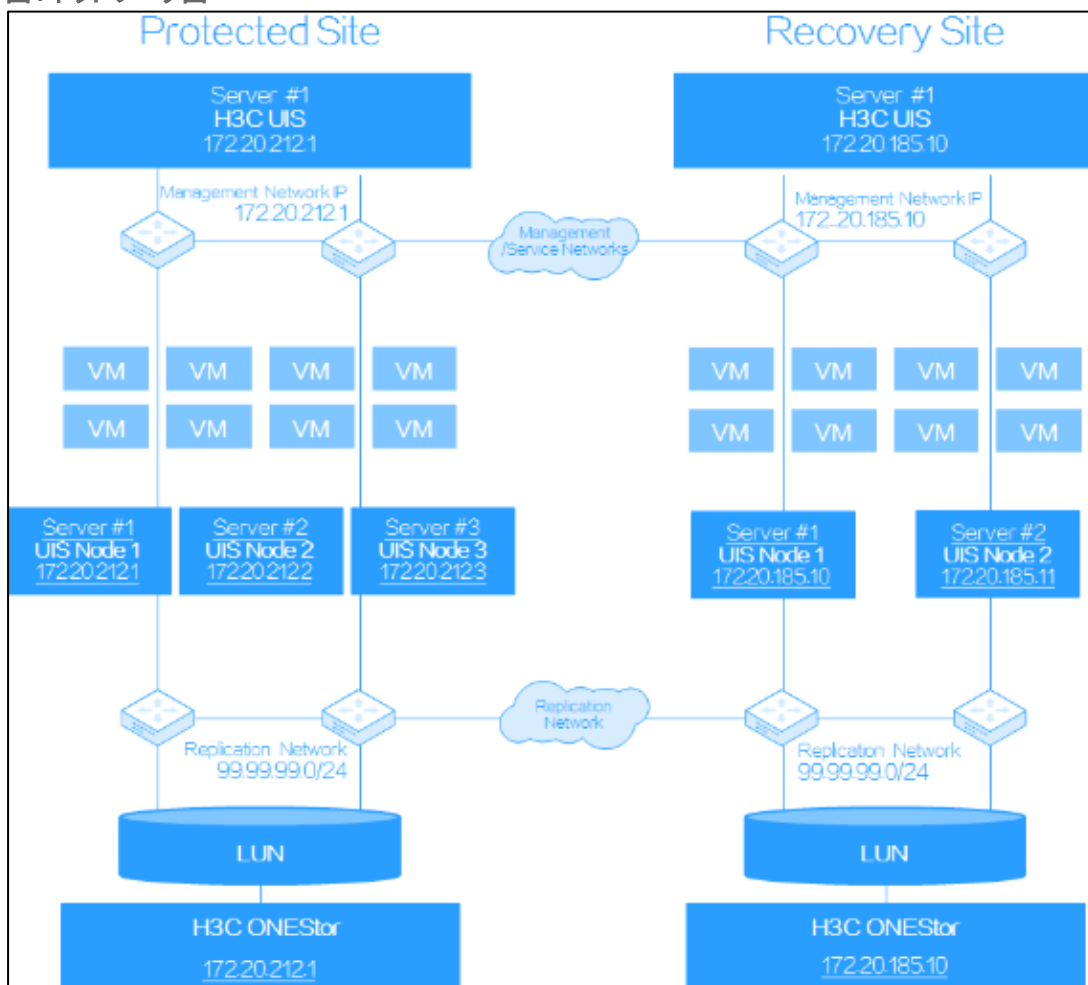
# 制限事項とガイドライン

- リカバリ プランを最初に行う前に、データの同期が実行されていることを確認してください。
- レプリケーション モードのレプリケーション ネットワークは、専用ネットワークまたは共有ネットワークにすることができます。ベスト プラクティスとしては、専用のレプリケーション ネットワークを使用します。
- 次のブロック デバイス要件に従ってください。
  - 実動サイトと復旧サイトのブロック デバイスのサイズを同じに設定します。
  - SRA 以外のストレージの場合、まずバックアップ側でブロック デバイスを共有ファイル システムとしてマウントします。ブロック デバイスが特定のホストにマウントされている場合、リカバリ プランの実行中にストレージの同期がスキップされ、ディザスタ リカバリ VM が直接復元される可能性があります。

# ネットワーク計画

1. 統合デプロイメントで 2 つの UIS システムを展開します。
2. 保護サイトとリカバリ サイトに CVK と ONESstor を展開します。
3. サーバー #1 を管理ノードおよびサービス ノードとして使用します。
4. 保護サイトに 4 つの CVK ホストを展開し、リカバリ サイトに 2 つの CVK ホストを展開します。
5. 専用の管理およびレプリケーション ネットワークをセットアップします。

図1ネットワーク図



# サイトを追加

SRM は、異なるサイト (データ センター) 間でのサービス リカバリを提供します。SRM を使用すると、ローカル UIS マネージャーを保護対象サイトとして構成し、保護対象サイトのリカバリ サイトを構成できます。保護対象サイトがサービスの提供を停止すると、リカバリ サイトが引き継いで中断のないサービスを保証します。

- ・保護サイトまたはリカバリ サイトのいずれかにローカル サイトとリモート サイトを構成します。サイトは構成を同期します。
- ・サイトの作成中に SRA を構成する必要はありません。ストレージ ディザスタ リカバリの構成が完了したら、ローカル サイトとリモート サイトの SRA を構成します。

## ローカルサイトを追加する

1. 保護されたサイトの UIS システムにログインします。
2. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Disaster Recovery Management > Sites** を選択します。
3. **Add Site** をクリックします。
4. ローカルサイトを構成します。

ローカル UIS システムの IP アドレスを入力します。

図1ローカルサイトの追加

Details	
Site Name	near_end
Site Type	Local
IP	172.20.212.1

5. **Next** をクリックします。
6. **Finish** をクリックします。

図2ローカルサイト

Site Name	IP	Username	Site Type	Actions
near_end	172.20.212.1	admin	Local	

## リモートサイトを追加する

1. 上部のナビゲーション バーで **Services** をクリックし、左側のナビゲーション ペインから **Disaster Recovery Management > Sites** を選択します。
2. **Add Site** をクリックします。
3. リモートサイトを構成します。

リモート UIS システムの IP アドレスを入力します。

図3リモートサイトの追加

1 Site Info      2 Storage Array Info

Site Name\*      far\_end

Site Type      Remote

IP\*      172.20.185.10

Username\*      admin

Password\*      .....

Next

Details

Site Name	far_end
Site Type	Remote
IP	172.20.185.10
Username	admin

4. **Next**をクリックします。
5. **Finish**をクリックします。

図4ローカルサイトとリモートサイト

Site Name	IP	Username	Site Type	Actions
near_end	172.20.212.1	admin	Local	
far_end	172.20.185.10	admin	Remote	

## リモートサイトを追加する

1. 上部のナビゲーション バーで**Services**をクリックし、左側のナビゲーション ペインから**Disaster Recovery Management > Sites**を選択します。
2. **Add Site**をクリックします。
3. リモートサイトを構成します。  
リモート UIS システムの IP アドレスを入力します。

図3リモートサイトの追加

**Add Site**

1 Site Info | 2 Storage Array Info

Site Name\*

Site Type Remote

IP\*

Username\*

Password\*

Next

**Details**

Site Name	far_end
Site Type	Remote
IP	172.20.185.10
Username	admin

4. **Next**をクリックします。
5. **Finish**をクリックします。

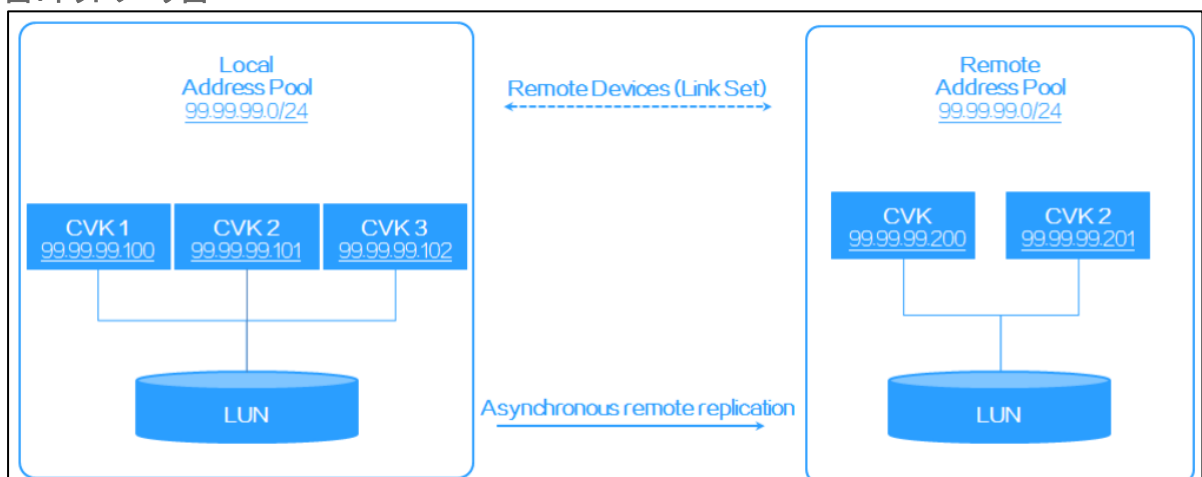
図4ローカルサイトとリモートサイト

Site Name	IP	Username	Site Type	Actions
near_end	172.20.212.1	admin	Local	
far_end	172.20.185.10	admin	Remote	

## ストレージの災害復旧を構成する

- 保護されたサイトの CVK ホストをローカル アドレス プールに割り当て、リカバリ サイトの CVK ホストをリモート アドレス プールに割り当てます。
- アドレス プールのリモート デバイスを作成し、非同期レプリケーション設定を構成します。

図1ネットワーク図



## アドレスプールを追加する

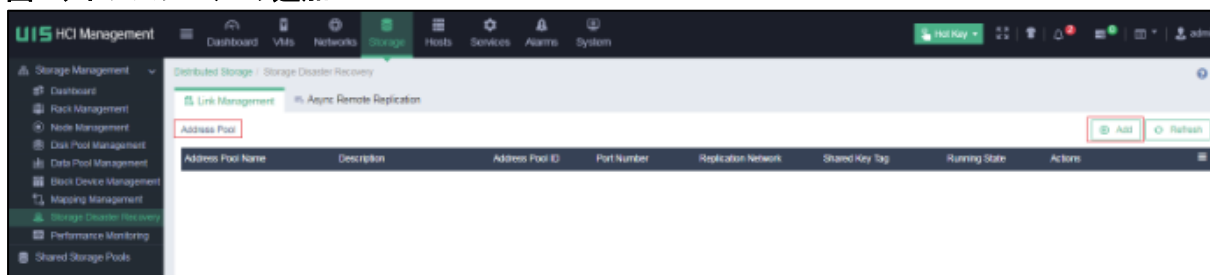


アドレス プールは、クラスター内で同じレプリケーション ネットワークが構成されたホストのグループです。アドレス プール内のホストは、レプリケーション ノードと呼ばれます。

## ローカルアドレスプールの追加

1. 上部のナビゲーション バーで**Storage**をクリックし、左側のナビゲーション ペインから**Storage Disaster Recovery**を選択します。
2. **Link Management** タブをクリックします。
3. **Address Pools**セクションで**Add** をクリックします。

図1 アドレスプールの追加



4. 開いたダイアログ ボックスで、アドレス プール パラメーターを構成し、**OK**をクリックします。レプリケーション ネットワークは、保護されたサイトとリカバリ サイトのブロック デバイス間でデータを同期するために使用されます。

図2 アドレスプール情報の設定

The 'Create Address Pool' dialog box contains the following fields and values:

- Address Pool Name\*: near\_end
- Replication Network\*: 99.99.99.0/24
- Shared Key Tag\*: admin
- Shared Key\*: .....
- Confirm Shared Key\*: .....
- Description: (empty)

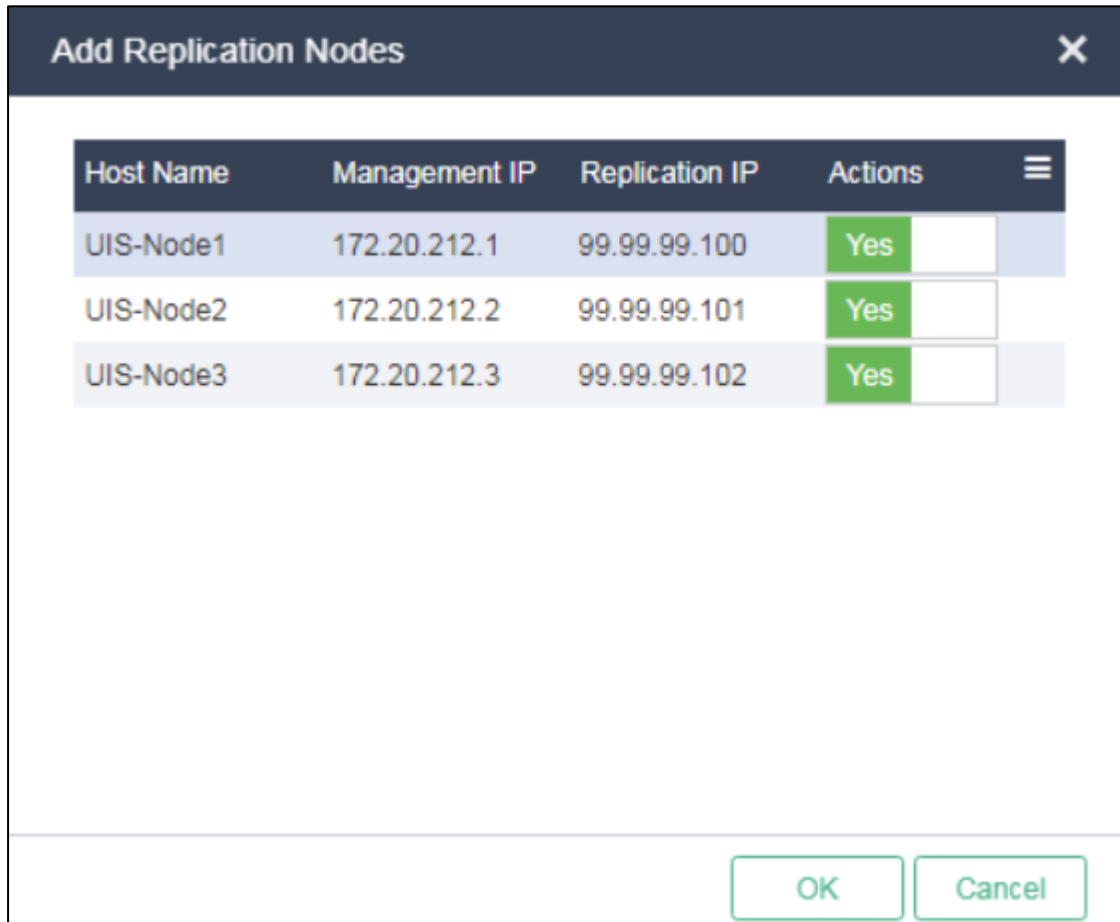
Buttons for 'OK' and 'Cancel' are located at the bottom right of the dialog.

パラメーター	説明
Address Pool Name	ローカル アドレス プールの名前を入力します。
Replication Network	ローカル アドレス プール内のレプリケーション ノードがリモート アドレス

パラメーター	説明
	プール内のレプリケーション ノードへのリンクを確立するネットワークを入力します。
Shared Key Tag	認証用の共有キータグを入力します。
Shared Key	認証用の共有キーを入力します。
Description	アドレス プールの説明を入力します。

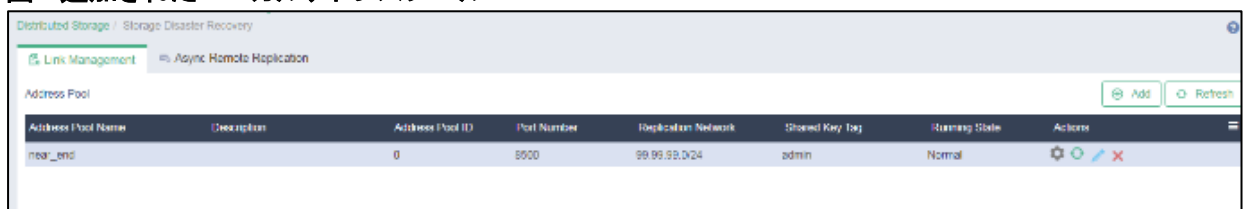
5. 冗長性を確保するために、複数のレプリケーション ノードをローカル アドレス プールに割り当て、OKをクリックします。

図3 レプリケーションノードの選択



ローカル アドレス プールが正常に追加されました。

図4 追加されたローカルアドレスプール



リモートアドレスプールを追加する

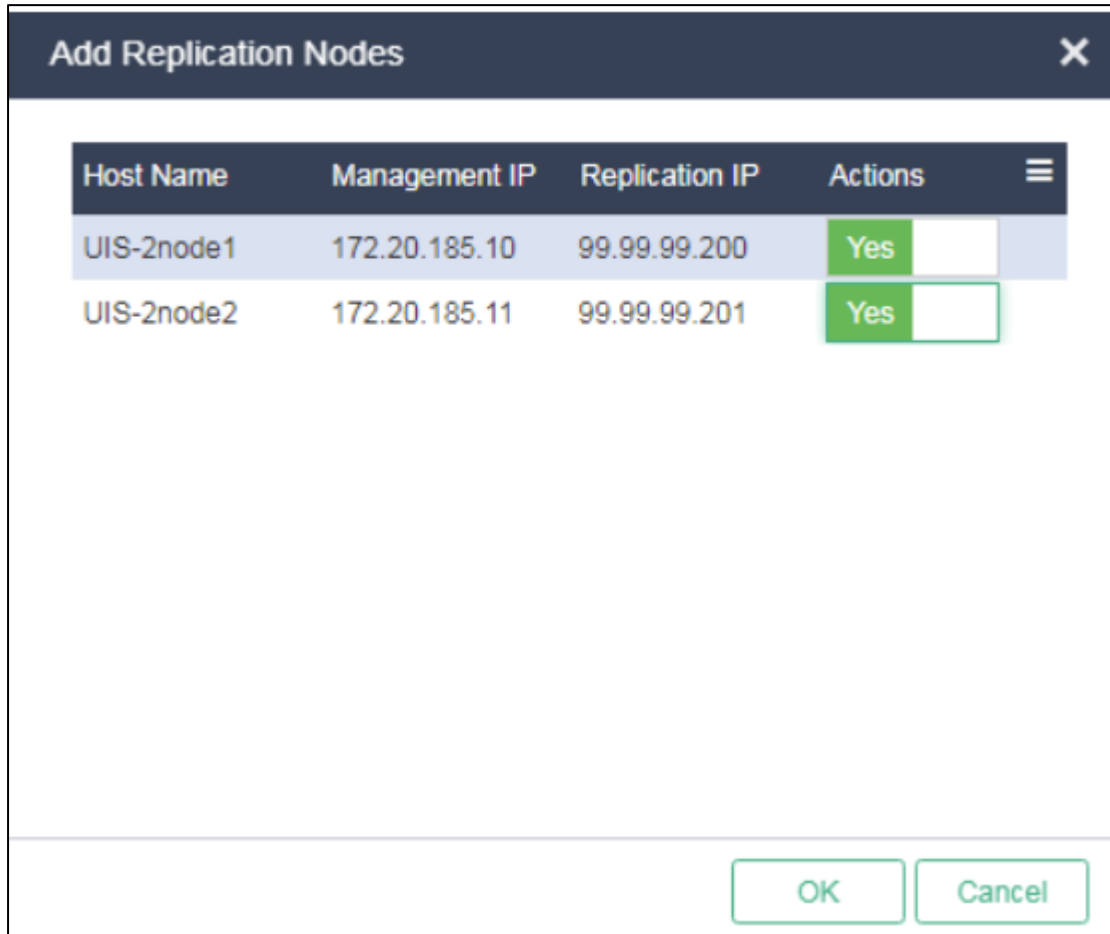
1. リカバリ サイトの UIS コンソールにログインします。
2. 上部のナビゲーション バーで**Storage**,をクリックし、左側のナビゲーション ペインから **Storage Disaster Recovery**を選択します。
3. **Link Management**タブをクリックします。
4. **Address Pools**セクションで**Add**をクリックします。
5. 開いたダイアログ ボックスで、アドレス プール パラメーターを設定し、**OK**をクリックします。

図5 リモートアドレスプールの追加

パラメーター	説明
Address Pool Name	リモート アドレス プールの名前を入力します。
Replication Network	ローカル アドレス プール内のレプリケーション ノードがリモート アドレス プール内のレプリケーション ノードへのリンクを確立するネットワークを入力します。
Shared Key Tag	認証用の共有キータグを入力します。
Shared Key	認証用の共有キーを入力します。
Description	リモート アドレス プールの説明を入力します。

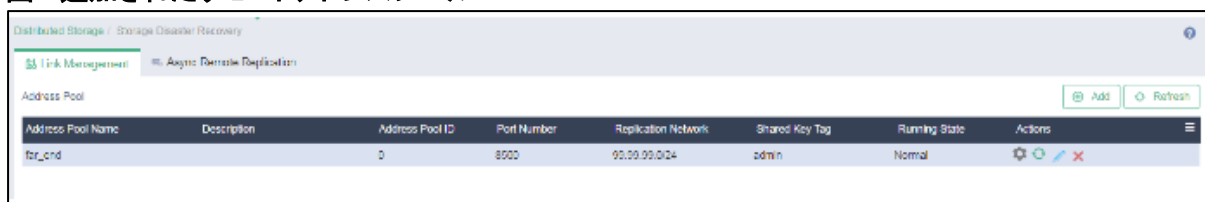
6. 冗長性を確保するために、複数のレプリケーション ノードをリモート アドレス プールに割り当て、**OK**をクリックします。

図6 レプリケーションノードの選択



リモート アドレス プールが正常に追加されました。

図7 追加されたリモートアドレスプール



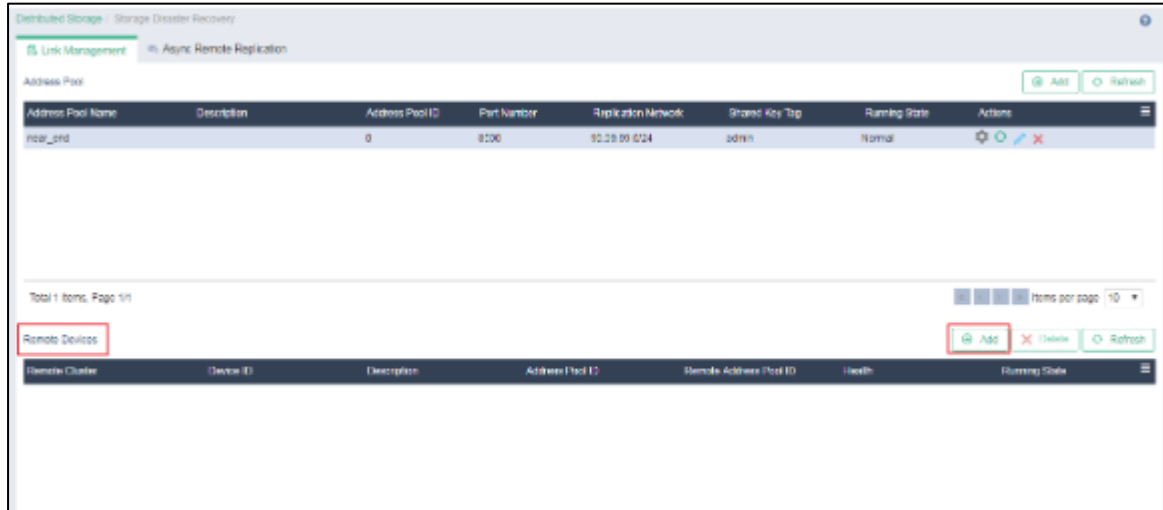
## リモートデバイスを追加する

リモート デバイスは、リモート アドレス プールとローカル アドレス プール間のリンクのセットから抽象化されま  
す。

保護サイトまたはリカバリ サイトのいずれかにリモート デバイスを追加できます。この例では、保護サ  
イトにリモート デバイスを作成します。

1. 上部のナビゲーション バーで**Storage**をクリックし、左側のナビゲーション ペインから**Storage Disaster Recovery**を選択します。
2. **Link Management**タブをクリックします。
3. **Remote Devices**セクションで**Add** をクリックします。

図1 リモートデバイスの追加



- 開いたダイアログ ボックスで、必要に応じてリモート デバイスのパラメーターを設定し、OKをクリックします。

図2 リモートデバイスの設定

**Create Remote Device** ✕

Address Pool Name\*

Remote Address Pool ID\*

Local IP\*

Remote IP\*

Remote Port Number\*

Remote Shared Key Tag\*

Remote Shared Key\*

Description

パラメーター	説明
Address Pool Name	ローカル クラスター内のアドレス プールを選択します。
Remote Address Pool ID	リモート アドレス プール ID を指定します。この ID は、リモート アドレス プールの作成時に自動的に割り当てられます。リモート リカバリ サイトの UIS コンソールにログインして、このパラメーターを確認できます。
Local IP	ローカル クラスター内のレプリケーション ネットワーク IP アドレスを選択します。ローカル アドレス プール内の任意のレプリケーション ノードの IP アドレス

パラメーター	説明
	を選択できます。この IP アドレスはリンクの確立にのみ使用されます。すべてのレプリケーション ノードがデータ同期に参加します。
Remote IP	リモート クラスターのレプリケーション ネットワーク IP アドレスを入力します。リモート アドレス プール内の任意のレプリケーション ノードの IP アドレスを入力できます。この IP アドレスはリンクの確立にのみ使用されます。すべてのレプリケーション ノードがデータ同期に参加します。
Remote Port Number	リモート アドレス プールのポート番号を指定します。このポート番号は、リモート アドレス プールの作成時に自動的に割り当てられます。リモート リカバリ サイトの UIS コンソールにログインして、このパラメーターを確認できます。
Remote Shared Key Tag	リモート アドレス プールの共有キー タグを入力します。このパラメーターを確認するには、リモート リカバリ サイトの UIS コンソールにログインします。
Remote Shared Key	リモート アドレス プールの共有キーを入力します。

リモート デバイスが正常に作成されました。

図3 作成されたリモートデバイス

Remote Cluster	Device ID	Description	Address Pool ID	Remote Address Pool ID	Health	Running State
ONEStar 10510	0		0	0	Optimal	Online

## 非同期レプリケーションペアを作成する

非同期レプリケーションは、非同期レプリケーション ペアと呼ばれるレプリケーション関係に基づいて、ローカル ブロック デバイスからリモート ブロック デバイスにデータをコピーします。ローカル ブロック デバイスに障害が発生した場合、リモート ブロック デバイス上のバックアップ データを使用してサービスを迅速に再開できます。

### 制限事項とガイドライン

ローカル ブロック デバイスとリモート ブロック デバイスの容量は同じである必要があります。

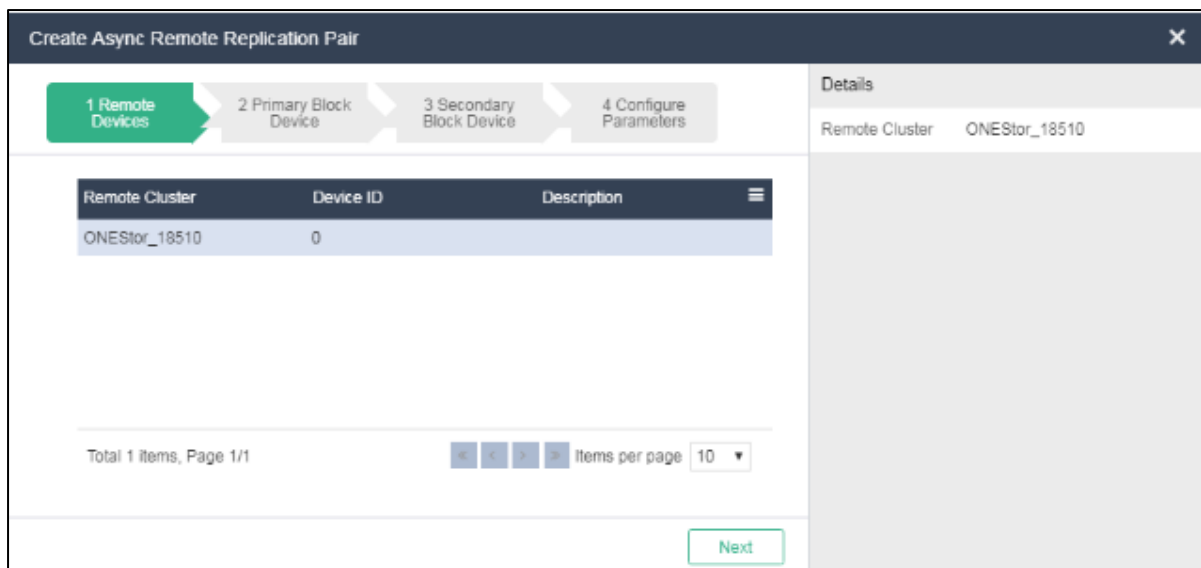
### 手順

1. 上部のナビゲーション バーで**Storage**をクリックし、左側のナビゲーション ペインから**Storage Disaster Recovery**を選択します。
2. **Async Remote Replication**タブをクリックします。
3. **Add**をクリックします。

