vSphere の単一ホスト管理：VMware Host Client

VMware vSphere 8.0
VMware ESXi 8.0
VMware Host Client 2.5.0

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

目次

『vSphere 単一ホスト管理：VMware Host Client』について

「vSphere 単一ホスト管理：VMware Host Client」では、VMware Host Client での単一ホスト管理に関する情報を提供します。

vCenter Server を使用できない場合には、VMware Host Client を使用して緊急時管理を実施できます。VMware Host Client では、管理タスク、基本的なトラブルシューティング タスク、および高度な管理タスクを実行できます。

VMware では、多様性の受け入れを尊重しています。お客様、パートナー企業、社内コミュニティとともにこの原則を推進することを目的として、多様性の受け入れに適切でない言葉遣いを削除するため、このガイドを更新しました。

対象読者

この情報は、VMware Host Client を使用して単一の ESXi ホストの管理を行うユーザーを対象としています。ここに記載の情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を想定しています。

更新情報

1

『vSphere の単一ホスト管理：VMware Host Client』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere の単一ホスト管理：VMware Host Client』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2022 年 10 月 21 日	VMware Host Client でのシステム設定の管理のマイナー更新。
2022 年 10 月 19 日	VMware Host Client での既存の仮想マシン上の仮想化ベース セキュリティの有効化または無効化のマイナー更新。
2022 年 10 月 13 日	新しいバージョンの ESXi にアップグレードした後に VMware Host Client から ESXi ホストに接続できないのコード スニペット内の空白スペースを削除
2022 年 10 月 11 日	初期リリース。

VMware Host Client について

2

VMware Host Client は HTML5 ベースのクライアントであり、単一の ESXi ホストに接続してそのホストを管理するのに使用されます。

VMware Host Client を使用して、以下のことを行えます。

- 管理タスクと基本的なトラブルシューティング タスクを実行できるほか、ターゲット ESXi ホスト上で高度な管理タスクを実行することもできます。
- vCenter Server を使用できない場合には、緊急時管理を実施します。

VMware Host Client が vSphere Client とは異なることを理解しておくことが重要です。vSphere Client は vCenter Server に接続して複数の ESXi ホストを管理するのに使用しますが、VMware Host Client は単一の ESXi ホストを管理するのに使用します。

VMware Host Client では次の操作を実行できますが、これらの操作に限定されるものではありません。

- 複雑さの度合いが異なる仮想マシンのデプロイと構成など、基本的な仮想化操作。
- ネットワークおよびデータストアの作成と管理。
- ホスト レベル オプションでの詳細な調整によるパフォーマンスの向上

VMware Host Client のシステム要件

使用するブラウザが VMware Host Client をサポートしていることを確認します。

VMware Host Client は、次のゲスト OS と Web ブラウザのバージョンをサポートしています。

サポート対象ブラウザ	Mac OS	Windows 32 ビットおよび 64 ビット	Linux
Google Chrome	89+	89+	75 以降
Mozilla Firefox	80+	80+	60 以降
Microsoft Edge	90+	90+	該当なし
Safari	9.0+	該当なし	該当なし

この章には、次のトピックが含まれています。

- 以下を使用します。VMware Host Client

以下を使用します。VMware Host Client

vCenter Server が一時的に使用不能になった場合は、VMware Host Client を使用して緊急時管理を実施します。

VMware Host Client の起動とログイン

VMware Host Client を使用して、単一の ESXi ホストを管理し、仮想マシンに対してさまざまな管理タスクおよびトラブルシューティング タスクを実行することができます。

ESXi ホストにログインするには、次の手順を実行します。

手順

1 Web ブラウザから次のフォームを使用してターゲット ホスト名または IP アドレスを入力します。**`https://host-name/ui`** または **`https://host-IP-address/ui`**。

ログイン画面が表示されます。

2 ユーザー名およびパスワードを入力します。

3 [ログイン] をクリックして、続行します。

4 [VMware カスタマ エクスペリエンス改善プログラム (CEIP)] ページを参照し、プログラムへの参加を希望するかどうかを選択します。

本プログラムの詳細および構成の方法については、VMware Host Client のカスタマ エクスペリエンス改善プログラムの離脱および再加入を参照してください。

5 [OK] をクリックします。

VMware Host Client からのログアウト

ターゲット ESXi ホストの表示や管理が不要になったら、VMware Host Client からログアウトします。

注： VMware Host Client セッションを閉じても、ホストは停止しません。

手順

- ESXi ホストからログアウトするには、VMware Host Client ウィンドウの上部に表示されているユーザー名をクリックし、ドロップダウン メニューから [ログアウト] を選択します。

  これで、VMware Host Client からログアウトされます。ターゲット ESXi ホストは、その通常のアクティビティすべての実行を継続します。

VMware Host Client のユーザー インターフェイス テーマをカスタマイズする方法

vSphere 8.0 を使用すると、VMware Host Client のユーザー インターフェイスのブランディング、およびその外観とコンテンツの表示方法をカスタマイズできます。

事前設定されている 3 つのテーマ（明るい、暗い、クラシック）から選択して、好みに応じてテーマを VMware Host Client に適用できます。

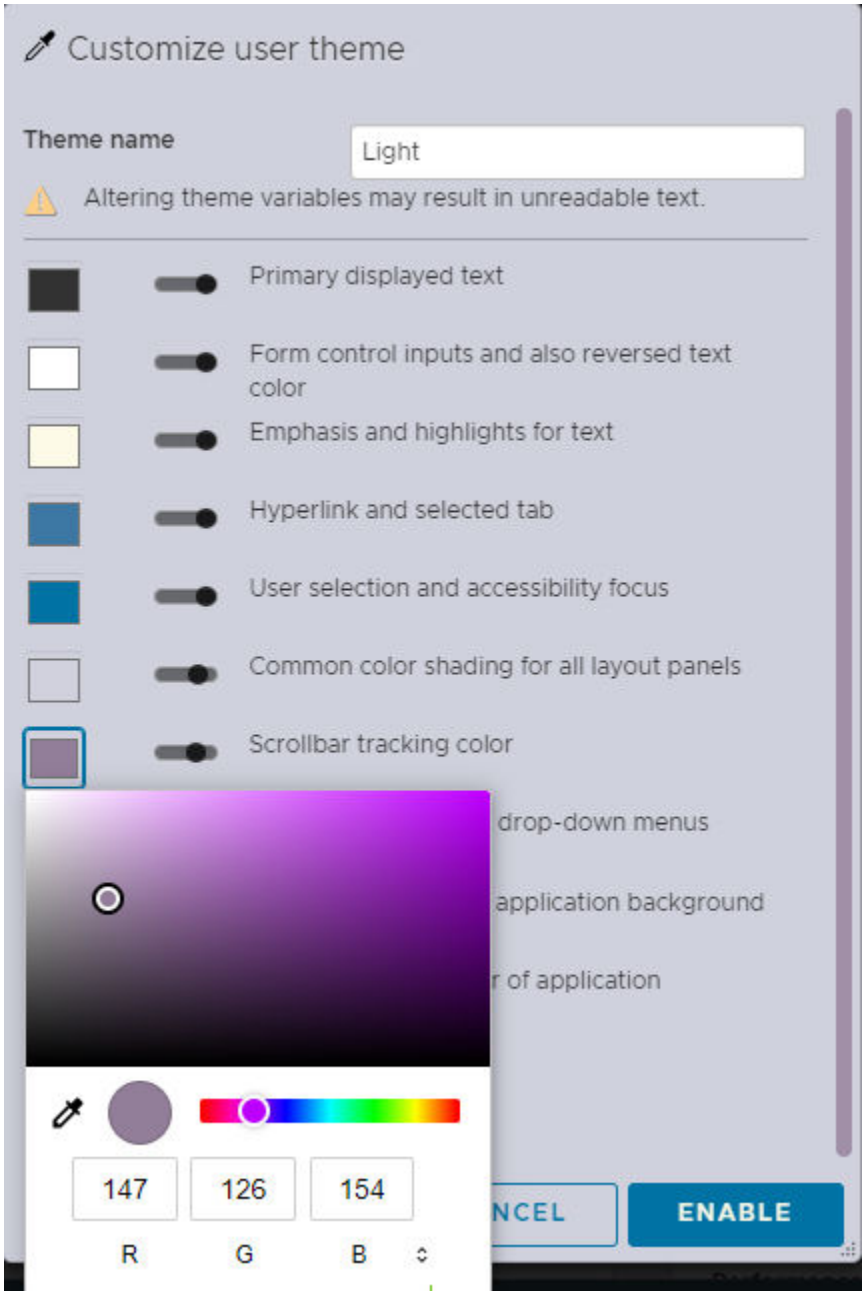
手順

1 VMware Host Client ツールバーで、[ヘルプ] をクリックし、[バージョン情報] をクリックします。

[バージョン情報] ウィンドウが表示されます。

2 [ユーザー インターフェイス設定テーマ] ドロップダウン メニューから、適用するテーマを選択します。

3 テーマ名を変更したり、選択するテーマの最大 10 個のパラメータを変更するには、[カスタマイズ] ボタンをクリックします。



a [テーマ名] フィールドに、テーマのカスタム名を入力します。

b 各パラメータのカスタム色を選択するには、各パラメータの前にある色付きのボックスをクリックし、色を選択して、[有効化] をクリックします。

a デフォルトのパレットに戻すには、[リセット] ボタンをクリックします。

VMware Host Client のユーザー インターフェイス ログイン画面のログイン バナーの構成

法的警告または公式発表を表示するには、制限されている形式の Markdown 構文を使用してログイン ページ バナーを構成します。

テキスト ファイル `/etc/vmware/welcome` をホストで直接変更することで、ユーザー名とパスワードのログイン フィールドの右側に表示されるログイン バナーの内容を変更できます。

注： Markdown パーサーがコンテンツ ブロックに適用され、`#`, `` ` ``, `*` などの特定の文字シーケンスにより誤って Markdown フォーマット ルールがトリガされることがあります。

`welcome` ファイルでは、次の限定された一連の Markdown ディレクティブを適用できます。

レイアウトの概念	Markdown コード構文	出力
見出しラベル	■ 新しい行から、1 ～ 6 つのハッシュ マーク記号を入力します。 [例] `# My Title。`	「My Title」に対し長い HTML `<H1>` タグを生成します。 **My Title**
水平ルール	■ 新しい行から、3 つ以上の一連のダッシュ文字のみを入力します。 [例] `-----。`	HTML で `<hr />` ルール タグを生成します。 ---

リテラルまたはコード ブロック	■ 新しい行から、3 つのバッククォート文字のみを入力します。
	■ 後続行でソース資料を追加します。
	■ ソースを閉じるには、新しい行で 3 つのバッククォート文字を入力します。
	[例]
	```` ```
	My content - - -
	Login Secure >_
	Read the policy
	``` ````
		フォーマットまたは解釈なしでバッククォート行間のテキスト ブロックを等幅フォントで表示します。
		``
		My content - - -
		Login Secure >_
		Read the policy
		``
		注： コンテンツが誤って Markdown パーサによってフォーマットされている場合は、バッククォート文字行のペアでコンテンツをラップします。スペース文字は保持されるため、等幅フォントが使用されているときは ASCII アートを使用できます。

太字テキスト	テキストの文字列の両側を二重アスタリスク文字で囲みます。 [例] `**important message**。` **注：** URL との競合を回避するため、Markdown 二重アンダースコア文字構文は省略されます。	`<b>`[important message]`</b>`

レイアウトの概念	Markdown コード構文	出力
斜体テキスト	テキストの文字列の両側を一重アスタリスク文字で囲みます。 [例] `*A named document*`。 **注：** URL との競合を回避するため、Markdown アンダースコア文字構文は省略されます。	`<i>`A named document`</i>`
ハイパーリンク	絶対 URL をリンクするには、リンク テキストを囲む角括弧に続いて、括弧で囲まれた URL を挿入する Markdown 構文を使用します。 [例] `[My link](https://www.example.com?search=virtual)`	クリック可能なテキストを含む通常のハイパーリンク アンカー タグを生成します。`<a href="https://www.example.com?search=virtual">My link</a>`

[サポートされている変数]

テキスト ファイル内の任意の場所に次の変数を挿入できます。

変数の概念	メタ タグ変数コード	出力
現在のホストまたは IP アドレスの完全修飾ドメイン名	`{hostname}`	現在のホストのフル ネームが表示されます。たとえば、`sample.host.com`。
ドット付き数値形式の ESXi バージョン	`{esxversion}`	たとえば、`7.0.0` が表示されます。
ESXi の完全製品名、バージョン、およびビルド番号	`{esxproduct}`	たとえば、`VMware ESXi 7.0.0 build-16324942` が表示されます。
ユーザーのマシンの現在の日付	`{client-current-date}`	たとえば、`Tuesday, August 30, 2022` が表示されます。 **注：** これはロケール固有です。
ユーザーのマシンの現在の時刻	`{client-current-time}`	たとえば、`08:00 AM` が表示されます。 **注：** これはロケール固有です。

[高度なタグ]

高度なタグにより、ログイン ページに適用するルールに応じて、視覚的および動作的な変更が提供されます。これらのタグをテキスト ファイルの一番最後に挿入します。

ユーザー インターフェイスの概念	メタ タグ変数コード	出力
カスタム イメージ	`{logo src="https://site/logo.png" width="100" height="100" align="center"}My Secured ESXi Server Tooltip{/logo}`	メッセージ ブロック上に水平方向に中央に配置された 100x100 ピクセルのイメージ `logo.png` が表示されます。`My Secured ESXi Server Tooltip` のアクセス可能なツールチップ タイトルがイメージに追加されます。 **注：** `width`、`height`、および `align` の各属性はオプションですが、必ず使用してください。すべての Web イメージ形式がサポートされています。
ユーザー契約書チェック ボックス	`{accept}Please accept the terms{/accept}`	メッセージ内容の下部に「条項に同意してください」というラベルが付いたチェック ボックスが表示されます。
強制同意エラー メッセージ	`{mustaccept}You must agree before logging into the system{/mustaccept}`	フォーム検証を追加して、ログイン前にチェック ボックスを選択するようユーザーに要求します。ユーザーがチェック ボックスを選択しない場合、ログイン ボタン上に「システムにログインする前に同意する必要があります」というメッセージが表示されます。

[例]

[シンプルな Markdown]

シンプルなテキストのみのメッセージの 1 行の Markdown

```
## Warning: Authorized Users Only
```

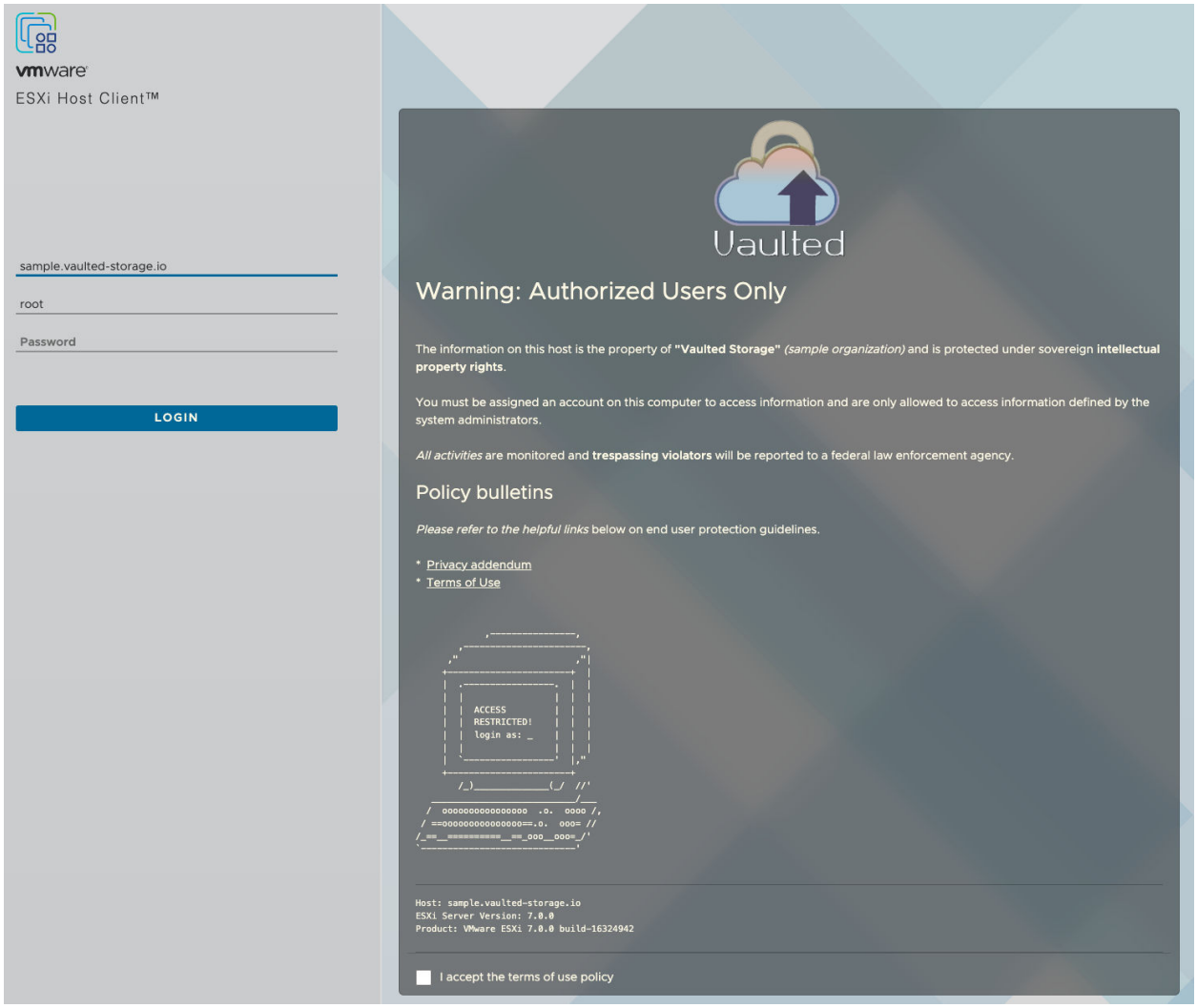
[高度な Markdown]

架空のクラウド ストレージ会社 Vaulted の高度な Markdown のサンプル。フォームにロゴ、リンク、および必須の同意チェック ボックスが付いています。

```
## Warning: Authorized Users Only

The information on this host is the property of **"Vaulted Storage"** *(sample organization)*
and is protected under sovereign **intellectual property rights**.

You must be assigned an account on this computer to access information and are only allowed
to access information defined by the system administrators.

*All activities* are monitored and **trespassing violators** will be reported to a federal
law enforcement agency.

### Policy bulletins
*Please refer to the helpful links* below on end user protection guidelines.

* [Privacy addendum](https://en.wikipedia.org/wiki/Computer_security)
* [Terms of Use](https://en.wikipedia.org/wiki/
Terms_of_service#:~:text=Terms%20of%20service%20(also%20known,to%20use%20the%20offered%20servi
ce.)

```
             ,----------------,
        ,-----------------------,
      ,"   ,"|
     +-----------------------+ |
     | .-----------------. | |
     | | | | |
     | | ACCESS | | |
     | | RESTRICTED! | | |
     | | login as: _ | | |
     | | | | |
     | `-----------------' |,"
     +-----------------------+
        /_)_____________(_/ //'
   ___________________________/___
  / oooooooooooooooo .o. oooo /,
 / ==ooooooooooooooo==.o. ooo= //
/_==__==========__==_ooo__ooo=_/'
`--------------------------------'

Host: {hostname}
ESXi Server Version: {esxversion}
Product: {esxproduct}

```
{logo align="center" width="200" height="200" src="https://i.postimg.cc/y6wZXTPm/vaulted-logo-white-text.png"}Vaulted Enterprise Storage{/logo}

{accept}I accept the terms of use policy{/accept}

{mustaccept}User must check terms of use to login. LOG OFF immediately if you do not agree to the conditions stated in the warning.{/mustaccept}
```



VMware Host Client のカスタマ エクスペリエンス改善プログラムの離脱および再加入

カスタマー エクスペリエンス向上プログラム (CEIP) に参加すると、匿名のフィードバックや情報を VMware に提供して VMware の製品およびサービスの品質、信頼性、機能の向上に貢献できます。

カスタマ エクスペリエンス改善プログラム (CEIP) の離脱、および同プログラムへの再加入はいつでも可能です。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、Trust & Assurance センター (http://www.vmware.com/trustvmware/ceip.html) に記載されています。

手順

1 CEIP からの離脱および再加入を行うには、VMware Host Client ページ上部のユーザー名をクリックしてください。

2 [設定]> [使用統計の送信] をクリックし、CEIP から離脱または CEIP に再加入します。

VMware Host Client でのホスト管理 3

VMware Host Client では、vCenter Server のアップグレード中、または vCenter Server が応答を停止したか使用不能になった場合に、単一の ESXi ホストを管理できます。

VMware Host Client には、重要なトラブルシューティング機能のセットが備わっており、vCenter Server が使用不能になった場合には、それらの機能を使用して、ログインしている ESXi ホスト上でタスクを実行できます。使用できる機能は、ホストの詳細設定、ライセンス、証明書の管理、ESXi Shell の使用、ロックダウン モードの有効化などです。

この章には、次のトピックが含まれています。

VMware Host Client でのシステム設定の管理

VMware Host Client を使用して、ホストの詳細設定の管理、ホストの証明書の割り当てまたは削除、ホスト サービスの開始ポリシーと停止ポリシーの構成、ホストの日時構成の管理を実行できます。

VMware Host Client での詳細設定の管理

VMware Host Client を使用して、ホストの設定を変更できます。

注意： VMware テクニカル サポートまたはナレッジ ベースの記事で特に指示がない限り、詳細オプションの変更はサポートされていないと見なされます。その他の場合はすべて、これらのオプションの変更はサポートされていないと見なされます。ほとんどの場合、デフォルトの設定で最適な結果が得られます。

手順

1. VMware Host Client インベントリ内で [管理] > [システム] の順にクリックします。
2. [詳細設定] をクリックします。
3. リスト内の該当するアイテムを右クリックし、ドロップダウン メニューから [オプションの編集] を選択します。

   [オプションの編集] ダイアログ ボックスが表示されます。
4. 値を編集し、[保存] をクリックして変更を適用します。
5. （オプション） アイテムの元の設定に戻すには、リスト内の該当するアイテムを右クリックし、[デフォルトにリセット] を選択します。

ダイレクト コンソール ユーザー インターフェイスおよび VMware Host Client に対する最初のウェルカム メッセージの作成

VMware Host Client を使用して、ダイレクト コンソール ユーザー インターフェイス (DCUI) の最初の画面および VMware Host Client のログイン ウィンドウに表示されるウェルカム メッセージを作成できます。VMware Host Client にログインした後に表示されるウェルカム メッセージを作成し、ウェルカム メッセージを表示するかどうかを決定することもできます。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

オプション	操作
DCUI および VMware Host Client にログインする前に表示されるウェルカム メッセージの作成	a [検索] テキスト ボックスに「**Annotations.WelcomeMessage**」と入力し、[検索] アイコンをクリックします。 b `Annotations.WelcomeMessage` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 [オプションの編集] ダイアログ ボックスが開きます。 c [新しい値] テキスト ボックスに、ウェルカム メッセージを入力します。 デフォルトのメッセージを設定するには、[新しい値] テキスト ボックスを空にしておきます。
VMware Host Client にログインした後に表示されるウェルカム メッセージの作成	a [検索] テキスト ボックスに「**UserVars.HostClientWelcomeMessage**」と入力し、[検索] アイコンをクリックします。 b `UserVars.HostClientWelcomeMessage` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 [オプションの編集] ダイアログ ボックスが開きます。 c [新しい値] テキスト ボックスに、ウェルカム メッセージを入力します。 デフォルトのメッセージを設定するには、[新しい値] テキスト ボックスを空にしておきます。
VMware Host Client にログインした後のウェルカム メッセージの表示の有効化または無効化	a [検索] テキスト ボックスに「**UserVars.HostClientEnableMOTDNotification**」と入力し、[検索] アイコンをクリックします。 b `UserVars.HostClientEnableMOTDNotification` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 [オプションの編集] ダイアログ ボックスが開きます。 c [新しい値]テキスト ボックスに新しい値を入力します。 ゼロ (0) の値を指定すると、ウェルカム メッセージの表示が無効になります。 1 の値を指定すると、ウェルカム メッセージの表示が有効になります。

2 [保存] をクリックします。

3 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

VMware Host Client ユーザー インターフェイス セッション タイムアウトの構成

VMware Host Client では、ユーザー インターフェイス セッションが自動的に 15 分ごとにタイムアウトするため、VMware Host Client に再度ログインする必要があります。

詳細構成パラメータを変更して、デフォルトのアクティビティ停止のタイムアウトを増やすことができます。デフォルト値は 900 秒です。

手順

◆ ユーザー インターフェイス セッション タイムアウトを構成します。

オプション	操作
VMware Host Client の詳細設定から	a VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。 b [検索] テキスト ボックスに「**UserVars.HostClientSessionTimeout**」と入力し、[検索] アイコンをクリックします。 c `UserVars.HostClientSessionTimeout` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 [オプションの編集] ダイアログ ボックスが開きます。 d [新しい値] テキスト ボックスに、タイムアウト設定を秒単位で入力します。 **注：** ゼロ (0) の値を指定すると、タイムアウトが無効になります。 e [保存] をクリックします。 f （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。
[ユーザー設定] ドロップダウン メニューから	a VMware Host Client ウィンドウの上部でユーザー名をクリックし、[設定] - [アプリケーションのタイムアウト] - [.] の順に選択します。 b アクティビティ停止のタイムアウトを指定するには、時間を選択します。 c アクティビティ停止のタイムアウトを無効にするには、`Off` を選択します。

VMware Host Client での SOAP セッション タイムアウトの構成

VMware Host Client で、SOAP セッションのタイムアウトを構成できます。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

2 [検索] テキスト ボックスに「**Config.HostAgent.vmacore.soap.sessionTimeout**」と入力し、[検索] アイコンをクリックします。

3 `Config.HostAgent.vmacore.soap.sessionTimeout` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。

[オプションの編集] ダイアログ ボックスが開きます。

4 [新しい値] テキスト ボックスに、タイムアウト設定を秒単位で入力します。

ゼロ (0) の値を指定すると、タイムアウトが無効になります。

5 [保存] をクリックします。

6 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

VMware Host Client でのパスワードとアカウント ロックアウト ポリシーの構成

ESXi ホストに対して、事前に定義された要件を満たすパスワードを使用する必要があります。必要なパスワード長の変更、文字の種類に関する要件の変更や、パスフレーズの許可を行う場合はすべて、`Security.PasswordQualityControl` の詳細オプションを使用します。`Security.PasswordHistory` の詳細オプションを使用して、ユーザーごとに記憶するパスワードの数を設定することもできます。`Security.PasswordMaxDays` 詳細オプションを使用すると、パスワード変更までの最大日数を設定できます。

注： デフォルトのパスワード設定を変更したら、必ず追加テストを実行してください。

誤った認証情報を使用してログインを試行した場合は、アカウント ロックアウト ポリシーによって、システムがアカウントをロックするタイミングと期間が指定されます。

ESXi のパスワード

ESXi により、アクセスに使用するパスワードの要件が適用されます。

- デフォルトでは、パスワードを作成する際に、4 種類の異なる文字クラス、すなわち、小文字、大文字、数字、特殊文字（アンダースコアやダッシュなど）の中の任意の 3 つの文字を組み合わせる必要があります。
- デフォルトでは、パスワードの長さは 7 文字以上、40 文字以下にする必要があります。
- パスワードに、辞書ファイル内の単語または単語の一部を含めることはできません。
- パスワードには、ユーザー名またはユーザー名の一部を含めることはできません。

注： パスワードの先頭に大文字を使用する場合、これは文字の種類に含まれません。パスワードの末尾を数字にする場合、これは文字の種類に含まれません。

ESXi パスワードの例

ここでは、次のようにオプションが設定されている場合のパスワードの候補を示します。

```
retry=3 min=disabled,disabled,disabled,7,7
```