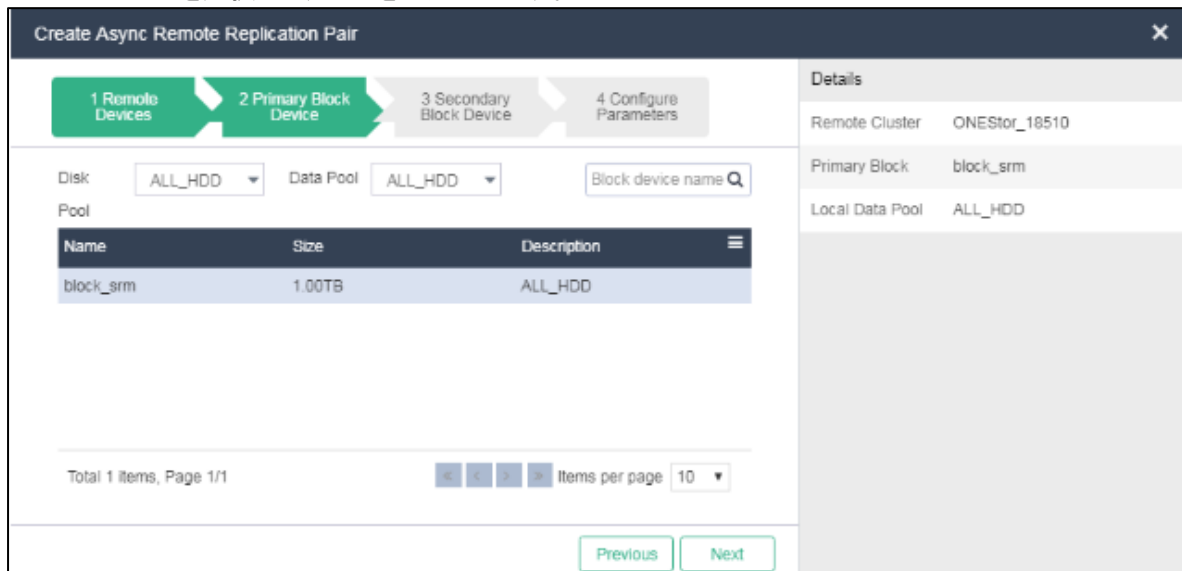
図1 非同期レプリケーションペアの作成

Primary Block	Primary Data Pool	Secondary Block Device	Secondary Data Pool	Remote Devic...	Role	Running State	Health	Actions
---------------	-------------------	------------------------	---------------------	-----------------	------	---------------	--------	---------

4. 開いたダイアログ ボックスでリモート デバイスを選択し、**Next**をクリックします。



5. **Primary Block Device**セクションで、ディスク プールとデータ プールを選択します。次に、プライマリ ブロック デバイスを選択して、**Next**をクリックします。



6. **Secondary Block Device**セクションで、ディスク プールとデータ プールを選択します。次に、セカンダリ ブロック デバイスを選択し、**Next**をクリックします。
7. レプリケーション設定を構成します。

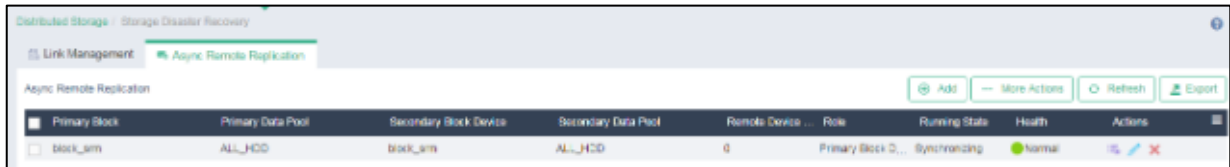
ベストプラクティスとして、自動初期同期モードを選択します。別のオプションを選択した場合は、回復計画のテストの前にデータを手動で同期する必要があります。

パラメーター	説明
Initial Sync	<p>非同期レプリケーション ペアの初期同期ポリシーを指定します。</p> <ul style="list-style-type: none"> <li>• <b>Automatic-</b> レプリケーション ペアが作成された直後に、システムはデータの一貫性を保つためにプライマリ ブロック デバイスとセカンダリ ブロック デバイスを自動的に同期します。</li> <li>• <b>Manual-</b> レプリケーション ペアの作成後に必ず同期を実行してください。手動同期を実行するまで、ペアは分割状態のままになります。</li> <li>• <b>Skip-</b> プライマリ ブロック デバイスとセカンダリ ブロック デバイスのデータに一貫性があることが確実な場合にのみ、このオプションを選択します。災害復旧の実行時にセカンダリ ブロック デバイスでのデータ損失を回避するためのベストプラクティスとして、プライマリ ブロック デバイスとセカンダリ ブロック デバイスの初期データが一貫しているかどうか判断できない場合は、このオプションを選択しないでください。</li> </ul>
Speed	<p>データ複製速度を指定します。</p> <ul style="list-style-type: none"> <li>• <b>Low-</b> 速度は 5 Mbps 以下です。</li> <li>• <b>Medium-</b> 速度は 20 Mbps 以下です。</li> <li>• <b>High-</b> 速度は 70 Mbps 以下です。</li> <li>• <b>Ultra -</b> 速度は制限されず、クラスターのネットワーク状態に依存します。</li> </ul>
Restore Mode	<p>非同期レプリケーション ペアの復元モードを指定します。</p> <ul style="list-style-type: none"> <li>• <b>Auto-</b> 障害が発生すると、システムは定期的に同期を自動的に実行し、障害からデータを回復します。</li> <li>• <b>Manual-</b> 障害発生後、システムは自動同期を実行しません。 <b>More Actions &gt; Sync on the Async Remote Replication</b>から手動でデータを回復できます。</li> </ul>
Sync Policy	<p>プライマリ ブロック デバイスとセカンダリ ブロック デバイス間のスケジュールされた自動同期のタイミング ポリシーを指定します。</p> <ul style="list-style-type: none"> <li>• <b>Interval-Based (Timer Starts on Start of Sync) -</b>この同期の開始時にタイマーが開始されます。間隔タイマーの期限が切れると、次の同期が自動的に開始されます。</li> <li>• <b>Interval-Based (Timer Starts on Completion of Sync) -</b>この同期の完了時にタイマーが開始されます。間隔タイマーの期限が切れると、次の同期が自動的に開始されます。</li> <li>• <b>Time-Not Configurable- Async Remote Replication</b>タブの <b>More Actions &gt; Sync</b>から手動で同期を実行できます。</li> </ul>
Sync Interval	<p>同期間隔を設定します。このパラメーターは、同期ポリシーに「間隔ベース (同期</p>



パラメーター	説明
	の開始時にタイマーが開始)または「間隔ベース (同期の完了時にタイマーが開始)」を選択した場合に使用できます。
Sync Time	同期を実行する時点を指定します。このパラメーターは、 <b>Sync Policy</b> で <b>Time-Based</b> を選択した場合に使用できます。

8. **Finish**をクリックします。  
非同期レプリケーション ペアが作成され、データの同期が進行中です。



## ローカルサイトとリモートサイトにSRAを追加する

保護サイトとリカバリ サイトのストレージ アレイが SRA をサポートしている場合は、サイトのストレージ アレイ マネージャーを構成する必要があります。サイトとストレージ アレイ マネージャーを追加したら、ストレージ レプリケーション情報を同期します。

1 つのサイトの UIS コンソールからサイトの災害復旧設定を構成し、それを他のサイトに同期することができます。

### ローカルサイトのSRAを追加する

1. 上部のナビゲーション バーで、**Services**をクリックします。
2. 左側のナビゲーション ペインから、**Services > SRM > Sites**を選択します。
3. ローカル サイトを選択し、**Add Storage Array Manager**をクリックします。
4. ストレージ アレイ タイプとして**ONEStor**を選択し、ONEStor ストレージ クラスターの IP アドレス、ONEStor ストレージ アレイへのログインに使用するユーザー名とパスワードを入力し、UIS 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て、**OK**をクリックします。  
ONEStor ストレージ クラスターの IP アドレスを取得するには、クラスターの概要情報を表示します。

**Add Storage Array Manager** ✕

Storage Array ONEStor MacroSan

Type\*

Name\*

IP\*

Username\*

Password\*

パラメーター	説明
Storage Array Type	ローカル サイトで使用するストレージ アレイの製造元を選択します。
Name	ストレージ アレイ マネージャーの名前を入力します。
IP	ストレージ アレイの IP アドレスを入力します。この IP アドレスは、ストレージ環境の管理 IP アドレスです。
Username	ストレージ アレイ マネージャーにアクセスするためのユーザー名を入力します。
Password	ストレージ アレイ マネージャーにアクセスするためのパスワードを入力します。
Multipathing	マルチパスを有効にするかどうかを選択します。HCI 展開でストレージ アレイを構成するには、この機能を有効にし、マルチパスの IP アドレスを構成する必要があります。
IP Address for Multipathing	ストレージ環境のストレージ ネットワーク IP アドレスを入力します。これらの IP アドレスは、ストレージ プールの作成時に構成された IP アドレスです。複数の IP アドレスを入力すると、ストレージ側でマルチパスが自動的に実装されます。

5. **Connectivity Test** をクリックして、ストレージ クラスターに到達できることを確認します。

6. **OK**をクリックし、**Finish**をクリックします。

Site Name	IP	Username	Site Type	Actions
near_0ns	172.20.212.1	admin	Local	[Edit] [Delete]

## リモートサイトのSRAを追加する

1. 上部のナビゲーション バーで、**Services**をクリックします。
2. 左側のナビゲーション ペインから、**Services > SRM > Sites**を選択します。
3. リモート サイトを選択し、**Add Storage Array Manager**をクリックします。
4. ストレージ アレイ タイプとして**ONEStor**を選択し、ONEStor ストレージ クラスターの IP アドレス、ONEStor ストレージ アレイへのログインに使用するユーザー名とパスワードを入力し、UIS 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て、**OK**をクリックします。  
ONEStor ストレージ クラスターの IP アドレスを取得するには、クラスターの概要情報を表示します。

**Add Storage Array Manager** [Close]

Storage Array: ONEStor MacroSan

Type\*

Name\*

IP\*

Username\*

Password\*

Connectivity Test OK Cancel

5. **Connectivity Test** をクリックして、ストレージ クラスターに到達できることを確認します。
6. **OK**をクリックし、**Finish**をクリックします。

Site Name	IP	Username	Site Type	Actions
near_end	172.20.212.1	admin	Local	
far_end	172.20.185.10	admin	Remote	

## ストレージレプリケーションペアを同期する

1. **[ストレージレプリケーション情報の同期]**をクリックします。  
このタスクは、サイトとストレージ アレイ マネージャーを追加した後に必要になります。
2. ストレージ アレイ マネージャーのアイコン をクリックすると、ストレージレプリケーション ペアが表示されます。

Local LUN	Replication...	Remote LUN	Remote Storage
SRM	→	SRM	srm

パラメーター	説明
Local LUN	ローカル LUN の名前。
Replication Direction	ローカル LUN とリモート LUN 間のレプリケーション関係。
Remote LUN	リモート LUN の名前。
Remote Storage	リモート LUN が属するストレージ アレイ マネージャーの名前。

# 保護グループを構成する

保護グループは、保護ポリシーに基づいて、同じストレージ プール (ストレージ アレイ内の LUN) を使用する一連の VM を保護します。障害が発生すると、アレイベースのレプリケーションを通じて、ローカル ストレージ アレイ内の LUN に保存されている VM データをリモート ストレージ アレイ内の LUN に複製します。リソース マッピング関係は、保護されたサイト内の保護された VM によって使用されるリソースをリカバリ サイトのソースに関連付けます。VM がリカバリ サイトでリカバリされると、VM が使用するリソースはリカバリ サイトのリソースに自動的に置き換えられます。

1. 上部のナビゲーション バーで、**Services**をクリックします。
2. 左側のナビゲーション ペインから、**Services > SRM > Protection Groups**を選択します。
3. **Add Protection Group**をクリックします。
4. 保護グループのパラメータを構成し、**Next**をクリックします。

Details	
Name	protect1
Description	
Protection Site	near_end(172.20.212.1)
Recovery Site	far_end(172.20.185.10)
Original Host Pool	UISC
Target Host Pool	UISC
Auto VM Protection	No

パラメータ	説明
<b>Name</b>	保護グループの名前を入力します。名前は UIS マネージャー内で一意である必要があります。
<b>Protection Site</b>	保護グループに関連付ける保護されたサイトを選択します。
<b>Recovery Site</b>	保護グループに関連付ける回復サイトを選択します。
<b>Original Host Pool</b>	保護されたサイトのホスト プールを選択します。
<b>Target Host Pool</b>	リカバリ サイトのホスト プールを選択します。
<b>Auto VM Protection</b>	この機能を有効にすると、特定の条件が満たされたときに VM が保護グループに自動的に追加されます。

- 次の条件が満たされると、VM は保護グループに自動的に追加されます。
- VM が使用するストレージ リソース、vSwitch、およびポート プロファイルは、保護グループに属します。
  - 保護グループ内に同じ名前の VM が存在しません。
    - VM は光学ドライブやフロッピー ドライブを使用しません。

5. リソース マッピング関係を追加するには、  または  アイコンをドラッグします。左側のリソー

スは保護されたサイトの VM によって使用され、右側のリソースはリカバリ サイトの VM によって使用されます。

- ストレージ マッピングを追加するときは、ストレージ プール タイプとストレージ タイプを指定する必要があります。
- SRA をサポートしていないストレージ アレイの場合は、ストレージ プール タイプとして **Shared File System** を選択する必要があります。

## 6. Finish をクリックします。

The screenshot shows the 'Add Protection Group' wizard in step 2, 'Mapping Relationship'. The interface displays two host pools: 172.20.212.1 and 172.20.185.10. Each host pool has three components: SRM (Storage), vswitch0 (vSwitch), and Default (Profile). Green lines indicate the mapping between corresponding components of the two host pools. The 'Finish' button is highlighted at the bottom right.

7. 保護グループを選択し、**Add VM** をクリックします。

8. VM を選択し、**OK** をクリックします。

保護グループを選択すると、保護グループ内の VM が **VMs Under Protection** 領域に表示されます。

The screenshot shows the 'VMs Under Protection' table. The table has columns for Name, Alias, Status, and Actions. The 'Add VM' button is highlighted in red in the top right corner.

Name	Alias	Status	Actions
<input type="checkbox"/> Windows7	Windows7	Shutdown	Refresh Delete
<input type="checkbox"/> Windows7-2	Windows7-2	Shutdown	Refresh Delete
<input type="checkbox"/> Windows7-3	Windows7-3	Shutdown	Refresh Delete

## 回復計画を作成する

リカバリプランには、保護グループ内の VM をリカバリするための一連のポリシーが含まれています。

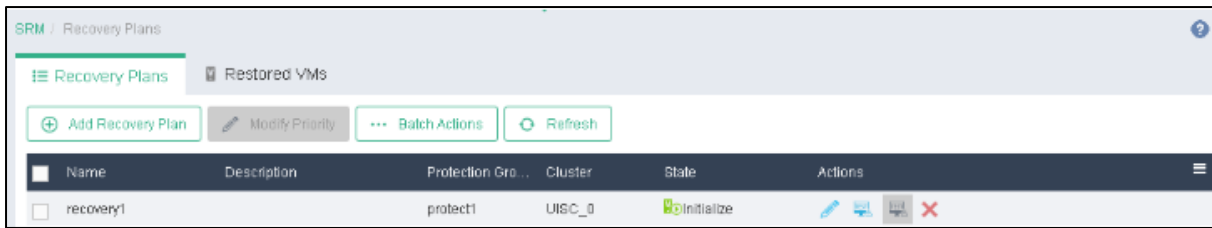
1. 上部のナビゲーションバーで、**Services**をクリックします。
2. 左側のナビゲーションペインから、**Services > SRM > Recovery Plans**を選択します。
3. **Add Recovery Plan** をクリックします。
4. 名前と説明を入力し、保護された VM を復元する保護グループとクラスターを選択します。

保護グループは 1 つの回復計画によってのみ保護できます。

Name	Type
SRM	iSCSI Shared Directory

パラメータ	説明
Protection Group	保護された VM を復元する保護グループを選択します。保護グループは 1 つの復旧プランでのみ保護できます。
Cluster	保護された VM を復元するクラスターを選択します。
Shared Storages	保護グループのストレージリソースマッピングで構成されている、ローカルサイトに関する共有ストレージ情報。

5. **OK**をクリックします。リカバリプランは作成後、**Initialize**状態になります。



## 回復計画を実行する

システムには、リカバリ計画を実行するための次のオプションが用意されています。

- 復旧計画のテスト。
- スケジュールされたリカバリを実行しています。
- 障害回復を実行しています。
- リバースリカバリを実行しています。
  - リカバリ計画を最初に実行する前に、ストレージレプリケーションペアのデータ同期が実行されていることを確認します。
  - ストレージデバイスが正しく起動し、リカバリ計画が正しく実行されるようにするには、リカバリ計画を実行する前に、非 SRA ストレージのリカバリサイトでリソース保護を無効にします。
  - リカバリ計画の実行中に、保護された VM がストレージマッピングで指定されたストレージデバイスにアクセスできること、およびリカバリクラスターに保護された VM を復元するのに十分なリソースがあることを確認します。
  - リカバリ計画の実行中に、保護されたサイトとリカバリサイトが接続されていることを確認します。マップされたストレージデバイスが接続されているホストが正しく動作することを確認します。

## 復旧計画をテストする

リカバリ計画テストは、保護されたサイトで障害が発生した場合にリカバリサイトでサービスをリカバリするプロセスをシミュレートして、リカバリ計画の正確性を検証します。テストは保護されたサイトによって提供されるサービスには影響せず、手動で開始および停止されます。

リカバリ計画テストでは、保護された VM がリカバリサイトの LUN に接続されます。リカバリ計画テストの終了後は、環境を手動でクリアする必要があります。

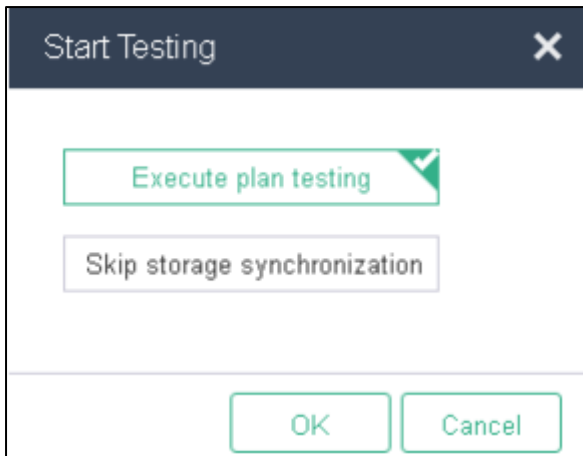
### 復旧計画のテストを開始する

1. 上部のナビゲーションバーで、**Services** をクリックします。
2. 左側のナビゲーションペインから、**Services > SRM > Recovery Plans > recovery plan name** を選択します。
3. **Start Testing** をクリックします。

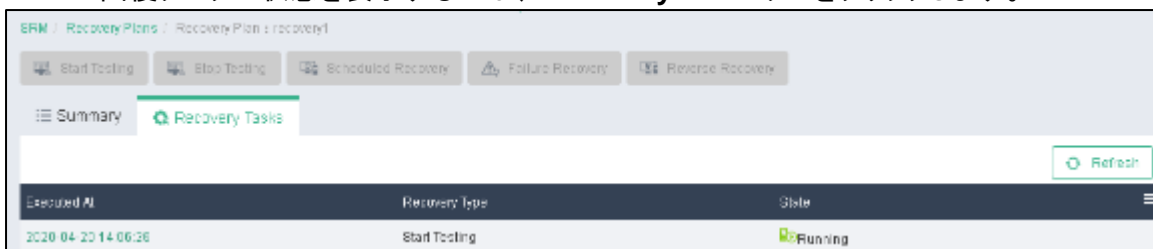


4. 開いたダイアログボックスで実行モードを選択し、**OK** をクリックします。

ストレージデバイスに同期されたデータがある場合は、**Skip storage synchronization** を選択できます。



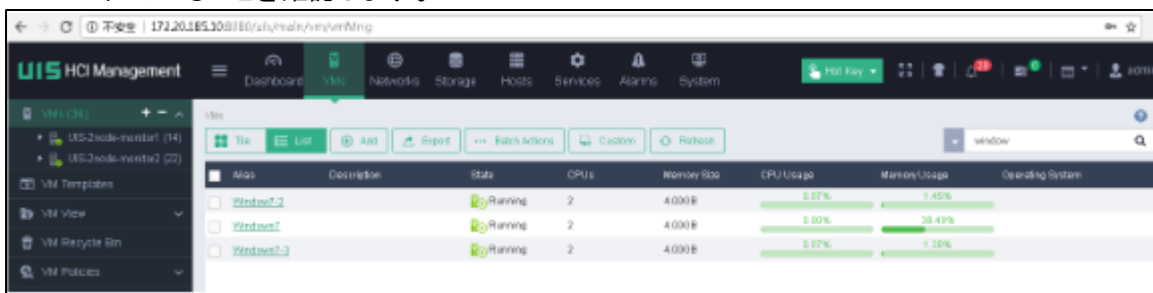
5. 回復タスクの状態を表示するには、**Recovery Tasks**タブをクリックします。



6. テストの詳細を表示するには、リカバリ タスクの実行時間リンクをクリックします。

Recovery Steps	State
1. Perform storage switch and failover	
SRM	Succeeded
2. Mount storage for recovery site	Succeeded
3. Restore VMs for recovery site	
Windows7	Succeeded
Window7-2	Succeeded
Windows7-3	Succeeded

7. 保護された VM が、リカバリ サイトでマップされたストレージ リソースが接続されたホストに復元されていることを確認します。



復旧計画のテストを完了する



災害復旧データをクリアし、復旧計画の状態を「準備完了」に復元するには、復旧計画テストを手動で完了する必要があります。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Services > SRM > Recovery Plans > recovery plan name** を選択します。
3. **Stop Testing** をクリックします。
4. 回復タスクの状態を表示するには、**Recovery Tasks** タブをクリックします。



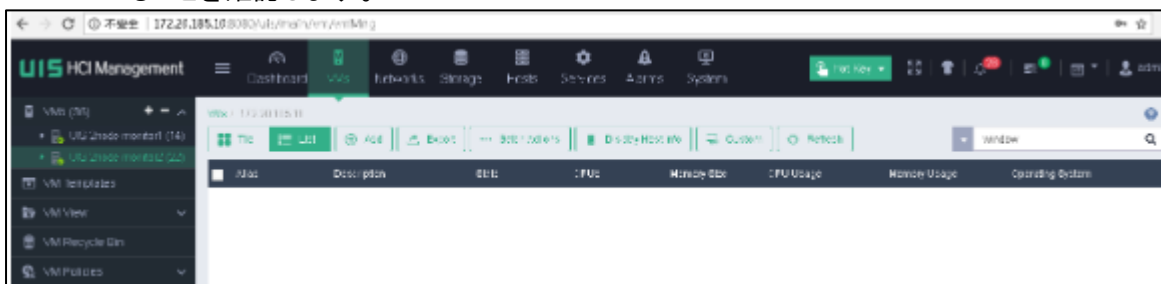
Executed At	Recovery Task	State
2020-04-21 16:33:44	Start Testing	Running
2020-04-21 16:19:43	Start Testing	Succeeded

5. テストの詳細を表示するには、リカバリ タスクの実行時間リンクをクリックします。



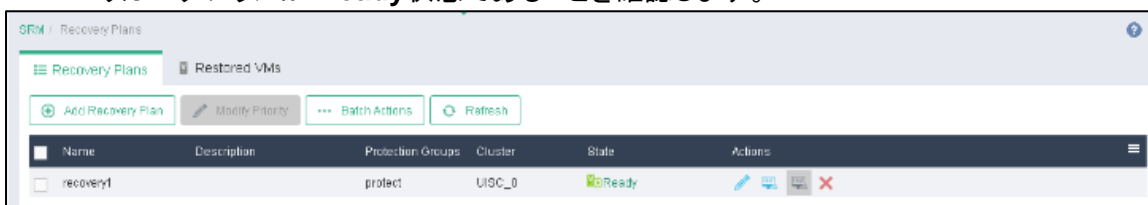
Recovery Steps	State
1.Remove VMs from recovery site	Succeeded
2.Remove storage from recovery site	Succeeded
SRM	Succeeded
3.Test recovering storage configuration	Running
SRM	Running

6. 保護された VM がリカバリ サイトから削除され、マップされたストレージ リソースが一時停止されていることを確認します。



Name	Description	State	Priority	Memory GB	CPU Usage	Memory Usage	Operating System
VM1 (10)							
UIS-2node-mount1 (14)							
UIS-2node-mount1 (22)							
VM Templates							
VM View							
VM Recycle Bin							
VM Policies							

7. リカバリ プランが **Ready** 状態であることを確認します。

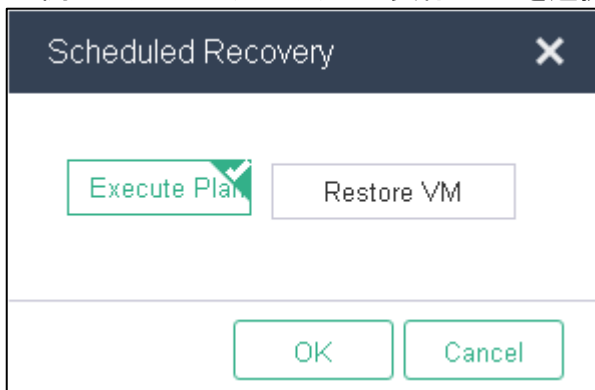


Name	Description	Protection Groups	Cluster	State	Actions
recovery1		protect	UISC_0	Ready	

## スケジュールされたリカバリを実行する

スケジュールされたリカバリでは、両方のサイトが正常に動作している場合、保護されたサイトで保護された VM をシャットダウンし、メンテナンスのためにそのデータをリカバリ サイトに複製します。リカバリ プランを実行するには、リカバリ手順に従って実行するか、VM の復元前にリカバリ プランのすべての手順が準備できている必要があります。

1. 上部のナビゲーション バーで、**Services** をクリックします。
2. 左側のナビゲーション ペインから、**Services > SRM > Recovery Plans > recovery plan name** を選択します。
3. **Scheduled Recovery** をクリックします。
4. 開いたダイアログ ボックスで実行モードを選択し、**OK** をクリックします。



5. 回復タスクの状態を表示するには、**Recovery Tasks** タブをクリックします。

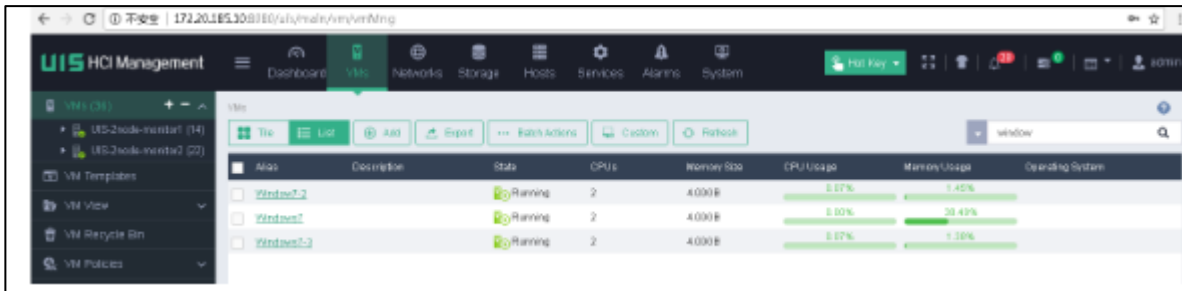


Executed At	Recovery Type	State
2020-04-21 15:36:21	Scheduled Recovery	Running
2020-04-21 15:33:44	Stop Testing	Succeeded
2020-04-21 15:19:49	Start Testing	Succeeded

6. タスクの詳細を表示するには、回復タスクの実行時間リンクをクリックします。

Recovery Steps	State
<ul style="list-style-type: none"> <li>1.Sync Storage           <ul style="list-style-type: none"> <li>SRM <span style="float:right">✔ Succeeded</span></li> </ul> </li> <li>2.Close protection site resource <span style="float:right">✔ Succeeded</span></li> </ul>	
<ul style="list-style-type: none"> <li>3.Perform Storage Switch and Promotion           <ul style="list-style-type: none"> <li>SRM <span style="float:right">✔ Succeeded</span></li> </ul> </li> <li>4.Mount storage for recovery site <span style="float:right">✔ Succeeded</span></li> </ul>	
<ul style="list-style-type: none"> <li>5.Restore VMs for recovery site           <ul style="list-style-type: none"> <li>Windows7-2 <span style="float:right">✔ Succeeded</span></li> <li>Windows7 <span style="float:right">✔ Succeeded</span></li> <li>Windows7-3 <span style="float:right">✔ Succeeded</span></li> </ul> </li> </ul>	