この設定では、新しいパスワードが十分に強力ではない場合、またはパスワードが 2 回正しく入力されなかった場合、ユーザーは最大 3 回 (retry=3) 入力を要求されます。1 種類または 2 種類の文字が含まれるパスワードと、パスワード フレーズは許可されません。これは、最初の 3 つのアイテムが無効に設定されているためです。パスワードには 3 種類および 4 種類の文字を使用し、7 文字の長さが必要です。

次のパスワード候補は、パスワードの要件を満たしています。

- xQaTEhb!： 3 種類の文字を使用した 8 文字のパスワード。
- xQaT3#A： 4 種類の文字を使用した 7 文字のパスワード。

次に示すパスワード候補は、パスワードの要件を満たしていません。

- Xqat3hi：先頭が大文字であるため、有効な文字クラスの数が 2 に減っています。パスワードには、3 種類以上の文字を使用する必要があります。

- xQaTEh2：数字で終わるため、有効な文字クラスの数が 2 に減っています。パスワードには、3 種類以上の文字を使用する必要があります。

パスワード品質管理

Security.PasswordQualityControl 詳細オプションを使用して、パスワードの品質を管理できます。

Security.PasswordQualityControl は、次のパターンに従ういくつかの設定で構成されています。

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

パスワード品質管理の設定	説明	デフォルト
retry=N	パスワードが正しくない場合や強度が十分でない場合に、ユーザーが新しいパスワードを入力する必要がある回数。	retry=3
min=N0,N1,N2,N3,N4	文字クラスとパスフレーズの最小長の要件。 ■ N0 は、1 つの文字クラスで構成されたパスワードの最小長です。 ■ N1 は、2 種類の文字で構成されたパスワードの最小長です。 ■ N2 はパスフレーズの最小長です。 ■ N3 は、3 種類の文字で構成されている場合の最小長です。 ■ N4 は、4 種類の文字で構成されている場合の最小長です。 disabled を使用して、指定した数の文字の種類を含むパスワードを許可しないようにすることができます。	min=disabled,disabled,disabled,7,7
max=N	許可される最大パスワード長。	max=40
passphrase=N	パスフレーズに必要な単語の数。passphrase が認識されるようにするには、min 設定の N2 を disabled に設定しないでください。	passphrase=3
similar=permit|deny	古いパスワードに似たパスワードを許可するかどうかを示します。この設定を使用するには、Security.PasswordHistory オプションをゼロ以外の値に設定してください。	similar=deny

ESXi パスフレーズ

パスワードの代わりに、パスフレーズを使用できます。パスフレーズはデフォルトで無効になっています。Security.PasswordQualityControl 詳細オプションを使用して、デフォルト設定を変更できます。

たとえば、このオプションは次のように変更できます。

```
retry=3 min=disabled,disabled,16,7,7
```

この例では、16 文字以上のパスフレーズを使用できます。パスフレーズは、スペースで区切られた 3 つ以上の単語で構成する必要があります。

パスワード履歴およびローテーション ポリシーの例

5 つのパスワードの履歴を記憶するには、`Security.PasswordHistory` オプションを 5 に設定します。

90 日間のパスワード ローテーション ポリシーを適用するには、`Security.PasswordMaxDays` オプションを 90 に設定します。

ESXi アカウント ロックアウト ポリシー

連続した失敗の数が事前設定された回数に達すると、ユーザーはロックアウトされます。デフォルトでは、3 分間に連続して 5 回失敗するとユーザーはロックアウトされ、15 分後にロックアウトは自動的に解除されます。`Security.AccountLockFailures` および `Security.AccountUnlockTime` 詳細オプションを使用して、許可される最大失敗回数とユーザー アカウントのロックアウト期間を変更できます。

管理者パスワードとアカウント ロックアウト動作を構成するには、次の手順を実行します。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

オプション	操作
必要なパスワードの長さ、文字の種類の要件、または許可パスフレーズを構成する	a [検索] テキスト ボックスに「**Security.PasswordQualityControl**」と入力し、[検索] アイコンをクリックします。 b `Security.PasswordQualityControl` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。
ユーザーごとに記憶するパスワードの数を構成する	a [検索] テキスト ボックスに「**Security.PasswordHistory**」と入力し、[検索] アイコンをクリックします。 b `Security.PasswordHistory` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 **注：** ゼロを指定すると、パスワード履歴は無効になります。
パスワード変更までの最大日数を構成する	a [検索] テキスト ボックスに「**Security.PasswordMaxDays**」と入力し、[検索] アイコンをクリックします。 b `Security.PasswordMaxDays` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。
ロックアウトするまでに許可されるログイン試行失敗の最大回数を構成する	a [検索] テキスト ボックスに「**Security.AccountLockFailures**」と入力し、[検索] アイコンをクリックします。 b `Security.AccountLockFailures` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。 **注：** ゼロ (0) にすると、アカウントのロックは無効になります。
ユーザーのアカウントがロックアウトされる期間を構成する	a [検索] テキスト ボックスに「**Security.AccountUnlockTime**」と入力し、[検索] アイコンをクリックします。 b `Security.AccountUnlockTime` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。

[オプションの編集] ダイアログ ボックスが開きます。

2 [新しい値]テキスト ボックスに新しい設定を入力します。

3 [保存] をクリックします。

4 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

VMware Host Client での Syslog の構成

Syslog サービスを構成するには、VMware Host Client を使用します。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

2 [検索] テキスト ボックスに変更する設定の名前を入力し、[検索] アイコンをクリックします。

オプション	説明
Syslog.global.LogHost	Syslog メッセージの転送先のリモート ホストと、そのリモート ホストが Syslog メッセージを受信するポート。`protocol://hostName1:port` のようにプロトコルとポートを含めることができます。`protocol` には udp、tcp、または ssl を指定できます。UDP にはポート 514 のみを使用できます。ssl プロトコルは TLS 1.2 を使用します（例：`ssl://hostName1:1514`）。`port` の値には、1 ～ 65535 の任意の 10 進数を指定できます。 Syslog メッセージを受信するリモート ホストの数にハード制限はありませんが、リモート ホストの数は 5 台以下にすることを推奨します。
Syslog.global.logCheckSSLCerts	リモート ホストのログイン時に SSL 証明書の確認を実施します。
Syslog.global.defaultRotate	保持するアーカイブの最大数です。この数字はグローバルに、また個別のサブロガーについて設定できます。
Syslog.global.defaultSize	システムのログ ローテーションを行う前のログのデフォルト サイズ（KB 単位）です。この数字はグローバルに、また個別のサブロガーについて設定できます。
Syslog.global.LogDir	ログが保管されるディレクトリです。ディレクトリは、マウントされた NFS または VMFS ボリュームに配置できます。リブート後も変わらないのは、ローカル ファイル システムの `/scratch` ディレクトリのみです。ディレクトリを [*datastorename*] *path_to_file* と指定します。ここで、パスはデータストアをバッキングするボリュームのルートへの相対パスです。例えば、パスの `[storage1] /systemlogs` はパスの `/vmfs/volumes/storage1/systemlogs` にマッピングします。
Syslog.global.logDirUnique	このオプションを選択すると、ESXi ホストの名前を持つサブディレクトリを [Syslog.global.LogDir] で指定されるディレクトリの下に作成します。同一の NFS ディレクトリが複数の ESXi ホストによって使用される場合、固有のディレクトリを作成しておくと便利です。

3 設定名を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。

[オプションの編集] ダイアログ ボックスが開きます。

4 リモート ホストにログインするときに SSL 証明書の確認を実行するには、[新しい値] で [True] をクリックします。

5 [保存] をクリックします。

6 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

TLS/SSL キーの詳細オプションの構成

ESXi ホストとの通信を暗号化するために使用されるセキュリティ プロトコルと暗号化アルゴリズムを構成できます。

詳細については、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/79476) を参照してください。

トランスポート レイヤー セキュリティ (TLS) キーは、TLS プロトコルを使用してホストとの通信を保護します。最初の起動時に、ESXi ホストは TLS キーを 2048 ビットの RSA キーとして生成します。現在、ESXi は TLS 用 ECDSA キーの自動生成を実装していません。TLS プライベート キーは、管理者が処理するものではありません。

SSH キーは、SSH プロトコルを使用して、ESXi ホストとの通信を保護します。最初の起動時に、SSH キーは 2048 ビットの RSA キーとして生成されます。SSH サーバはデフォルトで無効になっています。SSH アクセスは、主にトラブルシューティングを目的としています。SSH キーは、管理者が処理するものではありません。SSH を使用してログインするには、完全なホスト制御と同等の管理者権限が必要になります。SSH アクセスを有効にする手順については、VMware Host Client でのセキュア シェル (SSH) の有効化を参照してください。

次の ESXi ホスト セキュリティ キーを構成できます。

注： UserVars.ESXiVPsAllowedCiphers セキュリティ キー設定は、I/O フィルタにのみ影響します。

キー	デフォルト	説明
UserVars.ESXiVPsAllowedCiphers	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	デフォルトの暗号制御文字列。
Config.HostAgent.ssl.keyStore.allowAny	False	ESXi CA トラスト ストアに任意の証明書を追加できます。
Config.HostAgent.ssl.keyStore.allowSelfSigned	False	CA 以外の自己署名証明書、つまり CA ビット セットが含まれていない証明書を ESXi CA トラスト ストアに追加できます。
Config.HostAgent.ssl.keyStore.discardLeaf	True	ESXi CA トラスト ストアに追加されたリーフ証明書を破棄します。

ESXi のセキュリティ キーを設定するには、次の手順を実行します。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

2 [検索] テキスト ボックスにセキュリティ キーを入力し、[検索] アイコンをクリックします。

3 セキュリティ キーを右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。

[オプションの編集] ダイアログ ボックスが開きます。

4 [新しい値] フィールドに新しい値を入力して、[保存] をクリックします。

5 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

UserWorld メモリ ゼロクリアの構成

VMware Host Client では、`Mem.MemEagerZero` 詳細オプションを使用して、仮想マシンおよびユーザー領域アプリケーションのページをゼロクリアする方法を決定できます。

仮想マシンおよびユーザー領域アプリケーションにページを割り当てるときに、すべてのページをゼロクリアするには、`Mem.MemEagerZero` を 1 に設定します。メモリが再利用されない場合は、この設定により、メモリ内の以前のコンテンツを保持したまま仮想マシンまたはユーザー領域アプリケーションから他のクライアントに情報を公開することができなくなります。

`Mem.MemEagerZero` を 1 に設定すると、ユーザー領域アプリケーションが終了したときに、ページがゼロクリアされます。仮想マシンでこのようなページがゼロクリアされるのは、次の場合です。

- 仮想マシンがパワーオフ状態である。
- 仮想マシンのページが移行される。
- ESXi ホストで、仮想マシンのメモリが再利用される。

注： 仮想マシンの場合は、`sched.mem.eagerZero` 詳細オプションを **`TRUE`** に設定することでこの動作を実現できます。

仮想マシンの詳細オプションの設定方法については、『vSphere リソース管理』ドキュメントを参照してください。

UserWorld メモリのゼロクリアを構成するには、次の手順を実行します。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

2 [検索] テキスト ボックスに「**`Mem.MemEagerZero`**」と入力し、[検索] アイコンをクリックします。

3 `Mem.MemEagerZero` を右クリックし、ドロップダウン メニューで [オプションの編集] を選択します。

[オプションの編集] ダイアログ ボックスが開きます。

4 [新しい値]テキスト ボックスに新しい値を入力します。

デフォルト値は 0 です。

5 [保存] をクリックします。

6 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

VMware Host Client での、自動起動設定の変更

ESXi ホストの自動起動オプションを設定して、ホストの起動および停止時にセットアップが行われるようにします。

手順

1 VMware Host Client インベントリ内で [管理] > [システム] の順にクリックします。

2 [自動起動] をクリックします。

3 [設定の編集] をクリックします。

4 [はい] を選択して、自動起動設定の変更を有効にします。

オプション	説明
起動遅延時間	ユーザーが ESXi ホストを起動すると、ESXi ホストは自動起動が構成されている仮想マシンのパワーオンを開始します。ESXi ホストは、最初の仮想マシンをパワーオンした後、指定されている遅延時間だけ待機し、続いて次の仮想マシンをパワーオンします。
停止遅延時間	停止遅延時間は、ESXi ホストがシャットダウン コマンドの完了を待機する最大時間です。仮想マシンのシャットダウンは起動順の逆順で行われます。指定した時間内に最初の仮想マシンを ESXi ホストがシャットダウンすると、ホストは次の仮想マシンをシャットダウンします。指定された遅延時間内に仮想マシンがシャットダウンしない場合、ホストはパワーオフ コマンドを実行し、次の仮想マシンのシャットダウンを開始します。ESXi ホストのシャットダウンは、すべての仮想マシンがシャットダウンした後で行われます。
停止アクション	ホストがシャットダウンするときにそのホスト上の仮想マシンに適用されるシャットダウン アクションを選択します。 ■ [システムのデフォルト] ■ [パワーオフ] ■ [サスペンド] ■ [シャットダウン]
ハートビートを待機	[はい] を選択して、[ハートビートを待機] オプションを有効にします。このオプションは、仮想マシンのゲスト OS に VMware Tools がインストールされている場合に使用できます。ESXi ホストは、最初の仮想マシンをパワーオンしてすぐに次の仮想マシンをパワーオンします。仮想マシンがパワーオンされる起動順序は、仮想マシンが最初のハートビートを受信した後も継続します。

遅延オプションを `-1` に設定すると、システムはデフォルトのオプションを使用します。

5 [[保存]] をクリックします。

VMware Host Client での ESXi ホストの時間設定の編集

VMware Host Client を使用すると、ホストの時間を手動で設定することも、ホストの日時を NTP または PTP サーバと同期することもできます。NTP は、ミリ秒単位の精度を提供し、PTP はマイクロ秒単位の精度を維持します。

ホストの NTP サービスは、NTP サーバーから時刻と日付を定期的に取得します。[開始]、[停止]、または [再開] ボタンを使用して、NTP サービス用に選択した起動ポリシーに関係なく、いつでもホストの NTP サービスの状態を変更できます。

PTP は、ネットワーク内の仮想マシンに正確な時刻同期をプロビジョニングします。ホストの PTP サービスは、[開始]、[停止]、または [再開] の各ボタンを使用して、いつでも変更できます。PTP サービスを開始または停止すると、PTP が自動的に有効または無効になります。PTP を手動で有効または無効にする場合に変更を適用するには、PTP サービスを開始または停止します。

サービスの詳細については、 VMware Host Client でのサービスの管理を参照してください。

注： NTP サービスと PTP サービスを同時に実行することはできません。

手順

1 VMware Host Client インベントリの [管理] をクリックします。

2 [システム] タブで、[時刻と日付] をクリックします。

3 ホストの時刻と日付を設定します。

オプション	操作
このホストの日付および時刻を手動で構成します	a [NTP 設定の編集] をクリックします。 [NTP 設定の編集] ダイアログ ボックスが表示されます。 b ホストの時刻と日付を手動で設定します。 c [保存] をクリックします。
Network Time Protocol を使用 (NTP クライアントを有効にする)	a [NTP 設定の編集] をクリックします。 [NTP 設定の編集] ダイアログ ボックスが表示されます。 b [ネットワーク時間プロトコルを使用] ラジオ ボタンを選択します。 c [NTP サーバ] テキスト ボックスに、使用する NTP サーバの IP アドレスまたはホスト名を入力します。 d [NTP サービス起動ポリシー] ドロップダウン メニューで、ホストで NTP サービスを開始および停止する場合のオプションを選択します。 ■ [ポートの使用状況にしたがって起動および停止]。ホストのセキュリティ プロファイルでアクセス用の NTP クライアント ポートが有効化または無効化されると、NTP サービスを起動または停止します。 ■ [ホストと連動して起動および停止]。ホストのパワーオンおよびシャットダウン時に NTP サービスを開始および停止します。 ■ [手動で開始および停止]。手動での NTP サービスの開始および停止を有効にします。[手動で開始および停止] ポリシーを選択した場合、NTP サービスの状態は、ユーザーがユーザー インターフェイス コントロールを使用するときにのみ変更されます。 e [保存] をクリックします。
Precision Time Protocol を使用 (PTP クライアントを有効にする)	a [PTP 設定の編集] をクリックします。 b [有効化] チェック ボックスを選択します。 c [ネットワーク インターフェイス] ドロップダウン メニューから、ネットワーク インターフェイスを選択します。 IPv4 とサブネットマスクが表示されます。 d [保存] をクリックします。

VMware Host Client を使用した ESXi ホストのハードウェアの管理

ESXi ホストに VMware Host Client を使用してログインしている場合に、PCI デバイスの管理や電源管理設定の構成を実行できます。

ホストの電源管理ポリシー

ESXi で、ホスト ハードウェアが提供するいくつかの電源管理機能を適用して、パフォーマンスと消費電力のバランスを調整できます。電源管理ポリシーを選択することにより、これらの機能を ESXi でどのように使用するかを制御できます。

高パフォーマンス ポリシーを選択すると、絶対的なパフォーマンスは高まりますが、1 ワットあたりの電力の使用効率とパフォーマンスは低下します。省電力ポリシーを使用すると、絶対的なパフォーマンスは低くなりますが、電力の使用効率は向上します。

管理対象ホストのポリシーは、VMware Host Client を使用して選択できます。ポリシーを選択しない場合、ESXi ではデフォルトで [バランシング済み] が使用されます。

表 3-1. CPU 電源管理ポリシー

電源管理ポリシー	説明
高パフォーマンス	電源管理機能は使用しないでください。
バランシング済み （デフォルト）	パフォーマンスへの影響を最小限に抑えてエネルギー消費を削減します
省電力	パフォーマンスが低下するおそれがありますがエネルギー消費を削減します
カスタム	ユーザー定義の電源管理ポリシーです。高度な設定が可能になります。

CPU が低い周波数で実行されると、電圧も低くなるため、電力消費を削減できます。このタイプの電源管理は、通常、Dynamic Voltage and Frequency Scaling (DVFS) と呼ばれます。ESXi では、仮想マシンのパフォーマンスに影響を与えないように、CPU 周波数を調整します。

CPU がアイドル状態の場合、ESXi は C ステートと呼ばれるさまざまなレベル（深度）の停止状態を適用できます。C ステートの深度が深いほど、CPU での電力消費は少なくなりますが、CPU が稼動を再開するまでに時間がかかります。CPU がアイドル状態になると、ESXi はアイドル状態の時間を予想するアルゴリズムを適用し、適切な C ステートを選択します。深い C ステートに移動しない電源管理ポリシーでは、ESXi は、アイドル状態の CPU に対して深度が最も浅い停止状態 (C1) を使用します。

VMware Host Client での、電源管理ポリシーの変更

管理対象ホストの電源管理ポリシーを変更して、ホストのエネルギー消費を制御します。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[ハードウェア] をクリックします。

2 [電源管理] をクリックし、[ポリシーの変更] をクリックします。

使用可能な電源管理ポリシーが表示されます。

3 適用するポリシーを選択し、[OK] をクリックします。

VMware Host Client でのハードウェア ラベルの変更

VMware Host Client では、仮想マシン上の使用可能なすべての PCI パススルー デバイスのハードウェア ラベルを変更できます。ハードウェア ラベルを使用して、仮想マシンを特定のハードウェア インスタンスに配置するよう

制限できます。ハードウェア ラベルが同じ、または空のハードウェア ラベルがある、使用可能なすべてのデバイスを仮想マシンに追加できます。

手順

1 VMware Host Client インベントリの [管理] をクリックします。

2 [ハードウェア] タブで [PCI デバイス] をクリックします。

3 リストから使用可能なデバイスを選択し、[ハードウェアのラベル] をクリックします。

選択したデバイスに対して、パススルーの切り替えが有効である必要があります。

[デプロイ ルールの編集] ダイアログ ボックスが表示されます。

4 ハードウェア ラベルを編集し、[保存] をクリックして変更を適用します。

結果

新しいハードウェア ラベルがハードウェア ラベル列に表示されます。

ESXi ホストのライセンス

ESXi ホストには vSphere のライセンスが供与されます。各 vSphere ライセンスには一定のキャパシティがあり、これを使用して ESXi ホスト上の複数の物理 CPU をライセンス供与できます。

vSphere 7.0 以降では、1 つの CPU ライセンスは最大 32 個のコアがある 1 つの CPU をカバーします。CPU のコア数が 32 個を超える場合は、追加の CPU ライセンスが必要になります。

CPU の数	CPU あたりのコア数	CPU ライセンス数
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

VSphere ライセンスをホストに割り当てる場合、使用されるキャパシティの量は、ホスト上の物理 CPU の数と各物理 CPU のコア数によって決まります。VDI 環境用の vSphere Desktop は、仮想マシン単位ベースでライセンス供与されます。

ESXi ホストにライセンス供与するには、次の要件を満たす vSphere ライセンスを割り当てる必要があります。

- ホスト上のすべての物理 CPU をライセンス供与できるキャパシティがある。
- ホストで使用するすべての機能をサポートしている。たとえば、ホストが vSphere Distributed Switch に関連付けられている場合、割り当てるライセンスで vSphere Distributed Switch 機能がサポートされている必要があります。

キャパシティの不十分なライセンスや、ホストで使用する機能をサポートしていないライセンスを割り当てようとすると、ライセンス割り当ては失敗します。

最大 32 個のコアを持つライセンス モデルを使用する場合は、32 コアを持つ 10 CPU の vSphere ライセンスを、次のいずれかのホストの組み合わせに割り当てることができます。

- CPU あたり 32 コアを持つ 2 CPU ホスト 5 台
- CPU あたり 64 コアを持つ 1 CPU ホスト 5 台
- CPU あたり 48 コアを持つ 2 CPU ホスト 2 台および CPU あたり 20 コアを持つ 1 CPU ホスト 2 台

2 個または 4 個の独立した CPU をシングル チップに結合する Intel CPU などのデュアルコア CPU およびクワッドコア CPU は、1 CPU としてカウントされます。

評価モード

ESXi をインストールすると、最長で 60 日間、評価モードで動作します。評価モード ライセンスでは、最も高い vSphere 製品エディションの全機能が提供されます。

ESXi ホストにライセンスを割り当てると、評価期間が終了する前にいつでも、ホストを評価モードに戻して、残りの評価期間に使用可能なすべての機能を評価検討できます。

たとえば、ESXi ホストを評価モードで 20 日間使用し、そのホストに vSphere Standard ライセンスを割り当ててから 5 日後に評価モードに戻すと、残りの 35 日間の評価期間、ホストで使用可能なすべての機能を評価検討できます。

ライセンスと評価期間の有効期限

ESXi ホストの場合、ライセンスまたは評価期間の有効期限が切れると、ホストが vCenter Server から切断されます。パワーオン状態のすべての仮想マシンの実行が継続しますが、パワーオフ状態の仮想マシンをパワーオンすることはできません。使用中の機能の現在の設定を変更することはできません。ライセンスの有効期限が切れる前に使用していない機能は使用することはできません。

注： 有効期限のあるライセンスの場合、ライセンスの有効期限が切れる 90 日前に通知が表示されます。

アップグレード後の ESXi ホストへのライセンス供与

ESXi ホストを同じ番号で始まるバージョンにアップグレードする場合は、既存のライセンスを新しいライセンスで置き換える必要はありません。たとえば、ESXi 5.1 から 5.5 にホストをアップグレードする場合、ホストで同じライセンスを使用できます。

ESXi ホストを異なる番号で始まるメジャー バージョンにアップグレードすると、評価期間が新たに開始されるため、新しいライセンスを割り当てる必要があります。たとえば、ESXi ホストを 5.x から 6.x にアップグレードする場合、ホストに vSphere 6.x のライセンスを供与する必要があります。

vSphere Desktop

vSphere Desktop は、Horizon View などの VDI 環境向けです。vSphere Desktop のライセンス使用量は、vSphere Desktop ライセンスが割り当てられているホストで動作中のパワーオン状態のデスクトップ仮想マシンの総数と同じです。

VMware Host Client 環境に関するライセンス情報の表示

VMware Host Client で、使用可能なライセンス、それらの有効期限、ライセンス キー、およびさまざまな機能を表示できます。使用可能な製品および資産を表示することもできます。

手順

- VMware Host Client インベントリで [管理] > [ライセンス] の順にクリックします。

  ライセンス キー、有効期限、および利用可能なすべての機能と資産を表示できます。

VMware Host Client での、ESXi ホストへのライセンス キーの割り当て

VMware Host Client を使用して、既存または新規のライセンス キーを ESXi ホストに割り当てることができます。

前提条件

グローバル.ライセンス権限を保有していることを確認します。

注： ESXi ホストの管理に vCenter Server を使用する場合、ライセンスは vSphere Client からのみ変更できます。

手順

1. VMware Host Client インベントリで [管理] をクリックし、[ライセンス] をクリックします。
2. [ライセンスの割り当て] をクリックし、***xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*** 形式でライセンス キーを入力し、[ライセンスの確認] をクリックします。
3. [ライセンスの割り当て] をクリックして変更内容を保存します。

VMware Host Client での ESXi ホストからのライセンスの削除

vSphere で使用する製品のライセンス モデルへの準拠を維持するには、インベントリから未割り当てのライセンスをすべて削除する必要があります。Customer Connect でライセンスを分割、結合、またはアップグレードした場合、古いライセンスを削除する必要があります。

たとえば、Customer Connect で vSphere ライセンスを 6.5 から 6.7 にアップグレードした場合を考えます。そのライセンスを ESXi 6.7 ホストに割り当てます。新しい vSphere 6.7 ライセンスを割り当てたら、古い vSphere 6.5 ライセンスをインベントリから削除する必要があります。

手順

1. VMware Host Client インベントリで [管理] > [ライセンス] の順にクリックします。
2. [ライセンスを削除] > [OK] の順にクリックします。

VMware Host Client でのサービスの管理

VMware Host Client で、ログインしているホストで実行されているサービスを開始、停止、および再起動したり、ホストのサービス ポリシーを構成したりできます。ホストの構成を変更するときや、機能またはパフォーマンスの問題が疑われる場合に、サービスを再起動できます。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[サービス] をクリックします。

2 [サービス] リストからサービスを選択します。

3 [アクション] ドロップダウン メニューから、操作を選択します。

- [再起動]
- [開始]
- [停止]

4 （オプション）[アクション] ドロップダウン メニューから [ポリシー] を選択し、サービスのオプションをメニューから選択します。

- [ファイアウォール ポートに連動して開始および停止]
- [ホストに連動して開始および停止]
- [手動で開始および停止]

VMware Host Client を使用した ESXi ホストのセキュリティおよびユーザーの管理

ESXi ハイパーバイザー アーキテクチャには、セキュリティを強化するように構成できる、多くのセキュリティ機能が組み込まれています。VMware Host Client を使用して、Active Directory などの機能を構成したり、証明書を管理したりできます。

VMware Host Client を使用したホスト認証の管理

ESXi ホストに VMware Host Client を使用してログインしている場合に、Active Directory とスマート カードの認証が有効化されているかどうかを確認したり、ホストをディレクトリ サービス ドメインに追加したりできます。

VMware Host Client を使用した ESXi ホストのディレクトリ サービス ドメインへの追加

ホストでディレクトリ サービスを使用するには、ディレクトリ サービス ドメインにそのホストを追加する必要があります。

ドメイン名は次のいずれかの方法で入力できます。

- **`name.tld`**（たとえば **`domain.com`**）： アカウントはデフォルトのコンテナ下に作成されます。
- **`name.tld/container/path`**（たとえば **`domain.com/OU1/OU2`**）： アカウントは特定の組織単位（OU） 下に作成されます。

vSphere Authentication Proxy サービスの使用については、vSphere のセキュリティを参照してください。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [認証] をクリックし、[ドメインに参加] をクリックします。

3 ドメイン名を入力します。

`name.tld` または **`name.tld/container/path`** の形式を使用します。

4 ホストをドメインに追加する権限を持つディレクトリ サービス ユーザー アカウントのユーザー名とパスワードを入力し、[ドメインに参加] をクリックします。

5 （オプション） 認証プロキシを使用する場合は、プロキシ サーバの IP アドレスを入力し、[ドメインに参加] をクリックします。

Active Directory を使用した ESXi ユーザーの管理

Active Directory などのディレクトリ サービスを使用してユーザーを管理するように ESXi を構成できます。

各ホストにローカル ユーザー アカウントを作成すると、複数のホストのアカウント名およびパスワードを同期しなければならないという問題が生じます。ESXi ホストを Active Directory ドメインに参加させて、ローカル ユーザー アカウントを作成および管理しなくても済むようにします。ユーザー認証に Active Directory を使用すると、簡単に ESXi ホストを構成し、未承認のアクセスにつながる構成問題のリスクを減らすことができます。

Active Directory を使用している場合は、ホストをドメインに追加する際に Active Directory 認証情報と Active Directory サーバのドメイン名を指定します。

vSphere Authentication Proxy の使用

ESXi ホストを Active Directory ドメインに明示的に追加する代わりに、vSphere Authentication Proxy を使用して Active Directory ドメインに追加することができます。

Active Directory サーバのドメイン名と vSphere Authentication Proxy の IP アドレスを特定できるようにホストを設定するだけです。vSphere Authentication Proxy が有効な場合、Auto Deploy によってプロビジョニングされるホストは自動的に Active Directory ドメインに追加されます。Auto Deploy を使用してプロビジョニングされないホストでも、vSphere Authentication Proxy を使用できます。

vSphere Authentication Proxy が使用する TCP ポートについては、#unique_39 を参照してください。

vSphere Authentication Proxy を有効にする方法と、vSphere Authentication Proxy に必要な vCenter Server ポートについては、vSphere のセキュリティのドキュメントを参照してください。

Auto Deploy

Auto Deploy でホストをプロビジョニングする場合は、Authentication Proxy をポイントするリファレンス ホストをセットアップできます。その後、Auto Deploy でプロビジョニングされるすべての ESXi ホストにリファレンス ホストのプロファイルを適用するルールを設定します。vSphere Authentication Proxy のアクセス コントロール リストには、Auto Deploy が PXE を使用してプロビジョニングするすべてのホストの IP アドレスが格納されます。ホストを起動すると、ホストは vSphere Authentication Proxy と通信を行います。vSphere Authentication Proxy は、アクセス コントロール リストに含まれているホストを Active Directory ドメインに追加します。

VMCA でプロビジョニングされた証明書またはサードパーティ証明書を使用する環境で vSphere Authentication Proxy を使用する場合でも、Auto Deploy でカスタム証明書を使用する場合と同じ手順を実行すれば、プロセスはシームレスに機能します。

#unique_40 を参照してください。

その他の ESXi ホスト

他のホストを vSphere Authentication Proxy を使用するようにセットアップすることで、Active Directory 認証を使用することなくドメインに参加できます。Active Directory 認証をホストに送信する必要も、Active Directory 認証をホスト プロファイルに保存する必要もありません。

ホストの IP アドレスを vSphere Authentication Proxy アクセス コントロール リストに追加すれば、vSphere Authentication Proxy はデフォルトで、IP アドレスに基づいてホストを認証します。クライアント認証を有効にすると、ホストの証明書が vSphere Authentication Proxy によってチェックされます。

注： IPv6 のみをサポートする環境では、vSphere Authentication Proxy を使用できません。

VMware Host Client を使用したホスト証明書の管理

ESXi ホストに VMware Host Client を使用してログインしている場合に、発行者や有効期間など、ホストの証明書の詳細を表示したり、新しい証明書をインポートしたりできます。

VMware Host Client での ESXi ホストの証明書詳細の表示

証明書情報はデバッグに使用することができます。

手順

1. VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。
2. [証明書] をクリックします。

   証明書に関する次の詳細情報を確認できます。

フィールド	説明
発行者	証明書の発行者。
次の日付以降は無効	証明書の有効期限。
次の日付以前は無効	証明書が生成された日付。
件名	証明書の生成中に使用される件名。

VMware Host Client での ESXi ホストの新しい証明書のインポート

VMware Host Client で ESXi ホストにログインしているときに、信頼できる認証局から証明書をインポートできます。

手順

1. VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。
2. [証明書] をクリックし、[新しい証明書のインポート] をクリックします。

3 証明書署名要求の生成：

オプション	説明
FQDN 署名要求の生成	■ [FQDN 署名要求の生成] をクリックし、[クリップボードにコピー] ボタンをクリックして、[閉じる] をクリックします。 ■ 署名付き証明書を生成するには、証明書署名要求を認証局 (CA) に渡します。 ■ [証明書] テキスト ボックスに、PEM 形式の生成された署名付き証明書を貼り付け、[インポート] をクリックします。
IP アドレス署名要求の生成	■ [IP 署名要求の生成] をクリックし、[クリップボードにコピー] ボタンをクリックして、[閉じる] をクリックします。 ■ 署名付き証明書を生成するには、証明書署名要求を CA に渡します。 ■ [証明書] テキスト ボックスに、PEM 形式の生成された署名付き証明書を貼り付け、[インポート] をクリックします。

証明書をすぐにインポートする必要はありません。署名付き証明書を使用できるようにするには、証明書署名要求を生成してから証明書をインポートするまでの間にホストを再起動しないでください。

証明書署名要求は認証局に渡されて、正式な証明書が生成されます。

FQDN 要求の場合は、証明書の共通名フィールドにホストの完全修飾ホスト名が入力されます。IP 署名要求の場合は、共通名フィールドにホストの現在の IP アドレスが入力されます。

VMware Host Client を使用したユーザーの管理

ユーザーを管理して ESXi にログインできるユーザーを制御します。

ユーザーとロールによって、ESXi ホスト コンポーネントにアクセスできるユーザーと、各ユーザーが実行できるアクションが制御されます。

vSphere 5.1 以降では、ESXi ユーザー管理は次の点に注意します。

- ESXi ホストに直接接続するときに作成されるユーザーは、vCenter Server ユーザーとは異なります。ホストが vCenter Server によって管理される場合、vCenter Server は、ホストで直接作成されるユーザーを無視します。
- vSphere Client を使用して ESXi ユーザーを作成することはできません。ESXi ユーザーを作成するには、VMware Host Client でホストに直接ログインする必要があります。
- ESXi 5.1 以降では、ローカル グループはサポートされません。ただし、Active Directory グループはサポートされています。

ダイレクト コンソール ユーザー インターフェイス (DCUI) や ESXi Shell で root ユーザーなどの匿名ユーザーに対してホストへのアクセス制限を行うには、ホストのルート フォルダでのユーザーの管理者権限を削除します。これは、ローカル ユーザーと Active Directory ユーザーおよびグループの両方に適用されます。

VMware Host Client での ESXi ユーザーの追加

ユーザーをユーザー テーブルに追加すると、ホストで保持している内部のユーザー リストが更新されます。

前提条件

パスワード要件の詳細については、VMware Host Client でのパスワードとアカウント ロックアウト ポリシーの構成または vSphere のセキュリティドキュメントを参照してください。

手順

1 VMware Host Client を使用して ESXi にログインします。

vSphere Client では ESXi ユーザーは作成できません。VMware Host Client ユーザーを作成するには、ESXi を使用してホストに直接ログインする必要があります。

2 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

3 [ユーザー] をクリックします。

4 [ユーザーの追加] をクリックします。

5 ユーザー名とパスワードを入力します。

注： **ALL** という名前のユーザーは作成しないでください。**ALL** という名前に関連付けられた権限は、すべてのユーザーが使用できない場合があります。たとえば、**ALL** という名前のユーザーに管理者権限がある場合、ReadOnly 権限があるユーザーはホストにリモートにログインできる場合があります。これは意図された動作ではありません。

- ユーザー名にスペースを含めないでください。
- ユーザー名に非 ASCII 文字を含めないでください。
- 長さと複雑さの要件を満たすパスワードを作成します。デフォルトの認証プラグイン `pam_passwdqc.so` を使用して、ホストがパスワードの整合性を確認します。パスワードが整合していない場合、エラー メッセージにパスワード要件が示されます。

6 ESXi Shell へのローカル アクセスを有効にするには、[シェル アクセスの有効化] チェック ボックスを選択します。

7 [追加] をクリックします。

VMware Host Client での ESXi ユーザーの更新

VMware Host Client で、ESXi ユーザーの説明とパスワードを変更できます。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ユーザー] をクリックします。

3 ユーザーをリストから選択し、[ユーザーの編集] をクリックします。

4 ユーザー詳細を更新して、[保存] をクリックします。

VMware Host Client でのホストからのローカル ESXi ユーザーの削除

ホストからローカル ESXi ユーザーを削除できます。

注意： root ユーザーは削除しないでください。

ホストからユーザーを削除すると、これらのユーザーはホスト上のすべてのオブジェクトの権限を失い、再度ログインできなくなります。

注： ログインしているユーザーがドメインから削除された場合、それらのユーザーはホストを再起動するまでホストの権限を保持します。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ユーザー] をクリックします。

3 リストから削除するユーザーを選択して、[ユーザーの削除] をクリックし、[はい] をクリックします。

理由のいかんを問わず、root ユーザーは削除しないでください。

VMware Host Client での ESXi ロールの管理

ESXi では、オブジェクトに対する権限が割り当てられているユーザーにのみ、そのオブジェクトへのアクセス権を付与します。オブジェクトのユーザー権限を割り当てる場合、ユーザーとロールのペアを作ります。ロールとは、事前に定義された権限セットです。権限の詳細については、『vSphere のセキュリティ』を参照してください。

ESXi ホストは、3 つのデフォルト ロールを提供します。これらのロールに関連付けられている権限は変更できません。後続の各デフォルト ロールには、先行するロールの権限が含まれます。たとえば、システム管理者ロールは読み取り専用ロールの権限を引き継ぎます。ユーザーが作成したロールは、どのデフォルト ロールの権限も継承しません。

カスタム ロールを作成するには、VMware Host Client のロール編集機能を使用して、ユーザー ニーズに合った権限セットを作成します。また、ホストで直接作成したロールは、vCenter Server ではアクセスできません。これらのロールを使用できるのは、VMware Host Client から直接ホストにログインした場合だけです。

注： カスタム ロールを追加し、それに権限を割り当てない場合、そのロールは読み取り専用ロールとして作成され、System.Anonymous、System.View、および System.Read というシステム定義権限が付与されます。

vCenter Server を介して ESXi ホストを管理する場合、ホストと vCenter Server でカスタム ロールを保持していると、混乱や誤用が生じることがあります。このタイプの構成では、vCenter Server のみでカスタム ロールを保持します。

VMware Host Client で ESXi ホストに直接接続して、ホストのロールを作成し、権限を設定できます。

VMware Host Client でのロールの追加

環境に必要なアクセス コントロールに適合するロールを作成できます。

前提条件

root や vpxuser など、管理者権限を持つユーザーとしてログインしていることを確認します。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ロール] をクリックします。

3 [ロールの追加] をクリックします。

4 新しいロールの名前を入力します。

5 リストから新しいロールと関連付ける権限を選択し、[追加] をクリックします。

VMware Host Client でのロールの更新

ロールを編集するときに、そのロールに対して選択した権限を変更できます。処理が完了すると、編集されたロールに割り当てられているユーザーまたはグループに権限が適用されます。

前提条件

root や vpxuser など、管理者権限を持つユーザーとしてログインしていることを確認します。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ロール] をクリックします。

3 ロールをリストから選択し、[ロールの編集] をクリックします。

4 ロール詳細を更新して、[保存] をクリックします。

VMware Host Client でのロールの削除

いずれのユーザーまたはグループにも割り当てられていないロールを削除する場合、ロールのリストから定義が削除されます。ユーザーまたはグループに割り当てられたロールを削除する場合、割り当てを削除するか、別のロールを割り当てるかを選択できます。

注意： すべての割り当ての削除または置き換えを行う前に、ユーザーに与える影響を把握しておく必要があります。権限が付与されていないユーザーはログインできません。

前提条件

root や vpxuser など、管理者権限を持つユーザーとしてログインしていることを確認します。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ロール] をクリックします。

3 リストから削除するロールの名前を選択します。

4 [ロールの削除] をクリックして、[未使用の場合のみ削除します] を選択し、[はい] をクリックします。

vCenter Server でのホストの管理

仮想環境内のすべてのホストを 1 か所から監視し、ホスト設定を簡素化するには、ホストを vCenter Server システムに接続します。

ESXi ホストの設定管理の詳細については、『vSphere のネットワーク』、『vSphere のストレージ』、『vSphere のセキュリティ』の各ドキュメントを参照してください。

VMware Host Client 最新バージョンへのアップデート

VMware Host Client の最新バージョンを使用しているかどうかを確認するには、環境にどの VIB がインストールされているかをチェックし、VIB のバージョン情報を確認します。VIB ファイルまたは ESXi オフライン バンドル パッケージの `metadata.zip` ファイルへの URL またはデータストア パスを入力して、VMware Host Client 環境を更新できます。

VIB ファイルを指定すると、VMware Host Client 環境にインストールされている既存の VIB が新しい VIB に更新されます。

オフライン バンドルを指定すると、ESXi ホスト全体がバンドル内の `metadata.zip` ファイルで指定されているバージョンに更新されます。オフライン バンドル全体が URL で使用可能であること、またはデータストアにアップロードされていることを確認します。

手順

◆ 環境を最新バージョンに更新するには、次のタスクを実行します。

タスク	手順
データストアに VIB をアップロードします	a VMware Host Client 環境から [ストレージ] をクリックします。 b リストからデータストアを選択し、[データストア ブラウザ] をクリックします。 c VIB を保存するには、ディレクトリを選択して、[アップロード] をクリックします。 d ファイルを参照して、ダブルクリックします。
データストアにオフライン バンドルをアップロードします	a ESXi オフライン バンドル パッケージをダウンロードします。 b ESXi オフライン バンドル パッケージを ESXi ホストにアップロードします。オフライン バンドル パッケージをアップロードするには、[データストア ブラウザ] を使用するか、SCP または WinSCP を使用します。 c ESXi ホスト上のオフライン バンドルのコンテンツを抽出します。たとえば、SSH を使用してホストにログインします。 d オフライン バンドルをアップロードしたディレクトリに移動します。 e コマンドを使用して、 `unzip` コンテンツを抽出します。
環境を更新します	a VMware Host Client 内で [管理] をクリックし、[パッケージ] をクリックします。 b [アップデートのインストール] をクリックし、VIB ファイル、またはオフライン バンドルの `metadata.zip` ファイルへの URL またはデータ ストアパスを入力します。 c [更新] をクリックします。 **注意：** vSphere Lifecycle Manager で管理されている ESXi ホストを更新する場合、ホストが非準拠になることがあります。 d [更新] をクリックして、正常に更新されたことを確認します。

新しいバージョンの ESXi にアップグレードした後に VMware Host Client から ESXi ホストに接続できない

ホストを ESXi から新しいバージョンにアップグレードした後に、VMware Host Client を使用して ESXi ホストにアクセスすると、ブラウザ コンソールにエラー メッセージが表示され、接続に失敗することがあります。

問題

ESXi ホストを新しいバージョンにアップグレードした後に、**`https://host-fqdn/ui`** または **`https://1.2.3.4/ui`** に移動すると、次のエラーが表示されることがあります。

```
「503 サービスを利用できません （エンドポイントに接続できませんでした: [N7Vmacore4Http16LocalServiceSpecE:0xffa014e8]
_serverNamespace = /ui _isRedirect = false _port = 8308)」
```

原因

アップグレード後でも `/etc/vmware/rhttpproxy/endpoints.conf` への変更が維持されるため、`/ui` エンドポイントによって VMware Host Client がオーバーライドされます。

ESXi 6.0 以降のホストの `endpoint.conf` ファイルに `/ticket` がない場合、ブラウザ内の仮想マシン コンソールに「接続に失敗しました」というエラー メッセージが表示されますが、VMware Remote Console は機能し続けます。

解決方法

1 SSH または ESXi Shell を使用して ESXi ホストにログインします。

SSH を使用する場合は、最初に SSH を有効にする必要がある場合があります。SSH は DCUI を使用して有効にできます。

2 `endpoints.conf` ファイルをバックアップします。

```
cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
```

3 エディタで `/etc/vmware/rhttpproxy/endpoints.conf` ファイルを開き、次の行を削除します。

```
/ui local 8308 redirect  allow
```

4 リバース Web プロキシを再起動します。

```
/etc/init.d/rhttpproxy restart
```

5 VMware Host Client にアクセスするには、**`https://host-fqdn/ui`** を含むセキュアな URL 内でホストに指定されたフル ネームを使用するか、有効な数値形式の IP アドレス **`https://1.2.3.4/ui`** を使用します。

vSphere Client へのスイッチ

ESXi ホストのすべての機能、および高度な管理機能とトラブルシューティング機能を利用するには、ESXi ホストを vCenter Server に接続します。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、ドロップダウン メニューから [vCenter Server を使用した管理] を選択します。

vCenter Server のログイン ページが新しいウィンドウに開きます。

2 認証情報を入力し、[ログイン] をクリックします。

VMware Host Client を使用した vCenter Server からの ESXi ホストの切断

vCenter Server で使用可能な高度なホスト管理機能セットが不要になった場合や、vCenter Server に障害が発生しホスト上で緊急時操作を実行する必要が生じた場合は、ESXi ホストと vCenter Server の接続を解除できます。

ESXi ホストの接続を解除するには、数分かかる場合があります。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、ポップアップ メニューから [vCenter Server からの切断] を選択します。

注： ホストを切断すると、そのホストが応答していないことが vCenter Server に伝えられます。

2 [vCenter Server からの切断] をクリックします。

VMware Host Client での ESXi ホストの再起動またはシャットダウン

VMware Host Client を使用して ESXi ホストをパワーオフまたは再起動できます。管理対象ホストをパワーオフすると vCenter Server との接続が切断されますが、インベントリから削除されるわけではありません。

前提条件

ホストを再起動またはシャットダウンするには、次の権限が必要です。

- ホスト.構成.メンテナンス
- グローバル.ログ イベント

ホストを再起動またはシャットダウンする前に、必ず次のタスクを実行します。

- ホストのすべての仮想マシンをパワーオフします。
- ホストをメンテナンス モードにします。

手順

1 ホストを右クリックし、[ホストのシャットダウン] または [ホストの再起動] を選択します。

注： メンテナンス モードではないホストをシャットダウンまたは再起動した場合、そのホスト上で実行中の仮想マシンが安全に停止されず、未保存のデータが失われる可能性があります。ホストが vSAN クラスタ内にある場合は、そのホスト上の vSAN データにアクセスできなくなる可能性があります。

2 手順を完了するには、[シャットダウン] または [再起動] をクリックします。

ESXi Shell の使用

ESXi Shell は重要なメンテナンス コマンドを提供し、ESXi ホストではデフォルトで無効になっています。このシェルへのローカル アクセスおよびリモート アクセスは、必要に応じて有効にすることができます。不正アクセスのリスクを低減するためには、トラブルシューティングにのみ ESXi Shell を有効にします。

ESXi Shell は、ロックダウン モードに依存しません。ホストがロックダウン モードで実行されている場合でも、有効な場合は ESXi Shell にログインできます。

vSphere のセキュリティを参照してください。

適用可能なサービスは次のとおりです。

ESXi Shell

ローカルで ESXi Shell にアクセスする場合は、このサービスを有効にします。

SSH

SSH を使用して ESXi Shell にリモート アクセスするには、このサービスを有効にします。

ダイレクト コンソール UI （DCUI）

ロックダウン モードで動作しているときにこのサービスを有効にすると、root ユーザーでダイレクト コンソール ユーザー インターフェイスにローカルでログインし、ロックダウン モードを無効にできます。その後、VMware Host Client への直接接続を使用する、または ESXi Shell を有効にすることで、ホストにアクセスできます。

root ユーザーおよび管理者ロールを持つユーザーは、ESXi Shell にアクセスできます。Active Directory グループ ESX Admins 内のユーザーには、管理者ロールが自動的に割り当てられます。デフォルトでは、root ユーザーのみが、ESXi Shell を使用してシステム コマンド（`vmware -v` など）を実行できます。

注： ESXi Shell は、実際にアクセスが必要にならない限り有効にしないでください。

VMware Host Client でのセキュア シェル (SSH) の有効化

セキュア シェル (SSH) を使用して ESXi Shell にリモート アクセスするには、SSH を有効化します。

手順

1. セキュア シェル (SSH) を有効化または無効化するには、VMware Host Client インベントリ内で [ホスト] を右クリックします。
2. ドロップダウン メニューから [サービス] を選択します。
3. セキュア シェル (SSH) を有効化するには、[SSH の有効化] を選択します。
4. ESXi Shell を有効化するには、[ESXi Shell の有効化] を選択します。

VMware Host Client での ESXi コンソール シェルの有効化

ロックダウン モードで動作しているときにこのサービスを有効にすると、root ユーザーでダイレクト コンソール ユーザー インターフェイスにローカルでログインし、ロックダウン モードを無効にできます。その後、VMware Host Client への直接接続を使用する、または ESXi Shell を有効にすることで、ホストにアクセスできます。

手順

1. コンソール シェルを有効化または無効化するには、VMware Host Client インベントリ内で [ホスト] を右クリックします。
2. ドロップダウン メニューから [サービス] を選択し、[Console Shell（コンソール シェル）] を選択します。
3. 実行するタスクを選択します。
   - コンソール シェルが有効化されている場合は、[無効化] をクリックして無効化します。
   - コンソール シェルが無効化されている場合は、[有効化] をクリックして有効化します。

VMware Host Client での ESXi Shell 可用性のタイムアウトの作成

ESXi Shell はデフォルトでは無効になっています。ESXi Shell を有効にする際にセキュリティを強化するため、可用性タイムアウトを設定できます。

可用性タイムアウトは、ローカルおよびリモートの両方のシェル ログインが許可される時間を定義します。この時間が経過すると、シェルを介したログインが無効になります。可用性タイムアウトの期限が切れると、既存のシェル セッションは残りますが、新しいシェル セッションは許可されません。

手順

1 VMware Host Client インベントリの [管理] をクリックします。

2 [システム] タブで [詳細設定] を選択します。

3 [検索] テキスト ボックスに「**UserVars.ESXiShellTimeOut**」と入力し、[検索] アイコンをクリックします。

4 `UserVars.ESXiShellTimeOut` を選択し、[オプションの編集] をクリックします。

[オプションの編集] ダイアログ ボックスが開きます。

5 [新しい値] テキスト ボックスに、タイムアウト設定を入力します。

ゼロ (0) の値を指定すると、タイムアウトが無効になります。

6 [保存] をクリックします。

タイムアウトを有効にするには、SSH サービスと ESXi Shell サービスの再起動が必要です。

7 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

VMware Host Client でのアイドル ESXi Shell セッションのタイムアウトの作成

ホストで ESXi Shell を有効にしていてセッションからログアウトし忘れた場合、アイドル セッションは無期限に接続されたままになります。接続を開いたままにすると、他のユーザーが ESXi ホストに対するアクセス権を取得する可能性が高くなります。アイドル セッションのタイムアウトを設定することによって、これを防止できます。

アイドル タイムアウト設定は、対話形式のアイドル セッションからログアウトされるまでの許容経過時間を示します。

手順

1 VMware Host Client インベントリの [管理] をクリックします。

2 [システム] タブで [詳細設定] をクリックします。

3 [検索] テキスト ボックスに「**UserVars.ESXiShellInteractiveTimeOut**」と入力し、[検索] アイコンをクリックします。

4 `UserVars.ESXiShellInteractiveTimeOut` を選択し、[オプションの編集] をクリックします。

[オプションの編集] ダイアログ ボックスが開きます。

5 [新しい値] テキスト ボックスに、タイムアウト設定を入力します。

ゼロ (0) の値を指定すると、タイムアウトが無効になります。

6 [保存] をクリックします。

タイムアウトは、新しくログインされたセッションに対してのみ有効です。

7 （オプション） キー設定をデフォルトにリセットするには、リスト内の該当するキーを右クリックし、[デフォルトにリセット] を選択します。

結果

セッションがアイドル状態の場合、タイムアウト期間が経過した後、ユーザーがログアウトされます。

VMware Host Client でのホストのメンテナンス モードへの切り替え

メモリの増設など、ホストの保守作業を行う必要がある場合は、ホストをメンテナンス モードにします。ホストは、ユーザーの要求があった場合のみ、メンテナンス モードを開始または終了します。

実行中の仮想マシンがパワーオフされるか別のホストに移行されるまで、ホストは [メンテナンス モードに切り替えています] 状態になります。メンテナンス モードの、またはメンテナンス モードに切り替え中のホストで仮想マシンをパワーオンしたり、そのホストに仮想マシンを移行したりすることはできません。

ホストをメンテナンス モードに切り替えるには、そのホストで実行されているすべての仮想マシンをパワーオフするか、別のホストに移行する必要があります。仮想マシンを実行しているホストをメンテナンス モードに切り替える場合、そのタスクを完了するため、DRS で実行中の仮想マシンのパワーオフまたは移行を実行する必要があります。仮想マシンのパワーオフまたは移行が完了する前にタイムアウトになると、エラー メッセージが表示されます。

ホスト上のすべての仮想マシンが無効になると、ホストのアイコンが [under maintenance（メンテナンス中）] に変化し、そのホストのサマリ パネルに新しい状態が示されます。メンテナンス モードの間は、そのホストでは、仮想マシンをデプロイしたり、パワーオンしたりすることはできません。

前提条件

ホストをメンテナンス モードに切り替える前に、そのホスト上で実行されている仮想マシンをパワーオフするか、手動または DRS を使用して自動で別のホストに移行します。

手順

◆ ホストを右クリックし、[メンテナンス モードへの切り替え] を選択します。

結果

[メンテナンス モードの終了] を選択するまで、そのホストはメンテナンス モードになります。

VMware Host Client での権限の管理

ESXi の場合、権限は、仮想マシンまたは ESXi ホストなどのさまざまなオブジェクトに対しユーザーに割り当てられるロールから構成される、アクセス ロールとして定義されます。権限は、割り当てられているオブジェクトのロールで指定されたアクティビティを実行する権利をユーザーに付与します。

たとえば、ホストに対しメモリを構成するには、ユーザーに ホスト.構成.メモリ構成 権限を含むロールが付与されなければなりません。オブジェクトごとに異なるロールをユーザーに割り当てることによって、VMware Host Client を使用してユーザーが実行できるタスクを制御できます。

VMware Host Client でホストに直接接続している場合、root および vpxuser ユーザー アカウントには、すべてのオブジェクトでシステム管理者ロールを割り当てられているユーザーと同じアクセス権が付与されます。

その他すべてのユーザーには最初、どのオブジェクトに対する権限もありません。つまり、ユーザーはオブジェクトでタスクを表示することも、実行することもできません。システム管理者権限を持つユーザーが、これらのユーザーに権限を付与し、タスクを実行できるようにする必要があります。

多くのタスクが、複数のオブジェクトでの権限を必要とします。次のルールを使用して、特定のタスクを実行できるようにするためにユーザーに割り当てるロールを決定できます。

- 仮想ディスクの作成やスナップショットの作成など、ハード ディスク容量を使用するタスクにはターゲット データストアへの データストア.領域の割り当て 権限が必要です。また、操作を実行する権限も必要です。
- 各ホストおよびクラスタには、そのホストまたはクラスタのすべてのリソースが含まれる、独自のリソース プールが必ず存在します。仮想マシンをホストまたはクラスタに直接展開するには、リソース.仮想マシンのリソース プールへの割り当て 権限が必要です。

特権のリストは、ESXi と vCenter Server のどちらも同一です。

ESXi ホストに直接接続して、ロールを作成し、権限を設定できます。

権限の検証

Active Directory を使用する vCenter Server および ESXi ホストは、Windows Active Directory ドメインと比較して、定期的にユーザーおよびグループを検証します。検証は、ホスト システムの起動時、および vCenter Server の設定で指定された定期的な間隔で実行されます。