7. 保護された VM がリカバリ サイトで復元されたことを確認します。



8. 保護されたサイトで保護された VM がシャットダウンされていることを確認します。



# リバースリカバリを実行する

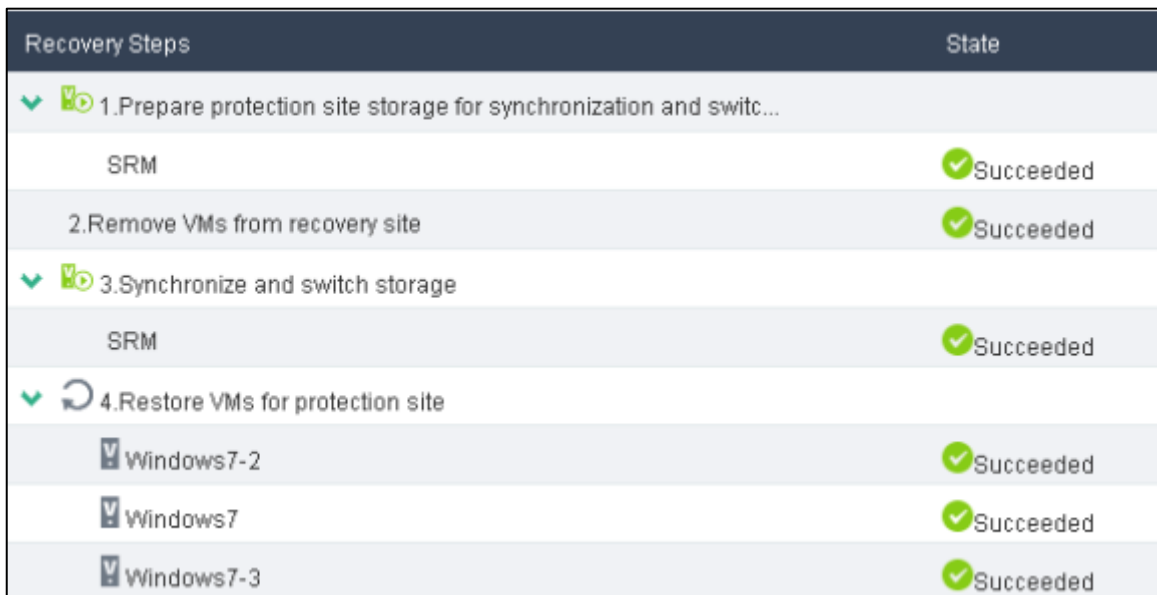
リバースリカバリでは、保護されたサイトが回復したとき、またはスケジュールされたリカバリが実行された後に、リカバリサイトの保護されたVMを保護されたサイトに復元します。

リバースリカバリを実行する前に、保護されたサイトとリカバリサイトが正しく動作し、接続されていること、およびマップされたストレージリソースが接続されたホストが正しく動作していることを確認します。

1. 上部のナビゲーションバーで、**Services** をクリックします。
2. 左側のナビゲーションペインから、**Services > SRM > Recovery Plans > recovery plan name** を選択します。
3. **Reverse Recovery** をクリックします。
4. **Recovery Tasks** タブをクリックし、回復タスクの実行時間リンクをクリックします。

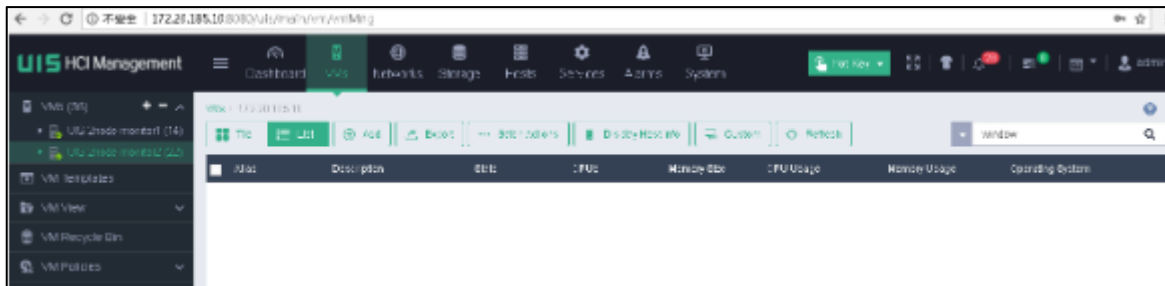


Executed At	Recovery Type	State
2020-04-22 10:20:20	Reverse Recovery	Running
2020-04-22 10:09:02	Scheduled Recovery	Succeeded
2020-04-22 10:08:00	Reverse Recovery	Succeeded
2020-04-22 09:52:08	Scheduled Recovery	Succeeded

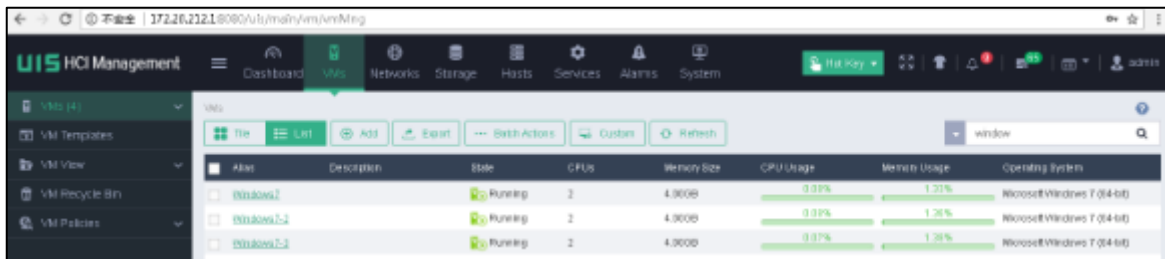


Recovery Steps	State
1. Prepare protection site storage for synchronization and switc...	
SRM	Succeeded
2. Remove VMs from recovery site	Succeeded
3. Synchronize and switch storage	
SRM	Succeeded
4. Restore VMs for protection site	
Windows7-2	Succeeded
Windows7	Succeeded
Windows7-3	Succeeded

5. 保護されたVMがリカバリサイトから削除され、マップされたストレージリソースが一時停止されていることを確認します。



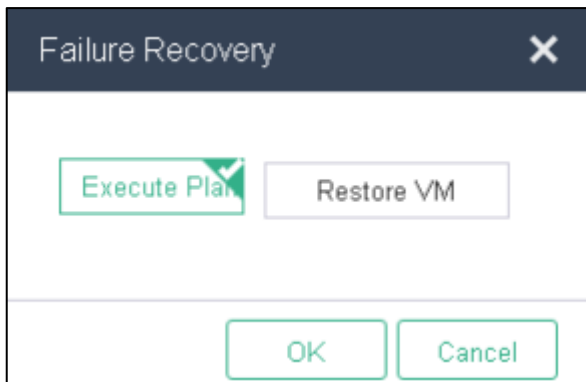
6. 保護されたサイトで保護された VM が復元されたことを確認します。



## 障害回復を実行する

VM の復元前にリカバリプランのすべての手順が準備されている場合は、リカバリ手順に従ってリカバリプランを実行するか、VM を直接復元することができます。

1. 上部のナビゲーションバーで、**Services** をクリックします。
2. 左側のナビゲーションペインから、**Services > SRM > Recovery Plans > recovery plan name** を選択します。
3. **Failure Recovery** をクリックします。開いたダイアログボックスで実行モードを選択し、**OK** をクリックします。



4. 回復タスクの状態を表示するには、**Recovery Tasks** タブをクリックします。

SRM / Recovery Plans / Recovery Plan : recovery1

Start Testing | Stop Testing | Scheduled Recovery | Failure Recovery | Reverse Recovery

Summary | Recovery Tasks

Executed At	Recovery Type	State
2020-04-22 10:30:57	Failure Recovery	Running
2020-04-22 10:20:20	Reverse Recovery	Succeeded
2020-04-22 10:09:02	Scheduled Recovery	Succeeded
2020-04-22 10:00:00	Reverse Recovery	Succeeded
2020-04-22 09:52:08	Scheduled Recovery	Succeeded

5. タスクの詳細を表示するには、回復タスクの実行時間リンクをクリックします。

Recovery Steps	State
1.Perform Storage Switch and Promotion	
SRM	Succeeded
2.Mount storage for recovery site	Succeeded
3.Restore VMs for recovery site	
Windows7-2	Succeeded
Windows7	Succeeded
Windows7-3	Succeeded

6. 保護された VM がリカバリ サイトで復元されたことを確認します。

UIS HCI Management

Dashboard | VMs | Networks | Storage | Backups | Services | Alerts | System

VMs (4)

名前	ステータス	コア	メモリ	CPU 利用率	メモリ利用率	オペレーティングシステム
Windows7	Running	2	4.0GB	8.6%	1.5%	Microsoft Windows 7 (64-bit)
Windows7-2	Running	2	4.0GB	8.6%	1.5%	Microsoft Windows 7 (64-bit)
Windows7-3	Running	2	4.0GB	8.6%	1.5%	Microsoft Windows 7 (64-bit)

7. 保護されたサイトで保護された VM がシャットダウンされていることを確認します。

UIS HCI Management

Dashboard | VMs | Networks | Storage | Backups | Services | Alerts | System

VMs (4)

名前	説明	ステータス	CPU	メモリ	CPU 利用率	メモリ利用率	オペレーティングシステム
Windows7		ShutDown	2	4.0GB	0.0%	0.0%	Microsoft Windows 7 (64-bit)
Windows7-1		ShutDown	2	4.0GB	0.0%	0.0%	Microsoft Windows 7 (64-bit)
Windows7-2		ShutDown	2	4.0GB	0.0%	0.0%	Microsoft Windows 7 (64-bit)

# ディスクバックアップベースの災害復旧を構成する

ディスクバックアップベースの災害復旧では、CDPを使用して災害復旧用のオペレーティングシステムデータを複製します。DRMは、保護されたオブジェクトが存在するホストにインストールされたCDPエージェントからホスト情報を取得し、データブロックの変更をキャプチャし、増分データをH3C UIS復旧サイトのストレージノードに送信します。

スナップショットチェーンとリアルタイム同期メカニズムにより、データを数秒でバックアップおよび同期して、高性能RPOデータ復旧の要件を満たすことができます。ディスクバックアップベースの災害復旧は、異なるインフラストラクチャを持つ複数のクラウドプラットフォームのサービスを1つの復旧サイトでバックアップすることをサポートします。DRMのすべてのアプリケーションシナリオで使用できます。

## アプリケーションシナリオ

ディスクバックアップベースの災害復旧は、次のシナリオに適用できます。

- **同種のクラウド**- 保護サイトとリカバリサイトに同じバージョンのUISマネージャーが展開され、保護されるオブジェクトはVMです。
- **異機種クラウド**- UISマネージャーがリカバリサイトに展開されており、保護されたサイトに次のいずれかの条件が存在します。
  - 保護されたVMはUIS以外のクラウドプラットフォームで実行されています。
  - 保護されたサイトのUISマネージャーのバージョンは、リカバリサイトのUISマネージャーのバージョンよりも低くなっています。
  - 保護されるオブジェクトはベアメタルサーバーです。
- **ハイブリッドインフラストラクチャ**- UISマネージャーはリカバリサイトに展開され、保護されたサイトにはVMとベアメタルサーバーの両方が収容されます。

ディスクバックアップベースの災害復旧により、RPOとRTOを数分に短縮できます。

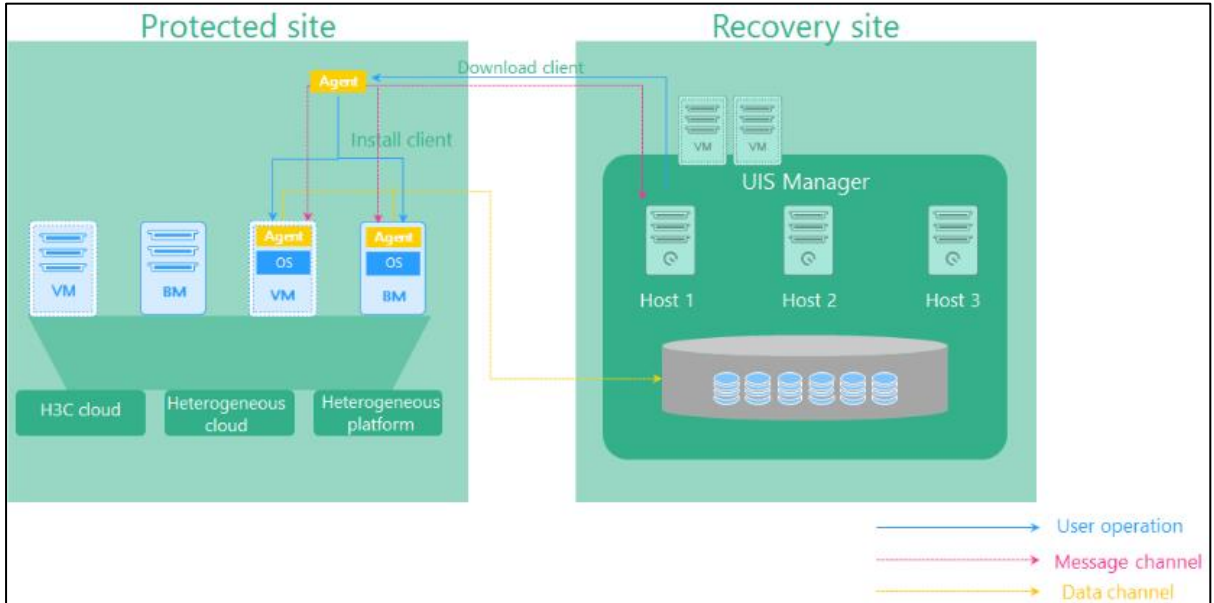
## 構成環境

- **ストレージ**— 要件はありません。
- **計画サイト**- x86クラウドプラットフォームまたは物理サーバー。
- **リカバリサイト**- UIS Manager 0716H06、UIS Manager 拡張エディションライセンス、およびディスクバックアップベースの災害復旧ライセンス。
- **保護されたノード上のオペレーティングシステム**- Windows Server または Linux。詳細については、「付録UISハイパーコンバージド管理プラットフォームディスクバックアップベースのディザスタリカバリクライアントとオペレーティングシステムの互換性」を参照してください。

## メカニズム

DRMは、ディザスタリカバリクライアントがインストールされたVMまたはベアメタルサーバー(運用ノード)を保護します。ディザスタリカバリクライアントのリアルタイムディスクレプリケーション機能は、保護されたオブジェクトのデータをOSごとにリカバリサイトにコピーし、DRMが保護されたオブジェクトをVMとして復元できるようにします。

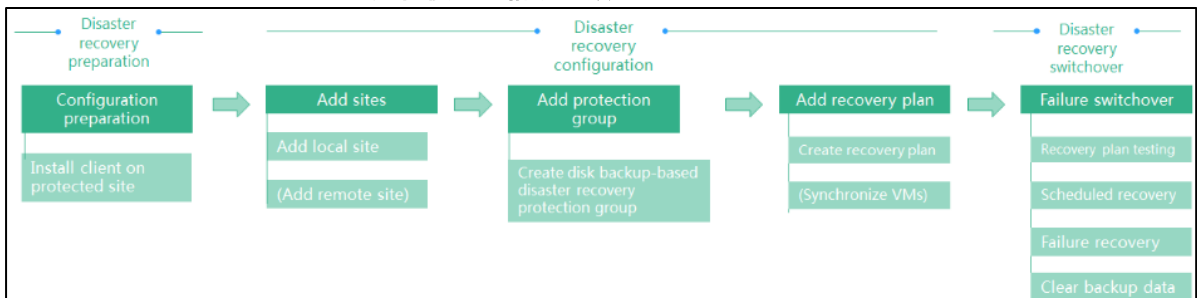
図1 ディスクバックアップベースの災害復旧手順



## 設定手順

図 1 は、ディスク バックアップ ベースの災害復旧の一般的な構成手順を示しています。構成手順の詳細については、「災害復旧の準備」、「DRM タスク」、および「災害復旧のシナリオ」。

図2 ディスクバックアップベースの災害復旧の構成手順



## 災害復旧の準備

ディスク バックアップ ベースの災害復旧を構成する前に、次のタスクを実行します。

- 管理プラットフォーム上のホストに CDP コンポーネントをインストールします。
- 保護されたサイトで、保護された VM またはベア メタル サーバーにディザスタリカバリ クライアントをインストールします。

## DRMタスク

### サイトを構成する

保護サイトまたはリカバリ サイトのいずれかで、CAS 上にローカル サイトとリモート サイトを構成します。異機種クラウドでのディスク バックアップ ベースの災害復旧の場合は、ローカル サイトのみを構成できます。

### 保護グループを構成する



ディスク バックアップ保護グループは、保護対象オブジェクトのデータをリアルタイムで自動的に同期することにより、災害復旧クライアントにインストールされた一連の VM またはベア メタル ノードを保護します。ディスク バックアップ保護グループは、保護対象オブジェクトで実行されているサービスに応じて、次のいずれかのモードで動作できます。

- **共通モード**- VM または実稼働ノードは独立して動作します。
- **デュアルノード モード**- 2 つの VM または運用ノードには、両方からアクセスできるデータを保存するための共有ストレージが必要です。
- **クラスター モード**- VM または実稼働ノードには、それらすべてがアクセスできるデータを保存するための共有ストレージが必要です。

ディスク バックアップ保護グループは、次のシナリオをサポートします。

- **同種のクラウド**-保護サイトとリカバリサイトで同じバージョンの UIS システムを実行して、UIS VM を保護します。このシナリオでは、保護サイトとリカバリ サイトを指定し、保護サイトでディザスタリカバリ クライアントと共にインストールされた VM を保護対象オブジェクトとして選択し、ディザスタリカバリ ポリシーを選択して、これらのサイト間のネットワーク マッピングを構成する必要があります。
- **異機種混在クラウド**- UIS は、下位バージョンの UIS システム上の VM または他のプラットフォーム上の VM またはベア メタル サーバーを保護し、上位バージョンの UIS システムでそれらを回復します。このシナリオでは、ローカル サイトを回復サイトとして使用し、ディザスタリカバリ クライアントとともにインストールされた VM またはベア メタル サーバーを保護対象オブジェクトとして指定し、ディザスタリカバリ ポリシーを選択してから、回復サイトで運用ノードのネットワーク リソースを構成します。

保護グループを作成すると、UIS は VM データを自動的に同期します。同種クラウドのシナリオでは、フェイルオーバー前に VM データを手動で同期することもできます。

## 復旧計画を構成する

DRM を使用すると、保護グループごとにリカバリ プランを作成して、災害復旧設定をカスタマイズできます。リカバリ プランが実行されると、DRM はリカバリ サイトで保護されたオブジェクトを自動的に復元します。

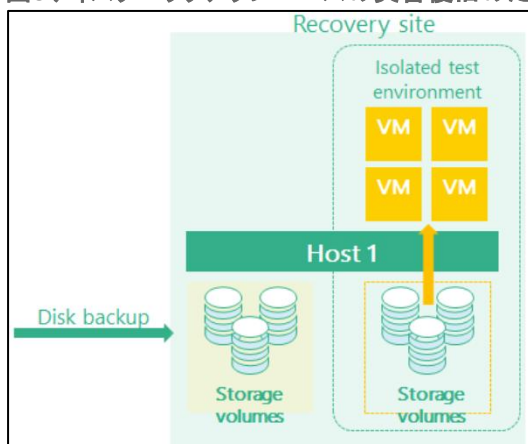
## 災害復旧シナリオ

### 復旧計画テスト

DRM を使用すると、サービスを中断することなく、リカバリ プランに基づいて保護されたオブジェクトをリカバリ サイト上の分離されたテスト環境にフェイルオーバーすることで、リカバリ プランが正しく動作するかどうかをテストできます。環境をクリアし、リカバリ プランの状態を準備完了に復元するには、リカバリ プラン テストを手動で終了する必要があります。

ディスク バックアップ ベースの災害復旧では、VM は復旧サイトのボリューム スナップショットに接続されます。

図3ディスクバックアップベースの災害復旧のための復旧計画テスト



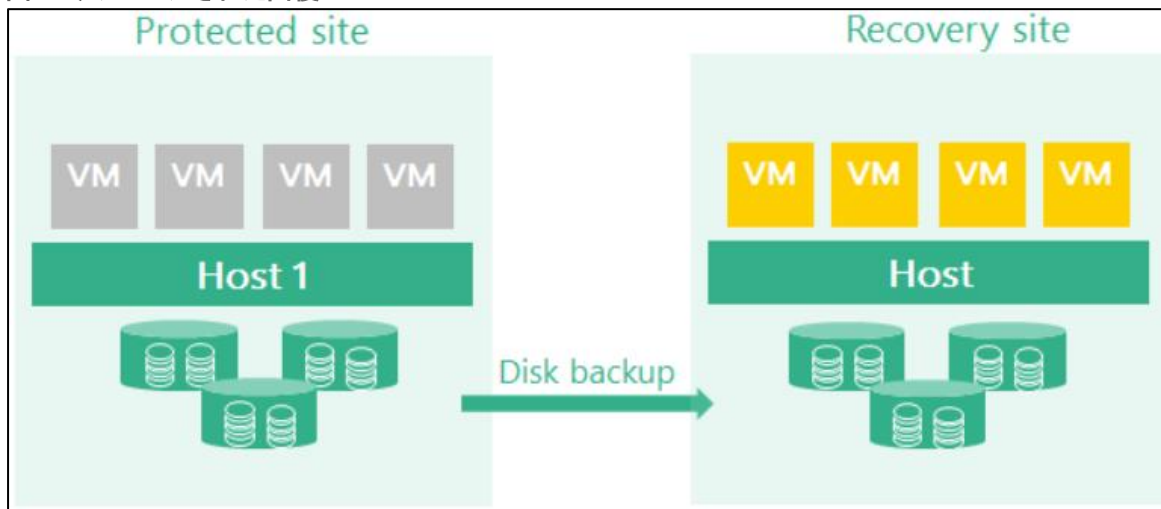
## スケジュールされた回復

スケジュールされたリカバリでは、保護されたサイトの定期的なメンテナンスのために、リカバリ サイト上の保護されたオブジェクトが再開されます。

同種クラウドのシナリオでは、スケジュールされたリカバリによって保護されたオブジェクトがシャットダウンされ、データのレプリケーションがトリガーされます。DRM は、保護されたすべてのデータをリカバリ サイトにコピーし終えた後にのみ、リカバリ サイトで VM を再開します。

異機種環境では、DRM は保護されたオブジェクトをシャットダウンしません。保護されたサイトで手動でシャットダウンする必要があります。

図4スケジュールされた回復

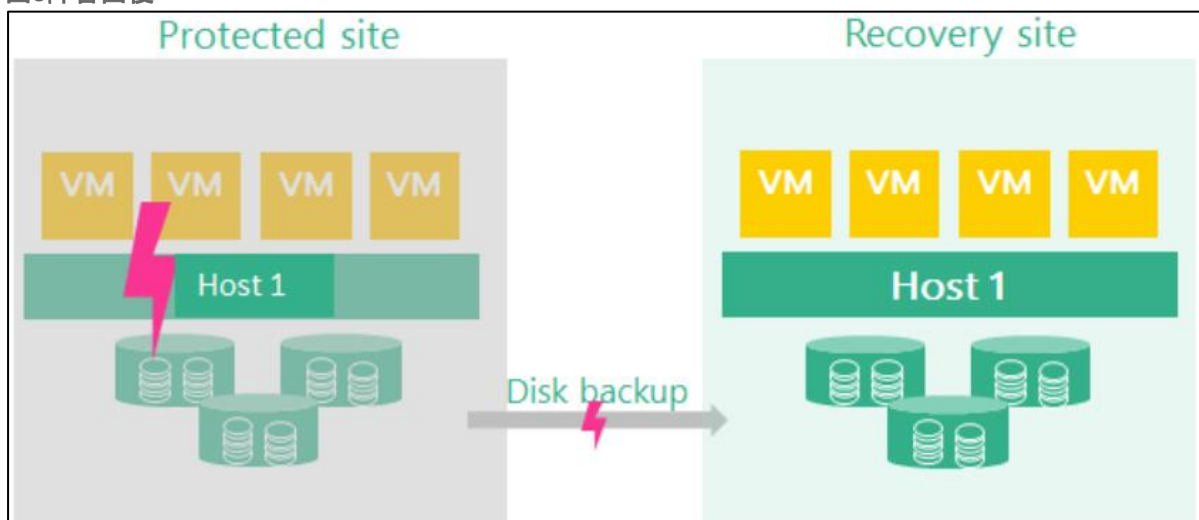


## 障害回復

障害回復では、回復計画に基づいて回復サイト上の保護されたオブジェクトを復元し、保護されたサイトに障害が発生した場合のサービス中断時間を短縮します。

ディスク バックアップ ベースの災害復旧の場合、フェイルオーバー復旧が実行されると RPO は 0 になります。

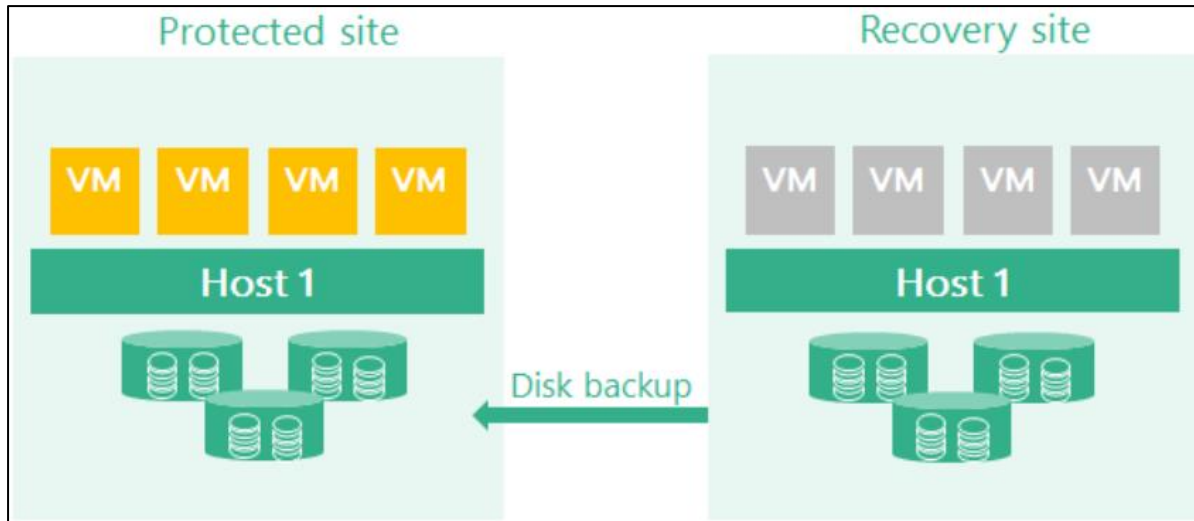
図5障害回復



## リバースリカバリ

ディスクレプリケーション ベースの災害復旧では、保護対象サイトが障害から復旧したときに、PE リバース復旧ツールを使用して、保護対象オブジェクトを復旧サイトから保護対象サイトにフォールバックできます。PE リバース復旧ツールは、保護対象サイトで実行されます。

図6リバースリカバリ

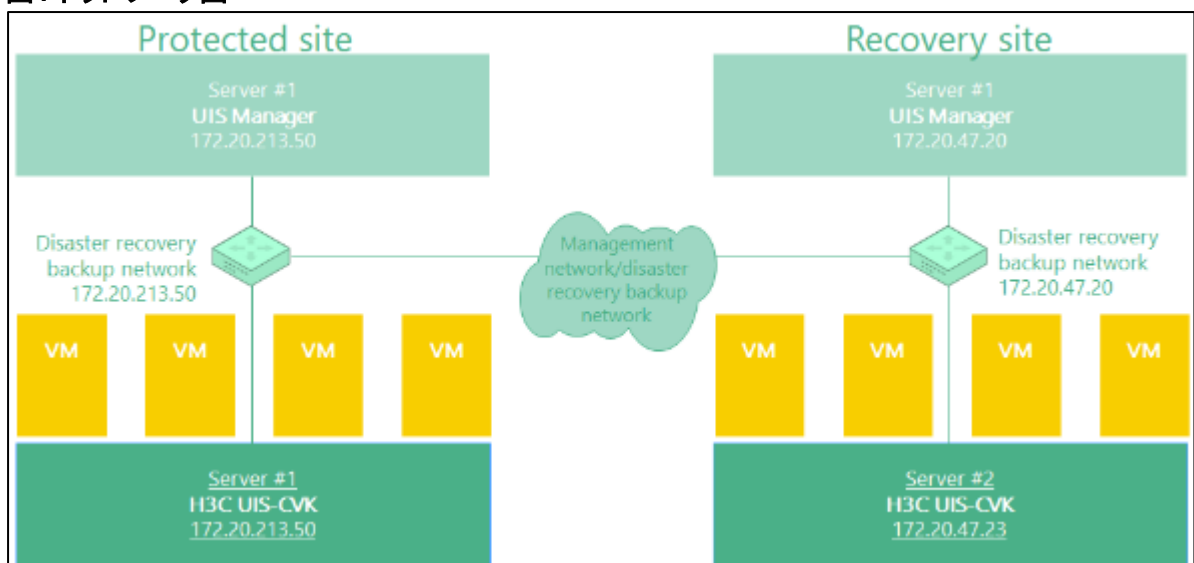


## バックアップデータの消去

ディスク バックアップ ベースの災害復旧の場合、サービスが保護サイトにフォールバックした後、復旧サイトから PE リバース復旧ツールを使用して、復旧した保護オブジェクトと一時データをクリアする必要があります。PE リバース復旧ツールは保護サイトで実行されます。