たとえば、Smith というユーザーが権限を割り当てられており、ドメインでそのユーザー名が Smith2 に変更された場合、ホストは Smith が存在しないと見なし、次回の検証が発生したときに、そのユーザーの権限を削除します。

同様に、Smith というユーザーがドメインから削除された場合、次回の検証が発生したときに、すべての権限が削除されます。次回の検証が発生する前に Smith という新しいユーザーがドメインに追加された場合、新規ユーザーの Smith には、古いユーザーの Smith に割り当てられていたすべての権限が付与されます。

VMware Host Client での ESXi ホストのユーザーへの権限の割り当て

ESXi ホストで特定のアクティビティを実行するために、ユーザーには特定のロールと関連付けられている権限が必要です。VMware Host Client で、ロールをユーザーに割り当て、ユーザーにホストでさまざまなタスクを実行するために必要な権限を付与することができます。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、[権限] をクリックします。

[権限の管理] ウィンドウが表示されます。

2 [ユーザーの追加] をクリックします。

3 [ユーザーを選択] テキスト ボックスから、ロールを割り当てるユーザーを選択します。

4 [ロールを選択] テキスト ボックスの横にある矢印をクリックして、リストからロールを選択します。

5 （オプション）[すべての子へ伝達] または [グループとして追加] を選択します。

権限を vCenter Server レベルで設定し、それを子オブジェクトに伝達すると、権限がデータセンター、フォルダ、クラスタ、ホスト、仮想マシン、そして vCenter Server インスタンス内のその他のオブジェクトに適用されます。

6 [ユーザーの追加] をクリックして、[閉じる] をクリックします。

VMware Host Client でのユーザーの権限の削除

ユーザーの権限を削除しても、そのユーザーは使用可能なユーザーのリストから削除されません。また、ロールも使用可能項目のリストから削除されません。選択したインベントリ オブジェクトから、ユーザーとロールとのペアが削除されます。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、[権限] をクリックします。

[権限の管理] ウィンドウが表示されます。

2 ユーザーをリストから選択し、[ユーザーの削除] をクリックします。

3 [閉じる] をクリックします。

VMware Host Client での仮想マシンのユーザー権限の割り当て

ロールを特定ユーザーに割り当て、そのユーザーに仮想マシンで特定タスクを実行するための権限を付与します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、[権限] を選択します。

[権限の管理] ウィンドウが表示されます。

3 [ユーザーの追加] をクリックします。

4 [ユーザーを選択] テキスト ボックスの横にある矢印をクリックして、ロールを割り当てるユーザーを選択します。

5 [ロールを選択] テキスト ボックスの横にある矢印をクリックして、リストからロールを選択します。

6 （オプション）[すべての子へ伝達] を選択します。

権限を vCenter Server レベルで設定し、それを子オブジェクトに伝達すると、権限がデータセンター、フォルダ、クラスタ、ホスト、仮想マシン、そして vCenter Server インスタンス内の類似オブジェクトに適用されます。

7 [ユーザーの追加] をクリックして、[閉じる] をクリックします。

VMware Host Client での仮想マシンの権限の削除

ユーザーが特定の仮想マシンでタスクを実行できないようにするには、その仮想マシンに対するユーザーの権限を削除します。

ユーザーの権限を削除しても、そのユーザーは使用可能なユーザーのリストから削除されません。また、ロールも使用可能項目のリストから削除されません。選択したインベントリ オブジェクトから、ユーザーとロールとのペアが削除されます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、[権限] を選択します。

[権限の管理] ウィンドウが表示されます。

3 ユーザーをリストから選択し、[ユーザーの削除] をクリックします。

4 [閉じる] をクリックします。

VMware Host Client でのサポート バンドルの生成

ログインしている ESXi ホストのサポート バンドルを生成できます。サポート バンドルには、問題を診断して解決するのに使用できる、ログ ファイルおよびシステム情報が含まれています。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、ドロップダウン メニューから [サポート バンドルの生成] を選択します。

サポート バンドルの作成時に、バンドルをダウンロードするためのリンクが含まれているダイアログ ボックスがポップアップ表示されます。

2 （オプション） VMware Host Client インベントリで [監視] をクリックし、[タスク] をクリックし、リストからログ バンドルをクリックします。

テーブルの下にログ バンドルへのリンクが表示されます。

VMware Host Client のロックダウン モード

ESXi ホストのセキュリティを向上させるために、ロックダウン モードにすることができます。ロックダウン モードでは、デフォルトで vCenter Server から操作を実行する必要があります。

通常ロックダウン モードと厳密なロックダウン モード

vSphere 6.0 以降では、通常のロックダウン モードまたは厳密なロックダウン モードを選択できます。

通常ロックダウン モード

通常ロックダウン モードでは、DCUI サービスがアクティブなままになります。vCenter Server システムへの接続が失われ、vSphere Client 経由でアクセスできない場合は、権限のあるアカウントで ESXi ホストのダ

イレクト コンソール インターフェイスにログインし、ロックダウン モードを終了することができます。ダイレクト コンソール ユーザー インターフェイスには、次のアカウントのみがアクセスできます。

- ホストでの管理権限を持っている、ロックダウン モードの例外ユーザー リストにあるアカウント。例外ユーザー リストは、特定のタスクを実行するサービス アカウントのリストです。このリストに ESXi 管理者を追加することは、ロックダウン モードの趣旨に反します。
- ホストの DCUI.Access 詳細オプションに定義されているユーザー。このオプションは、vCenter Server への接続が失われた場合に、ダイレクト コンソール インターフェイスに緊急アクセスするためのものです。これらのユーザーは、ホストの管理権限が不要になります。

厳密なロックダウン モード

厳密なロックダウン モードでは、DCUI サービスが停止します。vCenter Server への接続が失われ、vSphere Client を使用できなくなると、ESXi Shell および SSH サービスが有効で、かつ例外ユーザーが定義されていない限り、ESXi ホストが使用不能になります。vCenter Server システムへの接続をリストアできない場合は、ホストを再インストールする必要があります。

ロックダウン モードと ESXi Shell および SSH サービス

厳密なロックダウン モードでは DCUI サービスが停止します。ただし、ESXi Shell および SSH サービスは、ロックダウン モードに依存しません。ロックダウン モードを有効なセキュリティ対策とするため、ESXi Shell および SSH サービスも必ず無効にしてください。これらのサービスは、デフォルトで無効になっています。

ホストがロックダウン モードになっている場合、例外ユーザー リストのユーザーは、ホストでの管理者ロールを持っていれば、ESXi Shell から、および SSH を介して、そのホストにアクセスすることができます。このアクセスは、厳密なロックダウン モードになっている場合でも可能です。ESXi Shell サービスと SSH サービスを無効のままにするのが最も安全なオプションです。

注： 例外ユーザー リストは、ホストのバックアップなどの特殊なタスクを実行するサービス アカウントを登録するために用意されたものであり、管理者を対象とするものではありません。管理者を例外ユーザー リストに追加するのは、ロックダウン モードの目的を無視した使い方です。

VMware Host Client を使用した ESXi ホストの通常ロックダウン モードへの切り替え

VMware Host Client を使用して、通常ロックダウン モードに切り替えることができます。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、ドロップダウン メニューから [ロックダウン モード] を選択し、[通常のロックダウンへの切り替え] を選択します。

警告メッセージが表示されます。

2 [通常のロックダウンへの切り替え] をクリックします。

VMware Host Client を使用した ESXi ホストの厳密なロックダウン モードへの切り替え

VMware Host Client を使用して、厳密なロックダウン モードに切り替えることができます。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、ドロップダウン メニューから [ロックダウン モード] を選択し、[厳密なロックダウンへの切り替え] を選択します。

警告メッセージが表示されます。

2 [厳密なロックダウンへの切り替え] をクリックします。

VMware Host Client を使用したロックダウン モードの終了

ESXi ホスト上で通常のロックダウン モードまたは厳密なロックダウン モードに切り替えた場合は、VMware Host Client を使用してロックダウンを終了できます。

手順

◆ VMware Host Client インベントリ内で [ホスト] を右クリックし、ドロップダウン メニューから [ロックダウン モード] を選択し、[ロックダウンの終了] を選択します。

VMware Host Client でのロックダウン モード例外ユーザーの指定

vSphere 6.0 以降では、VMware Host Client を使用して、ユーザーを例外ユーザー リストに追加できます。例外ユーザー リストに追加されたユーザーは、ホストがロックダウン モードになってもアクセス許可を失いません。バックアップ エージェントなどのサービス アカウントを例外ユーザーのリストに追加できます。

例外ユーザーは、ESXi ホストにローカルに定義された権限を持つホスト ローカル ユーザーまたは Active Directory ユーザーです。例外ユーザーは Active Directory グループのメンバーではなく、vCenter Server ユーザーでもありません。例外ユーザーがホスト上で実行できる操作は、そのユーザーに付与されている権限によって決まります。たとえば、読み取り専用ユーザーがホスト上のロックダウン モードを無効にすることはできません。

注： 例外ユーザーのリストは、管理者ではなく、ホストのバックアップなどの特殊なタスクを実行するサービス アカウントの場合に便利です。管理者を例外ユーザー リストに追加するのは、ロックダウン モードの目的を無視した使い方です。

手順

1 VMware Host Client インベントリ内で [管理] > [セキュリティとユーザー] の順にクリックします。

2 [ロックダウン モード] をクリックします。

3 [ユーザー例外の追加] をクリックし、ユーザーの名前を入力し、[例外の追加] をクリックします。

4 （オプション） 例外ユーザーのリストから名前を選択し、[ユーザー例外の削除] をクリックし、[確認] をクリックします。

VMware Host Client を使用した、CPU リソースの管理

VMware Host Client で ESXi ホストに接続すると、特定のリソース管理設定にアクセスできます。

VMware Host Client を使用したプロセッサ情報の表示

VMware Host Client で、ログインしている ESXi ホストの現在の CPU 構成に関する情報にアクセスできます。

手順

1 VMware Host Client インベントリ内で [ホスト] をクリックします。

2 [ハードウェア] を展開し、[CPU] を展開します。

物理プロセッサの数とタイプ、および論理プロセッサの数についての情報を参照できます。

VMware Host Client での、特定のプロセッサへの仮想マシンの割り当て

CPU アフィニティを使用すると、特定のプロセッサに仮想マシンを割り当てることができます。この方法では、マルチプロセッサ システム内で使用可能な特定のプロセッサだけに、仮想マシンを割り当てることができます。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] の [CPU] を展開します。

3 [スケジュール設定のアフィニティ] で、仮想マシンの物理プロセッサ アフィニティを選択します。

範囲を示すにはハイフンを使用し、値の区切りにはカンマを使用します。

たとえば、**`0, 2, 4-7`** と入力すると、プロセッサ 0、2、4、5、6、および 7 が指定されます。

4 [保存] をクリックして変更内容を適用します。

VMware Host Client での ESXi ホストの監視

ホストに VMware Host Client を使用して接続している場合に、そのホストの健全性ステータスを監視し、パフォーマンス チャート、イベント、タスク、システム ログ、および通知を表示できます。

VMware Host Client でのチャートの表示

VMware Host Client にログインしているときに、管理対象の ESXi ホストのリソース使用率に関する情報を線グラフで表示できます。

メモリ消費を削減するため、VMware Host Client には過去 1 時間分の統計情報のみが含まれます。

手順

1 VMware Host Client 内で [監視] をクリックし、[パフォーマンス] をクリックします。

2 （オプション） 過去 1 時間分のホスト使用率を表示するには、ドロップダウン メニューからオプションを選択します。

- 過去 1 時間にホストが使用した CPU のパーセント値を表示するには、[CPU] を選択します。

- 過去 1 時間にホストが消費したメモリのパーセント値を表示するには、[メモリ] を選択します。
- 過去 1 時間にホストが消費したネットワークのパーセント値を表示するには、[ネットワーク] を選択します。
- 過去 1 時間にホストが消費したディスクの使用率を表示するには、[ディスク] を選択します。

VMware Host Client でのハードウェアの健全性ステータスの監視

VMware Host Client にログインしているときに、ESXi ホスト ハードウェアの健全性ステータスを監視できます。

注： ハードウェアの健全性ステータスは、基盤となるハードウェアでサポートされる場合にのみ、表示できます。

手順

1. VMware Host Client インベントリ内で [監視] をクリックし、[ハードウェア] をクリックします。
2. 表示する情報のタイプを選択します。
3. （オプション） リストの上にあるフィルタ コントロールを使用して、リストをフィルタリングします。
4. （オプション） 列見出しをクリックしてリストをソートします。

VMware Host Client でのイベントの表示

イベントは、ESXi ホスト上で発生するユーザー アクションまたはシステム アクションの記録です。VMware Host Client にログインしているときに、管理対象ホストと関連付けられているすべてのイベントを表示できます。

前提条件

必要な権限：読み取り専用

手順

- VMware Host Client インベントリ内で [監視] をクリックし、[イベント] をクリックします。
  a （オプション） イベント詳細を表示するイベントを選択します。
  b （オプション） リストの上にあるフィルタ コントロールを使用して、リストをフィルタリングします。
  c （オプション） 列見出しをクリックしてリストをソートします。

VMware Host Client でのタスクの表示

VMware Host Client にログインしているときに、ESXi ホストと関連するタスクを表示できます。タスクの開始者、タスクの状態、タスクの結果、タスクの説明などに関する情報を表示できます。

手順

- VMware Host Client インベントリ内で [監視] をクリックし、[タスク] をクリックします。
  a （オプション） 詳細を表示するタスクを選択します。
  b （オプション） リストの上にあるフィルタ コントロールを使用して、リストをフィルタリングします。
  c （オプション） 列見出しをクリックしてリストをソートします。

VMware Host Client でのシステム ログの表示

ESXi ホストに VMware Host Client を使用してログインしている場合、ログ エントリを表示して、イベントを生成した人、イベントの作成された日時、イベントのタイプなどの情報を取得できます。

手順

1 VMware Host Client インベントリ内で [監視] をクリックし、[ログ] をクリックします。

ログのリストが表示されます。

2 （オプション） 詳細を表示するログをクリックします。

3 （オプション） ログを右クリックし、次のオプションのいずれかを選択します。

- ［新しいウィンドウで開く］
- ［サポート バンドルの生成］

VMware Host Client での通知の表示

VMware Host Client にログインしているときに、ホスト通知と、実行する必要がある関連タスクに関する推奨を表示できます。

手順

1 VMware Host Client インベントリ内で [監視] をクリックし、[通知] をクリックします。

2 リストから通知を選択し、推奨されるアクションを表示します。

推奨されるアクションとメッセージ、および説明が、通知リストの下に表示されます。

VMware Host Client を使用した仮想マシンの管理

4

仮想マシンは物理コンピュータと同様に構成でき、物理コンピュータと同じタスクを実行できます。仮想マシンは、物理コンピュータがサポートしない特殊な機能もサポートします。

VMware Host Client を使用して、仮想マシンの作成、登録、および管理を実行できるほか、日常的な管理タスクやトラブルシューティング タスクも実行できます。

この章には、次のトピックが含まれています。

VMware Host Client での仮想マシンの作成

仮想マシンは、仮想インフラストラクチャの主要コンポーネントです。仮想マシンを作成してホスト インベントリに追加することができます。仮想マシンを作成する際には、その仮想マシンを特定のデータストアに関連付け、オペレーティング システムと仮想ハードウェアのオプションを選択します。仮想マシンのパワーオン後、リソースは、ワークロードが増加すると動的に消費され、ワークロードが減少すると動的に解放されます。

どの仮想マシンにも、物理ハードウェアと同じ機能を備えた仮想デバイスがあります。仮想マシンは、CPU とメモリ、ストレージへのアクセス、および仮想マシンを実行するホストからのネットワーク接続を取得します。

前提条件

仮想マシン.インベントリ.作成権限を持っていることを確認します。

作成する仮想マシンのプロパティに応じて、次の権限も必要になる場合があります。

- 仮想マシン.構成.AddExistingDisk（既存の仮想ディスク ファイル（RDM ではない）を参照する仮想ディスク デバイスを含める場合）。
- 仮想マシン.構成.AddNewDisk（新しい仮想ディスク ファイル（RDM ではない）を作成する仮想ディスク デバイスを含める場合）。
- 仮想マシン.構成.RawDevice（Raw デバイス マッピング (RDM) または SCSI パススルー デバイスを含める場合）。
- 仮想マシン.構成.HostUSBDevice（ホストの USB デバイスでバックアップされる仮想 USB デバイスを含める場合）。
- 仮想マシン.構成.AdvancedConfig（`ConfigSpec.extraConfig` で値を設定する場合）。
- 仮想マシン.構成.SwapPlacement（スワップの配置を設定する場合）。
- データストア.AllocateSpace（仮想マシンおよびその仮想ディスクが作成されるすべてのデータストア上で必要）。
- ネットワーク.割り当て（作成中の新規仮想マシンに割り当てられるネットワーク上で必要）。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、[仮想マシンの作成/登録] を選択します。

[新規仮想マシン] ウィザードが開きます。

2 [新規仮想マシンの作成] を選択し、[次へ] をクリックします。

3 [名前とゲスト OS の選択] 画面で仮想マシンの一意の名前を入力し、ゲスト OS を構成します。

a [名前] テキスト ボックスに、仮想マシンの名前を入力します。

b [互換性] ドロップダウン メニューで、仮想マシンの互換性を選択します。

c [ゲスト OS ファミリ] ドロップダウン メニューで、ゲスト OS を選択します。

d [ゲスト OS のバージョン] ドロップダウン メニューで、ゲスト OS のバージョンを選択します。

e 仮想マシンで VBS を有効にするには、[Windows 仮想化ベースのセキュリティの有効化] チェック ボックスをオンにして、[次へ] をクリックします。

注： [Windows 仮想化ベースのセキュリティの有効化] オプションが表示されるのは、Windows 10 や Windows Server 2016 などの最新の Windows OS バージョンを使用している場合や、仮想マシンと互換性のあるバージョンが ESXi 6.7 以降である場合のみです。

このオプションを有効にすると、ハードウェア仮想化、IOMMU、EFI、およびセキュア ブートがゲスト OS で使用可能になります。この仮想マシンのゲスト OS 内で、[仮想化ベースのセキュリティ] を有効にする必要もあります。

4 [次へ] をクリックします。

5 [ストレージの選択] 画面で、仮想マシンのストレージ タイプと仮想マシン ファイルを保存するデータストアを選択します。

a すべての仮想マシン ディスクと設定ファイルを標準のデータストアに保存するには、[標準] ボタンをクリックします。

b 仮想マシンのハード ディスクをホストのローカル PMEM データストアに保存するには、[永続的なメモリ] ボタンをクリックします。

c リストからデータストアを選択し、[次へ] をクリックします。

注： 構成ファイルを PMEM データストアに保存することはできません。PMEM を選択する場合は、仮想マシンの設定ファイルを格納する場所として通常のデータストアを選択する必要があります。

6 [設定のカスタマイズ] 画面で、仮想マシンのハードウェアとオプションを構成し、[次へ] をクリックします。

異なるタイプのデバイスの追加手順など、仮想マシンのオプションおよび仮想ディスクの構成に関する詳細は、vSphere の仮想マシン管理を参照してください。

a [設定のカスタマイズ] 画面で [仮想ハードウェア] をクリックし、新しい仮想ハードウェア デバイスを追加します。

- 新規仮想ハード ディスクを追加するには、[ハード ディスクの追加] アイコンをクリックします。

  注： 標準的なメモリ ハード ディスクまたは永続的なメモリ ハード ディスクを仮想マシンに追加できます。永続的なメモリ ハード ディスクは、ホストのローカル PMEM データストアに保存されます。

- NIC を仮想マシンに追加するには、[ネットワーク アダプタの追加] アイコンをクリックします。
- その他のデバイスのタイプを選択して仮想マシンに追加するには、[その他のデバイスの追加] アイコンをクリックします。

  注： 仮想マシンが PMEM ストレージを使用している場合は、PMEM データストアに格納されているハード ディスクと、仮想マシンに追加する NVDIMM デバイスすべてが、同じ PMEM リソースを共有します。そのため、ホストで使用できる PMEM の量に合わせて、新しく追加したデバイスのサイズを調整する必要があります。設定のいずれかの段階で注意が必要な場合は、ウィザードにアラートが表示されます。

b （オプション） デバイス設定を表示および構成するには、任意のデバイスを展開します。

オプション	説明
CPU	CPU またはプロセッサは、コンピュータ プログラムの命令を実行するコンピュータ システムの一部であり、コンピュータの機能を実行する主な要素です。CPU にはコアが含まれています。仮想マシンで使用可能な仮想 CPU の数は、ホスト上でライセンス供与されている CPU の数、およびゲスト OS でサポートされている CPU の数によって変わります。VMware の仮想マルチコア CPU の機能を使用するには、ゲスト OS の EULA の要件に準拠している必要があります。
メモリ	仮想マシンのメモリ リソースまたはオプションを追加、変更、または構成し、仮想マシンのパフォーマンスを向上できます。ほとんどのメモリ パラメータは、仮想マシンの作成中にも、ゲスト OS のインストール後にも設定できます。仮想マシンのメモリ リソース設定では、仮想マシンに割り当てるホストのメモリの容量を特定します。仮想ハードウェアのメモリ サイズでは、仮想マシンで実行されるアプリケーションで使用可能なメモリの容量を特定します。
ハード ディスク	仮想マシンが実行中であっても、仮想マシンに大容量仮想ディスクを追加したり、既存のディスクに容量を追加したりできます。ほとんどの仮想ディスク パラメータは、仮想マシンの作成中にも、ゲスト OS のインストール後にも設定できます。
SCSI コントローラ	ストレージ コントローラは、BusLogic パラレル、LSI Logic パラレル、LSI Logic SAS、および VMware 準仮想化 SCSI など、さまざまな SCSI コントローラとして仮想マシンに認識されます。仮想マシンの SCSI バス共有のタイプを設定し、SCSI バスを共有するかどうかを指定できます。共有タイプによっては、同一サーバ上または別のサーバ上の同じ仮想ディスクに仮想マシンが同時にアクセスできます。変更できるのは、ESXi ホスト上の仮想マシンの SCSI コントローラ構成のみです。

オプション	説明
SATA コントローラ	仮想マシンに複数のハード ディスクまたは CD/DVD-ROM デバイスがある場合、SATA コントローラをさらに最大 3 つまで追加してデバイスを割り当てることができます。デバイスを複数のコントローラに分散させるとパフォーマンスを向上させデータ トラフィックの輻湊を避けることができます。1 つのコントローラに対して 30 デバイスの上限を超える場合には、さらにコントローラを追加することもできます。SATA コントローラから仮想マシンを起動し、大容量仮想ハード ディスクで使用できます。
ネットワーク アダプタ	仮想マシンを構成するときに、ネットワーク アダプタ （NIC） を追加し、アダプタ タイプを指定できます。ネットワーク アダプタのタイプは、次の要因を条件として利用可能になります。 ■ 仮想マシンの互換性。これは、仮想マシンを作成したホスト、または最近仮想マシンを更新したホストに依存します。 ■ 仮想マシンの互換性が、現在のホストの最新バージョンに更新されているかどうか。 ■ ゲスト OS。
CD/DVD ドライブ	DVD または CD デバイスを、クライアント デバイス、ホスト デバイス、またはデータストア ISO ファイルに接続するように構成できます。
ビデオ カード	デフォルト設定を選択するか、カスタム設定を指定することができます。ディスプレイの数、ビデオ メモリの合計を指定し、VMware が 3D をサポートするゲスト OS に対して 3D サポートを有効にすることができます。
PCI デバイス	ESXi ホスト上で PCI デバイスを構成して、パススルーで使用可能にすることができます。また、ハードウェア ラベルを変更して、仮想マシンを特定のハードウェア インスタンスに配置するよう制限することもできます。
動的 PCI デバイス	PCI パススルー デバイスは、ベンダーとモデル名によって自動的にグループ化されます。ハードウェア アドレスによって物理 PCI デバイスを選択しないで、ベンダーとモデル名によって目的のデバイスを構成できます。ハードウェア ラベルが同じ、または空のハードウェア ラベルがある、使用可能なすべてのデバイスを仮想マシンに追加できます。仮想マシンをパワーオンすると、ベンダーとモデル名が一致する特定の物理 PCI パススルー デバイスが仮想マシンに接続されます。
セキュリティ デバイス	仮想マシンに Virtual Intel® Software Guard Extensions (vSGX) を設定し、ワークロードのセキュリティを強化できます。仮想マシンを作成するときや、既存の仮想マシンを編集するときに、vSGX を有効または無効にできます。

c （オプション） デバイスを削除するには、そのデバイスの隣にある削除 (⊗) アイコンをクリックします。

このオプションは、安全に削除できる仮想ハードウェアに対してのみ表示されます。

d （オプション） 仮想マシンのオプションをカスタマイズするには、[仮想マシン オプション] ボタンをクリックします。

7 [設定の確認] 画面で詳細を確認し、[完了] をクリックします。

VMware Host Client での既存の仮想マシンの登録

ホストで登録解除した仮想マシンをデータストアから削除しない場合は、VMware Host Client を使用してこの仮想マシンを再登録できます。仮想マシンを再登録すると、インベントリに表示されるようになります。

データストア ブラウザを使用して、データストア、ディレクトリ、`.vmx` ファイルのいずれかを選択し、登録する仮想マシンのリストに追加します。データストアまたはディレクトリを選択すると、そこにあるすべての `.vmx` ファイルを検索します。複数回参照して、このリストに仮想マシンを追加できます。

手順

1 VMware Host Client インベントリ内で [ホスト] を右クリックし、[仮想マシンの作成/登録] を選択します。

[新規仮想マシン] ウィザードが開きます。

2 [作成タイプの選択] 画面で、[既存の仮想マシンの登録] を選択し、[次へ] をクリックします。

3 [登録のための仮想マシンの選択] 画面で [仮想マシン、データストア、またはディレクトリを 1 つ以上選択してください] をクリックし、登録する仮想マシンを特定して [選択] をクリックします。

4 リストから仮想マシンを削除するには、ファイル名を選択して、[選択内容を削除] をクリックします。

5 選択項目をクリアして、登録し直すには、[すべて削除] をクリックします。

6 [次へ] をクリックします。

7 [設定の確認] 画面で詳細を確認し、[完了] をクリックします。

VMware Host Client でのコンソールの使用

VMware Host Client で、ブラウザ コンソールまたは VMware Remote Console (VMRC) を使用して、仮想マシンにアクセスし、その仮想マシンに対してさまざまなタスクを実行できます。

ブラウザ コンソールの使用

注： ESXi の 6.0 より前のバージョンでは、ブラウザ コンソールがサポートされません。ブラウザ コンソールにアクセスするには VMRC を使用する必要があります。

ブラウザ コンソールを使用すると、他のソフトウェアをインストールせずにゲスト OS にアクセスできます。ローカル ハードウェアの接続など、別のコンソール機能を使用するには、VMware Remote Console をインストールします。

注： 現在、ブラウザ コンソールでは、英語、日本語、およびドイツ語のキーボード レイアウトのみがサポートされます。コンソールを開く前に、使用するキーボード レイアウトを選択する必要があります。

VMware Remote Console の使用

VMware Remote Console は、リモート ホスト上の仮想マシンへのアクセスを可能にし、VMware vSphere 向けに、オペレーティング システムの設定や仮想マシン コンソールの監視など、コンソールおよびデバイスの操作を行います。仮想マシンのゲスト OS の再起動とシャットダウン、仮想マシンの再起動とサスペンド、VMware Tools 更新の構成、仮想マシンおよび他のデバイスの構成と管理など、さまざまなタスクを仮想マシンに対して実行できます。VMRC では、RAM、CPU コア、ディスクといった仮想マシンの設定を変更することもできます。VMware Workstation™、VMware Fusion™、VMware Player™ は VMRC クライアントとして機能するため、これらのいずれかがシステムにインストールされている場合は、VMRC をダウンロードしてインストールする必要がありません。