## ネットワーク図

図1ネットワーク図



# CDPコンポーネントをインストールする

CDP コンポーネントには、cdapServer と cdapStorage が含まれます。cdapServer コンポーネントは管理ノードにインストールする必要があるため、cdapStorage コンポーネントは CVK ホストにインストールする必要があります。

## 制限事項とガイドライン

- UIS 管理プラットフォームの個別の展開ノードでは、管理ノードではなく、1 つ以上の CVK ホストに cdapStorage コンポーネントをインストールする必要があります。
- ステートフル フェイルオーバー システムでは、プライマリ ノードに CDP コンポーネントをインストールするだけで済みます。
- 管理ノードに cdapServer コンポーネントと cdapStorage コンポーネントの両方をインストールするには、`cdap.inst/install_en.sh` コマンドを実行します。
- 管理プラットフォームが初期化された後、CDP コンポーネントをインストールします。

## 手順

1. cdapPackages.tgz パッケージをターゲット ホストにアップロードします。  
この例のパッケージ名は実際のパッケージ名と異なる場合があります。
2. ホストのバックエンドにログインし、`tar -vxzf cdapPackages.tgz` コマンドを実行して cdapPackages.tgz パッケージを解凍します。
3. 解凍されたパッケージが保存されているディレクトリにアクセスします。
4. `cdap.inst/cdapServer/server_en.sh` コマンドを実行して cdapServer をインストールします。
5. `cdap.inst/cdapStore/storage.sh` コマンドを実行して cdapStorage をインストールします。
6. cdapServer をアンインストールするには、`cdap.inst/removeServer.sh` コマンドを実行します。
7. cdapStorage をアンインストールするには、`cdap.inst/removeStore.sh` コマンドを実行します。

# 保護されたサイトを準備する

## 災害復旧クライアントをダウンロードする

### 制限事項とガイドライン

移行ライセンスを登録した後、プライマリ IP アドレスが使用できない場合に備えて、バックアップ サーバーのセカンダリ IP アドレスを設定できます。デフォルトでは、バックアップ サーバーのセカンダリ IP アドレスは UIS の管理ネットワーク IP アドレスです。

同種のクラウドの場合、保護された VM がバックアップ サーバーに自動的に接続できるように、バックアップ UIS システムからクライアントをダウンロードします。

## 手順


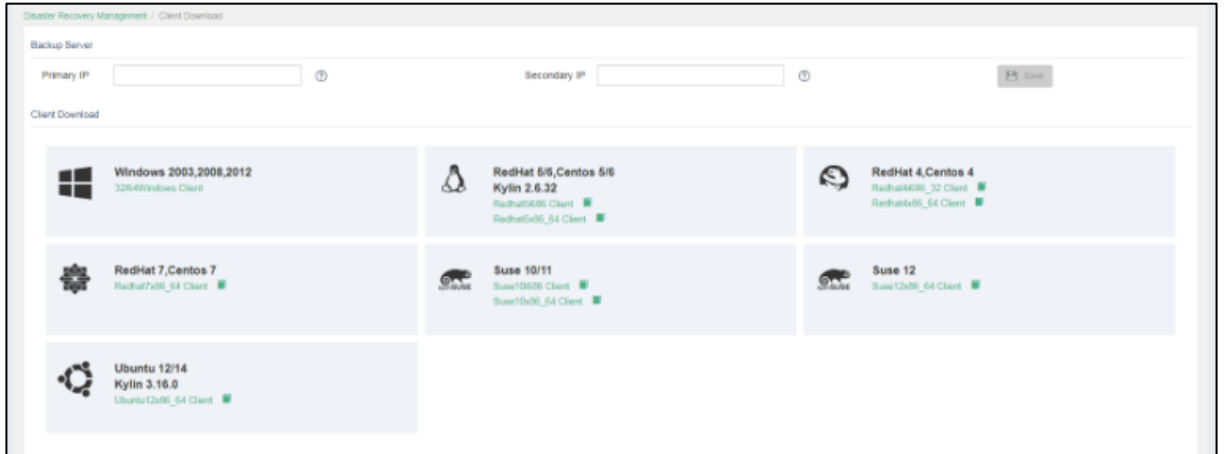
1. リカバリ サイトの UIS システムにログインします。
2. 上部のナビゲーション バーで **Services** をクリックし、ナビゲーション ペインから **Disaster Recovery Management > Download Client** を選択します。
3. 次のいずれかの方法を使用して、保護された VM 用の適切なクライアントをダウンロードします。
  - クライアント名をクリックして、名前の先頭に Clone\_Client が付いた ZIP パッケージ (例: `Clone_Client_Redhat5x86_64.zip`) をダウンロードします。次に、パッケージを解凍し、FTP ツールを使用してクライアントを保護された VM に転送します。
  - クライアントのアイコン  をクリックして URL を生成し、リモートコンソールを介してその URL を VM にコピーします。次に、URL からクライアントを VM にダウンロードします。

図1 災害復旧クライアントのダウンロード



## VM にディザスタリカバリ クライアントをインストールする(Windows クライアント)

### 制限事項とガイドライン

ベストプラクティスとして、ディザスタリカバリクライアントをインストールする前に、保護された VM のファイアウォールとセキュリティポリシーを無効にします。VM が UIS VM の場合は、セキュリティグループポリシーによって VM 上の移行ツールポートが開かれていることを確認します。

### 手順

1. コンソールから VM にログインします。

図2 VMへのログイン

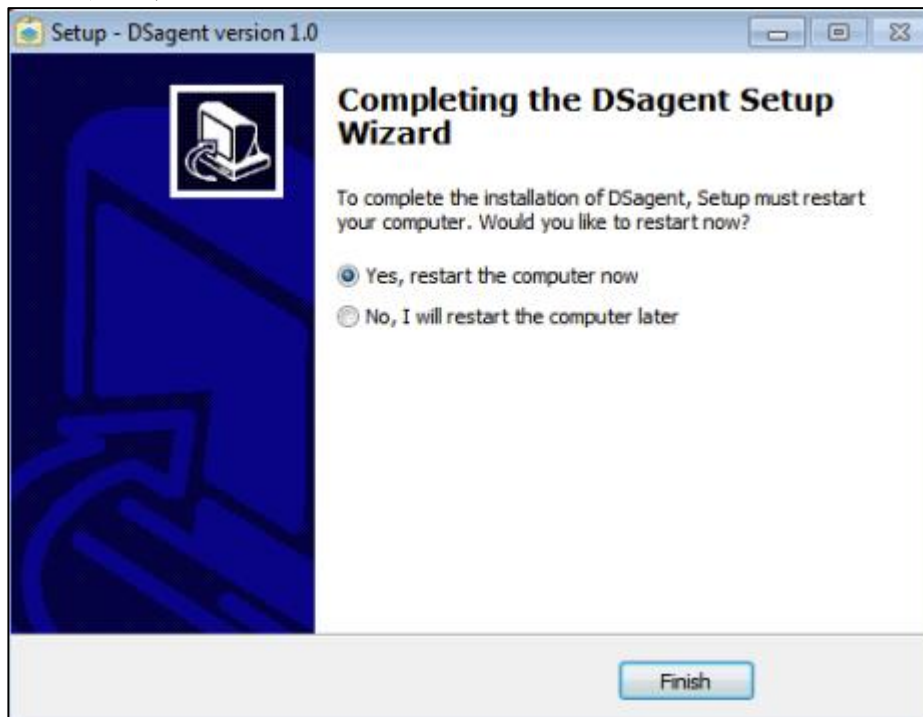


2. **Clone\_Client\_Win.exe** をダブルクリックし、言語を選択して、**OK**をクリックします。
3. ライセンス契約に同意し、インストール パスを選択して、クライアントのインストールを開始します。
4. CDP ドライバーのインストールを許可します。

5. VM を再起動するかどうかを選択します。

Windows VM を再起動するとサービスが中断されます。サービスへの影響を軽減するために再起動スケジュールを計画してください。

図3 取り付け完了



## 回復サイトを準備する

### 災害復旧ストレージノードを指定する

ディザスタリカバリ ストレージ ノードは、サービス保護とデータ転送中にデータを分散および処理し、より多くのストレージ スペースと機能を提供できます。ディザスタリカバリ ストレージ ノードとして動作するホストのみが、VM の復元先ホストとして使用できます。

災害復旧ストレージ ノードを指定するには:


1. 上部のナビゲーション バーで**Hosts**をクリックし、左側のナビゲーション ペインからターゲット ホストを選択します。
2. **More Actions**をクリックし、**Set as Storage Node**を選択します。
3. 開いたダイアログボックスで、**OK**をクリックします。

### 災害復旧ストレージノード上のストレージメディアとしてストレージプールを構成する

ストレージ メディアには、災害復旧バックアップ データが保存されます。ストレージ プールは、ストレージ メディアとして構成された後にのみ、ディスク バックアップ ベースの災害復旧の宛先ストレージ プールとして使用できます。ストレージ プールをストレージ メディアとして構成すると、ストレージ ノードはオフラインになり、その後オンラインになります。

災害復旧ストレージ ノード上のストレージ メディアとしてストレージ プールを構成するには、次の手順を実行します。


1. 上部のナビゲーション バーで **Hosts**をクリックし、左側のナビゲーション ペインからターゲット ホストを

- 選択します。
- 2. **Storage**タブをクリックします。
- 3. ストレージ プールの **Actions**列 にあるアイコン  をクリックします。
- 4. 開いたダイアログボックスで、**OK**をクリックします。

## vSwitch のネットワーク タイプをバックアップから災害復旧に変更する

ディザスタリカバリ ネットワークは、ディザスタリカバリ用のバックアップ データを送信します。ネットワーク タイプがバックアップ ネットワークの場合、vSwitch のネットワーク タイプをバックアップからディザスタリカバリに変更できます。ディザスタリカバリ ネットワーク vSwitch を指定しない場合、バックアップ データは管理ネットワーク vSwitch **vswitch0** を介して送信されます。

vSwitch のネットワーク タイプをバックアップから災害復旧に変更するには:

1. 上部のナビゲーション バーで**Hosts**をクリックし、左側のナビゲーション ペインからターゲット ホストを選択します。
2. **vSwitches**タブをクリックします。
3. バックアップ ネットワーク vSwitch または vswitch0 の**Actions**]列 のアイコン  をクリックします。
4. 開いたダイアログボックスで、**OK**をクリックします。

## ディスクバックアップベースの災害復旧を構成する サイトを構成する

1. 保護されたサイトの UIS システムにログインします。
2. 上部のナビゲーション バーで**Services**をクリックし、左側のナビゲーション ペインから**Recovery Management > Sites**を選択します。
3. **Add Site**をクリックします。
4. ローカルサイトを構成します。  
ローカル UIS システムの IP アドレスを入力します。
5. リモートサイトを構成します。

ディスク バックアップ ベースの災害復旧のためにストレージ アレイ設定を構成する必要はありません。

## 保護グループを構成する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**Disaster Recovery Management > Protection Groups**を選択します。
2. **Add Protection Group**をクリックします。
3. 災害復旧の種類として**Disk Backup**を選択し、基本設定を構成して、**Next**をクリックします。
  - ・均質クラウドの場合は、保護サイトとリカバリ サイトを選択する必要があります。
  - ・異種クラウドの場合、保護されたサイトを選択する必要はありません。

図1 基本的な保護グループ設定の構成

The screenshot shows the 'Add Protection Group' dialog box with the 'Basic Info' tab selected. The 'Disaster Recovery Type' is set to 'Disk Backup'. The 'Service Type' is 'Standalone'. The 'Next' button is highlighted in green. The 'Details' pane on the right lists the configuration details.

4. 既存の災害復旧ポリシーを選択するか、新しいポリシーを作成して、**Next**をクリックします。災害復旧ポリシーには、同期とスナップショットの設定が含まれます。災害復旧ポリシーの構成の詳細については、UIS のオンライン ヘルプを参照してください。

保護されたサイトとリカバリ サイト間のデータの一貫性を確保するには、サービスに基づいて適切な同期間隔を設定します。値が 0 の場合、同期は無効です。

5. ターゲット クラスター、ホスト、およびストレージ プールを選択します。  
6. とアイコンをクリックしてドラッグし、それぞれ vSwitch とネットワーク プロファイルを構成します。災害復旧バックアップ ネットワーク vSwitch または vswitch0 とデフォルトのネットワーク プロファイルを使用します。

異機種クラウドの場合は、災害復旧ネットワーク vSwitch とポート プロファイルを指定してネットワーク マッピングを構成します。

7. **Finish**をクリックします。  
8. 保護グループの**Add VM**をクリックします。  
9. VM を選択し、**OK**をクリックします。  
システムには、災害復旧クライアントがインストールされ、ネットワーク設定が正しい VM が表示されます。

## 回復計画を作成する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**Disaster Recovery Management > Recovery Plans**を選択します。
2. **Add Recovery Plan**をクリックします。
3. 名前と説明を入力し、追加した保護グループを選択し、保護された VM を選択して、**OK**をクリックします。

保護グループ内の VM のさまざまな要件を満たすために、複数のリカバリ プランを構成できます。この例では、すべての VM が同じリカバリ プランを使用します。

4. リカバリ プランは作成後、**Initialize**状態になります。



## 復旧計画のテストを実行する

### 復旧計画のテストを開始する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**Disaster Recovery Management > Recovery Plans > Recovery Plan Name**を選択します。
2. **Start Testing**をクリックします。
3. 開いたダイアログ ボックスで**OK**をクリックするか、保護グループ マッピング ページにアクセスして、リカバリ サイトの vSwitch とネットワーク プロファイルを編集します。
4. 回復タスクの状態を表示するには、**Recovery Tasks**タブをクリックします。
5. テストの詳細を表示するには、リカバリ タスクの実行時間リンクをクリックします。
6. 保護されたサイトで保護された VM が正しく実行されていることを確認します。
7. 保護された VM が、リカバリ サイトにマッピングされたストレージ リソースが接続されたホストに復元されていることを確認します。

UIS は、宛先ストレージ プールに接続されているホストから最適なホストを選択して、VM を復元します。

### 復旧計画のテストを完了する

1. リカバリ プランの概要ページで**Stop Testing**をクリックします。
2. 回復タスクの状態を表示するには、**Recovery Tasks**タブをクリックします。
3. テストの詳細を表示するには、リカバリ タスクの実行時間リンクをクリックします。
4. 保護された VM がリカバリ サイトから削除され、マップされたストレージ リソースが削除されていることを確認します。
5. リカバリ プランが**Recovery Tasks**状態であることを確認します。

通信の問題を回避するには、マッピングされたポート プロファイルと vSwitch のネットワーク設定をテスト前の状態に変更する必要があります。

## スケジュールされたリカバリを実行する

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**Disaster Recovery Management > Recovery Plans > Recovery Plan Name**を選択します。
2. **Scheduled Recovery**をクリックします。

異機種クラウドの場合、データエラーを回避するために、プロンプトに従って保護された VM または運用ノードをシャットダウンします。
3. 回復タスクの状態を表示するには、**Recovery Tasks**タブをクリックします。
4. タスクの詳細を表示するには、回復タスクの実行時間リンクをクリックします。
5. 保護されたサイトで保護された VM がシャットダウンされていることを確認します。
6. 保護された VM が、リカバリ サイトにマップされたリソースが接続されたホストに復元されていることを確認します。

## バックアップデータを消去

1. 上部のナビゲーション バーで**Services**をクリックし、ナビゲーション ペインから**Disaster Recovery Management > Recovery Plans > Recovery Plan Name**を選択します。
2. 「**Clear Backup Data**」をクリックします。
3. 開いたダイアログ ボックスでプロンプトを読み、**OK**をクリックします。
4. 回復タスクの状態を表示するには、**Recovery Tasks**タブをクリックします。

5. タスクの詳細を表示するには、回復タスクの実行時間リンクをクリックします。
6. 保護された VM がリカバリ サイトから削除され、マップされたストレージ リソースが削除されていることを確認します。

## 障害回復を実行する

1. 上部のナビゲーション バーで **Services** をクリックし、ナビゲーション ペインから **Disaster Recovery Management > Recovery Plans > Recovery Plan Name** を選択します。
2. **Failure Recovery** をクリックします。
3. 回復タスクの状態を表示するには、**Recovery Tasks** タブをクリックします。
4. 保護されたサイトで保護された VM がシャットダウンされていることを確認します。
5. 保護された VM が、リカバリ サイトにマップされたリソースが接続されたホストに復元されていることを確認します。

# DPDKを構成する

図1 DPDK構成フローチャート

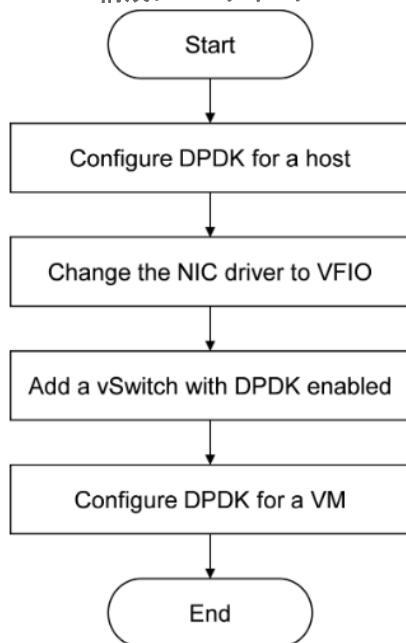


表1 DPDK構成ワークフロー

手順	備考
ホストのDPDKを有効にする	必須。 ホストで DPDK を有効にするには、HugePages、IOMMU、CPU 分離、割り込みアフィニティ設定など、ホストのブート設定を構成する必要があります。
NICドライバを編集する	必須。 ホストで DPDK を有効にした後、ホスト上に DPDK 対応の vSwitch を作成し、VM が外部ネットワークと通信できるように物理 NIC を vSwitch にバインドする必要があります。このタスクを実行して、vSwitch にバインドする物理 NIC のドライバーを VFIO に変更します。
DPDKを有効にした vSwitchを追加する	必須。 DPDK 対応ホストで DPDK が有効になっている vSwitch を作成するには、このタスクを実行します。
VMのDPDK設定を構成する	必須。 このタスクを実行して、VM の HugePages および仮想 NUMA 機能を有効にし、vNIC が DPDK 対応の vSwitch に接続できるようにします。

## ホストのDPDKを有効にする

### ブート設定を構成する

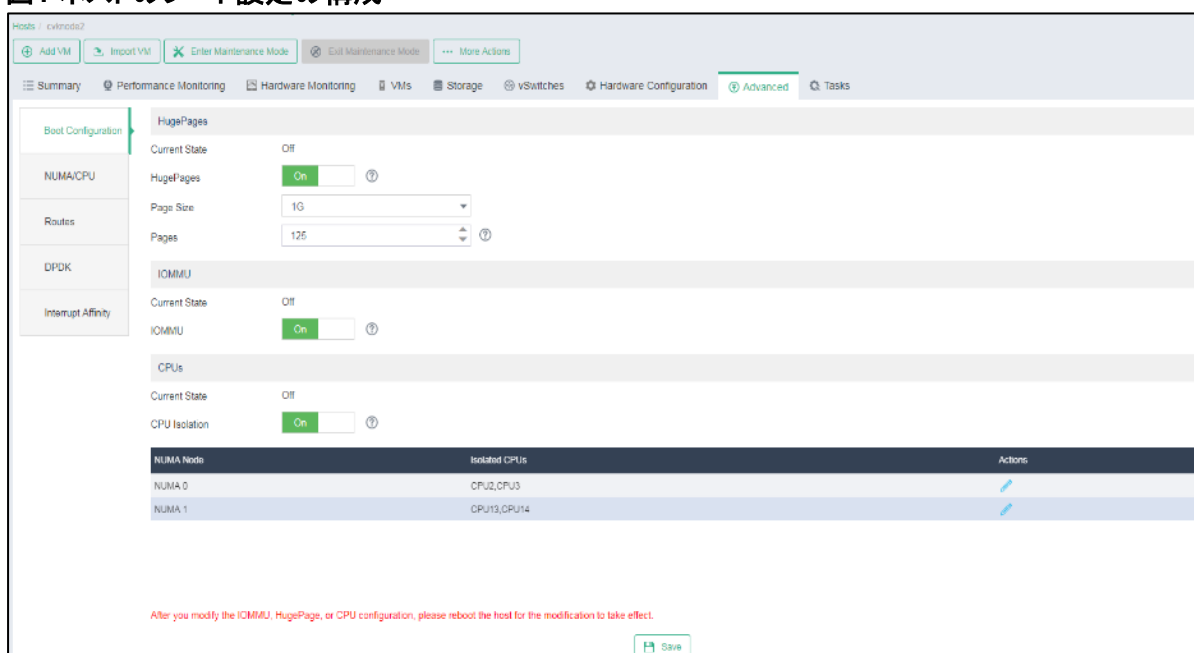
この機能を使用すると、HugePages、IOMMU、CPU 分離設定など、ホストのブート設定を構成できます。

- **HugePages** — HugePages を使用すると、ページ サイズが 4K から 2MB または 1GB に増加し、ページ テーブル エントリへのアクセスに必要なシステム リソースの量が削減され、Translation Lookaside Buffer (TLB) ヒット率が向上します。
- **IOMMU** — 入出力メモリ管理ユニット (IOMMU) は、仮想アドレスを物理アドレスにマッピングし、物理デバイスが仮想メモリ システムで動作できるようにして、VM のパフォーマンスを

向上させます。

- **CPU 分離**- CPU 分離により、指定された CPU がホストの CPU スケジューリング ポリシーから削除されます。システムは、分離された CPU にタスクを割り当てません。分離された CPU は、DPDK が有効になっているホストと VM が CPU リソースを時間どおりに取得できるように、VM と DPDK 用に予約されます。
1. 上部のナビゲーション バーで、**Hosts**をクリックします。
  2. ターゲット ホストを選択し、**Advanced**タブをクリックします。
  3. HugePages を有効にし、必要に応じてページ サイズとページ数を設定します。
  4. IOMMU を有効にします。
  5. CPU 分離を有効にします。

図1 ホストのブート設定の構成

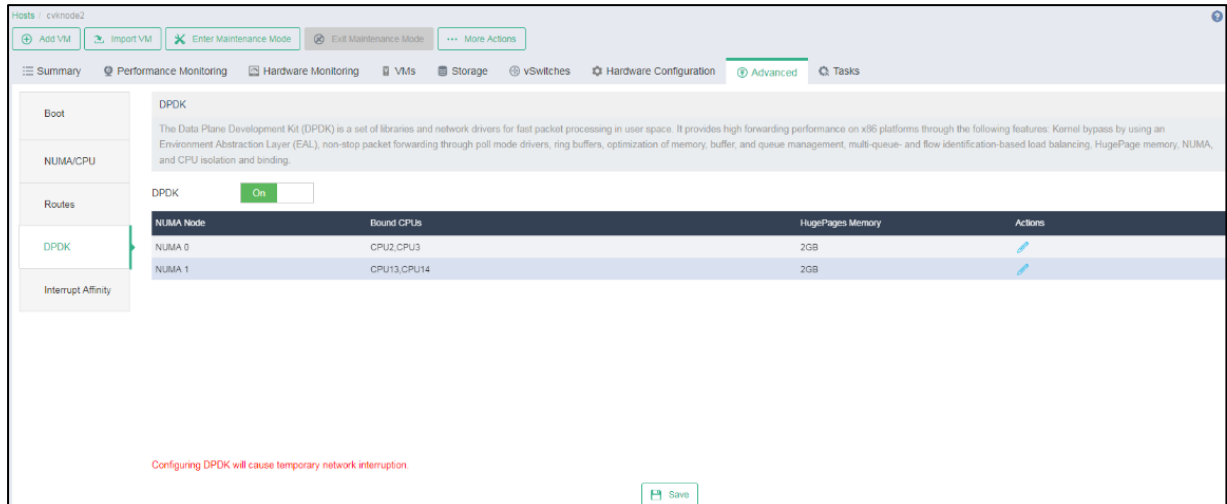


6. 「**Save**」をクリックします。
7. 設定を有効にするには、ホストを再起動します。
  - a. **Enter Maintenance Mode** をクリックし、開いたダイアログ ボックスで**OK**をクリックします。
  - b. **More Actions**をクリックし、**Restart Host**を選択して、開いたダイアログ ボックスで**OK**をクリックします。
  - c. ホストが再起動したら、**Exit Maintenance Mode**をクリックし、表示されるダイアログ ボックスで**OK**をクリックします。

## DPDK設定を構成する

1. 上部のナビゲーション バーで、**Hosts**をクリックします。
2. ターゲット ホストを選択し、**Advanced**タブをクリックします。
3. **DPDK**タブをクリックします。
4. DPDK を有効にします。
5. **NUMA ノードの編集**アイコンをクリックし、HugePages メモリ サイズを 2 GB に設定し、バインドされた CPU を選択して、**OK**をクリックします。

図2 ホストのDPDK設定の構成



6. 他の NUMA ノードも同様に構成します。
7. **Save**をクリックします。

## (オプション) 割り込みアフィニティ設定を構成する

この機能を使用すると、アフィニティ設定をサポートする割り込みを指定した CPU に割り当てることができます。その後、割り込み要求は指定した CPU によって処理されます。


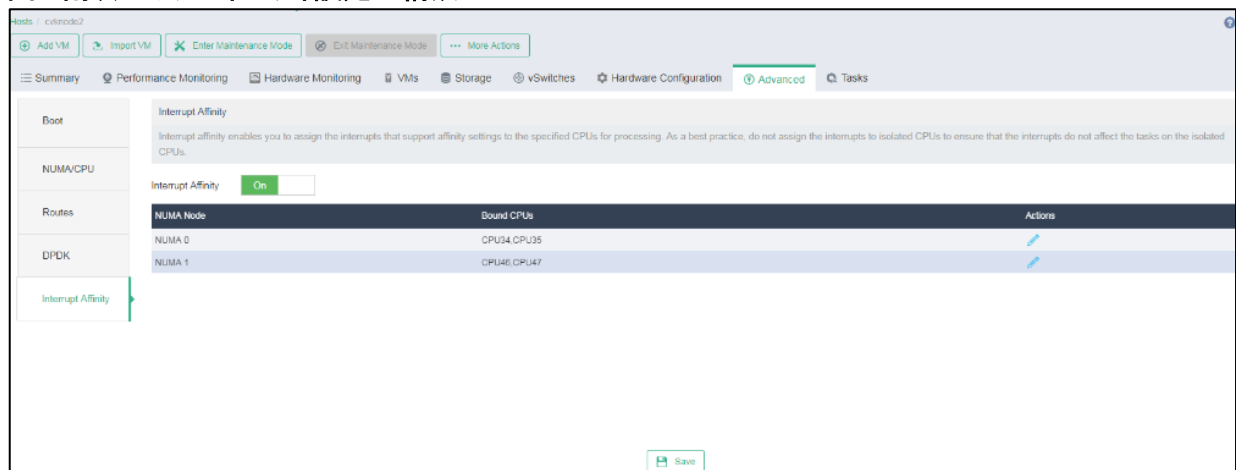
1. 上部のナビゲーション バーで、**Hosts**をクリックします。
2. ターゲット ホストを選択し、**Advanced**タブをクリックします。
3. **Interrupt Affinity**タブをクリックします。
4. 割り込みアフィニティを有効にします。
5. NUMA ノードの編集アイコンをクリックし、「ブート設定を構成する」の手順 5 で選択した CPU とは異なる CPU を選択して、**OK**をクリックします .

図3 割り込みアフィニティ設定の構成



6. **Save**をクリックします。

# NICドライバーを編集する


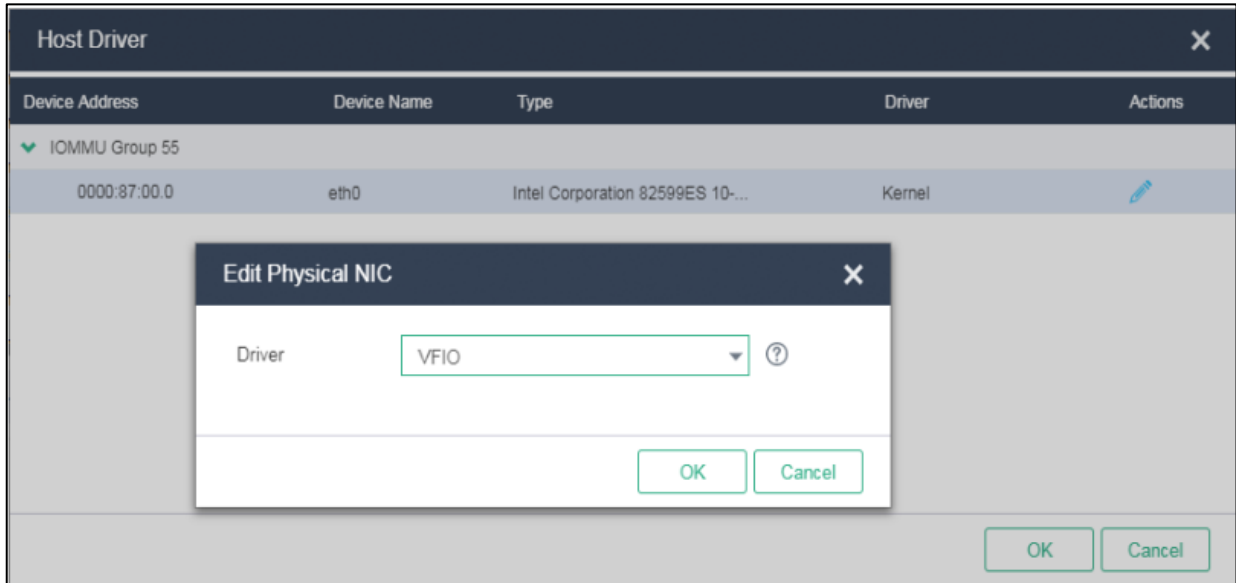
1. 上部のナビゲーションバーで、**Hosts**をクリックします。
2. ターゲットホストを選択し、**Hardware Configuration**タブをクリックします。
3. 対象の物理NICの**Edit**アイコンをクリックし、ドライバーを**VFIO**に設定して、**OK**をクリックします。

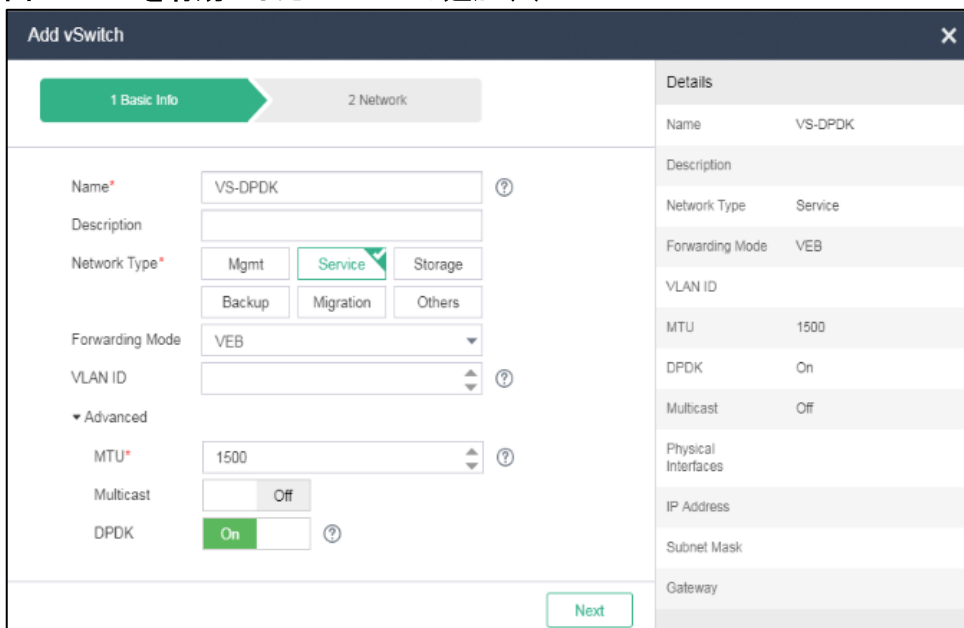
図1 NICドライバの編集



# DPDKを有効にしたvSwitchを追加する

1. 上部のナビゲーションバーで、**Hosts**をクリックします。
2. ホストを選択し、**vSwitches**タブをクリックします。
3. **Add**をクリックします。
4. 名前を指定し、**Service**ネットワークタイプを選択し、必要に応じてVLAN IDを指定し、**Advanced**をクリックしてDPDKを有効にし、**Next**をクリックします。

図1 DPDKを有効にしたvSwitchの追加(1)



5. ドライバーを変更した物理 NIC を選択し、物理 NIC の IP アドレスとサブネット マスクを指定して、**Finish** をクリックします。

図2 DPDKを有効にしたvSwitchの追加(2)

Details	
Name	VS-DPDK
Description	
Network Type	Service
Forwarding Mode	VEB
VLAN ID	
MTU	1500
DPDK	On
Multicast	Off
Physical Interfaces	pci_87_00_0
IP Address	
Subnet Mask	

## VMのDPDK設定を構成する

1. 上部のナビゲーション バーで、**VMs**をクリックします。
2. 左側のナビゲーション ペインから **VM** を選択し、**Edit**をクリックします。
3. CPUタブをクリックし、VM の動作モードをパススルーに変更します。

図1 VMの動作モードをパススルーに変更する

If a VM is running or suspended, modifications to the number of CPUs, CPU operating mode, physical CPU binding, and CPU resource reservation take effect after the VM is restarted. This restriction does not apply to VM OSs that support CPU hotplug.

Current Assigned	2
CPUs*	2
CPU Cores*	1
Host CPUs	48
Operating Mode	Straight-Through

▶ Advanced


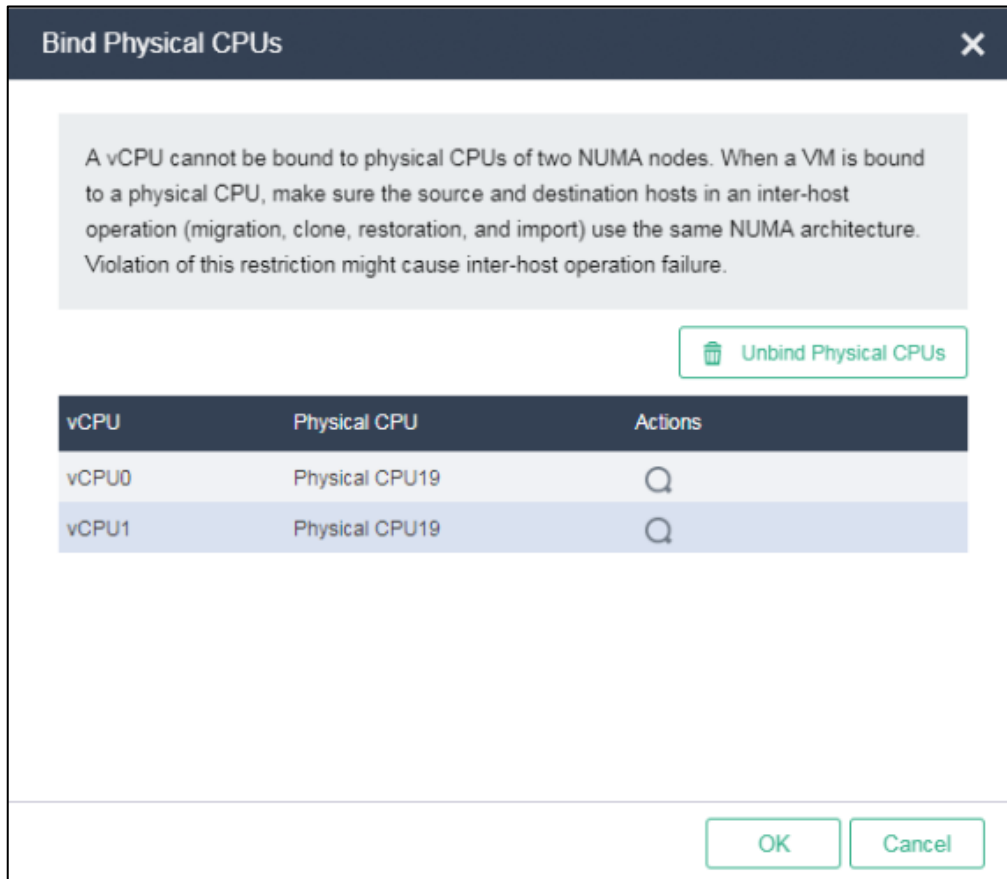
4. **CPU Cores**フィールドの右側にある**Bind Physical CPUs** アイコン  をクリックし、1 つまたは複数の物理 CPU を選択して、**OK** をクリックします。1 つの VM にバインドされた物理 CPU は、同じ NUMA ノードに属している必要があります。

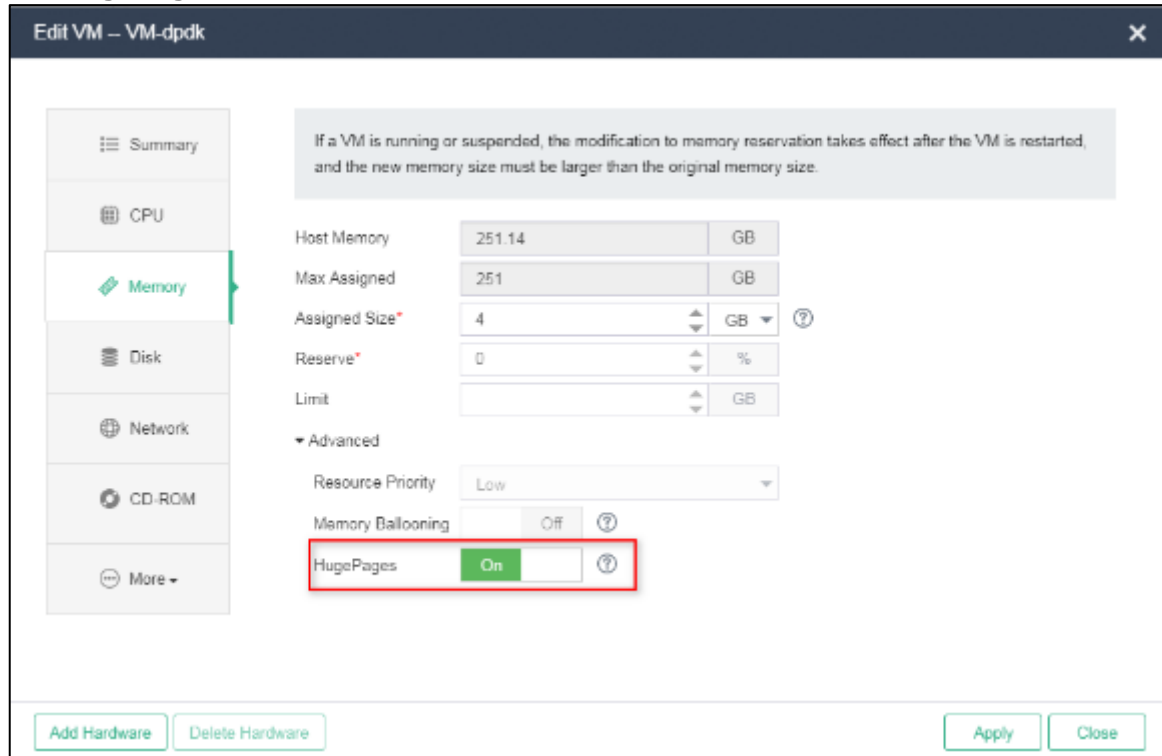
図2 vCPUを物理CPUにバインドする



5. HugePagesをオンにするには、**Memory**タブをクリックします。このオプションは、VM がシャットダウンしているときのみオンにできます。また、この機能は、メモリ予約、メモリ制限、リソース優先度、メモリバレーニングと相互に排他的です。

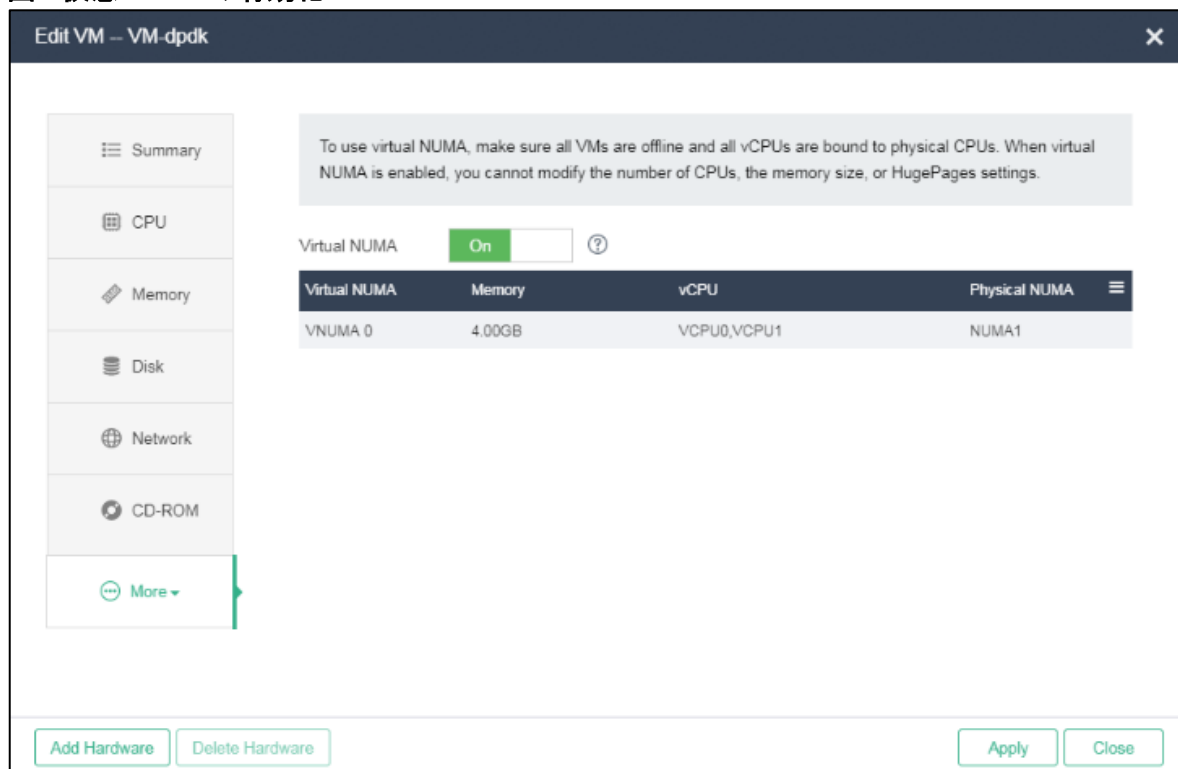


図3 HugePagesの有効化



6. Moreをクリックし、Virtual NUMAをクリックして仮想 NUMA を有効にします。

図4 仮想NUMAの有効化



7. Add Hardwareをクリックし、Hardware TypeリストからNetworkを選択して、Nextをクリックします。

図5 DPK NICの追加(1)

1 Hardware Type      2 Configure

Hardware Type    Network

NIC hardware is the interface that connects a VM to transmission medium.

Next

Details	
Hardware Type	Network
Device Model	High-Speed NIC
vSwitch	vs-dpdk
Port Profile	Default
MAC	Automatic
Bound IPv4	
MTU	1500

8. **Device Model**リストから**High-Speed NIC**を選択し、DPDK が有効になっている vSwitch を選択し、必要に応じてその他の設定を構成して、**Finish**をクリックします。

図6 DPK NICの追加(2)

1 Hardware Type      2 Configure

Device Model    High-Speed NIC

Hot Swappable    On

vSwitch\*        vs-dpdk

Port Profile\*    Default

Virtual Firewall    [Search] [X]

MAC Address      Automatic [Manual]

Assignment Method

MAC              0c:da:41:1d:db:95

Bound IPv4        [Empty]

MTU\*             1500

Previous      Finish

Details	
Hardware Type	Network
Device Model	High-Speed NIC
vSwitch	vs-dpdk
Port Profile	Default
MAC	Automatic
Bound IPv4	
MTU	1500

# SR-IOV設定を構成する

図1 SR-IOV構成フローチャート

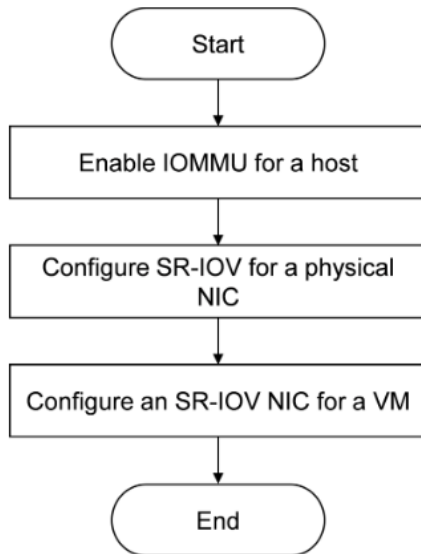


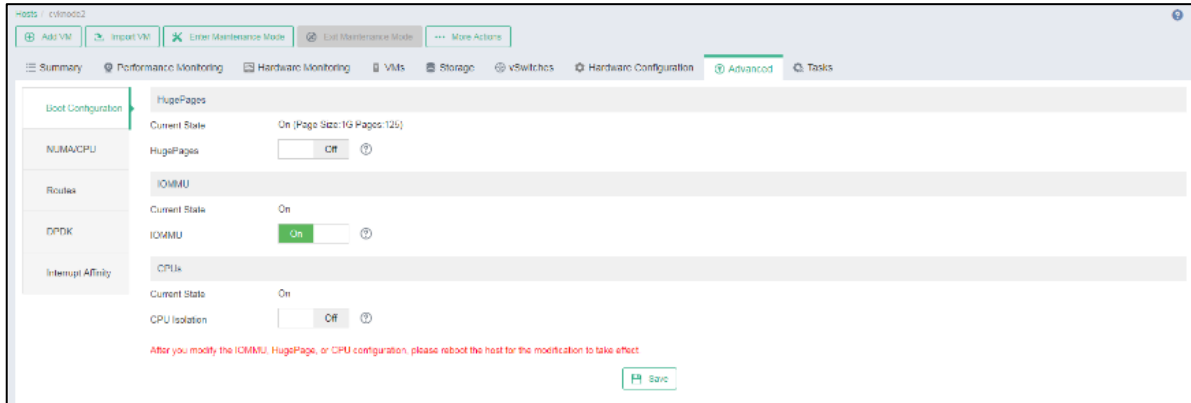
表1 SR-IOV設定ワークフロー

手順	備考
ホストのIOMMUを有効にする	必須。 ホスト上の物理 NIC に SR-IOV を構成する前に、このタスクを実行してホストの IOMMU を有効にする必要があります。構成を有効にするには、ホストを再起動する必要があります。
物理NICのSR-IOVを構成する	必須。 物理 NIC の SR-IOV を有効にし、vNIC の数を設定するには、このタスクを実行します。 H3C UIS マネージャーは、SR-IOV をサポートする複数のタイプの NIC およびゲスト OS と互換性があります。詳細については、「SR-IOV」を参照してください。
VM の SR-IOV NIC を構成する	必須。 VM の SR-IOV NIC を構成するには、このタスクを実行します。SR-IOV NIC で構成された VM の一部の機能は使用できなくなります。詳細については、「SR-IOV」を参照してください。

# ホストのIOMMUを有効にする

1. 上部のナビゲーション バーで、**Hosts**をクリックします。
2. ターゲット ホストを選択し、**Advanced**タブをクリックします。
3. IOMMU を有効にします。

図1 IOMMUの有効化

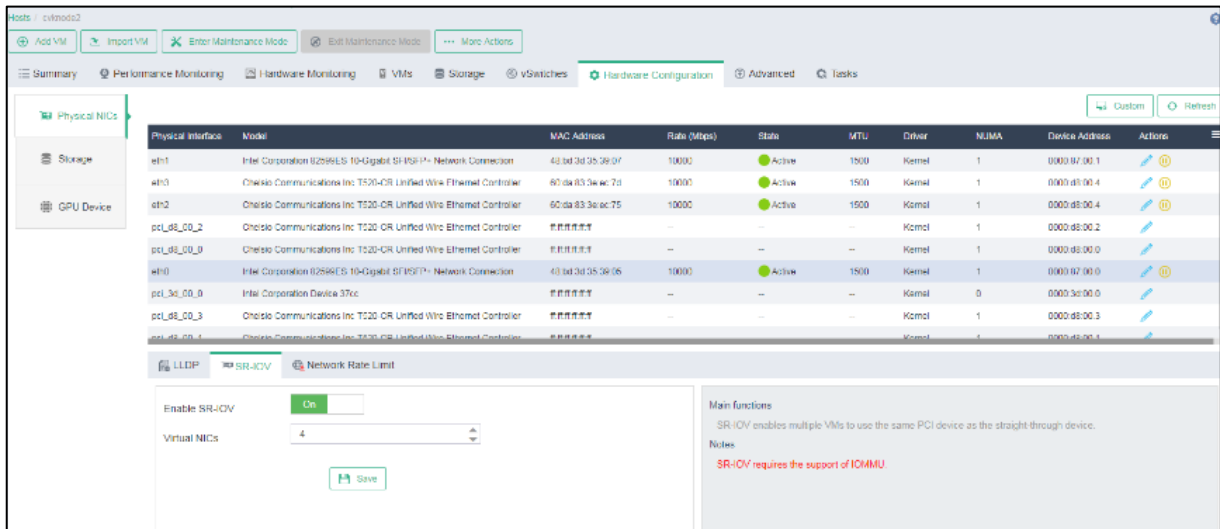


4. **Save**をクリックします。
5. 設定を有効にするには、ホストを再起動します。
  - a. **Enter Maintenance Mode** をクリックし、開いたダイアログ ボックスで**OK**をクリックします。
  - b. **More Actions**をクリックし、**Restart Host**を選択して、開いたダイアログ ボックスで**OK**をクリックします。
  - c. ホストが再起動したら、**Exit Maintenance Mode**をクリックし、表示されるダイアログ ボックスで**OK**をクリックします。

# 物理NICのSR-IOVを構成する

1. 上部のナビゲーション バーで、**Hosts**をクリックします。
2. ターゲット ホストを選択し、**Hardware Configuration**タブをクリックします。
3. 物理 NIC を選択し、**SR-IOV**タブをクリックします。
4. SR-IOV を有効にし、vNIC の数を設定して、**Save**をクリックします。

図1 SR-IOVの有効化



# VM の SR-IOV NIC を構成する

1. 上部のナビゲーション バーで、VMsをクリックします。
2. VM を選択し、**Edit**をクリックします。
3. **Add Hardware**をクリックします。
4. **Hardware Type**リストから**Network**を選択し、**Next** をクリックします

The screenshot shows the 'Add Hardware' dialog box with the 'Hardware Type' dropdown set to 'Network'. A red text message below the dropdown reads: 'NIC hardware is the interface that connects a VM to transmission medium.' The 'Next' button is visible at the bottom right. The 'Details' panel on the right shows the following configuration:

Details	
Hardware Type	Network
Device Model	High-Speed NIC
vSwitch	vswitch0
Port Profile	Default
MAC	Automatic
Bound IPv4	
MTU	1500

5. **Device Model**リストから**SR-IOV Straight-Through NIC**を選択し、SR-IOV が有効になっている物理 NIC を選択して、**Finish**をクリックします。

The screenshot shows the 'Add Hardware' dialog box in the 'Configure' step. The 'Device Model' dropdown is set to 'SR-IOV Straight-Through NIC' and the 'Physical NIC\*' dropdown is set to 'eth0'. The 'Driver Type' is set to 'VFIO'. The 'MAC Address' is set to 'Automatic'. The 'Details' panel on the right shows the following configuration:

Details	
Hardware Type	Network
Device Model	SR-IOV Straight-Through NIC
MAC	Automatic
Driver Type	VFIO
Physical NIC	eth0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection
VLAN ID	

6. VM を起動し、VM のゲスト OS にドライバーをインストールします。ゲスト OS が SR-IOV NIC モデルを識別できる場合、SR-IOV NIC は正常に構成されます。

# 分散仮想ファイアウォールを構成する

仮想ファイアウォールは、フィルタリング ルールのセットです。仮想ファイアウォールは、VM を攻撃から保護し、データセンター内の VM のセキュリティと信頼性を向上させます。

図1仮想ファイアウォール構成フローチャート

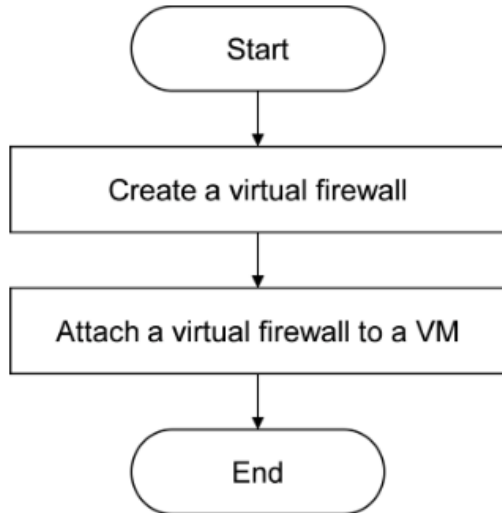


表1 仮想ファイアウォールの設定ワークフロー

手順	備考
仮想ファイアウォールを作成する	必須。 仮想ファイアウォールを作成し、仮想ファイアウォールのアクセス ルールを定義するには、このタスクを実行します。
VMに仮想ファイアウォールを接続する	必須。 仮想ファイアウォールを VM の NIC に接続するには、このタスクを実行します。 仮想ファイアウォールと ACL は相互に排他的です。VM に仮想ファイアウォールと ACL の両方が設定されている場合、仮想ファイアウォールが有効になります。

## 仮想ファイアウォールを作成する

1. 上部のナビゲーション バーで**System**をクリックし、ナビゲーション ペインから**Security Management > Virtual Firewalls**を選択します。
2. **Add** をクリックします。開いたダイアログ ボックスで、仮想ファイアウォールの名前を入力し、仮想ファイアウォールの種類を選択します。

図1 仮想ファイアウォールの作成

The screenshot shows a dialog box titled "Add Virtual Firewall". It has three input fields: "Name\*", "Description", and "Type" (set to "Whitelist"). A green "Add Rule" button is on the right. Below is a table with the following content:

Direction	IP Protocol	Port/Type-Code	Remote CIDR	Actions
Egress	Any	Any	0.0.0.0/0	

At the bottom right are "OK" and "Cancel" buttons.