コンソールのすべての機能を使用するには、VMRC をダウンロードしてインストールします。

VMware Host Client での VMware Remote Console アプリケーションのインストール

VMware Remote Console (VMRC) は、クライアント デバイスに接続し、リモート ホストで仮想マシン コンソールを起動できる、スタンドアローン コンソール アプリケーションです。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

ホスト上で利用可能な仮想マシンのリストが表示されます。

2 リストから仮想マシンを選択します。

3 [コンソール] ツールバー アイコンをクリックし、[VMRC のダウンロード] オプションを選択します。

VMware Host Client での仮想マシンのリモート コンソールの起動

VMware Remote Console を使用して、VMware Host Client で仮想マシンにアクセスできます。1 つ以上のコンソールを起動して、複数のリモート仮想マシンに一度にアクセスすることができます。

前提条件

ローカル システムに VMware Remote Console がインストールされていることを確認します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックし、リストから仮想マシンを選択します。

2 [コンソール] をクリックし、ドロップダウン メニューから [リモート コンソールの起動] を選択します。

選択した仮想マシンのスタンドアローン アプリケーションとして VMware Remote Console が開きます。

VMware Host Client での仮想マシン コンソールの表示

VMware Host Client では、仮想マシンのコンソールを起動することで、仮想マシンのデスクトップにアクセスできます。このコンソールから、オペレーティング システム設定の構成、アプリケーションの実行、パフォーマンスの監視などのタスクを仮想マシン内で実行できます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リストから、パワーオン状態の仮想マシンを選択します。

3 [コンソール] ツール バー アイコンをクリックし、コンソールを開く場所をポップアップ ウィンドウ、新しいウィンドウ、新しいタブのいずれかに指定します。

VMware Host Client でのゲスト OS の管理

VMware Host Client を使用して、仮想マシンのゲスト OS を管理できます。VMware Tools をインストールおよびアップグレードできるほか、構成済みのゲスト OS のシャットダウン、再起動、変更も可能です。

VMware Host Client を使用した、ゲスト OS のシャットダウンまたは再起動

仮想マシンのゲスト OS をシャットダウンおよび再起動するには、VMware Tools がその仮想マシンにインストールされている必要があります。

手順

- VMware Host Client インベントリで [仮想マシン] をクリックし、仮想マシンとタスクを選択します。
  - 仮想マシンをシャットダウンするには、仮想マシンを右クリックし、[ゲスト OS] - [シャットダウン] の順に選択します。
  - 仮想マシンを再起動するには、仮想マシンを右クリックし、[ゲスト OS の] - [再起動] を選択します。

VMware Host Client での、ゲスト OS の変更

仮想マシン設定のゲスト OS のタイプを変更するときには、仮想マシンの構成ファイル内のそのゲスト OS の設定を変更します。ゲスト OS 自体を変更するには、仮想マシンに新しいオペレーティング システムをインストールする必要があります。

新しい仮想マシンのゲスト OS のタイプを設定する場合、vCenter Server ではそのゲスト OS のタイプに基づいてデフォルトの構成が適用されます。ゲスト OS のタイプの設定を変更すると、仮想マシン設定の使用可能な範囲および推奨事項に影響が生じます。

前提条件

仮想マシンをパワーオフします。

手順

1. VMware Host Client のインベントリで仮想マシンを右クリックし、[設定の編集] を選択します。
2. [仮想マシン オプション] タブをクリックし、[一般オプション] を展開します。
3. ゲスト OS のタイプとバージョンを選択します。

   VBS をサポートする Windows OS のバージョンを選択し、仮想マシンの互換性が ESXi 6.7 以降の場合は、[仮想マシン オプション] タブに VBS 行が表示されます。
4. （オプション）[仮想化ベースのセキュリティの有効化] をクリックして VBS を有効にします。

   重要： VBS を有効にするには、EFI を使用して仮想マシンを起動する必要があります。ファームウェアを変更すると、ゲスト OS を起動できなくなる場合があります。
5. [保存] をクリックして変更内容を適用します。

結果

ゲスト OS 用の仮想マシン構成パラメータが変更されました。これでゲスト OS をインストールできます。

VMware Tools の概要

VMware Tools は、サービスとモジュールのセットです。VMware 製品でさまざまな機能を利用できるようにして、ゲスト OS の管理性を向上させ、ユーザーとのシームレスなやり取りを可能にします。

VMware Tools には次のような機能があります。

- ホスト OS からゲスト OS にメッセージを渡します。
- vCenter Server やその他の VMware 製品の一部としてゲスト OS をカスタマイズします。
- ゲスト OS の処理を自動化するスクリプトを実行します。これらのスクリプトは、仮想マシンの電源状態が変化すると実行されます。
- ゲスト OS の時刻をホスト OS の時刻と同期します。

VMware Tools Lifecycle Management は、VMware Tools のインストールとアップグレードを簡単に拡張性の高い方法で行えるようにします。複数の機能強化、ドライバ関連の強化、新しいゲスト OS のサポートが含まれています。

最新バージョンの VMware Tools を実行するか、Linux OS のディストリビューションで提供される open-vm-tools を使用する必要があります。ゲスト OS は VMware Tools なしでも実行できますが、最新の機能やアップデートを利用するには、ゲスト OS で最新バージョンの VMware Tools を常に実行する必要があります。

仮想マシンをパワーオンするたびに VMware Tools のアップグレードの有無を自動で確認して適用するように、仮想マシンを構成できます。

仮想マシンで VMware Tools の自動アップグレードを有効にする方法については、『vSphere 仮想マシン管理ガイド』を参照してください。

VMware Tools のインストール

ゲスト OS は VMware Tools をインストールせずに使用できますが、VMware Tools をインストールすると、多数の VMware 機能を利用することができます。VMware Tools は、使用しているゲスト OS のパフォーマンスを強化します。

VMware Tools のインストールは新しい仮想マシンの作成プロセスの一部です。更新が利用できるようになったら、VMware Tools をアップグレードすることが重要です。仮想マシンの作成に関する詳細は、『VMware Tools ユーザー ガイド』を参照してください。

VMware Tools のインストーラは ISO イメージ ファイルです。ゲスト OS では、ISO イメージ ファイルが CD-ROM のように認識されます。Windows、Linux、Solaris、FreeBSD、および NetWare などのゲスト OS のタイプごとに ISO イメージ ファイルがあります。VMware Tools をインストールまたはアップグレードする場合、仮想マシンの第 1 仮想 CD-ROM ディスク ドライブがゲスト OS の VMware Tools ISO ファイルに一時的に接続されます。

Windows 仮想マシン、Linux 仮想マシン、Mac OS X 仮想マシン、Solaris 仮想マシン、NetWare 仮想マシン、または FreeBSD 仮想マシンでの VMware Tools のインストールまたはアップグレードについての詳細は、『VMware Tools ユーザー ガイド』を参照してください。

VMware Host Client からの VMware Tools のインストール

VMware Tools は、仮想マシンのオペレーティング システムにインストールされる一連のユーティリティです。VMware Tools を使用すると、仮想マシンのパフォーマンスおよび管理が強化されます。

VMware Host Client を使用することにより、1 つまたは複数の仮想マシンの VMware Tools をインストールできます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リストから仮想マシンを選択します。

VMware Tools をインストールするには、仮想マシンがパワーオンになっている必要があります。

3 [アクション] をクリックし、ドロップダウン メニューから [ゲスト OS] を選択し、[VMware Tools のインストール] を選択します。

VMware Tools のアップグレード

VMware Tools は、手動でアップグレードするか、新しいバージョンを確認してインストールするように仮想マシンを設定することもできます。

ゲスト OS は、仮想マシンをパワーオンしたときに VMware Tools のバージョンを確認します。新しいバージョンが利用できる場合は、仮想マシンのステータス バーにメッセージが表示されます。

vSphere 仮想マシンの場合、インストールされている VMware Tools のバージョンが古い場合、ステータス バーに次のメッセージが表示されます。

```
新しいバージョンの VMware Tools がこの仮想マシンで利用可能です。
```

Windows 仮想マシンでは、アップグレードが利用可能な場合は通知するように VMware Tools を設定できます。この通知オプションを有効にした場合、VMware Tools のアップグレードが利用可能になると、Windows タスクバーの VMware Tools アイコンに黄色い注意アイコンが付けられます。

VMware Tools のアップグレードは、VMware Tools を最初にインストールしたときと同じ手順でインストールできます。VMware Tools のアップグレードとは、新しいバージョンをインストールするということです。

Windows および Linux ゲスト OS の場合、VMware Tools を自動的にアップグレードするように Windows の仮想マシンを構成できます。Windows ゲスト OS の場合、仮想マシンをパワーオンするとバージョン チェックが実行されますが、自動アップグレードは、仮想マシンをパワーオフまたは再起動したときに実行されます。アップグレードの進行中、ステータス バーには `VMware Tools をインストールしています...` というメッセージが表示されます。手順は次のとおりです。

注： Windows ゲスト OS 上で VMware Tools をアップグレードすると、WDDM グラフィックス ドライバが自動的にインストールされます。WDDM グラフィックス ドライバにより、ゲスト OS の電源設定でスリープ モードを使用して、スリープ オプションを調整できます。たとえば、スリープ モード設定の [コンピュータがスリープ状態になる時間を変更] では、一定時間が経過するとゲスト OS が自動的にスリープ モードになるように設定できます。また、しばらくアイドル状態であった後でも自動的にスリープ モードに切り替わらないように設定することも可能です。

vSphere 仮想マシンの場合、次に挙げるプロセスを使用して、同時に複数の仮想マシンをアップグレードできます。

次のプロセスのいずれかを使用して、同時に複数の仮想マシンをアップグレードできます。

- vCenter Server にログインして、ホストまたはクラスタを選択し、VMware Tools のアップグレードを実行する仮想マシンを[仮想マシン] タブで指定します。
- 仮想マシンの組織的なアップグレードをフォルダ レベルまたはデータセンター レベルで実行するには、vSphere Lifecycle Manager を使用します。

VMware 製品の一部の機能には、該当のリリースで提供される VMware Tools のインストールまたは該当のバージョンへのアップグレードが必要なものがあります。必須ではありませんが、VMware は VMware Tools を最新のバージョンにアップグレードすることを推奨しています。VMware Tools の新しいバージョンは、特定の ESXi ホストのバージョンと互換性があります。不必要なアップグレードを行わないように、新しいバージョンが提供する機能が環境に必要かどうかを確認してください。「仮想マシンの互換性の設定で使用できるハードウェア機能」を参照してください。VMware は、最新バージョンの VMware Tools をインストールすることをお勧めしています。

VMware 製品の一部の機能には、該当のリリースで提供される VMware Tools のインストールまたは該当のバージョンへのアップグレードが必要なものがあります。VMware Tools の最新バージョンへのアップグレードは、常に必要なわけではありません。VMware Tools の新しいバージョンは、特定のホストのバージョンと互換性があります。不必要なアップグレードを行わないように、新しいバージョンが提供する機能が環境に必要かどうかを確認してください。

表 4-1. 仮想マシンの互換性のオプション

互換性	説明
ESXi 8.0 以降	この仮想マシン（ハードウェア バージョン 20）は、ESXi 8.0 以降と互換性があります。
ESXi 7.0 Update 3 以降	この仮想マシン（ハードウェア バージョン 19）は、ESXi 7.0 Update 3 および ESXi 8.0 と互換性があります。
ESXi 7.0 Update 2 以降	この仮想マシン（ハードウェア バージョン 19）は、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。
ESXi 7.0 Update 1 以降	この仮想マシン（ハードウェア バージョン 18）は、ESXi 7.0 Update 1、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。
ESXi 7.0 以降	この仮想マシン（ハードウェア バージョン 17）は、ESXi 7.0、ESXi 7.0 Update 1、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。
ESXi 6.7 Update 2 以降	この仮想マシン（ハードウェア バージョン 15）は、ESXi 6.7 Update 2、ESXi 6.7 Update 3、ESXi 7.0、ESXi 7.0 Update 1、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。
ESXi 6.7 以降	この仮想マシン（ハードウェア バージョン 14）は、ESXi 6.7、ESXi 6.7 Update 2、ESXi 6.7 Update 3、ESXi 7.0、ESXi 7.0 Update 1、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。
ESXi 6.5 以降	この仮想マシン（ハードウェア バージョン 13）は、ESXi 6.5、ESXi 6.7、ESXi 6.7 Update 2、ESXi 6.7 Update 3、ESXi 7.0、ESXi 7.0 Update 1、ESXi 7.0 Update 2、ESXi 7.0 Update 3、および ESXi 8.0 と互換性があります。

詳細については、http://www.vmware.com/resources/compatibility の VMware 互換性ガイドを参照してください。

VMware Host Client での VMware Tools のアップグレード

仮想マシンの VMware Tools を VMware Host Client を使用してアップグレードできます。

前提条件

仮想マシンをオンにします。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リストから仮想マシンを選択します。
3. [アクション] をクリックし、ドロップダウン メニューから [ゲスト OS] を選択し、[VMware Tools のアップグレード] を選択します。

VMware Host Client での仮想マシンの構成

ほとんどの仮想マシン プロパティは、仮想マシンの作成プロセス中でも、仮想マシンの作成およびゲスト OS のインストール後でも、追加または構成できます。

次の 3 つのタイプの仮想マシン プロパティを構成できます。

ハードウェア

既存のハードウェア構成を表示し、ハードウェアを追加または削除します。

オプション

ゲスト OS と仮想マシン間の電力管理操作、VMware Tools の設定など、いくつかの仮想マシン プロパティを表示および構成します。

リソース

CPU、CPU のハイパースレッド ソース、メモリ、ディスクを構成します。

VMware Host Client での仮想マシンのハードウェア バージョンの確認

仮想マシンのサマリ ページで、仮想マシンのハードウェア バージョンを確認できます。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンをクリックします。

   仮想マシン名の下にハードウェア バージョンが表示されます。

VMware Host Client での、仮想マシン名の変更

仮想マシンの作成が終了した後に、仮想マシンの名前を変更できます。名前を変更しても、仮想マシン ファイルの名前や、そのファイルが格納されたディレクトリの名前は変更されません。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想マシン オプション] をクリックします。

4 [仮想マシン名] テキスト ボックスに、仮想マシンの新しい名前を入力します。

5 [[保存]] をクリックします。

VMware Host Client での仮想マシン構成ファイルの場所の表示

VMware Host Client を使用して、仮想マシンの構成ファイルおよび作業ファイルの場所を表示できます。

この情報は、バックアップ システムを構成するときに役立ちます。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 仮想マシンを右クリックし、[[設定の編集]] をクリックします。

3 [仮想マシン オプション] タブをクリックし、[一般オプション] を展開します。

4 構成ファイルおよび作業ファイルの場所を記録します。

5 画面を終了するには、[キャンセル] をクリックします。

VMware Host Client での、仮想マシン電源状態の構成

ホストでメンテナンスを行なっている場合、仮想マシンの電源状態を変更することは有益です。仮想マシンの電源制御のシステム デフォルト設定を使用することも、ゲスト OS を操作する制御を構成することもできます。たとえば、[パワーオフ] コントロールは、仮想マシンをパワーオフするよう構成することも、ゲスト OS をシャットダウンするよう構成することもできます。

仮想マシンの実行中でも、仮想マシンの複数の構成を変更することはできますが、一部の構成については、仮想マシンの電源状態を変更することが必要な場合があります。

[パワーオン]（  ）アクションを構成することはできません。このアクションでは停止状態の仮想マシンをパワーオンします。また、仮想マシンがサスペンド状態で、VMware Tools がインストールされていて利用可能な場合は、仮想マシンを起動してスクリプトを実行します。VMware Tools がインストールされていない場合は、サスペンド状態の仮想マシンを起動しますが、スクリプトは実行しません。

前提条件

- 仮想マシンで目的の電源操作を行う権限があることを確認します。
- オプションの電源機能を設定するには、仮想マシンに VMware Tools をインストールします。
- VMware Tools オプションを編集する前に、仮想マシンをパワーオフしておく必要があります。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ドロップダウン メニューから [設定の編集] を選択します。

3 [仮想マシン オプション] タブで、[VMware Tools] を展開します。

4 仮想マシンの [パワーオフ]（  ）コントロールのオプションを、ドロップダウン メニューから選択します。

オプション	説明
パワーオフ	仮想マシンをただちに停止します。パワーオフ アクションではゲスト OS をシャットダウンするか、仮想マシンをパワーオフします。ゲスト OS が正常にシャットダウンされない場合があることを示すメッセージが表示されます。このパワーオフ オプションは、必要な場合にのみ使用してください。
ゲストをシャットダウン	VMware Tools を使用して、仮想マシンのシステム シャットダウンを順次開始します。ソフト電源操作は、VMware Tools がゲスト OS にインストールされている場合のみ可能です。
システムのデフォルト	システムの設定に従います。システム設定の現在の値が括弧に表示されます。

5 [サスペンド]（  ）コントロールのオプションを、ドロップダウン メニューから選択します。

オプション	説明
サスペンド	すべての仮想マシンのアクティビティを一時停止します。VMware Tools がインストールされて利用可能な場合は、サスペンド動作によってスクリプトが実行され、仮想マシンがサスペンドされます。VMware Tools がインストールされていない場合、サスペンド アクションにより仮想マシンがサスペンドしますが、スクリプトは実行されません。
ゲストのスタンバイ	ゲスト OS をスタンバイ状態にします。このオプションはすべてのプロセスを停止しますが、すべての仮想デバイスは仮想マシンに接続されたままになります。
システムのデフォルト	システムの設定に従います。システム設定の現在の値が括弧に表示されます。

6 [リセット]（  ）コントロールのオプションを、ドロップダウン メニューから選択します。

オプション	説明
リセット	仮想マシンをパワーオフすることなく、ゲスト OS をシャットダウンして再起動します。VMware Tools がインストールされていない場合、リセット アクションにより仮想マシンがリセットされます。
ゲストを再起動	VMware Tools を使用して、再起動を順次開始します。ソフト電源操作は、VMware Tools がゲスト OS にインストールされている場合のみ可能です。
デフォルト	システムの設定に従います。システム設定の現在の値が括弧に表示されます。

7 [[保存]] をクリックします。

VMware Host Client での構成ファイル パラメータの編集

システムの特定の問題を修正するために、VMware のドキュメントで、または VMware のテクニカル サポート担当者が、仮想マシンの構成パラメータの変更または追加を指示する場合があります。

重要： システムに問題がないときにパラメータを変更したり追加したりすると、システムのパフォーマンスが低下したり不安定な状態となる場合があります。

次の条件が適用されます。

- パラメータを変更するには、キーワードと値のペアの既存の値を変更する必要があります。たとえば、キーワード/値という既存のペアをキーワード/値 2 に変更すると、新しいキーワードは値 2 になります。
- 構成パラメータのエントリを削除することはできません。

注意： 構成パラメータのキーワードに値を割り当てる必要があります。値を割り当てない場合、キーワードは 0 または false という値を受け取る可能性があり、結果として仮想マシンをパワーオンできないことがあります。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想マシン オプション] タブで、[詳細] を展開します。

4 [構成パラメータ] 行で、[構成の編集] をクリックします。

[構成パラメータ] ダイアログ ボックスが開きます。

5 （オプション） パラメータを追加するには、[パラメータの追加] をクリックし、パラメータの名前と値を入力します。

6 （オプション） パラメータを変更するには、そのパラメータの [値] テキスト ボックスに新しい値を入力します。

7 [OK] をクリックして変更内容を保存し、[構成パラメータ] ダイアログ ボックスを閉じます。

8 [[保存]] をクリックします。

VMware Host Client での、仮想マシンの自動起動の構成

仮想マシンの自動起動オプションを構成して、ホスト上の他の仮想マシンの前または後にその仮想マシンを起動するように設定します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックします。

3 ポップアップ メニューから [自動起動] を選択し、オプションをクリックして、その仮想マシンの自動起動オプションを構成します。

オプション	説明
優先順位を上げる	その仮想マシンが他の仮想マシンより前に起動するように、起動の優先順位を上げます。
優先順位を下げる	その仮想マシンが他の仮想マシンより後に起動するように、起動の優先順位を下げます。

VMware Host Client を使用した仮想マシン互換性のアップグレード

仮想マシンの互換性で仮想マシンが使用できる仮想ハードウェアを決定できます。仮想ハードウェアはホスト マシンで使用できる物理ハードウェアに対応しています。ホスト上で実行される ESXi の最新のバージョンに対して仮想マシンが互換性を持てるように、互換性レベルをアップグレードできます。

仮想マシンのハードウェア バージョンと互換性に関する詳細は、vSphere の仮想マシン管理 を参照してください。

前提条件

- 仮想マシンのバックアップまたはスナップショットを作成します。スナップショットによる仮想マシンの管理を参照してください。
- VMware Tools をアップグレードします。Microsoft Windows を実行している仮想マシン上で VMware Tools をアップグレードする前に互換性をアップグレードすると、仮想マシンのネットワーク設定が失われることがあります。
- VMFS3、VMFS5、または NFS のデータストアの ESXi ホストで、すべての `.vmdk` ファイルを使用できることを確認します。
- 仮想マシンが VMFS3、VMFS5、または NFS のデータストアに格納されていることを確認します。
- 仮想マシンの互換性設定がサポートされている最新バージョンではないことを確認します。
- 仮想マシンと互換性を持たせる ESXi バージョンを決定します。vSphere の仮想マシン管理 を参照してください。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [仮想マシンの互換性のアップグレード] を選択します。

3 サポートされている最新のバージョンを選択し、[アップグレード] をクリックします。

VMware Host Client での仮想マシンの管理

VMware Host Client で仮想マシンを作成した後に、さまざまな管理タスクをその仮想マシン上で実行できます。たとえば、ホストからの仮想マシンの削除、データストアからの仮想マシンの削除、データストアへの仮想マシンの再登録などを実行できます。また、その仮想マシンをホストに復元することも可能です。

VMware Host Client での仮想マシンへのアクセス

ログインしているホスト上の仮想マシンにアクセスして、仮想マシンのハードウェアおよびオプションを構成したり、管理タスクや基本的なトラブルシューティング タスクを実行することができます。

VMware Host Client インベントリに仮想マシンを表示するには、その仮想マシンをパワーオンします。

手順

- ログインしているホスト上で使用可能な仮想マシンにアクセスするには、VMware Host Client インベントリ内で [仮想マシン] をクリックします。

結果

利用可能な仮想マシンのリストが [仮想マシン] に表示されます。

ここで、リスト内の仮想マシンに対して、仮想マシン設定の編集や、他の管理タスクおよびトラブルシューティング タスクを実行できます。

VMware Host Client の仮想マシンの電源状態

仮想マシンの基本的な電源操作には、パワーオン、パワーオフ、サスペンド、リセットがあります。

仮想マシンの電源状態を変更する方法については、 VMware Host Client での、仮想マシン電源状態の構成を参照してください。

前提条件

- 仮想マシン.相互作用.パワーオン 権限を持っていることを確認します。
- 仮想マシン.相互作用.パワーオフ 権限を持っていることを確認します。
- 仮想マシン.相互作用.サスペンド 権限を持っていることを確認します。
- 仮想マシン.相互作用.リセット 権限を持っていることを確認します。

手順

1. VMware Host Client インベントリで、[仮想マシン] をクリックします。
2. 仮想マシンを右クリックし、電源操作を選択します。

オプション	説明
パワーオン（  ）	仮想マシンが停止したときに仮想マシンをパワーオンします。
[パワーオフ（  ）]	仮想マシンをパワーオフし、ゲスト OS をシャットダウンします。仮想マシンをパワーオフすると、データが失われることがあります。
[サスペンド（  ）]	実行中の仮想マシンをサスペンドし、ネットワークに接続したままにします。サスペンド状態の仮想マシンをレジュームすると、仮想マシンはサスペンドされた時点と同じ時点で動作を続行します。
[リセット（  ）]	仮想マシンをパワーオフすることなく、ゲスト OS をシャットダウンして再起動します。

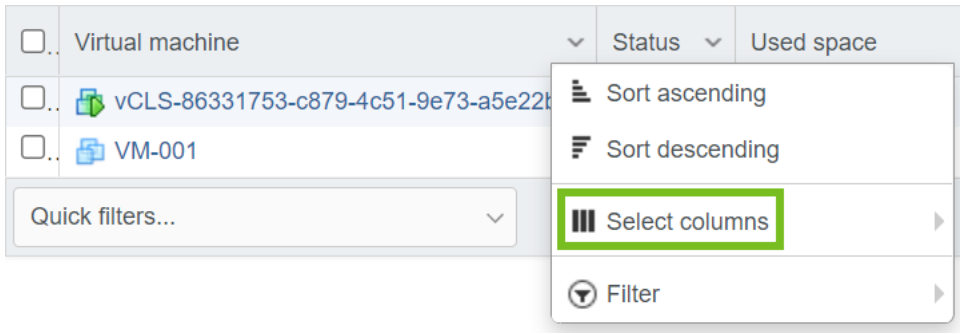
VMware Host Client での仮想マシン列構成の使用

VMware Host Client の仮想マシン パネルでは、表示する情報を構成できます。ステータス、使用容量、ホスト名、ホスト CPU などのさまざまな列を表示または非表示にできます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 仮想マシンのリストで、任意の列タイトルの横にある下矢印アイコンをクリックして、[列の選択] を選択します。



使用可能なすべての列を含むリストが表示されます。

3 仮想マシン パネルに表示する情報を選択します。

VMware Host Client でのホストからの仮想マシンの削除

仮想マシンをデータストアには維持するが VMware Host Client インベントリにはもう表示しない場合は、その仮想マシンの登録を解除できます。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、[登録解除] をクリックします。

3 [はい] をクリックして、インベントリからの仮想マシンの削除を確認します。

結果

ホストでは、その仮想マシンがインベントリから削除され、その状態が追跡されなくなります。

VMware Host Client でのデータストアからの仮想マシンの削除

データストアの容量を解放するために、不要になった仮想マシンを削除できます。VMware Host Client インベントリから仮想マシンを削除すると、構成ファイルや仮想ディスク ファイルを含むすべての仮想マシン ファイルがデータストアから削除されます。複数の仮想マシンを削除できます。

前提条件

- 仮想マシンをパワーオフします。

- その仮想マシンが別の仮想マシンとディスクを共有していないことを確認します。2 台の仮想マシンがディスクを共有している場合、ディスク ファイルは削除されません。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 削除する仮想マシンの横にある 1 つまたは複数のチェック ボックスを選択し、[アクション] - [削除] の順に選択します。

[仮想マシンの削除] ダイアログ ボックスが開きます。

3 [削除] をクリックします。

VMware Host Client での仮想マシンの登録

ホストから仮想マシンまたはテンプレートを削除したが、ホストのデータストアからは削除していない場合、その仮想マシンまたはテンプレートをホストのインベントリに復元できます。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックします。

2 リスト内のデータストアを右クリックし、[仮想マシンの登録] をクリックします。

3 登録する仮想マシンをリストから選択し、[登録] をクリックします。

スナップショットによる仮想マシンの管理

スナップショットには、スナップショット作成時の仮想マシンの状態とデータが保存されます。仮想マシンのスナップショットを作成すると、特定の状態の仮想マシンのイメージがコピーおよび保存されます。スナップショットは、繰り返し同じ状態の仮想マシンに戻る必要があるが、複数の仮想マシンを作成したくないという場合に便利です。

仮想マシンのスナップショットを複数作成して、線形処理でリストアする位置を作成できます。複数のスナップショットによって、さまざまなワーク プロセスに対応した多くの状態を保存できます。スナップショットは個々の仮想マシンで操作されます。チームの各メンバーの仮想マシン スナップショットを作成するなど、複数の仮想マシンのスナップショットを作成する場合は、各チーム メンバーの仮想マシンについて別々のスナップショットを作成する必要があります。

スナップショットは、未知の障害または有害な効果が発生する可能性のあるソフトウェアをテストするための、短期的なソリューションとして便利です。たとえば、線形処理、アップデート パッケージをインストールするような反復処理、または異なるバージョンのプログラムをインストールするような分岐処理において、スナップショットをリストア ポイントとして使用できます。スナップショットを使用すると、同一のベースラインから各インストールが開始します。