パラメータ	説明
タイプ	<p>仮想ファイアウォールの種類を選択します。オプションには、ホワイトリストとブラックリストがあります。ホワイトリスト仮想ファイアウォールのルールに一致するパケットは許可され、その他のパケットはドロップされます。ブラックリスト仮想ファイアウォールのルールに一致するパケットはドロップされ、その他のパケットは許可されます。</p> <ul style="list-style-type: none"> <li>ホワイトリスト仮想ファイアウォールを構成する場合、VM からリモート サイトへのすべてのトラフィックを許可する 2 つのデフォルトの出カールールが存在します。リモート サイトから VM への特定のトラフィックを許可するには、必要に応じて入カールールを構成します。VM からリモート サイトへのトラフィックを制御するには、2 つのデフォルトの出カールールを削除し、必要に応じて出カールールを構成します。</li> <li>ブラックリスト仮想ファイアウォールを構成する場合、デフォルトのルールは存在せず、すべてのパケットが許可されます。リモート サイトから VM への特定のトラフィックを拒否するには、必要に応じて入カールールを構成します。VM からリモート サイトへの特定のトラフィックを拒否するには、必要に応じて出カールールを構成します。</li> </ul>

3. ファイアウォールを追加するページで、**Add Rule**をクリックします。開いたダイアログ ボックスで、ルールの種類と方向を選択し、ポート、ピア IP アドレス、サブネット マスクを指定して、**OK**をクリックします。

図2 ルールの追加

パラメータ	説明
方向	ルールが適用される接続の方向を指定します。 <b>Ingress</b> は、リモート サイトによって開始された接続を示します。 <b>Egress</b> は、VM によって開始された接続を示します。
開始ポート/終了ポート	ポート番号の範囲を指定します。方向が入力の場合、ポート番号の範囲は、リモート サイトがアクセスする VM ポートです。方向が出力の場合、ポート番号の範囲は、VM がアクセスするリモート サイト ポートです。 <b>Custom TCP Rule</b> または <b>Custom UDP Rule</b> を選択した場合、このパラメーターは必須です。
タイプ	ICMP パケット タイプを選択します。 <b>Custom ICMP Rule</b> を選択した場合、このパラメーターは必須です。
コード	ICMP コードを選択します。 <b>Custom ICMP Rule</b> を選択した場合、このパラメーターは必須です。
IP プロトコル	仮想ファイアウォールがトラフィック制御を実装するプロトコルを選択します。 <b>Other Rule</b> を選択した場合、このパラメーターは必須です。
IPタイプ	IP パケット タイプを選択します。オプションには IPv4 と IPv6 があります。VM IPv6 アドレス管理が有効になっている場合は、このパラメーターが必要です。
リモート IP アドレス	リモート サイトの IPv4 または IPv6 アドレスをセミコロンで区切って入力します (例: 1.1.1.1;12.3.3.3/16、20:ef::;21:ef::90/64)。このパラメーターを設定しない場合は、デフォルト値 (IPv4 の場合は 0.0.0.0、IPv6 の場合は ::) が使用され、ルールはすべての IPv4 または IPv6 アドレスに一致します。

## VMに仮想ファイアウォールを接続する

1. 上部のナビゲーション バーでVMsをクリックし、左側のナビゲーション ペインから VM を選択します。
2. **Edit**をクリックします。
3. 開いたダイアログボックスで、**Network**をクリックします。




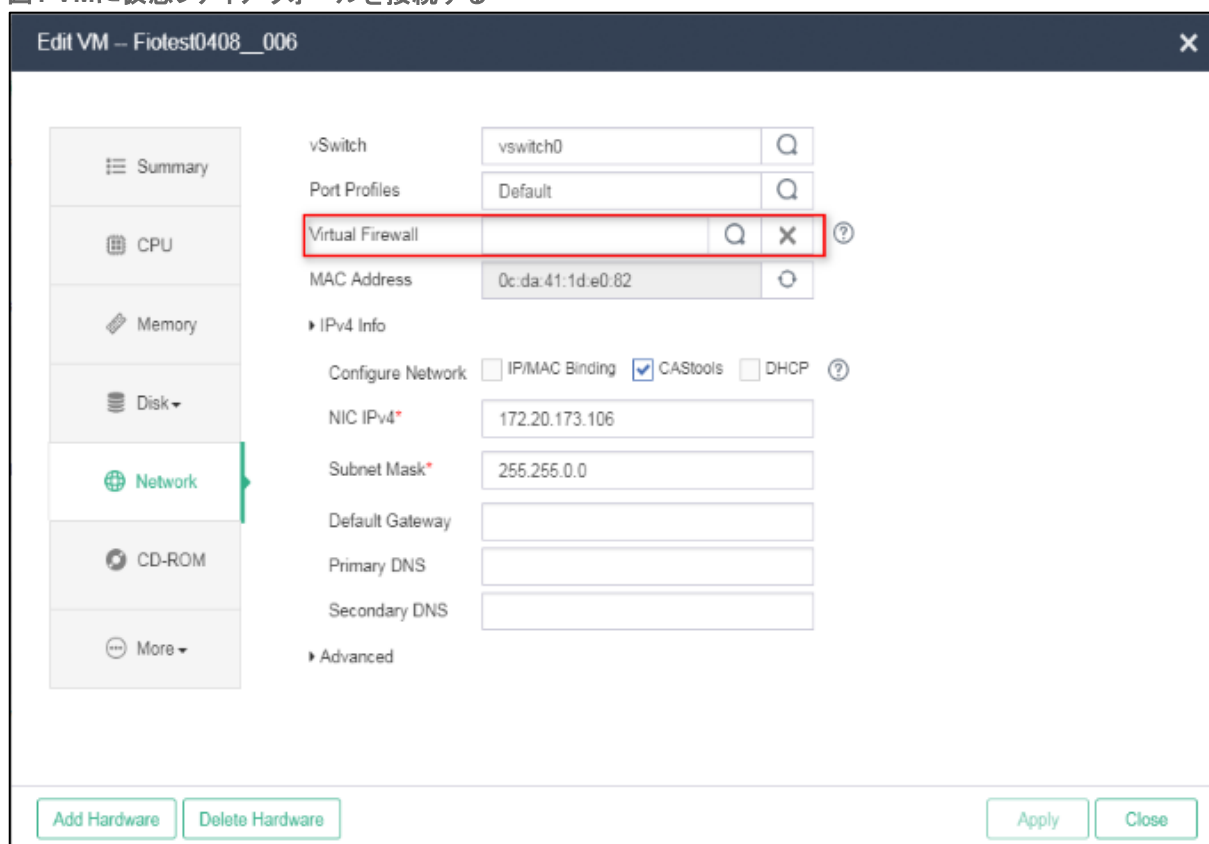
4. **Virtual Firewall**フィールドをクリックするか、検索アイコン  をクリックし、必要に応じてファイアウォール設定を編集し、**OK**をクリックして、**Apply**をクリックします。

図1 VMに仮想ファイアウォールを接続する



## よくある質問

### インストール関連

UIS サーバーは VM に対してどのようなゲスト OS をサポートしていますか？

*H3C UIS ソフトウェアとハードウェアの互換性を参照してください。*

UIS マネージャーをアップグレードするにはどうすればよいですか？

*H3C UIS アップグレード ガイドを参照してください。*

UIS ライセンスには期限がありますか？

ライセンス センターに登録された UIS ライセンスは、期限のない永続的なライセンスです。UIS Manager をインストールした後、90 日以内にライセンスを登録する必要があります。有効期限までにライセンスを登録しないと、仮想化管理機能を使用できなくなります。ただし、既存の VM は引き続き動作できます。

VM に複数のゲスト OS をインストールするにはどうすればよいですか？

以下の情報では、2 つの Windows ゲスト OS を使用して、VM に複数のゲスト OS をインストールする手順について説明します。

1. VM を作成し、そこに Windows OS をインストールします。たとえば、Windows Server 2003 Enterprise x64 Edition をインストールします。
2. VM をシャットダウンする。
3. 2 番目のゲスト OS (Windows 7 など) をインストールするために、VM に新しいディスクを追加します。
4. 2 番目のゲスト OS の ISO イメージ ファイルを VM の CD-ROM にマウントし、CD-ROM を最初の起動オプションとして設定します。
5. VM を起動します。VM は CD-ROM から 2 番目のゲスト OS を自動的にインストールします。
6. VM ユーザーが VM を起動すると、アクセスするゲスト OS の 1 つを選択します。

### 構成関連

VM ディスクのフォーマットを raw または qcow2 に設定する必要がありますか？

ベスト プラクティスとして、オンデマンドの動的ストレージ割り当てやスナップショットなどのメリットを得るには、qcow2 形式を使用します。

## VM のディスクを拡張するにはどうすればよいですか？

以下の情報では、Windows Server 2008 R2 Datacenter x64 Edition を使用して、VM のディスク拡張手順について説明します。

1. VM にスナップショットがないこと、複数レベルのイメージ ファイルが含まれていないこと、または **zeroed** または **delay zeroed** のボリューム プロビジョニング モードが使用されていないことを確認します。
2. VM の実行中に、ディスク サイズを、たとえば 15 GB から 20 GB に変更します。
3. サーバー マネージャーを開きます。
  - a. ナビゲーションパネルで、**Storage > Disk Management** を選択します。
  - b. **Disk Management** ペインで、拡張するディスクを右クリックし、**Extend Volume** を選択して、指示に従ってディスク サイズを変更します。
4. ディスクが IDE の場合、拡張を有効にするには VM を再起動します。ディスクが Virtio の場合は、この手順をスキップします。拡張は VM の実行中に有効になります。

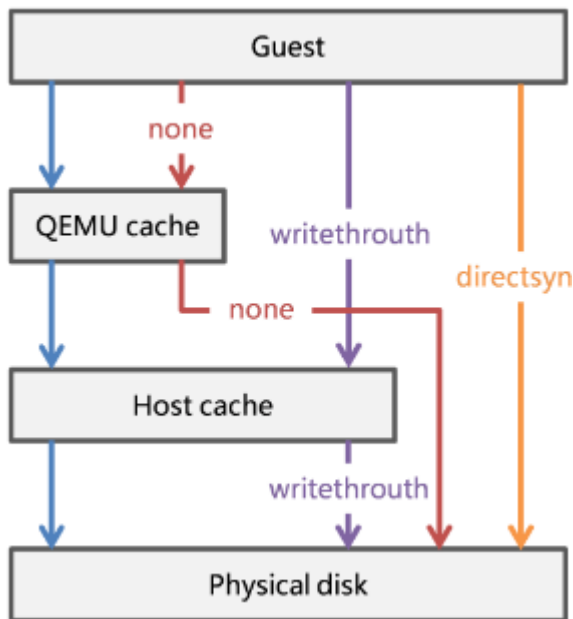
## VM ディスクにはどのキャッシュ モードを選択すればよいですか？

データの書き込みと読み取りの頻度、および必要な読み取りと書き込みのパフォーマンスに応じて、キャッシュ モードを選択します。

UIS マネージャーは次のキャッシュモードを提供します：

- **None-None** を選択すると、ホスト キャッシュは無効になります。システムは VM ディスク キャッシュにデータを書き込んだり、VM ディスク キャッシュからデータを読み取ります。
- **Directsync**—データ損失の影響を受けやすいアプリケーションの場合は、このオプションを選択します。このモードでは、システムは物理ディスクに直接データを書き込み、物理ディスクからデータを読み取ります。
- **Writethrough**—データを頻繁に再読み取りするアプリケーションの場合は、このオプションを選択します。ライトスルー モードでは、VM ディスクの書き込みキャッシュは無効になります。システムはデータをホスト キャッシュに書き込み、次に物理ディスクに書き込みます。ディスク読み取りキャッシュは読み取りデータを保存するために有効になります。読み取り要求は読み取りキャッシュから処理されます。
- **Writeback**—低レイテンシと高スループットを必要とする書き込み集中型アプリケーションの場合は、このオプションを選択します。ライトバック モードでは、システムは最初に VM キャッシュにデータを書き込み、次にホスト キャッシュに書き込み、最後に物理ディスクに書き込みます。ただし、すべてのデータがキャッシュに書き込まれるとすぐに I/O が終了することを確認します。

図 1 ディスクキャッシュモードの動作メカニズム



DirectSync 以外のすべてのモードでは、物理ディスクに書き込まれる前に、VM ディスク キャッシュまたはホスト キャッシュにデータが書き込まれます。システムが物理ディスクにデータを書き込んでいる間に停電が発生すると、データが失われます。停電によるデータ損失を防ぐために、UIS Manager はデフォルトで DirectSync キャッシュ モードを使用します。

## 最適な読み取りおよび書き込みパフォーマンスを得るには、VM ディスクをどのように構成すればよいですか？

ディスクの読み取りおよび書き込みパフォーマンスは、ディスクのフォーマットとキャッシュ モードによって異なります。UIS では、ディスクフォーマットを IDE または Virtio に設定し、キャッシュ モードを none、directsync、writeback、または writethrough に設定できます。

VMのディスクフォーマットとキャッシュモードを設定するためのベストプラクティスは次のとおりです：

- VM が読み取り集中型アプリケーションを実行する場合は、ディスクフォーマットを Virtio に設定し、キャッシュモードを writethrough に設定します。
- VM が書き込み集中型アプリケーションを実行する場合は、ディスクフォーマットを Virtio に設定し、キャッシュモードを writeback に設定します。

これらのベストプラクティスは、表 1 のテストデータから得られた、さまざまなディスクフォーマットとキャッシュモードの組み合わせでのディスクの読み取りとパフォーマンスに関する次の調査結果に基づいています。：

- 同じディスクキャッシュモードの場合、Virtio ディスクは IDE ディスクよりもパフォーマンスが高くなります。
- Virtio ディスクは、ライトスルーキャッシュモードで読み取りパフォーマンスが最も優れ、ライトバックキャッシュモードで書き込みパフォーマンスが最も優れています。

表 1 ディスクタイプとキャッシュモード設定が読み取りおよび書き込みパフォーマンスに与える影響

ストレージ形式	ディスクタイプ	ディスクキャッシュモード	Seq	512K	4K	4K QD32
QCOW2	IDE	Directsync	Read: 75.20 MB/s Write: 17.02 MB/s	Read: 43.21 MB/s Write: 17.33 MB/s	Read: 0.820 MB/s Write: 0.731 MB/s	Read: 0.952 MB/s Write: 0.817 MB/s
QCOW2	IDE	None	Read: 79.28 MB/s Write: 17.13 MB/s	Read: 42.23 MB/s Write: 18.16 MB/s	Read: 0.757 MB/s Write: 0.714 MB/s	Read: 0.932 MB/s Write: 0.799 MB/s
QCOW2	IDE	Writeback	Read: 306.0 MB/s Write: 264.5 MB/s	Read: 299.9 MB/s Write: 270.3 MB/s	Read: 11.08 MB/s Write: 9.635 MB/s	Read: 13.40 MB/s Write: 10.81 MB/s
QCOW2	IDE	Writethrough	Read: 344.2 MB/s Write: 262.7 MB/s	Read: 310.4 MB/s Write: 280.8 MB/s	Read: 11.09 MB/s Write: 8.063 MB/s	Read: 12.60 MB/s Write: 14.13 MB/s
QCOW2	Virtio	Directsync	Read: 86.79 MB/s Write: 64.55 MB/s	Read: 45.00 MB/s Write: 47.97 MB/s	Read: 0.817 MB/s Write: 0.689 MB/s	Read: 3.018 MB/s Write: 0.811 MB/s
QCOW2	Virtio	None	Read: 86.49 MB/s Write: 63.60 MB/s	Read: 46.94 MB/s Write: 48.43 MB/s	Read: 0.809 MB/s Write: 0.763 MB/s	Read: 3.022 MB/s Write: 0.854 MB/s
QCOW2	Virtio	Writeback	Read: 1634 MB/s Write: 846.4 MB/s	Read: 1103 MB/s Write: 633.1 MB/s	Read: 21.69 MB/s Write: 19.85 MB/s	Read: 41.80 MB/s Write: 32.80 MB/s
QCOW2	Virtio	Writethrough	Read: 1877 MB/s Write: 65.93 MB/s	Read: 1129 MB/s Write: 44.05 MB/s	Read: 22.64 MB/s Write: 0.704 MB/s	Read: 172.7 MB/s Write: 1.583 MB/s

- Seq: シーケンシャル読み取り/書き込みテスト (データブロック サイズ = 1024 KB)
- 512K: ランダム読み取り/書き込みテスト (データブロックサイズ = 512 KB)
- 4K: ランダム読み取り/書き込みテスト (データブロックサイズ = 4 KB)
- 4KQD32: ランダム読み取り/書き込みテスト (データ ブロック サイズ = 4 KB、キューの深さ = 32)

## VMware VM を UIS と互換性のある形式に変換するにはどうすればよいですか？

1. VMware VM ファイルを UIS Manager で管理されているホストにアップロードします。この例では、VM ファイル名は **1.ova** です。たとえば、VM ファイルをホスト 10.10.10.151 上のディレクトリ **/vms/defaultShareFileSystem0** にアップロードします。
2. VM ファイルが OVA パッケージ ファイルの場合、VM を変換する前にパッケージ ファイルを解凍する必要があります。ベスト プラクティスとしては、一時ディレクトリを作成し、そのディレクトリで OVA ファイルを解凍します。

たとえば、**/vms/defaultShareFileSystem** ディレクトリにサブディレクトリ **tmp** を作成し、VM パッケージ ファイル (**1.ova**) をサブディレクトリに移動し、**tar** コマンドを実行してファイルを解凍します。

```
root@cvknode1:/vms/defaultShareFileSystem0# mkdir tmp
```

```
root@cvknode1:/vms/defaultShareFileSystem0# ls
```

```
root@cvknode1:/vms/defaultShareFileSystem0# mv 1.ova tmp
```

```
root@cvknode1:/vms/defaultShareFileSystem0# cd tmp
```

```
root@cvknode1:/vms/defaultShareFileSystem0/tmp# tar -xf 1.ova
```

図 1 OVA パッケージ ファイルから抽出された VM ファイル

```
1 10.10.10.151:22 x 2 10.10.10.151:22 x +
root@cvknode1:/vms/defaultShareFileSystem0/tmp# ls
1.ova _____-disk1.vmdk _____ .mf _____ .ovf
root@cvknode1:/vms/defaultShareFileSystem0/tmp# du -ah
37G  ./1.ova
1.6M  ./_____ .ovf
37G   ./_____ -disk1.vmdk
512   ./_____ .mf
74G   .
root@cvknode1:/vms/defaultShareFileSystem0/tmp# █
```

3. ディレクトリ内の `.vmdk` ファイルを見つけて、`qemu-img convert` コマンドを実行し、`.vmdk` ファイルを `qcow2` 形式に変換します。

```
qemu-img convert -O qcow2 filename out_filename
```

`filename` 引数はソース VM イメージのファイル名を表し、`out_filename` 引数は変換された VM イメージのファイル名を表します。

図 2 VM イメージ形式の変換

```
root@cvknode1:/vms/defaultShareFileSystem0/tmp# qemu-img convert -O qcow2 _____-disk1.vmdk ykt-1
root@cvknode1:/vms/defaultShareFileSystem0/tmp# du -ah
37G  ./1.ova
1.6M  ./_____ .ovf
37G   ./_____ -disk1.vmdk
512   ./_____ .mf
86G   ./ykt-1
159G  .
root@cvknode1:/vms/defaultShareFileSystem0/tmp# qemu-img inof ykt-1
qemu-img: Command not found: inof
Try 'qemu-img --help' for more information
root@cvknode1:/vms/defaultShareFileSystem0/tmp# qemu-img info ykt-1
image: ykt-1
file format: qcow2
virtual size: 500G (536870912000 bytes)
disk size: 85G
cluster size: 262144
Format specific information:
  compat: 1.1
  lazy refcounts: false
  refcount bits: 16
  corrupt: false
root@cvknode1:/vms/defaultShareFileSystem0/tmp# mv ykt-1 ../
```

4. VM 作成のために、`qcow2` イメージをストレージ プールに移動します。

この例では、変換されたイメージ (`ykt-1`) をストレージ プール `/vms/defaultShareFileSystem0` に移動します。

```
root@cvknode1:/vms/defaultShareFileSystem0/tmp# mv ykt-1
/vms/defaultShareFileSystem0
```

```
root@cvknode1:/vms/defaultShareFileSystem0/tmp# cd ..
```

```
root@cvknode1:/vms/defaultShareFileSystem0#ls
```

5. UIS マネージャーで VM を作成します。変換されたイメージ ファイルを選択し、ディスク バス タイプを `IDE` に設定します。

In this example, select image `ykt-1` from the `defaultShareFileSystem0` storage pool.

6. Start the VM and verify that the VM can operate correctly.
7. 一時ディレクトリを削除します。この例では、`/vms/defaultShareFileSystem0/tmp` を削除します。

## vDisk を複数の VM にマウントできますか？

はい、できます。

ただし、ディスクを共有すると、データの不整合のリスクが高まります。ベスト プラクティスとして、vDisk を共有するように VM を構成する場合は、データの整合性を保証するメカニズムが VM にあることを確認してください。

## パフォーマンス監視ページで VM のメモリ使用量が 100% のままになるのはなぜですか？

この問題は、VM が CAStool とともにインストールされていないために発生する可能性があります。CAStool がない場合、ページに表示されるメモリ使用量は VM に割り当てられたメモリに基づいて計算されます。この計算では、常にメモリ使用量は 100% になります。


この問題を解決するには、VM に CAStools をインストールし、そのバージョンが UIS Manager と互換性があることを確認します。

## VM の MAC アドレスを変更するにはどうすればよいですか？

VM または VM クローンを作成すると、UIS Manager は MAC アドレス プールから 1 つまたは複数の MAC アドレスをその VM に自動的に割り当てます。これらの MAC アドレスの最初の 3 バイトは 0C:DA:41 に固定されており、これは H3C の組織固有識別子 (OUI) です。これらの MAC アドレスの残りの 3 バイトは、VM にランダムに割り当てられる一意の数値文字列です。MAC アドレス プールは、VM に 64K の一意の MAC アドレスを提供します。


VM の MAC アドレスは、ホスト間で移動しても変更されません。

VMのMACアドレスを変更するには:

1. VM をシャットダウンします。
2. Edit をクリックすると、VM 設定を編集するためのページが開きます。
3. **Network** タブで、MAC アドレスを手動で変更するか、自動的に割り当てられた新しい MAC アドレスを取得するために  をクリックします。
4. MAC アドレスを手動で指定する場合は、LAN 上で一意であることを確認してください。

## 実行している UIS マネージャーのバージョンはどれですか？

実行中のUISマネージャソフトウェアのバージョンに関する情報を確認するには、次のいずれかの方法を使用します。:

1. UIS Manager の Web インターフェイスにログインし、ページの右上にある  をクリックして、バージョン情報を選択します。

UIS マネージャーのソフトウェア バージョンを表示するダイアログ ボックスが開きます。

2. SSH クライアントを使用して UIS マネージャーの CLI にログインし、次のコマンドを実行します。:

```
[root@cvknode1 ~]# cat /etc/cas_cvk-version
```



V600R001B03D022 V6.5 E0709 Enterprise 49497

Build 2019-10-11 16:24:13, RELEASE SOFTWARE

## 実行している CVK カーネルのバージョンはどれですか？

SSHクライアントを使用してUIS CVKサーバーのCLIにログインし、次のコマンドを実行します。:

```
[root@cvknode1 ~]# uname -a
```

```
Linux cvknode1 4.14.0-generic #862.el7 SMP Sat May 25 17:05:06 CST 2019 x86_64 x86_64  
x86_64 GNU/Linux
```

## 実行している QEMU のバージョンはどれですか？

SSHクライアントを使用してUIS CVKサーバーのCLIにログインし、次のコマンドを実行します。:

```
[root@cvknode1 ~]# kvm -version
```

```
QEMU emulator version 2.12.0 (qemu-2.12-1.el7)
```

```
Copyright (c) 2003-2017 Fabrice Bellard and the QEMU Project developers
```

## UIS マネージャーの障害は、管理対象の VM の操作に影響しますか？

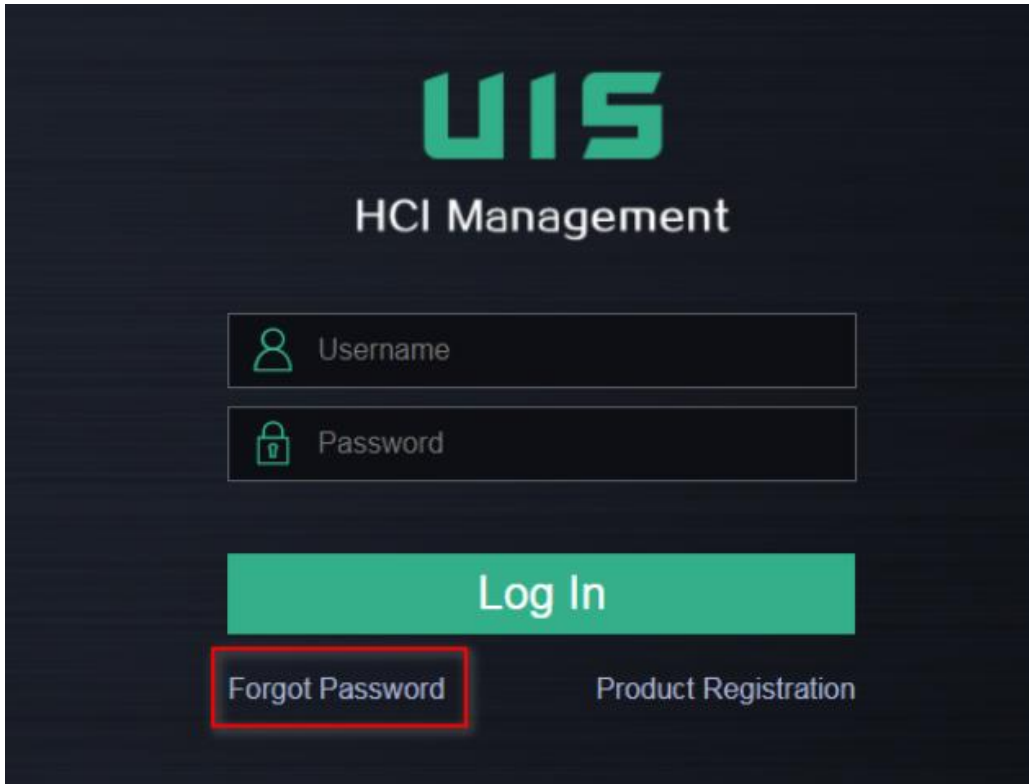
いいえ。

UIS マネージャーに障害が発生した後も、CVK ホスト上の VM は正常に動作し続けることができます。

さらに、ホスト クラスターの HA 機能も正常に動作します。クラスター内の 1 つの CVK ホストに障害が発生した場合、その VM は自動的に他の CVK ホストに移行できます。

## UIS Manager のパスワードを回復するにはどうすればよいですか？

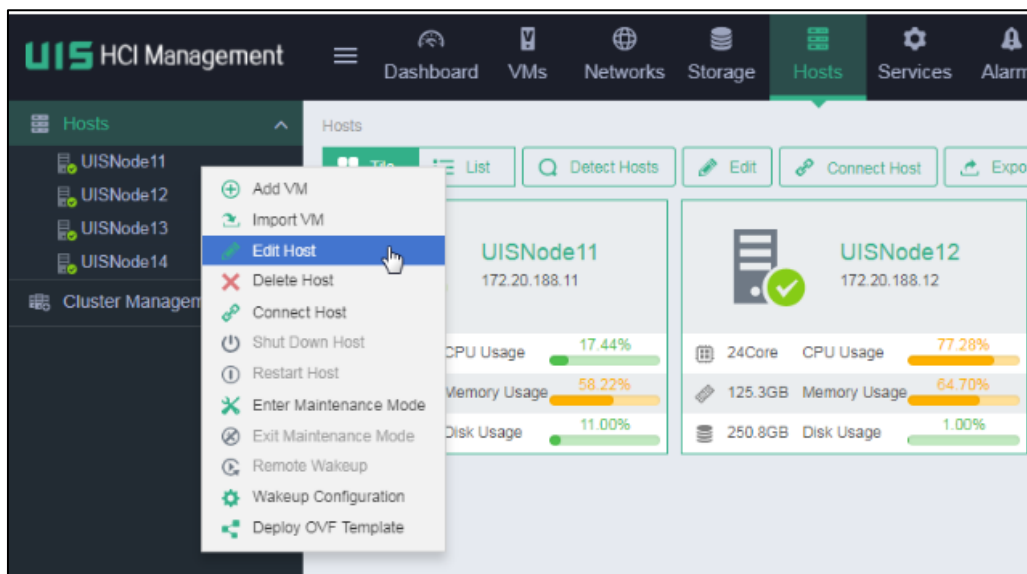
UIS Manager のパスワードを忘れた場合は、ログイン ページで **Forgot Password**をクリックし、ログイン ユーザー名とメール アドレスを入力してパスワードを回復してください。



## CVK ホストのルート パスワードを変更するにはどうすればよいですか？

CVK ホストのルート パスワードを変更するには、UIS マネージャーの Web インターフェイスにアクセスします。コマンド シェルから CVK ホストのルート パスワードを変更することはできません。

1. 上部のナビゲーション バーで、**Hosts** をクリックします。
2. ナビゲーション ペインで、対象の CVK ホストを右クリックし、**Edit Host** を選択します。



3. 開いたダイアログ ボックスで新しいルート パスワードを入力し、**OK** をクリックします。

After you change the password, the password of the corresponding username on the host will also be changed.