スナップショットがあれば、仮想マシンを変更する前に、ベースラインを保存できます。

vSphere Client では、仮想マシン スナップショットおよびスナップショット ツリーを作成および管理するための操作方法を提供します。これらの操作により、スナップショットの作成、スナップショット階層にあるスナップショットを元に戻す処理、スナップショットの削除などを行うことができます。後で仮想マシンの状態を元に戻すことができるように、特定の時点の仮想マシン状態を保存するスナップショット ツリーを作成することができます。スナップショット ツリーの各分岐には、最大で 32 のスナップショットを保存できます。

スナップショットには、次の情報が含まれます。

- 仮想マシンの設定。スナップショット作成後に追加または変更されたディスクを含む、仮想マシン ディレクトリ。
- 電源状態。仮想マシンは、パワーオン状態、パワーオフ状態、またはサスペンド状態にすることができます。
- ディスク状態。すべての仮想マシンの仮想ディスクの状態。
- （任意） メモリ状態。仮想マシンのメモリの内容。

スナップショットの階層

vSphere Client には、スナップショットのツリー階層が、1 つ以上の分岐付きで表示されます。階層内のスナップショットは、親と子の関係を持ちます。線形プロセスでは、各スナップショットに親スナップショットと子スナップショットが 1 つずつ存在します。ただし、最後に作成したスナップショットには親スナップショットのみ存在します。親スナップショットにはそれぞれ、複数の子スナップショットを作成できます。最新の親スナップショットに戻ったり、スナップショット ツリー内の任意の親スナップショットまたは子スナップショットに戻ったり、そのスナップショットからさらに別のスナップショットを作成することができます。スナップショットを元に戻し、別のスナップショットを作成するたびに、分岐（子スナップショット）が作成されます。

親スナップショット

最初に作成する仮想マシンのスナップショットは、ベース親スナップショットです。親スナップショットは仮想マシンの現在の状態を保存した、最新のバージョンです。スナップショットを作成すると、仮想マシンに接続された各ディスクについて差分ディスク ファイルが作成され、オプションでメモリ ファイルが作成されます。差分ディスク ファイルとメモリ ファイルは、基本となる `.vmdk` ファイルと一緒に保存されます。親スナップショットは、常にスナップショット マネージャの [現在点] アイコンのすぐ上に表示されるスナップショットです。スナップショットを元に戻した場合、そのスナップショットは現在の状態（[現在点]）の親になります。

注： 最近作成したスナップショットが親スナップショットになるとは限りません。

子スナップショット

親スナップショットの後に作成された、仮想マシンのスナップショットです。子スナップショットには、接続している各仮想ディスクの差分ファイルが含まれています。仮想ディスクの現在の状態（現在点）から参照するメモリ ファイルが含まれている場合もあります。各子スナップショットの差分ファイルは、親ディスクに到達するまで、過去の各子スナップショットとマージされます。子ディスクは、あとで、将来の子ディスク用の親ディスクになることができます。

スナップショット ツリーに複数の分岐がある場合、親スナップショットと子スナップショットの関係は変更できます。親スナップショットには複数の子スナップショットを作成できます。スナップショットの多くは子スナップショットが存在しません。

注意： 個々の子ディスクやスナップショットの構成ファイルを手動で操作しないでください。スナップショット ツリーに問題が発生し、データの損失につながる可能性があるためです。この制限には、`vmkfstools` コマンドを使用した、ディスクのサイズ変更とベース親ディスクの変更が含まれます。

スナップショットの動作

スナップショットを作成すると、特定の時点でのディスク状態を保存できます。これは、添付されている各仮想ディスクまたは仮想 RDM についての一連の差分ディスクが作成されることによって実現され、オプションでメモリ ファイルを作成してメモリと電源状態を保存することもできます。スナップショットの作成により、スナップショット マネージャに、仮想マシンの状態と設定を表すスナップショット オブジェクトが作成されます。

各スナップショットでは、差分ディスク ファイル （.vmdk） が追加で作成されます。スナップショットの作成時、スナップショット メカニズムにより、ゲスト OS による .vmdk ベース ファイルへの書き込みが防止され、代わりに、すべての書き込みが差分ディスク ファイルに対して行われます。差分ディスクは、仮想ディスクの現在の状態と、以前スナップショットを作成した時点の状態の違いを示します。複数のスナップショットが存在する場合、差分ディスクは各スナップショット間の違いを示すことがあります。ゲスト OS が仮想ディスクのすべてのブロックに書き込みを行うと、差分ディスク ファイルは短期間に肥大化し、仮想ディスク全体と同程度のサイズになることがあります。

スナップショット ファイル

スナップショットを作成する場合は、仮想マシン設定および仮想ディスクの状態を取得します。メモリ スナップショットを作成する場合、仮想マシンのメモリ状態も取得します。これらの状態は、仮想マシンのベース ファイルにあるファイルに保存されます。

スナップショット ファイル

スナップショットは、サポートされているストレージ デバイスに保存されているファイルで構成されます。スナップショットの作成操作により、vmdk、-delta.vmdk、.vmsd、および.vmsn の各ファイルが作成されます。デフォルトでは、最初のディスクとすべての差分ディスクは基本の .vmdk ファイルと一緒に保存されています。 .vmsd および .vmsn ファイルは仮想マシンのディレクトリに保存されています。

差分ディスク ファイル

ゲスト OS による書き込みが可能な .vmdk ファイル。差分ディスクは、仮想ディスクの現在の状態と、以前スナップショットを作成した時点の状態の違いを表します。スナップショットを作成すると、その時点の仮想ディスクの状態が保持され、ゲスト OS によるスナップショットへの書き込みは停止されます。これを利用して、差分ディスクまたは子ディスクが作成されます。

差分ディスクには、2 つのファイルが含まれます。1 つはサイズの小さい記述子ファイルであり、構造や子と親の関係情報など、仮想ディスクに関する情報が含まれます。もう 1 つは、raw データが格納された対応するファイルです。

差分ディスクを構成するファイルは、子ディスクまたは redo ログと呼ばれます。

フラット ファイル

基本ディスクを構成する 2 つのファイルの 1 つである -flat.vmdk ファイル。フラット ディスクには、基本ディスクの生データが含まれています。このファイルは、データストア ブラウザでは個別のファイルとして表示されません。

データベース ファイル

仮想マシンのスナップショット情報を格納する .vmsd ファイル。このファイルは、スナップショット マネージャにとっての第一の情報ソースです。このファイルには、スナップショット間、および各スナップショットの子ディスク間の関係を定義する行エントリが含まれています。

メモリ ファイル

仮想マシンのアクティブな状態を格納する .vmsn ファイル。仮想マシンのメモリ状態を取得すると、パワーオン状態の仮想マシンの状態に戻すことができます。メモリなしのスナップショットでは、パワーオフ状態の仮想マシンの状態にのみ戻せます。メモリ スナップショットの方が、メモリなしのスナップショットより作成に時間がかかります。ESXi ホストによるメモリのディスクへの書き込みにかかる時間は、仮想マシンで使用されるように構成されているメモリの量によって異なります。

[スナップショットの作成] 操作により、.vmdk、-delta.vmdk、vmsd、および vmsn の各ファイルが作成されます。

ファイル	説明
vmname-*number*.vmdk および *vmname*-*number*-delta.vmdk	スナップショット ファイルでは、仮想ディスクの現在の状態と、以前スナップショットを作成した時点の状態の違いを表すことができます。 ファイル名には、S1vm-000001.vmdk という構文が使用されます。S1vm は仮想マシンの名前を表し、000001 はディレクトリにすでに存在しているファイルに基づいた 6 桁の数字を表します。この数字では、仮想マシンに添付されたディスク数は考慮されません。
vmname.vmsd	仮想マシンのスナップショット情報を格納するデータベースであり、スナップショット マネージャの第一の情報ソースです。
vmname.Snapshot*number*.vmsn	スナップショットの作成時の仮想マシンのメモリ状態。ファイル名には、S1vm.snapshot1.vmsn という構文が使用されます。S1vm は仮想マシン名を表し、snapshot1 は最初のスナップショットを表します。 **注：** .vmsn ファイルは、メモリを選択するかどうかに関係なく、スナップショットを作成するたびに作成されます。メモリなしの場合の .vmsn ファイルは、メモリありの場合より小さくなります。

スナップショットの制限事項

スナップショットは、仮想マシンのパフォーマンスに影響を与える場合があります。また、スナップショットでは、一部のディスク タイプ、またはバスの共有が設定された仮想マシンはサポートされません。スナップショットは、特定の時点における仮想マシンの状態を取得するための短期的なソリューションとしては便利ですが、長期的な仮想マシンのバックアップには適しません。

- VMware では、Raw ディスク、RDM 物理モード ディスク、または iSCSI イニシエータをゲストで使用するゲスト OS のスナップショットはサポートしていません。
- 独立ディスク搭載の仮想マシンのスナップショットを作成する場合は、事前に仮想マシンをパワーオフする必要があります。独立ディスクを搭載したパワーオン状態の仮想マシンは、メモリ スナップショットをサポートできません。
- 静止スナップショットには、VMware Tools のインストールとゲスト OS のサポートが必要です。
- スナップショットは、PCI vSphere DirectPath I/O デバイスではサポートされません。

- VMware では、バスの共有が設定された仮想マシンのスナップショットはサポートしていません。バスの共有が必要な場合は、代替案として、ゲスト OS でバックアップ ソフトウェアを実行することを検討してください。現在、仮想マシンにスナップショットがあるためにバスの共有が構成できない場合は、スナップショットを削除（統合） してください。
- スナップショットは、ディスクの特定の時点におけるイメージを提供し、バックアップ ソリューションで使用することも可能ですが、バックアップやリカバリに適した方法として用意されているわけではありません。仮想マシンを含むファイルが失われると、そのスナップショット ファイルも失われます。さらに、大量のスナップショットは管理が難しく、ディスク容量を大量に使用します。また、ハードウェア障害が発生した場合には保護されません。
- スナップショットは、仮想マシンのパフォーマンスを低下させる可能性があります。パフォーマンスがどの程度低下するかは、スナップショットまたはスナップショット ツリーの保存期間、ツリーの深度、およびスナップショット作成以降に仮想マシンとそのゲスト OS が変更された頻度に基づいて異なります。さらに、仮想マシンがパワーオン状態になるまでにかかる時間が長くなる場合があります。本番環境の仮想マシンを常時スナップショットから実行することは避けてください。
- 仮想マシンに 2 TB を超える大きさの仮想ハード ディスクがある場合、スナップショットの操作は完了までの時間が大幅に長くなります。

VMware Host Client での仮想マシンのスナップショットの作成

仮想マシンのスナップショットを 1 つ以上作成して、スナップショット作成時の仮想マシンの設定状態、ディスク状態、およびメモリ状態を取得できます。スナップショットを作成する場合は、仮想マシンのファイルを静止したり、仮想マシン ディスクをスナップショットから除外することもできます。仮想マシンの電源がオン、オフ、サスペンドのいずれの場合でもスナップショットを作成できます。サスペンド状態の仮想マシンのスナップショットを作成するには、サスペンド処理が終了するまで待ってから、スナップショットを作成します。

スナップショットの作成時に、仮想マシンでほかのアクティビティが実行されていると、そのスナップショットに戻すときに、そのアクティビティがスナップショット プロセスに影響を与える可能性があります。ストレージの観点から言うと、スナップショットを作成するのに最も適したタイミングは、I/O の負荷があまり大きくないときです。サービスの観点から言うと、仮想マシン内のアプリケーションがほかのコンピュータと通信していないときにスナップショットを作成するのが最適です。仮想マシンがほかのコンピュータと通信しているとき、特に本番環境にある場合、問題が起こる可能性が高くなります。たとえば、仮想マシンがネットワーク上のサーバからファイルをダウンロードしているときにスナップショットを作成する場合、仮想マシンはファイルのダウンロードを継続し、サーバに進捗状況を通知します。そのスナップショットに戻すと、仮想マシンとサーバ間の通信は混乱し、ファイルの転送は失敗します。実行しているタスクによっては、メモリ スナップショットを作成したり、仮想マシンのファイル システムを静止したりできます。

メモリ スナップショット

スナップショット作成のデフォルトの設定です。仮想マシンのメモリの状態を取得する場合、スナップショットは仮想マシンのライブ状態を維持します。メモリ スナップショットでは、稼働中のソフトウェアをアップグレードするときなど、ある特定の時点でのスナップショットが作成されます。メモリ スナップショットを作成しておけば、アップグレードが予想どおりに完了しなかったとき、またはソフトウェアが期待に沿うものでなかったときに、仮想マシンを元の状態に戻すことができます。

メモリ状態の取得時に仮想マシンのファイルを静止させる必要はありません。メモリの状態を取得しない場合、スナップショットは仮想マシンのライブ状態を保存せず、ディスクは、静止しないかぎりクラッシュ時の整合性を保ちます。

仮想マシンのメモリ状態をキャプチャするスナップショットは、完了するまでに時間がかかります。ネットワークによっては、瞬間的に中断が生じる場合もあります。

静止スナップショット

仮想マシンを静止する場合、VMware Tools によって仮想システム内のファイル システムが静止されます。静止操作により、スナップショット ディスクはゲスト ファイル システムの一貫した状態を表します。静止操作によって、仮想マシン上で実行中のプロセス（特にリストア操作中、ディスク上に格納される情報を変更する場合があるプロセス）の状態が一時停止または変更されます。静止スナップショットは、自動バックアップや定期バックアップに適しています。たとえば、仮想マシンのアクティビティを把握していなくとも、最新の復元用バックアップが欲しいという場合に、ファイルを静止することができます。

仮想マシンがパワーオフ状態の場合、または VMware Tools を使用できない場合は、`Quiesce` パラメータは使用できません。大容量ディスクがある仮想マシンを静止させることはできません。

IDE ディスクまたは SATA ディスクが存在する仮想マシンでは、アプリケーションの整合性を保つ静止はサポートされていません。

重要： 唯一の、または長期的なバックアップ ソリューションとしてスナップショットを使用しないでください。

注： ダイナミック ディスク（Microsoft 固有のディスク タイプ）のスナップショットを作成すると、スナップショット テクノロジーによってファイル システムは静止状態が保持されますが、アプリケーションの静止状態は保持されません。

前提条件

- ディスク モードが異なる複数のディスクを持つ仮想マシンのメモリのスナップショットを作成している場合、仮想マシンがパワーオフ状態であることを確認します。たとえば、独立型ディスクが必要になる特別な構成の場合、スナップショットを作成する前に仮想マシンをパワーオフする必要があります。
- 仮想マシンのメモリ状態を取得するには、仮想マシンがパワーオン状態であることを確認します。
- 仮想マシン ファイルを静止するには、仮想マシンがパワーオン状態であり、VMware Tools がインストールされていることを確認します。
- 仮想マシン上で 仮想マシン.スナップショット管理.スナップショットの作成の権限があることを確認します。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、[スナップショット] - [スナップショットの作成] の順に選択します。
3. スナップショットの名前を入力します。
4. （オプション） スナップショットの説明を入力します。
5. （オプション） 仮想マシンのメモリを取得する場合は、[仮想マシンのメモリのスナップショット] チェック ボックスを選択します。

6 （オプション）［仮想マシンのメモリのスナップショット］を選択解除し、［静止ゲスト ファイル システム（VMware Tools のインストールが必要）］チェック ボックスを選択してゲスト OS 上で実行中のプロセスを停止すると、スナップショットの作成時にファイル システムの内容を既知の整合性のある状態にすることができます。

仮想マシンがパワーオン状態であり、仮想マシンのメモリを取得する必要がない場合にのみ、仮想マシン ファイルを静止してください。

7 ［スナップショットの作成］をクリックします。

VMware Host Client での最新のスナップショットへの復帰

仮想マシンを元の状態に戻す、またはスナップショット階層内の別のスナップショットに戻すには、スナップショットをリストアします。

スナップショットをリストアすると、仮想マシンのメモリ、設定、および仮想マシン ディスクの状態がスナップショット作成時の状態に戻ります。仮想マシンの起動時に、仮想マシンをサスペンド状態、パワーオン状態、パワーオフ状態のいずれかにするには、その状態でスナップショットを作成する必要があります。

スナップショットは、次の方法でリストアできます。

［最新のスナップショットに戻す］

［現在の場所］の位置から階層内で 1 つ上のレベルに親スナップショットをリストアします。［最新のスナップショットに戻す］を使用すると、仮想マシンの現在の状態の親スナップショットが起動します。

［戻す］

スナップショット ツリー内の任意のスナップショットをリストアし、そのスナップショットを、仮想マシンの現在の状態の親スナップショットにすることができます。このポイント以降でスナップショットを作成すると、スナップショット ツリーに新しい分岐が作成されます。

スナップショットをリストアすると、次のような影響が及ぼされます。

- 現在のディスクおよびメモリの状態は破棄され、仮想マシンは、親スナップショットのディスクおよびメモリの状態に戻ります。
- 既存のスナップショットは移動されません。これらのスナップショットはいつでもリストアできます。
- スナップショットにメモリ状態が含まれている場合、仮想マシンはスナップショットを作成したときの電源状態と同じ状態になります。

表 4-2. スナップショットをリストアした後の仮想マシンの電源状態

親スナップショット作成時の仮想マシンの状態	リストア後の仮想マシンの状態
パワーオン状態 （メモリを含む）	親スナップショットに戻り、仮想マシンはパワーオンになって、実行されます。
パワーオン状態 （メモリは含まない）	親スナップショットに戻り、仮想マシンはパワーオフになります。
パワーオフ状態 （メモリは含まない）	親スナップショットに戻り、仮想マシンはパワーオフになります。

特定のタイプのワークロードを実行している仮想マシンの場合、スナップショットから復帰して操作がレジュームされるまで数分かかる場合があります。

注： vApp にある仮想マシンの vApp メタデータは、仮想マシン構成のスナップショットのセマンティックに従っていません。このため、スナップショット作成後に削除、変更、または定義された vApp プロパティは、仮想マシンがそのスナップショット、またはそれ以前のスナップショットに戻されてもそのまま （削除、変更、または定義されたまま） となります。

前提条件

その仮想マシンに対する仮想マシン.スナップショット管理.スナップショットに戻す権限を持っていることを確認します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リストの仮想マシンを右クリックし、[スナップショット] - [スナップショットのリストア] の順に選択します。

注： スナップショットに保存しない限り、仮想マシンの現在の状態は失われます。

3 [リストア] をクリックして、仮想マシンを最新のスナップショットに戻します。

VMware Host Client での、スナップショットの削除

スナップショット マネージャを使用して、1 つのスナップショットを削除するか、ツリー内のすべてのスナップショットを削除できます。スナップショットを削除すると、そのスナップショットはスナップショット マネージャから消去されます。スナップショット ファイルは、統合されてスナップショット ディスクに書き込まれ、仮想マシンのベース ディスクにマージされます。

スナップショットを削除しても、仮想マシンや別のスナップショットは変更されません。スナップショットを削除すると、スナップショットと前回のディスク状態との差分が統合され、削除されたスナップショットに関する情報が含まれている差分ディスクのすべてのデータが親ディスクに書き込まれます。ベース親スナップショットを削除すると、すべての変更内容は、ベース仮想マシン ディスクにマージされます。

スナップショットを削除するには、大量の情報を読み取り、ディスクに書き込む必要があります。そのプロセスにより、統合が完了するまで、仮想マシンのパフォーマンスが低下する可能性があります。スナップショットを統合すると冗長ディスクが削除されます。これにより、仮想マシンのパフォーマンスが向上し、ストレージ容量を節約できます。スナップショットの削除とスナップショット ファイルの統合にかかる時間は、最後にスナップショットを作成してからゲスト OS が仮想ディスクに書き込むデータの量によって異なります。必要な時間は、統合中に仮想マシンが書き込むデータの量に比例します （仮想マシンがパワーオン状態の場合）。

ディスクの統合に失敗すると、仮想マシンのパフォーマンスが低下する可能性があります。リストを表示して、統合操作を別途実行する必要がある仮想マシンがあるかどうかを確認できます。複数の仮想マシンの統合状態を表示して判別し、統合操作を別途実行する方法については、vSphere の仮想マシン管理を参照してください。

[削除]

スナップショット ツリーから 1 つの親スナップショットまたは子スナップショットを削除するには、[削除] オプションを使用します。[削除] オプションでは、スナップショットの状態と以前のディスク状態との差分が親スナップショットに書き込まれます。

注： 1 つのスナップショットを削除する場合、仮想マシンの現在の状態は保持され、その他のスナップショットに影響はありません。

[削除] オプションを使用して、破損したスナップショットとそのファイルを、親スナップショットにマージせずに、スナップショット ツリーの破棄された分岐から削除することもできます。

[すべて削除]

スナップショット マネージャからすべてのスナップショットを削除するには、[すべて削除] オプションを使用します。[すべて削除] オプションでは、スナップショットと前回の差分ディスクの状態との差分が統合されてベース親ディスクに書き込まれ、ベース仮想マシン ディスクにマージされます。

アップデートやインストールに失敗した場合などに、スナップショット ファイルが親スナップショットとマージされないようにするには、まず [リストア] コマンドを使用して、前回のスナップショットにリストアします。この操作により、スナップショットの差分ディスクが無効にされ、メモリ ファイルが削除されます。続いて、[削除] オプションを使用して、スナップショットとそれに関連するファイルを削除します。

必要なスナップショットを誤って削除しないように注意してください。削除したスナップショットをリストアすることはできません。たとえば、a、b、c の複数のブラウザをインストールする必要があり、各ブラウザのインストール後に仮想マシンの状態を取得するとします。最初のスナップショット （またはベース スナップショット） にはブラウザ a を含む仮想マシンが取得され、2 番目のスナップショットにはブラウザ b が取得されます。ブラウザ a を含むベース スナップショットをリストアし、ブラウザ c を含む 3 番目のスナップショットを取得し、ブラウザ b を含むスナップショットを削除した場合、ブラウザ b を含む仮想マシンの状態に戻ることはできません。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リストの仮想マシンを右クリックし、[スナップショット] - [スナップショットの管理] の順に選択します。
3. 削除するスナップショットをクリックし、[スナップショットの削除] をクリックします。
4. （オプション） [スナップショットの削除] ダイアログ ボックスで [すべての子スナップショットを削除します。] チェック ボックスを有効にして、選択したスナップショットと、そのすべての子スナップショットを削除します。
5. [削除] をクリックし、削除することを確認します。
6. [閉じる] をクリックしてスナップショット マネージャから移動します。

スナップショットの削除

スナップショットを削除すると、そのスナップショットはスナップショット マネージャから消去されます。スナップショット ファイルは、統合されてスナップショット ディスクに書き込まれ、仮想マシンのベース ディスクにマージされます。

スナップショットを削除しても、仮想マシンや別のスナップショットは変更されません。スナップショットを削除すると、スナップショットと前回のディスク状態との差分が統合され、削除されたスナップショットに関する情報が含まれている差分ディスクのすべてのデータが親ディスクに書き込まれます。ベース親スナップショットを削除すると、すべての変更内容は、ベース仮想マシン ディスクにマージされます。

スナップショットを削除するには、大量の情報を読み取り、ディスクに書き込む必要があります。そのプロセスにより、統合が完了するまで、仮想マシンのパフォーマンスが低下する可能性があります。スナップショットを統合すると冗長ディスクが削除されます。これにより、仮想マシンのパフォーマンスが向上し、ストレージ容量を節約できます。スナップショットの削除とスナップショット ファイルの統合にかかる時間は、最後にスナップショットを作成してからゲスト OS が仮想ディスクに書き込むデータの量によって異なります。必要な時間は、統合中に仮想マシンが書き込むデータの量に比例します （仮想マシンがパワーオン状態の場合）。

ディスクの統合に失敗すると、仮想マシンのパフォーマンスが低下する可能性があります。リストを表示して、統合操作を別途実行する必要がある仮想マシンがあるかどうかを確認できます。複数の仮想マシンの統合状態を表示して判別し、統合操作を別途実行する方法については、vSphere の仮想マシン管理 を参照してください。

[削除]

スナップショット ツリーから 1 つの親スナップショットまたは子スナップショットを削除するには、[削除] オプションを使用します。[削除] オプションでは、スナップショットの状態と以前のディスク状態との差分が親スナップショットに書き込まれます。

注： 1 つのスナップショットを削除する場合、仮想マシンの現在の状態は保持され、その他のスナップショットに影響はありません。

[削除] オプションを使用して、破損したスナップショットとそのファイルを、親スナップショットにマージせずに、スナップショット ツリーの破棄された分岐から削除することもできます。

[すべて削除]

スナップショット マネージャからすべてのスナップショットを削除するには、[すべて削除] オプションを使用します。[すべて削除] オプションでは、スナップショットと前回の差分ディスクの状態との差分が統合されてベース親ディスクに書き込まれ、ベース仮想マシン ディスクにマージされます。

アップデートやインストールに失敗した場合などに、スナップショット ファイルが親スナップショットとマージされないようにするには、まず [リストア] コマンドを使用して、前回のスナップショットにリストアします。この操作により、スナップショットの差分ディスクが無効にされ、メモリ ファイルが削除されます。続いて、[削除] オプションを使用して、スナップショットとそれに関連するファイルを削除します。

VMware Host Client でスナップショット マネージャを使用する理由

仮想マシンのすべてのスナップショットを表示し、スナップショット マネージャを使用してそれらのスナップショットを管理することができます。

スナップショットを作成した後で、仮想マシンを右クリックし、[スナップショットに戻す] をクリックすると、その仮想マシンをスナップショットの状態にいつでも戻すことができます。

一連のスナップショットがある場合は、スナップショット マネージャを使用して、任意の親スナップショットまたは子スナップショットをリストアできます。リストアされたスナップショットから作成される子スナップショットにより、スナップショット ツリーの分岐が作成されます。ツリーからスナップショットを削除するには、スナップショット マネージャを使用します。

表 4-3. スナップショット マネージャ

オプション	説明
スナップショット ツリー	仮想マシンのすべてのスナップショットが表示されます。
[現在地点] アイコン	[現在点] アイコンは、仮想マシンの現在のアクティブな状態を表します。 [リストア]、[削除]、および [編集] の各アクションは、[現在点] 状態では無効になります。
[取得]、[リストア]、[削除]、[編集]	スナップショットのオプション。
詳細	スナップショットの名前と説明、スナップショットの作成日を表示します。コンソールには、スナップショット作成時の仮想マシンの電源状態が表示されます。スナップショットを選択していない場合、[名前]、[説明]、[作成] テキスト ボックスは空です。

VMware Host Client での仮想マシンの監視

VMware Host Client では、作成した仮想マシンについて、そのパフォーマンスのさまざまな要素を監視したり、実行されるアクションを追跡したりできます。

VMware Host Client での仮想マシンのパフォーマンス チャートの表示

VMware Host Client で作成した仮想マシンのリソース使用率に関する情報を、線グラフで表示できます。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンをクリックします。
3. VMware Host Client インベントリ内で仮想マシンを展開し、[監視] をクリックします。
4. [パフォーマンス] をクリックします。
5. 過去 1 時間分の仮想マシンのリソース使用率を表示するには、ドロップダウン メニューからオプションを選択します。
   - 過去 1 時間に仮想マシンが使用した CPU のパーセント値を表示するには、[CPU 使用率] を選択します。
   - 過去 1 時間にホストが消費したメモリを表示するには、[メモリ使用率] を選択します。

VMware Host Client での仮想マシン イベントの表示

イベントは、ユーザーが仮想マシンに対して実行するアクションの記録です。VMware Host Client で仮想マシンを作成する際に、仮想マシンと関連付けられているイベントを表示できます。

前提条件

必要な権限：読み取り専用.

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンをクリックします。

3 VMware Host Client インベントリ内で仮想マシンを展開し、[監視] をクリックします。

4 [イベント] をクリックします。

すべての仮想マシン イベントのリストが表示されます。

5 （オプション） リスト内のイベントをクリックして、イベントの詳細を表示します。

6 （オプション） リストの上にあるフィルタ コントロールを使用して、リストをフィルタリングします。

7 （オプション） 列見出しをクリックしてリストをソートします。

VMware Host Client での仮想マシン タスクの表示

VMware Host Client で仮想マシンを作成するときに、すべての仮想マシン タスクと、タスク ターゲット、開始者、キュー時刻、開始時刻、結果、および完了時刻に関する情報を表示できます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンをクリックします。

3 VMware Host Client インベントリ内で仮想マシンを展開し、[監視] をクリックします。

4 [タスク] をクリックします。

5 （オプション） 詳細を表示するタスクをリスト内でクリックします。

6 （オプション） リストの上にあるフィルタ コントロールを使用して、リストをフィルタリングします。

7 （オプション） 列見出しをクリックしてリストをソートします。

VMware Host Client での仮想マシン ログ ブラウザの表示

VMware Host Client を使用して、管理対象ホストのログを生成し、監視します。ホスト環境におけるさまざまな問題は、ログを使用して診断およびトラブルシューティングします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンをクリックします。

3 VMware Host Client インベントリ内で仮想マシンを展開し、[監視] をクリックします。

4 [ログ] をクリックします。

5 （オプション） トラブルシューティング用にすべてのログを統合するには、[サポート バンドルの生成] をクリックします。

6 ログを表示するには、リスト内のログを右クリックし、[新しいウィンドウで開く] を選択します。

VMware Host Client での仮想マシン通知の表示

VMware Host Client で、作成する仮想マシンについて、仮想マシン通知と、実行可能な関連タスクに関する情報を表示できます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンをクリックします。

3 VMware Host Client インベントリ内で仮想マシンを展開し、[監視] をクリックします。

4 [通知] をクリックします。

すべての仮想マシン通知が示されたリストが表示されます。

5 （オプション） 詳細を表示する通知をクリックします。

6 （オプション） 通知をクリックし、[アクション] をクリックして推奨されるタスクを表示します。

VMware Host Client での仮想マシン ハードウェアの構成

5

この章には、次のトピックが含まれています。

仮想 CPU 構成

CPU リソースを追加、変更、または構成し、仮想マシンのパフォーマンスを向上できます。ほとんどの CPU パラメータは、仮想マシンの作成時にも、ゲスト OS のインストール後にも設定できます。操作によっては、仮想マシンをパワーオフしないと設定を変更できないものがあります。

VMware では次の用語が使用されます。これらの用語を理解しておくと、CPU リソースの割り当て方法を計画するのに役立ちます。

CPU

CPU（プロセッサ）は、コンピュータのアプリケーションを動作させるために必要なタスクを実行するコンピュータ システムのコンポーネントです。CPU は、コンピュータの機能を実行する主要要素です。CPU にはコアが含まれています。

CPU ソケット

CPU ソケットはコンピュータ マザーボード上の物理コネクタであり、単一の物理 CPU に接続します。一部のマザーボードには複数のソケットがあり、複数のマルチコア プロセッサ (CPU) を接続できます。

コア

コアは、L1 キャッシュと、アプリケーションの実行に必要な機能ユニットが含まれた 1 個のユニットで構成されます。コアはアプリケーションまたはスレッドを独立して実行できます。1 つの CPU に複数のコアを搭載できます。

リソース共有

共有は、仮想マシン （またはリソース プール） の相対的な優先順位または重要度を指定します。ある仮想マシンのリソース共有が別の仮想マシンの 2 倍である場合、その仮想マシンは、別の仮想マシンの 2 倍のリソースを使用できます（2 台の仮想マシンがリソースを獲得するために競合する場合）。

リソースの割り当て

使用可能なリソース キャパシティが需要を満たさない場合、共有、予約、制限などの CPU リソース割り当て設定を変更できます。たとえば、年末に経理のワークロードが増加した場合は、経理のリソース プールの予約量を増加できます。

vSphere Virtual SMP （Virtual Symmetric Multiprocessing）

Virtual SMP (vSphere Virtual Symmetric Multiprocessing) は、単一の仮想マシンで複数のプロセッサを使用できるようにする機能です。

仮想 CPU の制限

仮想マシンに割り当てることができる仮想 CPU の最大数は 768 です。仮想 CPU の数は、ホストの論理 CPU 数、および仮想マシンにインストールされたゲスト OS の種類によって決まります。

次の制限を認識しておく必要があります。

- 仮想マシンで構成できる仮想 CPU の数は、ホストに実装される論理コアの数が上限となります。論理コアの数は、ハイパースレッディングが無効な場合は物理コアの数と同じになり、ハイパースレッディングが有効な場合は物理コアの数の 2 倍になります。
- 実行中の仮想マシンに搭載されている仮想 CPU が 128 個以下の場合は、ホット アドを使用して仮想 CPU の数をさらに増やすことはできません。仮想 CPU の数を制限を超えた値に変更するには、まず仮想マシンをパワーオフする必要があります。これに対して、実行中の仮想マシンの既存の仮想 CPU が 128 個を超えている場合は、ホット アドを使用して仮想 CPU の数を 768 個まで増やすことができます。
- 仮想マシンに搭載できる仮想 CPU ソケットの最大数は 128 です。仮想マシンに 128 個を超える仮想 CPU を構成する場合は、マルチコア仮想 CPU を使用する必要があります。
- すべてのゲスト OS が Virtual SMP をサポートしているわけではありません。この機能をサポートするゲスト OS は、ホストで使用可能な数よりも少ないプロセッサしかサポートしない場合があります。Virtual SMP のサポートの詳細については、http://www.vmware.com/resources/compatibility にある『VMware 互換性ガイド』 を参照してください。

マルチコア仮想 CPU の構成

VMware のマルチコア仮想 CPU のサポートにより、仮想マシン内の仮想ソケットあたりのコア数を制御できます。この機能を使用すると、ソケットに制限のあるオペレーティング システムで使用されるホスト CPU のコア数が増えて、全体的なパフォーマンスが向上します。

重要： 仮想マシンでマルチコア仮想 CPU 設定を構成する場合は、構成がゲスト OS EULA の要件に準拠するようにしてください。

仮想マルチコア CPU は、CPU ソケットの数が制限されているオペレーティング システムやアプリケーションを実行する場合に役立ちます。

ESXi 7.0 Update 1 以降と互換性のある仮想マシンは、最大 768 個の仮想 CPU を搭載するように構成できます。仮想マシンで構成できる仮想 CPU の数は、ホストに実装される論理 CPU の実際の数が上限となります。論理 CPU の数は、物理プロセッサ コアの数、またはハイパースレッディングが有効な場合はその 2 倍の数を示します。たとえば、ホストに 128 個の論理 CPU がある場合、仮想マシンに 128 個の仮想 CPU を構成できます。

コアおよびソケットごとのコアに関する、仮想 CPU の割り当て方法を構成します。シングルコア CPU、デュアルコア CPU、トライコア CPU などを使用するかどうかに応じて、仮想マシンに必要な CPU コアの数を指定してから、各ソケットに必要なコアの数を選択します。これを選択することで、仮想マシンが持つソケットの数が指定されます。

仮想マシンに搭載できる仮想 CPU ソケットの最大数は 128 です。仮想マシンに 128 個を超える仮想 CPU を構成する場合は、マルチコア仮想 CPU を使用する必要があります。

マルチコア CPU の詳細については、『vSphere のリソース管理』ドキュメントを参照してください。

仮想 CPU 数の変更

ESXi 7.0 Update 1 以降と互換性のある仮想マシンには、最大 768 個の仮想 CPU を搭載できます。仮想マシンのパワーオフ時に、仮想 CPU の数を変更できます。仮想 CPU のホット アドが有効になっている場合は、仮想マシンの実行中に仮想 CPU の数を増やすことができます。

仮想 CPU ホット アドは、ESXi 5.0 以降と互換性のある、マルチコア CPU 対応の仮想マシンでサポートされます。仮想マシンがパワーオン状態になっていて、CPU ホット アドが有効な場合は、実行中の仮想マシンに仮想 CPU をホット アドすることができます。ソケットごとに、コアの数の倍数のみを追加できます。

仮想マシンに搭載されている仮想 CPU が 128 個以下の場合は、ホット アドを使用して仮想 CPU の数をさらに増やすことはできません。仮想 CPU の数を制限を超えた値に変更するには、まず仮想マシンをパワーオフする必要があります。これに対して、仮想マシンの既存の仮想 CPU が 128 個を超えている場合は、ホット アドを使用して仮想 CPU の数を 768 個まで増やすことができます。

仮想マシンに搭載できる仮想 CPU ソケットの最大数は 128 です。仮想マシンに 128 個を超える仮想 CPU を構成する場合は、マルチコア仮想 CPU を使用する必要があります。

重要： 仮想マシンでマルチコア仮想 CPU 設定を構成する場合は、構成がゲスト OS EULA の要件に準拠するようにしてください。

前提条件

- CPU のホット アドが有効になっていない場合は、仮想 CPU を追加する前に仮想マシンをパワーオフします。
- マルチコア CPU のホット アドを実行するには、仮想マシンが ESXi 5.0 以降との互換性があることを確認します。
- 仮想マシン.構成.CPU カウントの変更権限を持っていることを確認します。

手順

1 インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] タブで、[CPU] を展開します。

3 [CPU] ドロップダウン メニューから、コアの数を選択します。

4 [ソケットあたりのコア] ドロップダウン メニューから、ソケットあたりのコアの数を選択し、[OK] をクリックします。

VMware Host Client での、CPU リソースの割り当て

シェア、予約、制限の各設定を使用することで、ワークロード需要を管理するために、仮想マシンに割り当てられる CPU リソースの量を変更できます。

仮想マシンにある次のユーザー定義の設定が、CPU リソース割り当てに影響を与えます。

制限

仮想マシンの CPU 時間の消費量に制限を設けます。この値は MH z または GHz で表します。

予約

仮想マシンに保証される最小割り当てを指定します。予約は MH z または GHz で表します。

シェア

各仮想マシンに CPU シェアが割り当てられます。仮想マシンに割り当てられるシェアが増えると、CPU のアイドル時間がない場合に、その仮想マシンはより多くの CPU タイム スライスを取得します。シェアは、割り当てる CPU 容量の相対的なメトリックを表します。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[CPU] を展開し、仮想マシンの CPU キャパシティを割り当てます。

オプション	説明
予約	この仮想マシン用に確保されている CPU の割り当て。
制限	この仮想マシンに割り当てる CPU の上限。制限を指定しない場合は、[制限なし] を選択します。
シェア	親の合計リソースに関連するこの仮想マシンの CPU シェア。兄弟仮想マシンは、予約と制限の範囲内で、相対的なシェア値に従ってリソースを共有します。[低]、[標準]、または [高] を選択します。これらの値はそれぞれ 1:2:4 の割合でシェア値を指定します。各仮想マシンに対して、比重に見合う特定のシェア値を指定するには、[カスタム] を選択します。

4 [[保存]] をクリックします。

仮想メモリの構成

仮想マシンのメモリ リソースまたはオプションを追加、変更、または構成し、仮想マシンのパフォーマンスを向上できます。ほとんどのメモリ パラメータは、仮想マシンの作成中にも、ゲスト OS のインストール後にも設定できます。操作によっては、仮想マシンをパワーオフしないと設定を変更できないものがあります。

仮想マシンのメモリ リソース設定では、仮想マシンに割り当てるホストのメモリの容量を特定します。仮想ハードウェアのメモリ サイズでは、仮想マシンで実行されるアプリケーションで使用可能なメモリの容量を特定します。仮想マシンは、仮想ハードウェアのメモリ サイズとして構成されたメモリ リソース以上のメモリ リソースを利用できません。ESXi ホストでは、仮想マシンで最大に使用できるメモリ リソース容量を制限しているため、メモリ リソースの設定をデフォルトの「制限なし」のままにすることができます。

メモリ構成の変更

仮想マシンに割り当てられたメモリ容量を再構成して、パフォーマンスを向上させることができます。

BIOS ファームウェアを使用した仮想マシンの最小メモリ サイズは 4 MB です。EFI ファームウェアを使用する仮想マシンには、少なくとも 96 MB の RAM が必要で、足りない場合はパワーオンできません。

BIOS ファームウェアを使用した仮想マシンの最大メモリ サイズは 24560 GB です。メモリ サイズが 6,128 GB を超える仮想マシンには、EFI ファームウェアを使用する必要があります。

仮想マシンの最大メモリ サイズは、ESXi ホストの物理メモリおよび仮想マシンの互換性の設定によって異なります。

仮想マシンのメモリがホストのメモリ サイズより大きい場合は、スワップが発生し、仮想マシンのパフォーマンスに重大な影響を与えることがあります。最適なパフォーマンスを得るための最大値がしきい値です。この値を超えると ESXi ホストの物理メモリが不足し、仮想マシンを最大速度で実行できなくなります。この値は、ホストの状況の変化 （たとえば、仮想マシンがパワーオンまたはパワーオフにされた場合など） に応じて変動します。

指定できるメモリ サイズは 4 MB の倍数です。

表 5-1. 仮想マシンの最大メモリ

ホスト バージョンで導入	仮想マシンの互換性	最大メモリ サイズ
ESXi 8.0	ESXi 8.0 以降	24560 GB
ESXi 7.0 Update 3	ESXi 7.0 Update 3 以降	24560 GB
ESXi 7.0 Update 2	ESXi 7.0 Update 2 以降	24560 GB
ESXi 7.0 Update 1	ESXi 7.0 Update 1 以降	24560 GB
ESXi 7.0	ESXi 7.0 以降	6128 GB
ESXi 6.7 Update 2	ESXi 6.7 Update 2 以降	6128 GB
ESXi 6.7	ESXi 6.7 以降	6128 GB
ESXi 6.5	ESXi 6.5 以降	6128 GB
ESXi 6.0	ESXi 6.0 以降	4080 GB

ESXi ホストのバージョンは、メモリ サイズ増加のサポートを開始したバージョンを示しています。たとえば、ESXi 6.5 で実行されている ESXi バージョン 6.0 以降の互換性を持つ仮想マシンのメモリ サイズは 4080 GB に制限されます。

前提条件

仮想マシン上で 仮想マシン.設定.メモリの変更の権限があることを確認します。

手順

1 インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] タブで [メモリ] を展開し、メモリの設定を変更します。

   a [メモリ] テキスト ボックスに、仮想マシンに割り当てる RAM の量を入力します。

   b メモリを MB、GB、TB のいずれで指定するかを選択します。

3 [OK] をクリックします。

メモリ リソースの割り当て

シェア、予約、制限の各設定を使用すると、仮想マシンに割り当てられるメモリ リソースの量を変更できます。ホストはこれらの設定を基にして、仮想マシンに割り当てる物理 RAM の最適な容量を決定します。負荷およびステータスに応じて、仮想マシンに高いまたは低いシェア値を割り当てることができます。

次のユーザー定義の設定が、仮想マシンのメモリ リソース割り当てに影響を与えます。

制限

仮想マシンのメモリの消費量に制限を設けます。値はメガバイトで表します。

予約

仮想マシンに保証される最小割り当てを指定します。予約はメガバイトで表します。予約を満たせない場合、仮想マシンはパワーオンされません。

シェア

各仮想マシンに割り当てられるメモリ シェア数です。仮想マシンのシェアが多いほど、仮想マシンが受け取るホスト メモリのシェアも大きくなります。シェアは、割り当てるメモリ容量の相対的なメトリックを表します。シェア値の詳細については、『vSphere リソース管理』 ドキュメントを参照してください。

構成されたメモリよりも大きい値の予約を仮想マシンに割り当てることはできません。仮想マシンに大量のメモリを予約し、構成されたメモリ サイズを小さくすると、新しく構成されたメモリ サイズに適合するように予約サイズが小さくなります。

前提条件

仮想マシンがパワーオフしていることを確認します。

手順

1 インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] タブで、[メモリ] を展開し、仮想マシンのメモリ容量を割り当てます。

オプション	説明
予約	この仮想マシン用に確保されているメモリの割り当て。
制限	この仮想マシンに割り当てるメモリの上限。制限を指定しない場合は、[制限なし] を選択します。
シェア	[低]、[標準]、[高]、[カスタム] の各値が、サーバ上のすべての仮想マシンのすべてのシェアの合計と比較されます。

3 [OK] をクリックします。

メモリのホット アド設定の変更

メモリのホット アドでは、仮想マシンがパワーオン状態のまま、その仮想マシンのメモリ リソースを追加できます。

メモリのホット アドを有効にすると、仮想マシンの ESXi ホストに多少のメモリ オーバーヘッドが生じます。

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンに、メモリのホット アド機能をサポートするゲスト OS があることを確認します。
- 仮想マシンに ESXi 4.x 以降との互換性があることを確認します。
- VMware Tools がインストールされていることを確認します。

手順

1 インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] タブで、[メモリ] を展開し、[有効化] を選択して、パワーオン時の仮想マシンへのメモリの追加を有効にします。

3 [OK] をクリックします。

結果

これで、仮想マシンがパワーオンの状態のときにもメモリを仮想マシンに追加できます。

注： NVIDIA vGPU を備えた仮想マシンにメモリをホット アドするには、ESXi ホストに vGPU の空きスロットが必要です。

VMware Host Client での仮想マシンへの NVDIMM デバイスの追加

仮想マシンに仮想 NVDIMM デバイスを追加すると、不揮発性メモリまたは永続的なコンピュータ メモリを使用できます。不揮発性メモリ (NVM)、または永続的なメモリ (PMEM) は、揮発性メモリの高いデータ転送速度と、従来のストレージの永続性および回復性を組み合わせたものです。仮想 NVDIMM デバイスは、再起動時や電源に問題が発生した場合に、格納したデータを保持できる仮想 NVM デバイスです。

仮想マシンは、NVDIMM (Virtual Non-volatile Dual In-line Memory Module)、または永続的な仮想メモリ ディスクを介して、ホストの PMEM リソースを使用します。

永続的なメモリの詳細については、永続的なメモリの管理を参照してください。

前提条件

- 仮想マシンのゲスト OS が PMEM をサポートしていることを確認します。
- 仮想ハードウェアのバージョンが 14 以降であることを確認します。
- データストア.容量の割り当て権限を持っていることを確認します。
- 仮想マシンを稼動するホストまたはクラスタに、使用可能な PMEM リソースがあることを確認します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] をクリックし、ドロップダウン メニューから [NVDIMM] を選択します。

仮想ハードウェア デバイスのリストに NVDIMM デバイスが表示されます。各仮想マシンには、最大 64 個の NVDIMM デバイスを配置できます。

4 新しく追加した NVDIMM デバイスを構成します。

a 仮想ハードウェア デバイスのリストで、[新しい NVDIMM] を展開します。

b 新しい NVDIMM デバイスのサイズを入力します。

注： NVDIMM デバイスのサイズは後で変更できます。仮想マシンをパワーオフする必要があります。

c NVDIMM コントローラの場所を選択するか、デフォルトのままにします。

5 ウィザードを終了して、[保存] をクリックします。

仮想マシンのネットワーク構成

ESXi のネットワーク機能では、同一ホスト上の仮想マシン間、異なるホスト上の仮想マシン間、他の仮想マシンおよび物理マシン間の通信が可能になります。

このネットワーク機能では、ESXi ホストの管理も可能で、VMkernel サービス（NFS、iSCSI、vSphere vMotion など）と物理ネットワーク間の通信も可能になります。仮想マシンのネットワークを構成するときは、アダプタ タイプ、ネットワーク接続、および仮想マシンをパワーオンしたときにネットワークに接続するかどうかを選択、または変更します。

ネットワーク アダプタの基本

仮想マシンを構成するときに、ネットワーク アダプタ （NIC） を追加し、アダプタ タイプを指定できます。

ネットワーク アダプタ タイプ

ネットワーク アダプタのタイプは、次の要因を条件として利用可能になります。

- 仮想マシンの互換性。これは、仮想マシンを作成したホスト、または最近仮想マシンを更新したホストに依存します。
- 仮想マシンの互換性が、現在のホストの最新バージョンに更新されているかどうか。
- ゲスト OS。

現在サポートされている NIC は、オンプレミス環境と VMware Cloud on AWS とで異なります。オンプレミス環境では、次の NIC タイプがサポートされています。

E1000E

Intel 82574 ギガビット イーサネット NIC のエミュレート バージョンです。E1000E は、Windows 8 および Windows Server 2012 のデフォルト アダプタです。

E1000

Intel 82545EM ギガビット イーサネット NIC のエミュレート バージョンです。Windows XP 以降および Linux バージョン 2.4.19 以降を含む、ほとんどの新しいゲスト OS で利用可能なドライバを備えています。

Flexible

仮想マシンの起動時には Vlance アダプタとして認識されますが、初期化され、Vlance アダプタまたは VMXNET アダプタとして機能します （初期化するドライバによる）。VMware Tools がインストールされていると、VMXNET ドライバは Vlance アダプタを高パフォーマンスの VMXNET アダプタに変更します。

Vlance

AMD 79C970 PCnet32 LANCE NIC のエミュレート バージョンです。32 ビット レガシー ゲスト OS で利用可能なドライバを備えた旧型の 10 Mbps NIC です。このネットワーク アダプタで構成された仮想マシンは、すぐにそのネットワークを使用できます。

VMXNET

仮想マシンのパフォーマンス向けに最適化されています。物理的にこれに対応するものはありません。オペレーティング システム ベンダーはこのカード用の組み込みドライバを提供していないため、VMware Tools をインストールして、VMXNET ネットワーク アダプタを利用するためのドライバを取得する必要があります。

VMXNET 2 （拡張）

VMXNET アダプタを基盤としていますが、最近のネットワークで一般的に使用される高パフォーマンス機能（ジャンボ フレームやハードウェア オフロードなど）を提供します。VMXNET 2（拡張）は、ESX/ESXi 3.5 以降にある一部のゲスト OS でのみ使用可能です。

VMXNET 3

パフォーマンス向上のために設計された、準仮想化 NIC です。VMXNET 3 は VMXNET 2 で使用可能なすべての機能を提供し、さらに、マルチキュー サポート （Windows では Receive Side Scaling とも呼ばれる）、IPv6 オフロード、および MSI/MSI-X 割り込み配信などのいくつかの新機能も提供します。VMXNET 3 は VMXNET または VMXNET 2 を基盤にしていません。

PVRDMA

OFED Verbs API を介して仮想マシン間のリモート ダイレクト メモリ アクセス (RDMA) をサポートする準仮想化 NIC。すべての仮想マシンに PVRDMA デバイスが必要で、分散スイッチに接続されている必要があります。PVRDMA は VMware vSphere vMotion およびスナップショット テクノロジーをサポートします。ハードウェア バージョン 13 およびゲスト OS の Linux カーネル 4.6 以降の仮想マシンで利用可能です。

仮想マシンへの PVRDMA ネットワーク アダプタの割り当てについては、『vSphere のネットワーク』ドキュメントを参照してください。

SR-IOV パススルー

SR-IOV をサポートする物理 NIC の仮想機能 （VF） の表現。仮想マシンと物理アダプタは、VMkernel を中継せずにデータを交換します。このアダプタ タイプは、遅延によって障害が発生したり、必要な CPU リソースが増加したりする可能性のある仮想マシンに適しています。

SR-IOV パススルーは、ESXi 6.0 以降の場合に Red Hat Enterprise Linux 6 以降および Windows Server 2008 R2 SP2 のゲスト OS で使用できます。オペレーティング システム リリースには特定の NIC のデフォルトの VF ドライバが装備されている場合がありますが、それ以外では NIC またはホストのベンダーが指定した場所からドライバをダウンロードし、インストールする必要があります。

SR-IOV パススルー ネットワーク アダプタを仮想マシンに割り当てる方法の詳細については、『vSphere のネットワーク』 ドキュメントを参照してください。

ネットワーク アダプタの互換性に関する考慮事項については、http://www.vmware.com/resources/compatibility の 『VMware 互換性ガイド』 を参照してください。

レガシー ネットワーク アダプタと ESXi の仮想ハードウェア バージョン

すべてのレガシー仮想マシンのデフォルトのネットワーク アダプタ タイプは、アダプタの使用可否、ゲスト OS との互換性、および仮想マシンが作成された仮想ハードウェアのバージョンに応じて変わります。

仮想ハードウェア バージョンを使用する仮想マシンをアップグレードしない場合、アダプタの設定は変更されません。最新の仮想ハードウェアを活用できるよう仮想マシンをアップグレードすると、デフォルトのアダプタ設定が変更されてゲスト OS およびアップグレードされたホスト ハードウェアと互換性を持つようになる場合があります。

サポートされているゲスト OS で使用可能な、vSphere ESXi の特定のバージョン向けのネットワーク アダプタを確認するには、『VMware 互換性ガイド』（http://www.vmware.com/resources/compatibility） を参照してください。

ネットワーク アダプタおよびレガシー仮想マシン

レガシー仮想マシンは、使用中の製品でサポートされる仮想マシンですが、その製品にとって最新の仮想マシンではありません。すべてのレガシー仮想マシンのデフォルトのネットワーク アダプタ タイプは、アダプタの使用可否、ゲスト OS との互換性、および仮想マシンが作成された仮想ハードウェアのバージョンに応じて変わります。

仮想マシンをアップグレードして ESXi ホストの新しいアップグレード バージョンと対応させなければ、アダプタ設定は変わりません。最新の仮想ハードウェアを活用できるよう仮想マシンをアップグレードすると、デフォルトのアダプタ設定が変更されてゲスト OS およびアップグレードされたホスト ハードウェアと互換性を持つようになる場合があります。

サポートされているゲスト OS で使用可能な、vSphere ESXi の特定のバージョン向けのネットワーク アダプタを確認するには、『VMware 互換性ガイド』(http://www.vmware.com/resources/compatibility) を参照してください。

VMware Host Client での、仮想ネットワーク アダプタの構成の変更

仮想マシンの仮想ネットワーク アダプタについて、パワーオン接続設定、MAC アドレス、およびネットワーク接続を変更できます。

前提条件

必要な権限：

- 仮想マシン.構成.デバイス設定の変更（MAC アドレスおよびネットワークの編集用）。
- 仮想マシン.相互作用.デバイス接続（[接続] および [パワーオン時に接続] の変更用）。
- ネットワーク.ネットワークの割り当て

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブをクリックし、ハードウェア リストから該当するネットワーク アダプタ (NIC) を選択します。
4. （オプション） 仮想マシンのパワーオンの状態で仮想 NIC を接続する場合は、[パワーオン時に接続] を選択します。
5. （オプション） [アダプタ タイプ] ドロップダウン メニューからアダプタ タイプを選択します。
6. MAC アドレス構成のオプションを選択します。

オプション	説明
自動	vSphere により、MAC アドレスが自動的に割り当てられます。
手動	使用する MAC アドレスを入力します。

7. [[保存]] をクリックします。

VMware Host Client での、仮想マシンへのネットワーク アダプタの追加

ネットワーク アダプタ (NIC) を仮想マシンに追加する場合は、アダプタ タイプやネットワーク接続を選択し、仮想マシンのパワーオン時にデバイスを接続するかどうかを選択する必要があります。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブをクリックし、[ネットワーク アダプタの追加] をクリックします。

4 ネットワーク接続パネルで、特定のラベルが付いたネットワークまたはレガシー ネットワークを選択します。

5 （オプション）仮想マシンのパワーオン時に仮想 NIC を接続するように構成するには、[パワーオン時に接続] を選択します。

6 [[保存]] をクリックします。

仮想ディスクの構成

仮想マシンが実行中であっても、仮想マシンにキャパシティの大きい仮想ディスクを追加したり、既存のディスクに容量を追加したりできます。ほとんどの仮想ディスク パラメータは、仮想マシンの作成中にも、ゲスト OS のインストール後にも設定できます。

仮想マシンのデータは、新しい仮想ディスク、既存の仮想ディスク、マッピングされた SAN LUN に格納できます。仮想ディスクは、ゲスト OS に対し、単一のハード ディスクとして提示されます。仮想ディスクは、ホスト ファイル システム上の 1 つ以上のファイルで構成されます。仮想ディスクは、同じホスト上またはホスト間でコピーまたは移動できます。