Host Name	UISNode11
Username	root
Old Password*	Enter the password
New Password*	Enter the password
Confirm*	Enter the password again

OK Cancel

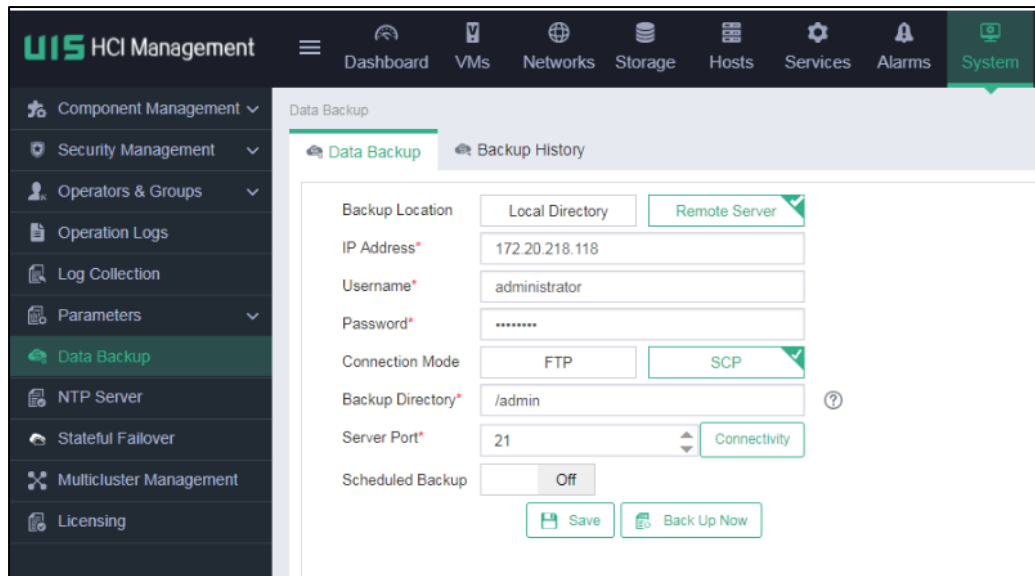
## ホストに障害が発生した後、UIS 管理ノードを回復するにはどうすればよいですか？

障害が発生した UIS 管理ノードを回復するには、データ バックアップ機能を使用します。

UIS 管理ノードのリカバリにこの機能を使用するには、管理ノードを手動でバックアップするか、データを自動的にバックアップするバックアップ スケジュールを構成する必要があります。

UIS マネージャノードをホスト障害から回復するには:

1. バックアップ サーバーに UIS マネージャーをインストールします。
- a. システム管理者として UIS マネージャーにアクセスします。
- b. 上部のナビゲーション バーで、**System** を選択します。
- c. ナビゲーション ペインから、**Data Backup** を選択します。
- d. **Data Backup** タブで、バックアップ ファイルにアクセスするためのバックアップ設定を構成し、**Connectivity** をクリックします。



2. テストが成功した場合は、**Save** をクリックします。テストが失敗した場合は、バックアップ設定に誤りがないか確認してください。

UIS マネージャーは、バックアップ ディレクトリからバックアップ ファイルを自動的に取得します。

3. **Backup History** タブをクリックします。

4. 復元する必要があるバックアップファイルを選択し、**Restore UIS Data** アイコン  をクリックします。

File Name	Created At	Version	MD5 Digest	Backup Destination	IP Address	Connect Meth	Backup Destination	Actions
UIS_INFO_BACK_E0715_20200621173008	2020-06-21 17:30:08	E0715	106340ec885f19eb0b6...	Remote Server	172.20.218.118	FTP	/admin	
UIS_INFO_BACK_E0715_20200620173009	2020-06-20 17:30:09	E0715	c091743d4967cb65ce...	Remote Server	172.20.218.118	FTP	/admin	
UIS_INFO_BACK_E0715_20200619173009	2020-06-19 17:30:09	E0715	289945e620214f6607d...	Remote Server	172.20.218.118	FTP	/admin	
UIS_INFO_BACK_E0715_20200619172529	2020-06-19 17:25:29	E0715	73a73d0398b689c19a...	Remote Server	172.20.218.118	FTP	/admin	

5. 開いたダイアログボックスで、**OK** をクリックします。

6. ブラウザのキャッシュをクリアしてから、UIS マネージャーに再度ログインします。

7. ライセンス転送プロセスを使用して、新しいアクティベーション ファイルを取得し、ソフトウェアを再登録します。ライセンス転送の詳細については、*H3C UIS Manager ライセンス登録ガイド*を参照してください。

- UIS Manager のデータ バックアップ機能では、バックエンドの ONEStor ストレージ クラスター構成を復元することはできません。バックエンドのストレージ クラスター構成を復元するには、バックエンド ストレージ システムの Web インターフェイスにアクセスします。
- リカバリにホストの交換が含まれない場合は、元のアクティベーション ファイルを使用して UIS Manager と ONEStor を再登録します。新しいアクティベーション ファイルを取得する必要はありません。
- UIS 管理ノードは、プライマリ システム ディスクとバックアップ システム ディスクの両方に障害が発生すると障害が発生します。管理ノードの回復を煩わしく行わないようにするには、障害が発生したシステム ディスクをできるだけ早く交換してください。

## CVK サービス ホストのハードウェア障害にはどのように対処す

## ればよいですか？

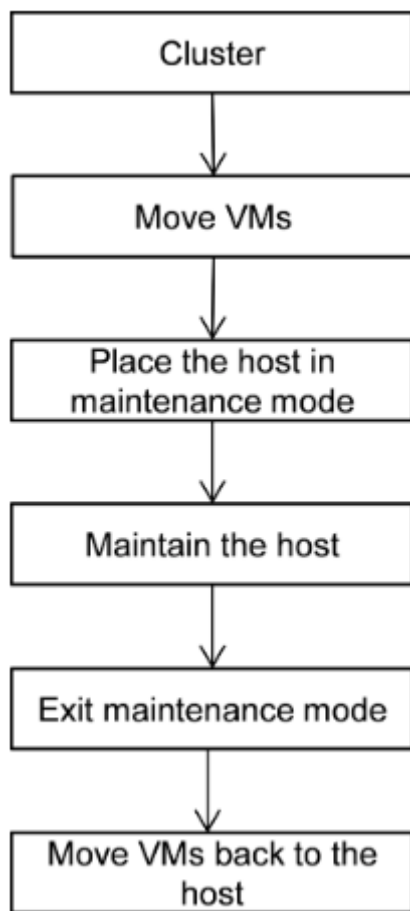
CVKホストのハードウェアに障害が発生した場合は、次のタスクを実行します。:

1. ノード上の VM を使用可能なノードに移動します。
2. 障害が発生したノードをメンテナンス モードにします。
3. ストレージ クラスターが 100% 正常であることを確認してから、ノードの電源をオフにします。

データの損失や未知のリスクを回避するために、障害が発生したノードを UIS マネージャーから削除しないでください。

4. ノードが復元されたらメンテナンス モードを終了し、VM をノードに戻します。

図 1 サービスノードのハードウェア障害を処理するプロセス



## クラスターをスケーリングするにはどうすればよいですか？

スケーリング手順の詳細については、H3C UIS ハイパーコンバージド インフラストラクチャのクラスター拡張ガイドを参照してください。

クラスターの拡張によりデータの再バランス調整が行われ、その間オンライン サービスのパフォーマンスが低下します。サービスへの影響を最小限に抑えるために、拡張はオフピークの時間帯にスケジュールし、テクニカル サポートに問い合わせることをお勧めします。

## UIS スーパーユーザー アカウント (管理者アカウント) のパスワードを変更するにはどうすればよいですか？

UIS-E0715 より前のバージョンでは、**admin** アカウントのデフォルトのパスワードは **admin** です。

UIS-E0715 以降では、**admin** アカウントのデフォルトのパスワードは **Cloud@1234** です。

このパスワードを変更するには:

1. **admin** アカウントで UIS マネージャーにログインします。
2. パスワードを変更するには、右隅にある管理者アイコンをクリックします。

## サービス計画関連

### アプリケーションを仮想化環境に移行するかどうかを決定する際に考慮すべき要素は何ですか？

仮想化環境はすべてのアプリケーションに適しているわけではありません。ベストプラクティスとして、次のアプリケーションを仮想化環境に移行しないでください。:

- **高負荷アプリケーション**—これらのアプリケーションは通常、I/O とメモリを大量に消費し、負荷分散をサポートしていません。高負荷アプリケーションの例としては、Exchange、データベース、ERP システムなどがあります。
- **高性能アプリケーション**—これらのアプリケーションには通常、特別なハードウェア アクセス要件があります。高性能アプリケーションの例としては、高性能コンピューティング アプリケーション、グラフィックス アプリケーション、特殊なシリアルまたはパラレル暗号化アプリケーションなどがあります。
- **特別なドライバーを必要とするアプリケーション**—典型的な例としては、3D ハードウェア アクセラレーション用のカスタム ビデオドライバーを必要とするアプリケーションがあります。

### 物理サーバーに仮想デスクトップをいくつ展開できますか？

サーバーのハードウェア構成、仮想デスクトップの構成、デスクトップ アプリケーションによって異なります。

- サーバーに展開できる仮想デスクトップの数は、次の状況で増加します。:
  - サーバーは高い CPU パフォーマンスとメモリ サイズを備えています。
  - 各仮想デスクトップに割り当てられた CPU およびメモリ リソースが不足していません。
  - デスクトップ アプリケーションはリソースを大量に消費しません。たとえば、Office アプリケーションは AutoCAD よりも複雑ではなく、ハードウェア リソースの使用量も AutoCAD よりも少なくなります。
- VM の展開を計画するときは、サーバーの安定性を確保するために、一定量のリソースを予約してください。実稼働環境では通常、デスクトップが利用可能で確実に動作するように、HA 機能と動的リソーススケジューリング (DRS) 機能を展開します。サーバーの CPU またはメモリ リソースが使い果たされると、DRS はそのサーバー上の一部の VM を他のサーバーに移動します。

ベストプラクティスとして、物理サーバーに展開されたデスクトップ VM がサーバーリソースの 3 分の 2 のみを使用するようにします。

たとえば、サーバーに 2 つの CPU、6 つの CPU コア、128 GB のメモリがあるとします。各デスクトップに 1 つの vCPU と 2 GB のメモリを割り当てると、理論的にはサーバー上で 50 ~ 60 のデスクトップを実行できます。サーバーの安定性を確保するには、サーバーに最大 40 のデスクトップを展開します。

## 共有ストレージ デバイスにデプロイできる VM の数はいくつですか？

ストレージシステム上の VM の最大数を見積もるには、次の式を使用します。:

最大 VM 数 = 最大システム IOPS / VM の必要 IOPS

以下は、最大システム IOPS と VM の IOPS 要件を決定する要因です:

- デバイスの IOPS パフォーマンス。

ストレージ デバイスの IOPS パフォーマンスは、ドライブの種類、キャッシュ サイズ、キューの深さ、アクセス方法 (ランダムまたはシーケンシャル) などの要素によって異なります。

- VM 上のアプリケーション システムの IOPS 要件。

- VM 上のアプリケーション システムの IOPS 要件。

- 通常、Oracle データベースなどの I/O 集約型または重要なアプリケーションを実行する場合、VM には別のストレージ スペースが必要です。

- ポータル Web サイトやファイル サーバーなどの一般的なエンタープライズ ビジネス システムは、通常、負荷が軽く、高い IOPS パフォーマンスを必要としません。一般的なエンタープライズ ビジネス システムを実行する 100 ~ 150 台の VM を、ローエンドから中程度のストレージ システムに展開できます。

たとえば、ストレージ デバイスに 10 krpm ドライブが 6 台あるとします。理論上の最大 IOPS は 900 (150 x 6) です。アプリケーションで 30 の IOPS が必要な場合、このアプリケーションを実行するためにストレージ システムに展開できる VM の最大数は 30 (900/30) です。

## 例外関連

### 相互に ping できる 2 つの Linux VM 間でパケットを送信すると、ホストへのルートが存在しないというメッセージが表示されるのはなぜですか？

これは、Linux ゲスト OS ではファイアウォールがデフォルトで有効になっているためです。

この問題を解決するには、Linux ゲスト OS の CLI で `setup` コマンドを実行してファイアウォールを無効にします。

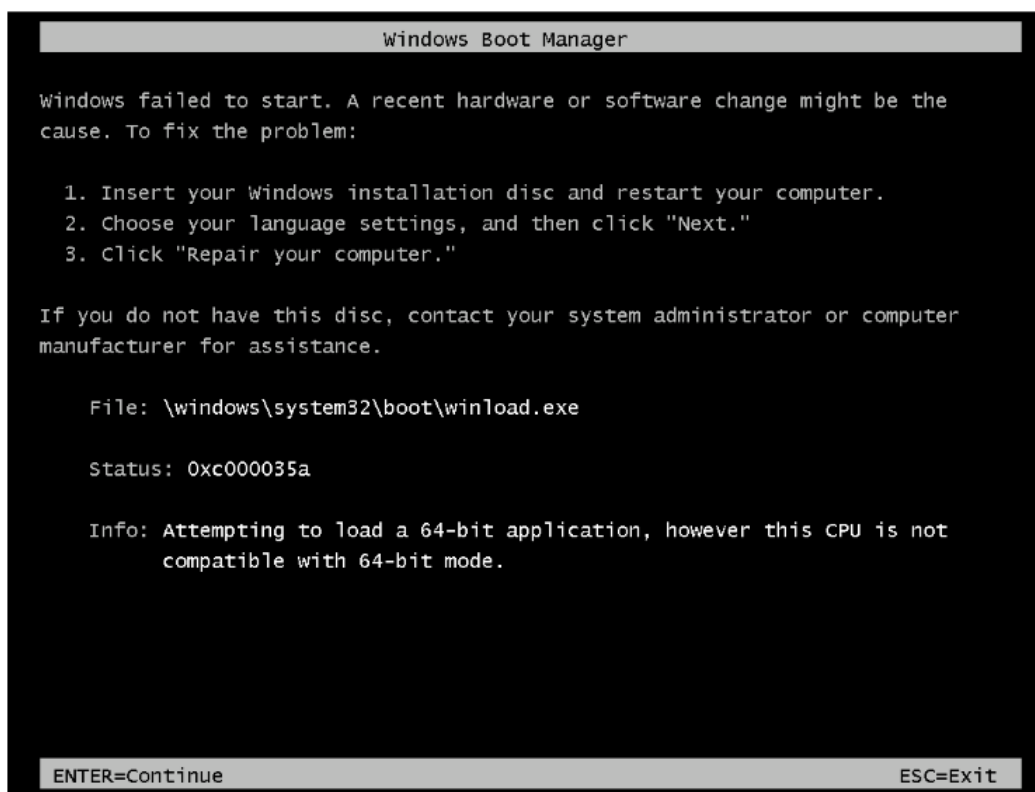
このコマンドを実行するには、root ユーザーとして Linux CLI にアクセスする必要があります。

### Windows Server 2008 R2 Datacenter x64 Edition のインストール時に受信した 0xc000035a エラーをどのように処理すればよいですか？

図 1 に示すように、32 ビット CPU アーキテクチャを使用する VM に 64 ビット Windows ゲスト OS をイン

ストールすると、0xc000035a エラー コードが表示される場合があります。

図 1 64 ビット Windows OS のインストール失敗メッセージ



この問題を解決するには:

1. VM をシャットダウンします。
2. VM を編集して、CPU アーキテクチャーを x86\_64 に変更します。
3. VM を再起動します。

## バックアップ ディスクに十分な容量があるにもかかわらず、CB バックアップを実行するときにディスク不足エラーが発生した場合、どうすれば対処できますか？

この問題を解決するには、CB バックアップの一時ディレクトリが FTP 共有のベース FTP ディレクトリに設定されていることを確認します。ベース ディレクトリの下の子ディレクトリを選択すると、この問題が発生します。

たとえば、FTP サイトではファイル共有にベース ディレクトリ E:\ftp1 を使用します。このベース ディレクトリには Localuser というサブディレクトリが含まれています。

この FTP サイトを CB バックアップに使用する場合は、一時ディレクトリを E:\ftp1 に設定する必要があります。一時ディレクトリを E:\ftp1\LocalUser に設定すると、ディスク容量不足のエラー メッセージが表示されます。

## UIS クラスタ内のノードへの管理 IP アドレスの割り当てには制限がありますか？



はい。UIS クラスター内のすべてのノードの中で、管理ノードに最も低い管理 IP アドレスを割り当てる必要があります。

## VM が暗号化ドングルを認識できない場合はどうすればよいですか？

暗号化ドングルを VM に追加するには、ドングルがネットワーク経由の USB をサポートしていることを確認してください。

## ウイルス対策が有効になっている VM の移行後に、CAStools コマンドの実行や AISware フロントエンドドライバーのアンインストールが予期せず失敗するのを回避するには、どうすればよいですか？

この問題を回避するには、VM を移動する前にウイルス対策機能を無効にします。VM の移行後、まずウイルス対策機能を有効にしてから VM を起動します。

## ウイルス対策が有効になっている VM の実行中に CPU を追加した後に頻繁に応答しなくなったり、起動時にブルー スクリーン (BSOD) が表示される問題が発生する場合、どうすれば対処できますか？

この問題を回避するには、vCPU を増減する前に VM をシャットダウンします。

## ウイルス対策が有効になっている VM で深刻な無応答の問題が発生したら、どうすれば解決できますか？

ウイルス対策が有効になっている VM で、次のいずれかの操作を実行すると、深刻な無応答状態が発生する可能性があります。:

- メモリに含まれるスナップショットから復元します。
- 休止状態のときに起動します。
- サスペンド状態のときに移動させます。

この問題を解決するには、VM を再起動します。

## VM をシャットダウンせずに VM のウイルス対策機能を無効にできますか？

いいえ、できません。VM のウイルス対策機能を無効にするには、まずその VM をシャットダウンする必要があります。

## ウイルス対策が有効な VM OVF テンプレートから作成された VM でウイルス対策機能が無効になっているのはなぜですか？

これは制限です。この問題を解決するには、VM を作成した後、手動でウイルス対策機能を有効にします。

## VM を復元ポイントまたはバックアップに復元した後、VM のウイルス対策制御設定を再構成する必要がありますか？

はい、VM バックアップまたは復元ポイントの作成後にウイルス対策制御の状態を変更した場合は、ウイルス対策制御設定を再構成する必要があります。

# UIS パフォーマンス最適化のベストプラクティス

このベスト プラクティスでは、最適なサーバー ハードウェアと VM 構成が提供され、最高のユーザー エクスペリエンスが保証されます。

## ハードウェア

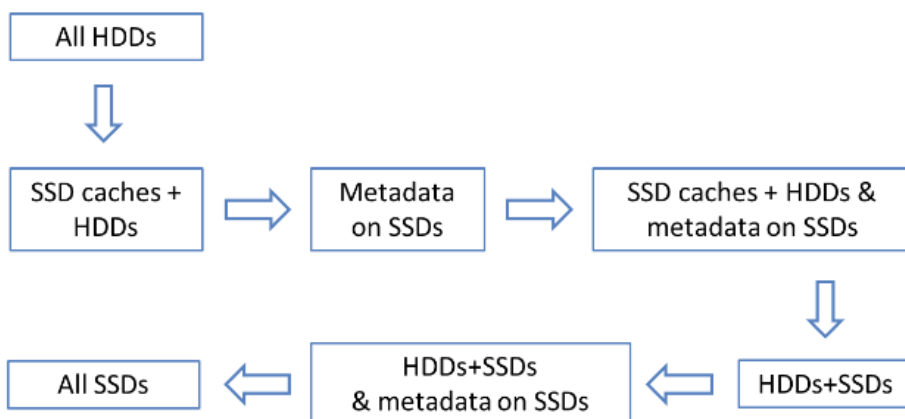
### ストレージコントローラ

- ストレージコントローラを省電力モードで動作するように構成すると、UIS のパフォーマンスが大幅に低下します。ベストプラクティスとして、ストレージコントローラの動作モードを最適なパフォーマンスに設定します。
- キャッシュが正しく機能するストレージコントローラを使用してください。キャッシュレス HBA や RAID キャッシュ バッテリーがインストールされていないストレージコントローラは使用しないでください。
- ストレージコントローラのバッテリーが正しく動作し、RAID キャッシュが有効になっていることを確認します。

### ストレージの展開

図1 UIS でサポートされているストレージ展開モードを、パフォーマンスの昇順で示します。

図 1 ストレージ展開モード



- **すべての HDD**—バックエンドストレージメディアとして HDD のみを使用する。
- **データディスク+キャッシュディスク**—HDD をデータ ディスクとして展開し、SSD を読み取りまたは書き込みキャッシュとして展開するか、SSD をデータ ディスクとして展開し、NVMe SSD を読み取りまたは書き込みキャッシュとして展開します。SSD と NVMe SSD は、キャッシュ ディスクとして使用される場合、永続的なデータを保存しません。
- **SSD 上のメタデータ**—書き込み高速化のために SSD にメタデータを保存します。このモードでは、UIS は LSI RAID コントローラのみをサポートします。
- **HDD+SSD**—異なるストレージ パフォーマンスを必要とするアプリケーションにストレージ サービスを提供するために、高パフォーマンス ストレージ プールと低パフォーマンス ストレージ プールにそれぞれ SSD と HDD をデータ ディスクとして導入します。

- すべての SSD—バックエンドストレージメディアとして SSD のみを使用します。

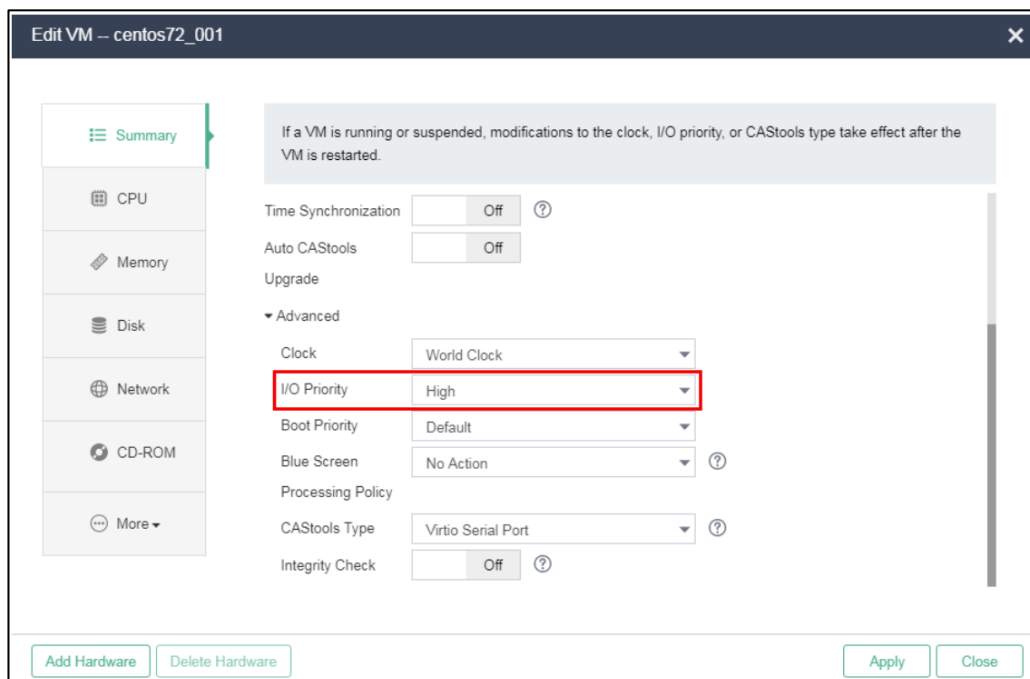
## ノードとディスク

一般的に、パフォーマンスはノードとディスクの数、およびディスクのパフォーマンスに応じて向上します。必要に応じて、ノードの数と各ノード上のディスクを計画できます。

## I/O優先度を設定する

1. 上部のナビゲーションバーで、**VMs** をクリックします。
2. VM を選択します。
3. **Summary** タブで **Edit** をクリックします。
4. **Summary** タブを選択し、**advanced settings** を展開し、**I/O Priority** を **High** に設定します。

図 1 I/O 優先度の設定

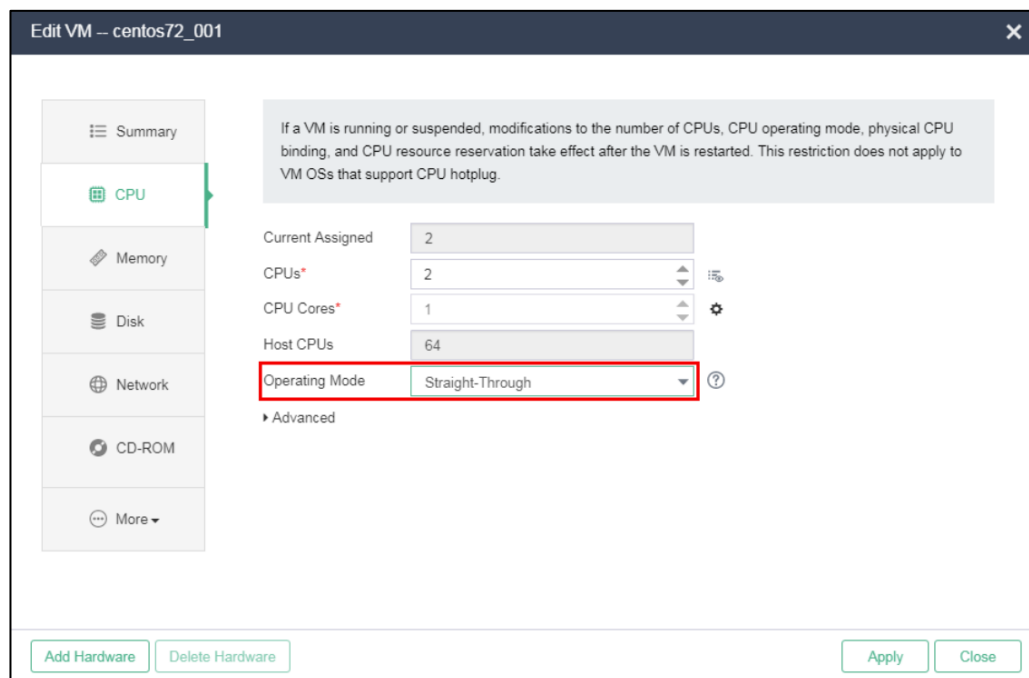


## CPU動作モードを設定する

1. 上部のナビゲーションバーで、**VMs** をクリックします。
2. VM を選択します。
3. **Summary** で **Edit** をクリックします。
4. **CPU** タブを選択し、**Operating Mode** を **Straight-Through** に設定します。
  - **Compatible**—異なる物理 CPU モデル上に汎用 vCPU を作成します。このモードは優れた互換性を備えています。

- **Straight-Through**—ゲスト OS がホストの物理 CPU に直接アクセスできるようにします。このモードでは、最適なパフォーマンスが得られます。

図 1 CPU 動作モードの設定

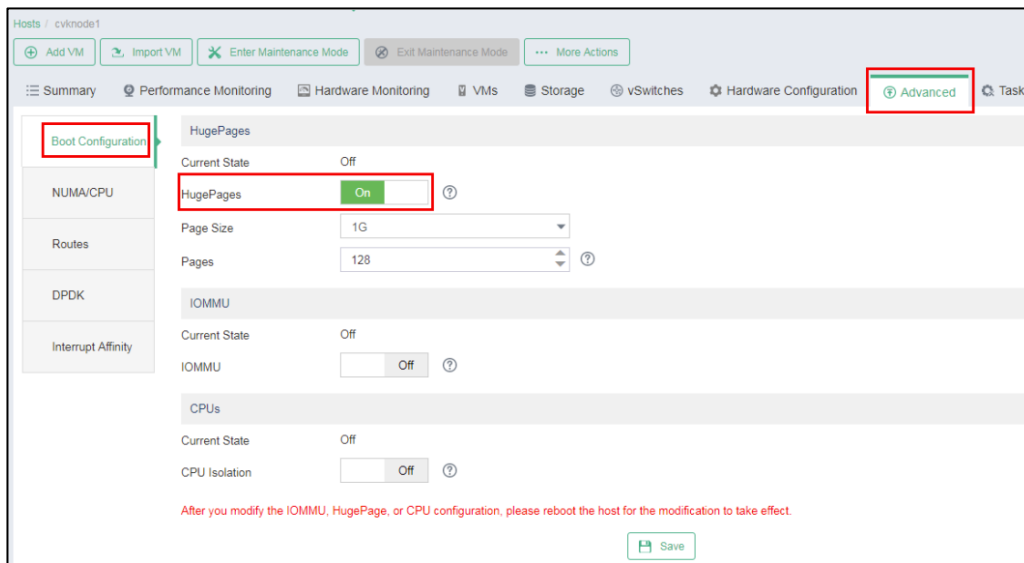


## HugePagesを有効にする

HugePages 構成を編集する前に、VM をシャットダウンします。

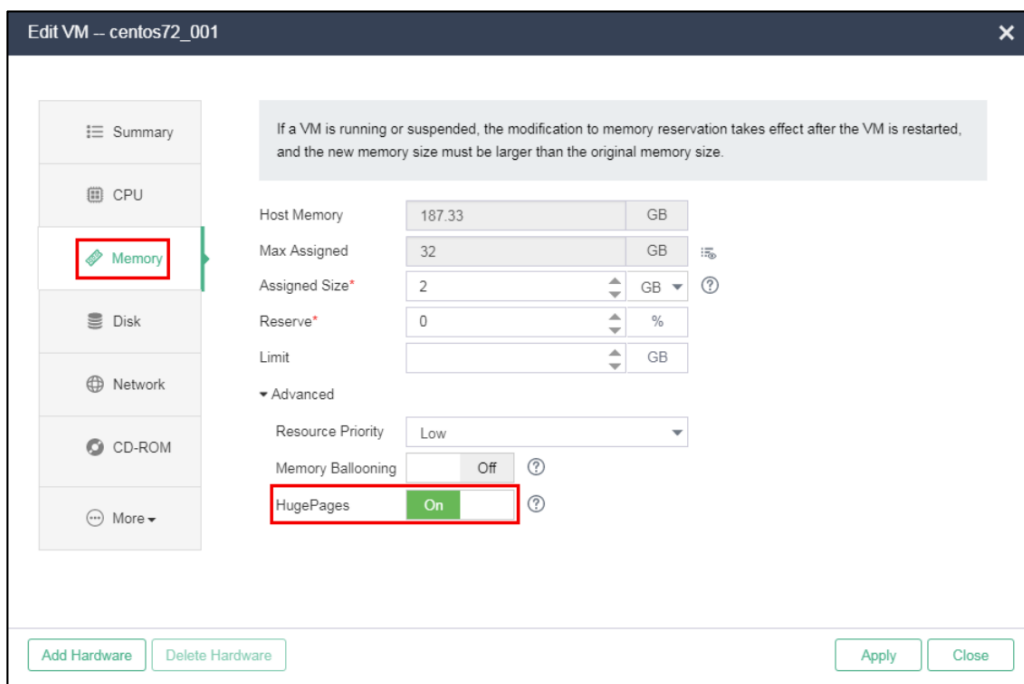
1. 上部のナビゲーションバーで、**Hosts** をクリックします。
2. ホストを選択し、そして **Advanced** タブをクリックします。
3. HugePages を有効にして、**Save** をクリックし、その後、ホストを再起動します。

図 1 HugePages を有効にする



4. 上部のナビゲーションバーで、VMs をクリックします。
5. HugePages が有効になっているホスト上の VM 常駐を選択します。
6. **Summary** タブで、**Edit** をクリックします。
7. **Memory** タブを選択し、詳細設定を展開し、HugePages を有効にします。

図 2 HugePages ステータスの編集



## VMディスクのプロビジョニングモードを設定する

共有ストレージを使用する VM にゼロ化されたストレージ ボリュームをディスクとしてマウントし、VM のパフォ

パフォーマンスを向上させます。

ストレージボリュームのプロビジョニングモードを設定するには:

1. 上部のナビゲーションバーで、**cHosts** をクリックします。
2. ホストを選択し、**Storage** タブをクリックします。
3. ストレージ プールを選択します。
4. ストレージ ボリュームを作成し、プロビジョニング モードをゼロに設定します。

図 1 プロビジョニングモードの設定

The screenshot shows a 'Create Storage Volume' dialog box with the following fields and values:

Name*	vol	
Available Space	794.51	GB
Max. Capacity*	50	GB
▶ Advanced		
Format	Raw	Qcow2
Provisioning	Zeroed	
Disk Cluster Size	256K	

Buttons: OK, Cancel

5. ストレージ ボリュームを VM にマウントします。

## ブロックデバイスをVMにマウントする

共有ストレージが存在する場合、UIS は VM の作成時に各 VM の共有ストレージ上にストレージ ボリュームを予約します。高パフォーマンスを実現するために、このようなストレージ ボリュームをブロック デバイスとして VM にマウントできます。

ブロックデバイスをVMにマウントするには:

1. 上部のナビゲーションバーで、**Storage** をクリックし、ナビゲーションパネルから **Block Storage > Block Device Management** を選択します。
2. **Add** をクリックし、ブロックデバイスを作成します。

図 1 ブロックデバイスの作成

Add Block Device
✕

The size of a volume in a thick-provisioned data pool cannot be larger than the available size of the pool. The size of a volume in a thin-provisioned data pool can exceed the available size of the pool, but over-allocation will cause service interruption. Please be cautious.

Name\*

Data Pool\*

Client Group\*  ?

Available Capacity

Capacity\*

Stripe  Off

Description

3. ブロックデバイスを VM にマウントする:
  - a. VM を編集します。
  - b. ブロック デバイスを新しいハードウェアとして追加します。

図 2 ストレージプールの種類の選択

Add Hardware
✕

1 Hardware Type

2 Configure

Bus Type

Type

Block Device Path\*

Size 0.00MB

▶ Advanced

Details

Hardware Type	Storage
Bus Type	High-Speed Hard Disk
Type	Existing Block Device
Block Device Path	
Capacity	0.00MB
Cache Mode	Directsync
Hot Swappable	Yes
Serial Number	

- c. ブロックデバイスパスを選択します。



- d. パス、IP アドレス、ターゲットなどのストレージ プール設定を構成します。

図 3 ストレージプール設定の構成

**Add Storage Pool**

1 Basic Info > 2 Other Info > 3 Select NAAs

Target Path\*

Targets + Add 🗑 Delete

<input checked="" type="checkbox"/>	IP Address	Target
<input checked="" type="checkbox"/>	127.0.0.1	iqn.2018-01.com.h3c.onestor:ae31ec58386144fbb23...

Previous Next

- e. ブロックデバイスを選択します。

図 4 ストレージの選択

**Add Hardware**

1 Hardware Type > 2 Configure

Bus Type

Type

Block Device Path\*

Size 88.00GB

▶ Advanced

Previous Finish

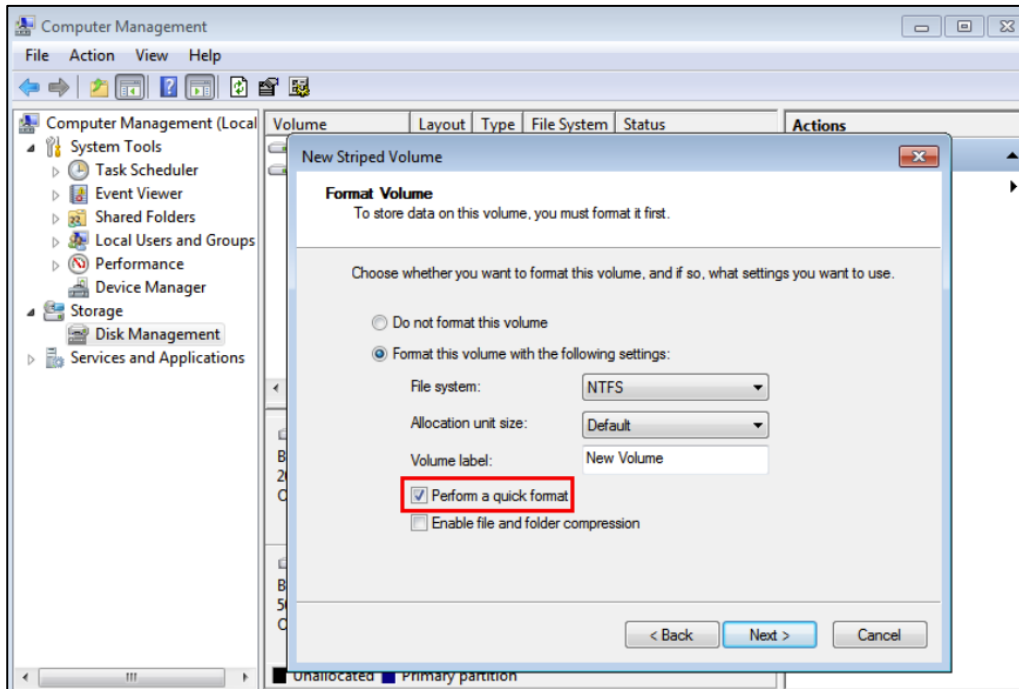
Details	
Hardware Type	Storage
Bus Type	High-Speed Hard Disk
Type	Existing Block Device
Block Device Path	/dev/disk/by-id/dm-nam...
Capacity	88.00GB
Cache Mode	Directsync
Hot Swappable	Yes
Serial Number	

# VMディスクをフォーマットする

## Windows を実行している VM でディスクをフォーマットする

VMのゲストOSでディスクをフォーマットするために、**Perform a quick format**を選択します。

図 1 クイックフォーマットを実行する



## Linux を実行している VM でディスクをフォーマットする

ディスクをフォーマットするための一部のコマンドには root 権限が必要なので、Linux にログインするには root ユーザー アカウントを使用します。

たとえば、CentOS 7 を実行している VM に新しく追加されたディスクをフォーマットするには:

1. 認識されているすべてのディスクとそのパーティションを表示するために **fdisk -l** コマンドを実行します。新しく追加されたディスクが CentOS 7 によって認識されていることを確認します。
2. 新しく追加されたディスクの名前を特定します。たとえば、**/dev/sdb**。
3. ディスク上にパーティションを作成するために **fdisk /dev/sdb** コマンドを実行します。ヘルプ情報を取得するには、**m** コマンドを入力します。パーティションを作成するには、**n** コマンドを入力します。指示に従ってパラメーターを設定します。

ディスク全体をパーティションとして使用する場合は、パーティションの最後のセクターを入力しないでください。

4. パーティションをフォーマットするために `mkfs.ext4 /dev/sdb1` コマンドを実行します。この例では、ext4 ファイル システムが使用されています。別のファイルシステムを使用するには、`ext4` を対応するコマンドで置き換えます。

## 推奨されるサーバー構成

データベースをインストールする前に、UIS 用に少なくとも 3 台のサーバーを準備します。

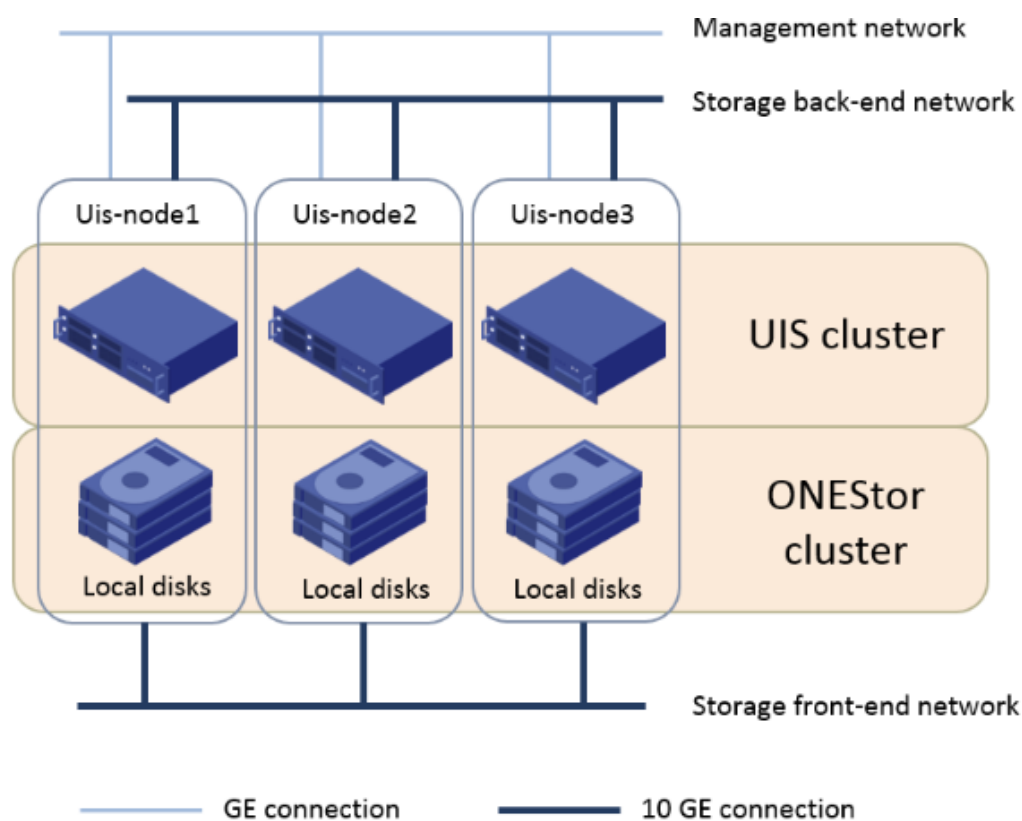
表 1 推奨されるサーバー構成

同時セッション	IOPS (4K)	TPMC	データサイズ	VM vCPU	VM メモリ	ディスク	CPU モデル	サーバーモデル
0 から 200	8000 から 15000	0 から 500000	100 GB から 300 GB	16	64 GB	SSD + HDD	Intel Xeon 6136 または、同じ性能を持つ他のモデル。	UIS3000/UIS9000 シリーズ
200 から 500	15000 から 25000	500000 から 750000	300 GB から 600 GB	16	96 GB	すべての SSD ノードあたり少なくとも 7 個。	Intel Xeon 6132, Intel Xeon 6136, または、同じ性能を持つ他のモデル。	UIS3000/UIS9000 シリーズ
500 から 800	25000 から 40000	750000 から 1000000	600 GB から 1 TB	24	128 GB	すべての SSD ノードあたり少なくとも 10 個。	Intel Xeon 6142, Intel Xeon 6242, または、同じ性能を持つ他のモデル。	UIS3000/UIS9000 シリーズ
800 から 1000	40000 以上	1000000 以上	600 GB から 1 TB	32	160 GB	すべての SSD ノードあたり少なくとも 15 個。	Intel Xeon 6154, Intel Xeon 6148, または、同じ性能を持つ他のモデル。	UIS3000/UIS9000 シリーズ

# ネットワーク計画

- 管理ネットワーク—UIS サービス ノード間の通信と管理に使用されます。
- ストレージネットワーク—以下のものが含まれます:
  - ストレージフロントエンドネットワーク—VM とストレージ クラスター間のトラフィックを転送します。
  - ストレージバックエンドネットワーク—データのバランス調整と復元のために、ストレージ クラスター内の内部トラフィックを転送します。
 ストレージ ネットワーク接続には専用の 10 GE NIC を使用します。
- サービスネットワーク—VM サービスデータを送信します。

図 1 ネットワーク計画



# ストレージディスクの種類

表 1 ストレージディスクの種類

パフォーマンス (tpmC)	展開モード	データディスク	データベースディスク

≥ 750000	すべての SSD	SATA SSD	ログディスク: SATA SSD データディスク: SATA SSD
< 750000	データディスク + キャッシュディスク	SATA SSD SAS\SATA HDD	ログディスク: SATA SSD データディスク: HDD or SSD データ ディスク + キャッシュ ディスク 展開モードで SSD をデータ ディスクとして使用する場合は、NVMe SSD をキャッシュ ディスクとして指定する必要があります。

## 推奨ディスク構成 キャッシュ

各ディスクに最低 50 GB のキャッシュを割り当てます。

- UIS セットアップが完了した後は、キャッシュ設定を変更できません。HDD 拡張が必要な場合は、ストレージ計画で SSD スペースを予約してください。
- 各キャッシュパーティションのサイズにストレージ ノード上のデータ ディスクの数を掛けた値が、キャッシュとして展開されている SSD の合計サイズよりも小さいことを確認してください。たとえば、ストレージ ノードに 600 GB の SSD が 2 台と HDD が 8 台あり、SSD が各 HDD に 100 GB のキャッシュを提供するとします。合計キャッシュ サイズは 800 GB で、キャッシュ ディスクの合計サイズよりも小さくなります。通常、ディスクの実際のサイズは、要求されたサイズよりも小さくなります。実際のサイズを使用してストレージを計画してください。説明のため、このドキュメントでは要求されたサイズを使用しています。
- 各 SSD で RAID 0 を使用します。
- 読み取り集中型の SSD (Intel S3500 シリーズ SSD など) をキャッシュ ディスクとして使用しないでください。

推奨される SSD と HDD の比率は次のとおりです。:

- 1 つの SATA SSD を使用して、5 つの SATA HDD にキャッシュを提供します。
- 1 つの SATA SSD を使用して 4 つの SAS HDD にキャッシュを提供します。
- 1 つの NVMe SSD を使用して 10 台の SATA HDD にキャッシュを提供します。
- 1 つの NVMe SSD を使用して、8 つの SAS HDD にキャッシュを提供します。

NVMe SSD はモデルによってパフォーマンスが大きく異なります。ベスト プラクティスとしては、200000 以上の IOPS をサポートする NVMe SSD を使用してください。

パフォーマンスを確保するには、SSD が十分でない場合はディスク キャッシュを有効にしないでください。

## メタデータディスク

メタデータは、ストレージ システムに保存されているユーザー データを管理するために使用されます。高パフ

パフォーマンスを得るには、メタデータを専用の SSD に保存します。

## ストレージデータディスク

- 各ストレージ ノードに少なくとも 4 つのディスクを展開します。データベースの場合、ディスクの数が増えるとパフォーマンスが向上します。
- 各 SSD で RAID 0 を使用します。
- ディスクは 10000 rpm (またはそれ以上) で使用してください。
- クラスタ内で同じディスク モデルを使用します。
- ベスト プラクティスとして、同じコネクタ タイプ (SAS または SATA)、容量、および回転速度を持つディスクを使用します。
- HDD および SSD データ ディスクのドライバー文字は、sd、df、nvme、fct、fio、または hio で始まることができます。読み取り集中型の SSD Intel S3500 シリーズ SSD、例えば、Intel S3500 シリーズ SSD など をデータ ディスクとして使用しないでください。
- ベスト プラクティスとして、サーバーに同じ数のデータ ディスクをインストールします。異なる数のデータ ディスクをインストールする必要がある場合は、最大数と最小数の差が最大数の 20% を超えないようにしてください。
- データのセキュリティを確保するには、レプリカを 3 つ使用します。データベースに高いパフォーマンスが必要な場合は、レプリカを 2 つ使用します。

ONEStor はレプリカを通じてデータの可用性を保証します。N 個のレプリカが使用される場合、使用可能な容量は生の容量を N で割った値になります。

## データベースディスクタイプの計画

データベース ディスクには、ログ ディスクとデータ ディスクがあり、同じ原則に従って計画されます。次の情報では、ログ ディスクを例として使用します。

ログ ディスクはデータベースのパフォーマンスを決定します。UIS 用のデータベースを展開する場合は、SSD をログ ディスクとして使用します。SSD は共有ストレージまたは RAW ボリュームとしてマウントできます。

- **共有ストレージ**—ブロック デバイスを共有ファイル システムとしてホストにマウントします。ストレージ ボリュームは共有ストレージ上に作成されます。ベスト プラクティスとして、複数の共有ストレージ システムを作成し、それらに同じボリュームを作成します。VM が Windows を実行している場合は、これらの同一のボリュームを使用してストリップ ボリュームを作成します。
- **Raw ボリューム**—ブロック デバイスを iSCSI ネットワーク ストレージとしてホストにマウントします。SSD のみを含むディスク プールにストレージ ボリュームを作成し、そのストレージ ボリュームを VM にマウントする必要があります。

- | ブロック デバイスを共有ストレージとしてマウントすると、その容量は 10% 以上減少します。
- RAW ボリュームはスナップショットや移行をサポートしていません。高可用性を実現するには、データベースがスタンドアロン サーバーにデプロイされている場合は共有

ストレージを使用し、データベースがクラスターにデプロイされている場合は RAW ボリュームを使用します。

- キャッシュ ディスクを備えた SSD ログ ディスクとデータ ディスクを使用したデータベースのパフォーマンスは、SSD ログ ディスクと SSD データ ディスクを使用した場合よりも 30% 低くなります。

## データベースストレージボリュームの計画

### SQL Server データベースのストレージ ボリューム計画

展開前に、ログ ディスクとデータ ディスクの数と容量を決定します。表1 SQL Server のディスク計画の例を示します。必要に応じてログ ディスクの容量を増やすことができます。

表 1 SQL Server ディスク計画の例

データベース	番号	ドライブ文字	共有ボリュームサイズ	ストレージプール名	ディスクグループ名
SQL Server 2016	1	/dev/vdb	100 GB	LOG1	LOG
	2	/dev/vdc	100 GB	LOG2	LOG
	3	/dev/vdd	100 GB	LOG3	LOG
	4	/dev/vde	200 GB	DATA1	DATA
	5	/dev/vdf	200 GB	DATA2	DATA
	6	/dev/vdg	200 GB	DATA3	DATA
	7	/dev/vdh	200 GB	DATA4	DATA
	8	/dev/vdi	200 GB	DATA5	DATA
	9	/dev/vdj	200 GB	DATA6	DATA
	10	/dev/vdk	200 GB	DATA7	DATA

## MySQL データベースのストレージ ボリューム計画

展開前に、ログ ディスクとデータ ディスクの数と容量を決定します。表2 MySQL のディスク計画の例を示しま

す。必要に応じてログ ディスクの容量を増やすことができます。

表 2 MySQL ディスク計画の例

データベース	番号	ドライブ文字	共有ボリュームサイズ	ストレージプール名	ディスクグループ名
My SQL 5.7	1	/dev/vdb	100 GB	LOG1	LOG
	2	/dev/vdc	100 GB	LOG2	LOG
	3	/dev/vdd	100 GB	LOG3	LOG
	4	/dev/vde	200 GB	DATA1	DATA
	5	/dev/vdf	200 GB	DATA2	DATA
	6	/dev/vdg	200 GB	DATA3	DATA
	7	/dev/vdh	200 GB	DATA4	DATA
	8	/dev/vdi	200 GB	DATA5	DATA
	9	/dev/vdj	200 GB	DATA6	DATA
	10	/dev/vdk	200 GB	DATA7	DATA

## Oracle データベースのストレージ ボリューム計画

展開前に、ログ ディスク、データ ディスク、クォーラム ディスクの数と容量を決定します。表3 Oracle のディスク計画の例を示します。必要に応じてログ ディスクの容量を増やすことができます。

表 3 Oracle ディスク計画の例

データベース	番号	ドライブ文字	共有ボリュームサイズ	ストレージプール名	ディスクグループ名
Oracle 12C	1	/dev/vdb	100 GB	LOG1	LOG



2	/dev/vdc	100 GB	LOG2	LOG
3	/dev/vdd	100 GB	LOG3	LOG
4	/dev/vde	200 GB	DATA1	DATA
5	/dev/vdf	200 GB	DATA2	DATA
6	/dev/vdg	200 GB	DATA3	DATA
7	/dev/vdh	200 GB	DATA4	DATA
8	/dev/vdi	200 GB	DATA5	DATA
9	/dev/vdj	200 GB	DATA6	DATA
10	/dev/vdk	50 GB	GRID1	GRID

## VM計画

CPU、メモリ、ディスク、NIC のサービス システムの要件に基づいて VM 構成を決定します。次の情報は VM 構成の例を示しています。

### SQL Server VM 構成

表 1 VM 構成

リソース	仕様
オペレーティング・システム	Windows Server 2016 64-bit
CPU	1 × 24 コア
メモリー	168 GB
システムディスク	100 GB
SQL Server ディスク	" <a href="#">SQL Server データベースのストレージ ボリューム計画</a> "を参照してください。

ディスクタイプ	VirtIO、インテリジェント
NIC	1 × 高速 NIC

## MySQL VM 構成

表 2 VM 構成

リソース	仕様
オペレーティング・システム	CentOS 7.5
CPU	24 vCPU
メモリー	128 GB
システムディスク	100 GB
MySQL ディスク	" <a href="#">MySQL データベースのストレージ ボリューム計画</a> "を参照してください。
ディスクタイプ	VirtIO、インテリジェント
NIC	1 × 高速 NIC

## Oracle VMの構成

表 3 VM 構成

リソース	スタンドアロン展開の仕様	RAC 導入の仕様
オペレーティング・システム	Red Hat 6.5	Red Hat 6.5
CPU	24 × 1 コア	24 × 1 コア
メモリー	128 GB	160 GB

システムディスク	200 GB	200 GB
Oracle ディスク	<u>"Oracle データベースのストレージ ボリューム計画"</u> を参照してください。	<u>"Oracle データベースのストレージ ボリューム計画"</u> を参照してください。
ディスクタイプ	VirtIO	VirtIO
NIC	高速 NIC	2 つの高速 NIC。1 つはプライベート IP アドレスを使用し、もう 1 つはパブリック IP アドレスを使用します。

# ドキュメントおよびソフトウェア

ドキュメント(英語版)はどこにありますか？

<https://www.h3c.com/jp/>



Cloud Computing

<b>Unified Infrastructure System</b> → UIS-Cell 3000 G3 Series → UIS-Cell 6000 G3 Series <b>→ UIS Manager</b> → UIS 2000 G6 Series → UIS 3000 G5 Series → UIS 3000 G6 Series → UIS 6000 G5 Series	<b>Workspace</b> → H3C Workspace	<b>CloudOS</b> → H3C CloudOS 5.0	<b>CAS</b> → CAS
--	-------------------------------------	-------------------------------------	---------------------

CAS

Home » Support » Cloud Computing » CAS

**Technical Documents** | Software Download

Select Version: All Version  Search in Current Product

<b>All Documents</b>	<b>Documentation Maps</b>
Documentation Maps	→ H3C CAS Documentation Map-5W100 24-06-2024
Doc Sets	<b>Doc Shelf</b>
Install & Upgrade	→ H3C Cloud Computing Product Document Shelf-5W101 21-05-2024
Configure & Deploy	

ドキュメント(日本語版)はどこにありますか？

<https://www.h3c.com/jp/>



Knowledge Base Doc Hub

Registration Login

Country/Region  
Global - English  
Japan - 日本語

Documents type: All Test Startup Technical Announcement Experience Case FAQ Key Cases

Product line: All Router Switch Wireless Network Management Security ADNET Solution Cloud Computing Servers  
Minicomputer Storage Big Data CloudComputingSolution Transceiver Common

Latest Hottest Recommended

Input key words

AC V7 portal user automatic logout function Portal V7 AC  
0 72 Pengqirui 2024-07-01 06:39:43 Published

How to implement remote MAC authentication using the MAC address as the username and a fixed password? MAC address authentication V7 AC  
0 56 Zhoutian 2024-06-28 08:37:09 Published

Example of SSID displayed an extra 2 on the laptop  
SSID WA6600/WA6500/WA6300/WA5600/WA5500/ WA5300/WA4600/WA4300 series  
0 61 Zhoutian 2024-06-28 08:32:53 Published

write

Collection Following Draft

ドキュメントセンター

登録 ログイン

ドキュメントセンターは、H3C製品に関する情報ナビゲーションの中心です。主に製品シリーズ全般にわたるインストールガイド、設定ガイド、メンテナンスマニュアル、トラブルシューティングマニュアルなどの資料を提供しています。これにより、ユーザーはインストール、設定、メンテナンスに関する問題に直面した際に、効果的な解決策を手に入れることができます。

投稿

製品別検索

ルーター	スイッチ	WLAN	セキュリティ
クラウドコンピューティング	ネットワーク管理	AD-NET ソリューション	サーバ
CloudNet	Cloud Lab	テクニカルサポート	Others

ソフトウェアはどこにありますか？

<https://www.h3c.com/jp/>

The screenshot shows the H3C website's Resource Center page. The navigation menu includes: 製品とソリューション, 業界ソリューション, サービス, サポート, トレーニングと認定, パートナー, 私たちについて. The main content area is titled "リソースセンター" (Resource Center). On the left sidebar, there are links for "リソースセンター", "オンラインヘルプ", "ポリシー", and "すべてのサポート >>". The main content area has two columns: "ソフトウェアのダウンロード" (Software Downloads) and "テクニカルドキュメント" (Technical Documents). The "ソフトウェアのダウンロード" link is highlighted with a red box. At the bottom, there are three icons: a shopping cart for "営業担当者へのお問い合わせ" (Contact Sales Representative), a server rack for "オンライン展示センター" (Online Exhibition Center), and a gear for "リソースセンター" (Resource Center).

The screenshot shows the H3C website's Product Category search page. The title is "製品カテゴリーから探す" (Search by Product Category). The page displays a grid of 12 product categories, each with an icon and text: "ルーター" (Router), "サーバー" (Server), "クラウドコンピューティング" (Cloud Computing), "スイッチ" (Switch), "無線" (Wireless), "セキュリティ" (Security), "ネットワーク管理" (Network Management), "その他" (Others), "クラウドネット" (Cloud Network), "ライセンスサーバー" (License Server), "ADNET", and "インテリジェント端末" (Intelligent Terminal). The "クラウドコンピューティング" category is highlighted with a red box. At the bottom right, there is a red button with the text "営業担当者へのお問い合わせ" (Contact Sales Representative).



# Cloud Computing

Home > Support > Software Download > Cloud Computing

Quick location of Software

Please input Product Model, like S12500

Note: Through search product Series, you can quickly locate the version.

Unified Infrastructure System

→ UIS

→ UIS-Cloud

Workspace

→ H3C Workspace

CAS

→ CAS

→ H3C UIS-E0802P01 バージョンソフトウェアおよびリリースノート (X86)	2024年5月16日	↓
→ H3C UIS-E0801P03 バージョンソフトウェアおよびリリースノート (X86)	2024年1月17日	↓
→ H3C UIS-E0750P11 バージョンソフトウェアおよびリリースノート (ARM)	2023年10月26日	↓
→ H3C UIS-E0750P11 バージョンソフトウェアおよびリリースノート (X86)	2023年10月26日	↓
→ H3C UIS-E0750P10 バージョンソフトウェアおよびリリースノート (X86)	2023年7月13日	↓
→ H3C UIS-E0750P09 バージョンソフトウェアおよびリリースノート (ARM)	2023年2月24日	↓
→ H3C UIS-E0750P09 バージョンソフトウェアおよびリリースノート (X86)	2023年2月24日	↓
→ H3C UIS-E0750P07 バージョンソフトウェアおよびリリースノート (X86)	2022年11月8日	↓
→ H3C UIS-E0750P07 バージョンソフトウェアおよびリリースノート (ARM)	2022年11月8日	↓
→ H3C UIS-E0750P06 バージョンソフトウェアおよびリリースノート (ARM)	2022年2月6日	↓
→ H3C UIS-E0750P06 バージョンソフトウェアおよびリリースノート (X86)	2022年2月6日	↓

## ソフトウェアダウンロード許可の説明:

1. ロックされたドキュメントを表示できるのは、許可されたユーザーのみです。
2. H3C 製品の顧客の場合は、代理店に連絡して対応するバージョンを入手してください。
3. H3C サービス契約の顧客の場合は、サービス開始通知に記載されているサービス アカウントを使用してダウンロードしてください。



ロックされたドキュメントを表示できるのは、許可されたユーザーのみです。