ESXi ホスト上で実行される仮想マシンでは、仮想ディスク ファイルを使用せずに、仮想マシンのデータを直接 SAN LUN 上に格納できます。このオプションは、ストレージ デバイスの物理的特性の検出が必要なアプリケーションを仮想マシンで実行する場合に有効です。SAN LUN をマッピングすると、既存の SAN コマンドを使用してディスクのストレージを管理することも可能になります。

VMFS ボリュームに LUN をマッピングすると、vCenter Server または ESXi ホストによって Raw LUN を示す Raw デバイス マッピング (RDM) ファイルが作成されます。ファイルに含まれるディスク情報をカプセル化すると、vCenter Server または ESXi ホストで LUN をロックし、1 台の仮想マシンのみが書き込みを行えるようにすることができます。このファイルには `.vmdk` 拡張子が付いていますが、ESXi システム上の LUN へのマッピングを示すディスク情報のみが格納されています。実際のデータは LUN に格納されます。テンプレートから仮想マシンをデプロイしたり、仮想マシンのデータを LUN 上に格納したりすることはできません。仮想マシンのデータは、仮想ディスク ファイルにのみ格納できます。

データストアの空き容量は常に変化します。仮想マシンの作成やその他の仮想マシン操作 （スパース ファイルの拡張、スナップショットなど） のために十分な空き容量を確保しておいてください。ファイル タイプ別のデータストアの使用量については、『vSphere の監視およびパフォーマンス』 ドキュメントを参照してください。

Thin Provisioning では、最初のアクセス時に割り当てられるブロックでスパース ファイルを作成できます。これによりデータストアのオーバー プロビジョニングが可能になります。スパース ファイルが増大し続け、データストアがいっぱいになる可能性があります。仮想マシンの実行中にデータストアのディスク容量が不足すると、仮想マシンが機能しなくなる可能性があります。

仮想ディスクのプロビジョニング ポリシーについて

特定の仮想マシン管理操作を実行するときは、仮想ディスク ファイルのプロビジョニング ポリシーを指定できます。操作には、仮想ディスクの作成、テンプレートへの仮想マシンのクローン作成、仮想マシンの移行などがあります。

ハードウェア アクセラレーションに対応する NFS データストアおよび VMFS データストアでは、次のディスク プロビジョニング ポリシーをサポートします。ハードウェア アクセラレーションに対応しない NFS データストアでは、シン フォーマットのみを使用できます。

Storage vMotion またはクロス ホスト Storage vMotion を使用して、仮想ディスクのフォーマットを変換することができます。

シック プロビジョニング (Lazy Zeroed)

仮想ディスクをデフォルトのシック フォーマットで作成します。ディスクの作成時に、仮想ディスクに必要な容量が割り当てられます。物理デバイスに残っているデータは、作成中には消去されませんが、仮想マシンへ初めて書き込みを行うときに必要に応じてゼロアウトされます。仮想マシンが物理デバイスから古いデータを読み取ることはありません。

シック プロビジョニング (Eager Zeroed)

Fault Tolerance などのクラスタリング機能をサポートする、シック仮想ディスクのタイプ。仮想ディスクに必要な容量は、作成時に割り当てられます。シック プロビジョニング （Lazy Zeroed） フォーマットの場合とは異なり、物理デバイスに残っているデータは、仮想ディスクの作成時にゼロアウトされます。このフォーマットで仮想ディスクを作成する場合、他のタイプのディスクに比べて長い時間がかかることがあります。Eager Zeroed シック仮想ディスクのサイズを増やすと、仮想マシンのサスペンド時間が著しく長くなることがあります。

シン プロビジョニング

このフォーマットを使用してストレージ容量を節約します。シン ディスクの場合、入力した仮想ディスク サイズの値に応じて、ディスクに必要な容量と同じデータストア容量をプロビジョニングします。ただし、シン ディスクは最初は小さく、初期処理に必要なデータストア容量のみを使用します。シン ディスクでさらに多くの容量が必要になったら、最大容量まで拡張して、プロビジョニングされたデータストア容量全体を占有できます。

シン プロビジョニングではヘッダ情報のみのディスクを作成するため、最も短時間で仮想ディスクを作成できます。また、シン プロビジョニングでは、ストレージ ブロックの割り当ておよびゼロアウトは行われません。ストレージ ブロックは、最初にアクセスされたときに割り当ておよびゼロアウトが行われます。

注： 仮想ディスクが Fault Tolerance などのクラスタ ソリューションをサポートしている場合は、シン ディスクを作成しないでください。

VMware Host Client での、仮想ディスク構成の変更

ディスク容量が不足した場合、ディスクのサイズを増やすことができます。仮想マシンの仮想ディスク構成について、仮想デバイス ノードおよび通常モードを変更できます。

前提条件

仮想マシンをパワーオフします。

次の権限があることを確認します。

- 仮想マシン.構成.デバイス設定の変更（仮想マシン上）
- 仮想マシン.構成.仮想ディスクの拡張（仮想マシン上）
- データストア.の容量の割り当て（データストア上）

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、ハード ディスクを展開してすべてのディスク オプションを表示します。

4 （オプション） ディスクのサイズを変更するには、テキスト ボックスに新しい値を入力し、ドロップダウン メニューから単位を選択します。

5 （オプション） スナップショットによってディスクがどのように影響を受けるかを変更するには、[ディスク モード] ドロップダウン メニューからディスク モードを選択します。

オプション	説明
依存型	依存型ディスクはスナップショットに含まれます。
独立型: 通常	通常モードのディスクは、物理コンピュータ上の従来のディスクと同様に動作します。通常モードのディスクに書き込まれたすべてのデータは、永続的にこのディスクに書き込まれます。
独立型: 読み取り専用	読み取り専用モードのディスクへの変更は、仮想マシンをパワーオフまたはリセットしたときに破棄されます。読み取り専用モードでは、仮想マシンを再起動しても、仮想ディスクの状態は常に同じです。ディスクへの変更は REDO ログ ファイルに書き込まれ、このファイルから読み取られます。REDO ログ ファイルは仮想マシンのパワーオフまたはリセット時に削除されます。

6 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへの新しい標準ハード ディスクの追加

既存の仮想マシンに仮想ハード ディスクを追加することができます。また、仮想マシンの作成プロセスで、仮想マシンのハードウェアをカスタマイズするときにハード ディスクを追加することも可能です。たとえば、作業負荷の高い既存の仮想マシンにディスク容量の追加が必要な場合があります。また、仮想マシン作成中に、起動ディスクとして事前構成されたハード ディスクを追加する場合もあります。

前提条件

- 仮想ハード ディスクの追加に関する構成オプションと注意点について理解しておいてください。仮想ディスクの構成を参照してください。
- 2 TB を超えるサイズのディスクを仮想マシンに追加する前に、『vSphere の仮想マシン管理』を参照してください。
- 接続先のフォルダまたはデータストア上で 仮想マシン.設定.新規ディスクの追加の権限があることを確認します。

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 （オプション） 既存のハード ディスクを削除するには、ディスク上にマウスのポインタを移動させて、[削除] アイコン ([X]) をクリックします。

ディスクが仮想マシンから削除されます。他の仮想マシンがディスクを共有している場合は、ディスク ファイルは削除されません。

4 [仮想ハードウェア] タブで、[ハード ディスクの追加] を選択し、ドロップダウン メニューから [新規標準ハード ディスク] を選択します。

ハード ディスクが、仮想ハードウェア デバイスのリストに表示されます。

5 [新規ハード ディスク] を展開します。

6 （オプション） ハード ディスク サイズの値を入力し、ドロップダウン メニューから単位を選択します。

7 仮想マシン ファイルを保存するデータストアの場所を選択します。

8 仮想マシン ディスク用のフォーマットを選択します。

オプション	説明
シック プロビジョニング (Lazy Zeroed)	仮想ディスクをデフォルトのシック フォーマットで作成します。仮想ディスクに必要な容量は、作成時に割り当てられます。物理デバイスに残っているあらゆるデータは、作成中には消去されませんが、仮想マシンへ初めて書き込みを行うときに必要に応じてゼロアウトされます。
シック プロビジョニング (Eager Zeroed)	Fault Tolerance などのクラスタリング機能をサポートする、シック ディスクを作成します。仮想ディスクに必要な容量は、作成時に割り当てられます。フラット フォーマットの場合とは異なり、物理デバイスに残っているデータは、作成時にゼロアウトされます。ほかのタイプのディスクに比べて、ディスクの作成に非常に長い時間がかかることがあります。
シン プロビジョニング	シン プロビジョニング フォーマットを使用します。シン プロビジョニング ディスクは、まず、そのディスクが初期に必要とするデータストア容量のみを使用します。あとでシン ディスクでさらに多くの容量が必要になると、割り当てられている最大キャパシティまで拡張できます。

9 [シェア] ドロップダウン メニューで、仮想ディスクに割り当てるシェアの値を選択します。

シェアは、ディスクのバンド幅を制御するための相対的な基準を表す値です。値の低、中、高、カスタムは、ホスト上にあるすべての仮想マシンのすべてのシェアの合計と比較されます。

10 [カスタム] を選択した場合は、テキスト ボックス内にシェア数を入力します。

11 [制限 - IOPs] ボックスで、仮想マシンに割り当てるストレージ リソースの上限を入力するか、[制限なし] を選択します。

この値は、仮想ディスクに割り当てられた 1 秒あたりの I/O 操作の上限です。

12 デフォルトをそのまま使用するか、別の仮想デバイス ノードを選択します。

ほとんどの場合、デフォルトのデバイス ノードをそのまま使用できます。ハード ディスクの場合、デフォルト以外のデバイス ノードを使用すると、起動順序の制御や別の SCSI コントローラ タイプの使用が容易になります。たとえば、LSI Logic コントローラから起動し、バスの共有を有効にした Buslogic コントローラを使用してデータ ディスクを別の仮想マシンと共有できます。

13 （オプション） ディスク モードを選択します。

オプション	説明
依存型	依存型ディスクはスナップショットに含まれます。
独立型: 通常	通常モードのディスクは、従来の物理コンピュータ ディスクと同様に動作します。通常モードのディスクに書き込まれたすべてのデータは、永続的にこのディスクに書き込まれます。
独立型: 読み取り専用	読み取り専用モードのディスクへの変更は、仮想マシンをパワーオフまたはリセットしたときに破棄されます。仮想ディスクは、仮想マシンが再起動されるたびに同じ状態に戻ります。ディスクへの変更は REDO ログ ファイルに書き込まれ、このファイルから読み取られます。REDO ログ ファイルはパワーオフまたはリセット時に削除されます。

14 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへの既存ハード ディスクの追加

仮想マシンへの既存の仮想ハード ディスクの追加は、仮想マシン作成プロセス中の仮想マシンのハードウェアのカスタマイズ時または仮想マシン作成後に行うことができます。たとえば、起動ディスクとして事前構成された既存のハード ディスクを追加する必要がある場合があります。

仮想マシンの作成中、選択したゲスト OS に基づいて、デフォルトでハード ディスクおよび SCSI または SATA コントローラが仮想マシンに追加されます。このディスクがニーズを満たさない場合には、ディスクを削除し、作成プロセスの最後に既存のハード ディスクを追加できます。

前提条件

- 異なる仮想ハード ディスク構成に対するコントローラおよび仮想デバイス ノードの動作について理解しておいてください。
- 接続先のフォルダまたはデータストア上で 仮想マシン.設定.既存ディスクの追加 の権限があることを確認します。

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[ハード ディスクの追加] を選択し、ドロップダウン メニューから [既存のハード ディスク] を選択します。

4 （オプション） 既存のハード ディスクを削除するには、ディスク上にマウスのポインタを移動させて、[削除] アイコン ([X]) をクリックします。

   ディスクが仮想マシンから削除されます。他の仮想マシンがディスクを共有している場合は、ディスク ファイルは削除されません。

5 データストア列で、データストアを展開し、仮想マシン フォルダを選択し、追加するディスクを選択します。

   [コンテンツ] 列にディスク ファイルが表示されます。[ファイル タイプ] メニューに、このディスクと互換性のあるファイル タイプが表示されます。

6 [選択] をクリックし、[保存] をクリックして既存のハード ディスクを追加します。

Host Client での永続的なメモリ ディスクの追加

既存の仮想マシンに仮想ハード ディスクを追加することができます。また、仮想マシンの作成プロセスで、仮想マシンのハードウェアをカスタマイズするときにハード ディスクを追加することも可能です。たとえば、作業負荷の高い既存の仮想マシンにディスク容量の追加が必要な場合があります。また、仮想マシン作成中に、起動ディスクとして事前構成されたハード ディスクを追加する場合もあります。

仮想マシンの作成中、選択したゲスト OS に基づいて、ハード ディスクおよび SCSI または SATA コントローラがデフォルトで仮想マシンに追加されます。このディスクでは不十分な場合は、ディスクを削除し、作成プロセスの最後に既存のハード ディスクを追加できます。

前提条件

- 仮想ハード ディスクの追加に関する構成オプションと注意点について理解しておいてください。仮想ディスクの構成を参照してください。
- 2 TB を超えるサイズのディスクを仮想マシンに追加する前に、『vSphere の仮想マシン管理』を参照してください。
- 接続先のフォルダまたはデータストア上で 仮想マシン.設定.新規ディスクの追加の権限があることを確認します。

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[ハード ディスクの追加] を選択し、ドロップダウン メニューから [新規の永続的なメモリ ディスク] を選択します。

   ハード ディスクが、仮想ハードウェア デバイスのリストに表示されます。デフォルトでは、ディスクはホストのローカル PMEM データストアに保存され、データストアを変更することはできません。

4 （オプション） 新規ハード ディスクを設定し、[保存] をクリックしてウィザードを終了します。

   a [新規ハード ディスク] を展開します。

   b ハード ディスク サイズの値を入力し、ドロップダウン メニューから単位を選択します。

   注： 仮想マシンに追加するすべての永続的なメモリ ハード ディスクと NVDIMM モジュールは、同一の PMEM リソースを共有します。そのため、ホストで使用できる PMEM の量に合わせて、新しく追加した永続的なメモリのサイズを調整する必要があります。設定のいずれかの段階で注意が必要な場合は、ウィザードにアラートが表示されます。

   c [シェア] ドロップダウン メニューで、仮想ディスクに割り当てるシェアの値を選択します。

   シェアは、ディスクのバンド幅を制御するための相対的な基準を表す値です。値の低、中、高、カスタムは、ホスト上にあるすべての仮想マシンのすべてのシェアの合計と比較されます。

d [コントローラの場所] ドロップダウン メニューから、新しいハード ディスクが使用するコントローラの場所を選択します。

e ディスク モードを選択します。

オプション	説明
依存型	依存型ディスクはスナップショットに含まれます。
独立型: 通常	通常モードのディスクは、従来の物理コンピュータ ディスクと同様に動作します。通常モードのディスクに書き込まれたすべてのデータは、永続的にこのディスクに書き込まれます。
独立型: 読み取り専用	読み取り専用モードのディスクへの変更は、仮想マシンをパワーオフまたはリセットしたときに破棄されます。仮想ディスクは、仮想マシンが再起動されるたびに同じ状態に戻ります。ディスクへの変更は REDO ログ ファイルに書き込まれ、このファイルから読み取られます。REDO ログ ファイルはパワーオフまたはリセット時に削除されます。

VMware Host Client でのディスク シェアを使用した仮想マシンの優先順位付け

仮想マシンのディスク リソースを変更できます。複数の仮想マシンが同じ VMFS データストアおよび同じ LUN（論理ユニット番号）にアクセスする場合、ディスク シェアを使用して、仮想マシンが割り当てる必要のあるアクセスのレベルに優先順位を付けます。ディスク シェアでは、優先順位の高い仮想マシンと優先順位の低い仮想マシンを区別します。

仮想マシンの仮想ハード ディスクに、ホストの I/O バンド幅を割り当てることができます。クラスタ間で I/O のディスクをプールすることはできません。

シェアは、すべての仮想マシンに対してディスク バンド幅を制御するための相対的な基準を表します。

ディスク シェアは、指定されたホスト内でのみ有効です。あるホストの仮想マシンに割り当てられたシェアは、別のホストの仮想マシンでは無効です。

仮想マシンに割り当てられるストレージ リソースの上限を設定する、IOP 制限を選択できます。IOPs は、1 秒あたりの I/O 処理数です。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、ハード ディスクを展開してディスク オプションを表示します。

4 [シェア] ドロップダウン メニューで、仮想マシンに割り当てるシェアの値を選択します。

5 [カスタム] を選択した場合は、テキスト ボックス内にシェア数を入力します。

6 [制限 - IOPs] テキスト ボックスで、仮想マシンに割り当てるストレージ リソースの上限を入力するか、[制限なし] を選択します。

7 [[保存]] をクリックします。

VMware Host Client での仮想マシン コントローラの構成

VMware Host Client で、USB コントローラ、SCSI コントローラ、準仮想化 SCSI コントローラ、SATA コントローラなど、さまざまなコントローラを仮想マシンに追加できます。また、SCSI バス共有の構成と SCSI コントローラのタイプを変更することもできます。

USB コントローラの仮想マシンへの追加

ESXi ホストまたはクライアント コンピュータから仮想マシンへの USB パススルーをサポートするために、USB コントローラを仮想マシンに追加できます。

vSphere Client では、1 個の xHCI コントローラおよび 1 個の EHCI+UHCI コントローラを追加できます。ハードウェア バージョン 11 からハードウェア バージョン 16 では、1 つの xHCI コントローラあたりでサポートされるルート ハブ ポート数は 8 です（4 つの論理 USB 3.1 SuperSpeed ポートと 4 つの論理 USB 2.0 ポート）。ハードウェア バージョン 17 では、1 つの xHCI コントローラあたりでサポートされるルート ハブ ポート数は 8 です（4 つの論理 USB 3.1 SuperSpeedPlus ポートと 4 つの論理 USB 2.0 ポート）。

コントローラの追加に必要な条件は、デバイスのバージョン、パススルーのタイプ （ホスト コンピュータまたはクライアント コンピュータ）、およびゲスト OS によって異なります。

表 5-2. USB コントローラのサポート

コントローラ タイプ	サポート対象の USB デバイスのバージョン	ESXi ホストから仮想マシンへのパススルーのサポート	クライアント コンピュータから仮想マシンへのパススルーのサポート
EHCI+UHCI	2.0 および 1.1	はい	はい
xHCI	3.1、2.0、および 1.1	はい USB 3.1、2.0、および 1.1 デバイスのみ。	はい Windows 8 以降、Windows Server 2012 以降、または 2.6.35 以降のカーネルを搭載した Linux ゲスト OS。

Mac OS X システムでは、EHCI+UHCI コントローラはデフォルトで有効で、USB マウスおよびキーボードへのアクセスに必要です。

Windows または Linux ゲスト OS を搭載した仮想マシンの場合は、異なるタイプのコントローラを 1 つまたは 2 つ追加できます。同じタイプのコントローラを 2 個追加することはできません。

ESXi ホストから仮想マシンへの USB パススルーでは、USB アービトレータは最大で 15 個の USB コントローラを監視できます。15 個を超えるコントローラがシステムにあり、それに USB デバイスを接続した場合、デバイスは仮想マシンで使用できません。

前提条件

- ESXi ホストに、USB 3.1、USB 2.0、および USB 1.1 デバイスをサポートする USB コントローラのハードウェアおよびモジュールがあることを確認します。
- クライアント コンピュータに、USB 3.1、USB 2.0、および USB 1.1 デバイスをサポートする USB コントローラのハードウェアおよびモジュールがあることを確認します。

- Linux ゲストで xHCI コントローラを使用するには、Linux カーネル バージョンが 2.6.35 以降であることを確認します。
- 仮想マシンがパワーオン状態であることを確認します。
- 必要な権限（ESXi ホスト パススルー）：仮想マシン.構成.デバイスの追加または削除

手順

1. vSphere インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。
2. [仮想ハードウェア] タブで [新規デバイスを追加] をクリックし、ドロップダウン メニューから [USB コントローラ] を選択します。

   コントローラが、[仮想ハードウェア] デバイスのリストに表示されます。
3. USB コントローラ タイプを変更するには、[新規 USB コントローラ] を展開します。

   互換性のエラーが表示された場合、コントローラを追加する前に修正する必要があります。
4. [OK] をクリックします。

次のステップ

仮想マシンに 1 つ以上の USB デバイスを追加します。

VMware Host Client での、SCSI コントローラの追加

既存の仮想マシンに SCSI コントローラを追加するには、未使用の SCSI バス番号にハード ディスクを追加します。

未使用の SCSI バス番号に新しいハード ディスクを追加すると、新しい SCSI コントローラが作成されます。

前提条件

仮想マシンをパワーオフします。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[ハード ディスクの追加] を選択し、ドロップダウン メニューから [新規ハード ディスク] を選択します。
4. ハード ディスクを展開してすべてのオプションを表示します。
5. [コントローラの場所] セクションで、ドロップダウン メニューから未使用の SCSI バス番号を選択します。

   たとえば、バスとデバイスの番号 0:0 - 0:15 は最初の SCSI コントローラに使用されます。2 番目の SCSI コントローラには、バスとデバイスの番号 1:0 - 1:15 が使用されます。
6. [[保存]] をクリックします。

結果

新しいハード ディスクと新しい SCSI コントローラが同時に作成されます。

VMware Host Client での、SCSI バス共有構成の変更

仮想マシンの SCSI バス共有のタイプを設定し、SCSI バスを共有するかどうかを指定できます。共有タイプによっては、同一サーバ上または別のサーバ上の同じ仮想ディスクに仮想マシンが同時にアクセスできます。

仮想マシンが ESXi ホスト上にある場合のみ、その仮想マシンの SCSI コントローラ構成を変更できます。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、編集する SCSI コントローラを展開します。

4 [SCSI バスの共有] リストで、次の共有タイプのいずれかを選択します。

オプション	説明
なし	ほかの仮想マシンと仮想ディスクを共有できません。
仮想	仮想ディスクは、同一サーバ上の仮想マシンと共有できます。
物理	仮想ディスクは、あらゆるサーバ上の仮想マシンと共有できます。

5 [[保存]] をクリックします。

VMware Host Client での、SCSI コントローラ タイプの変更

仮想マシン上の仮想 SCSI コントローラを構成すると、仮想マシンに仮想ディスクおよび RDM を接続できます。

どの SCSI コントローラを選択しても、仮想ディスクが IDE ディスクであるか SCSI ディスクであるかには影響しません。IDE アダプタは常に ATAPI です。ゲスト OS のデフォルトはすでに選択されています。以前のゲスト OS は、デフォルトのコントローラとして BusLogic アダプタを使用します。

LSI Logic 仮想マシンを作成し、BusLogic アダプタを使用する仮想ディスクを追加する場合、その仮想マシンは BusLogic アダプタのディスクから起動します。LSI Logic SAS は、ハードウェア バージョン 7 以降の仮想マシンでのみ使用できます。スナップショットがあるディスクは、LSI Logic SAS、VMware 準仮想化、および LSI Logic パラレル アダプタでパフォーマンスが向上しないことがあります。

注意： SCSI コントローラ タイプを変更すると、仮想マシンの起動でエラーが発生する場合があります。

前提条件

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブをクリックし、SCSI コントローラを展開します。

4 ドロップダウン メニューから SCSI コントローラ タイプを選択します。

5 [[保存]] をクリックします。

VMware 準仮想化 SCSI コントローラについて

VMware 準仮想化 SCSI コントローラは、スループットが高く CPU 使用率が低い、高パフォーマンスのストレージ コントローラです。これらのコントローラは、高いパフォーマンスが必要なストレージ環境に最適です。

VMware 準仮想化 SCSI コントローラは、ESXi 4.x 以降と互換性のある仮想マシンで使用できます。これらのコントローラ上のディスクにスナップショットがある場合、または ESXi ホストのメモリがオーバー コミットされている場合、コントローラ上のディスクで最適なパフォーマンス向上が得られないことがあります。このことによって、その他の SCSI コントローラ オプションに比べて VMware 準仮想化 SCSI コントローラを使用することによる全体的なパフォーマンス向上が低減することはありません。

VMware 準仮想化 SCSI コントローラ用のプラットフォーム サポートの詳細については、『VMware 互換性ガイド』（http://www.vmware.com/resources/compatibility）を参照してください。

VMware Host Client での、準仮想化 SCSI コントローラの追加

高パフォーマンスの VMware 準仮想化 SCSI ストレージ コントローラを追加することにより、スループットを向上させ、CPU 使用率を軽減できます。

VMware 準仮想化 SCSI コントローラは、大量の I/O が発生するアプリケーションを実行する環境（特に SAN 環境）に最適です。

前提条件

- 仮想マシンに、VMware Tools がインストールされたゲスト OS があることを確認します。
- 仮想マシンにハードウェア バージョン 7 以降が搭載されていることを確認します。
- VMware 準仮想化 SCSI の制限事項について確認します。vSphere の仮想マシン管理 を参照してください。
- VMware 準仮想化 SCSI コントローラに接続された起動ディスク デバイスにアクセスする場合は、仮想マシンに Windows 2003 または Windows 2008 ゲスト OS が実行されていることを確認してください。
- 一部のオペレーティング システムでは、コントローラ タイプを変更する前に、LSI Logic コントローラを使用して仮想マシンを作成し、VMware Tools をインストールする必要があります。

仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] をクリックし、ドロップダウン メニューから [SCSI コントローラ] を選択します。

新しい SCSI コントローラがハードウェア リストに表示されます。

4 [新規 SCSI コントローラ] をクリックし、ドロップダウン メニューから [VMware 準仮想化] を選択します。

5 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへの SATA コントローラの追加

仮想マシンに複数のハード ディスクまたは CD/DVD-ROM デバイスがある場合、SATA コントローラをさらに最大 3 つまで追加してデバイスを割り当てることができます。デバイスを別々のコントローラに割り当てると、パフォーマンスを向上させ、データ トラフィックの輻輳を避けることができます。1 つのコントローラに対するデバイスの上限 30 台を超える場合は、さらにコントローラを追加することもできます。

SATA コントローラから仮想マシンを起動し、大容量仮想ハード ディスクで使用できます。

すべてのゲスト OS で AHCI SATA コントローラをサポートしているわけではありません。通常、ESXi 5.5 以降と互換性がある Mac OS X ゲスト OS の仮想マシンを作成する場合、デフォルトで、仮想ハード ディスクと CD/DVD-ROM デバイス用に SATA コントローラが追加されます。Windows Vista 以降を含む大部分のゲスト OS には、CD/DVD-ROM デバイス用のデフォルトの SATA コントローラがあります。確認するには、http://www.vmware.com/resources/compatibility にある『VMware 互換性ガイド』を参照してください。

前提条件

- 仮想マシンに ESXi 5.5 以降との互換性があることを確認します。
- ストレージ コントローラの動作と制約事項を確認しておいてください。vSphere の仮想マシン管理 を参照してください。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。
- 仮想マシンをパワーオフします。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、ドロップダウン メニューから [SATA コントローラ] を選択します。

SATA コントローラがハードウェア リストに表示されます。

4 [[保存]] をクリックします。

VMware Host Client での NVMe コントローラの追加

仮想マシンに複数のハード ディスクがある場合は、ディスクを割り当てるための仮想 NVMe コントローラを最大 4 個追加できます。NVMe コントローラを使用すると、AHCI SATA または SCSI コントローラと比べて、ソフトウェアによるゲスト OS の I/O 処理のオーバーヘッドを大幅に軽減することができます。

NVMe コントローラは、オール フラッシュ ディスク アレイ、ローカルの NVMe SSD、および PMEM ストレージ上の仮想ディスクでの使用に最も適しています。

前提条件

- NVMe をサポートするゲスト OS が仮想マシンにインストールされていることを確認します。
- 仮想マシンに ESXi6.5 以降との互換性があることを確認します。
- ストレージ コントローラの動作と制約事項を確認します。詳細については、『仮想マシン管理』ガイドを参照してください。
- 仮想マシン上で 仮想マシン.設定.新規ディスクの追加の権限があることを確認します。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[その他のデバイスの追加] アイコンをクリックし、ドロップダウン メニューから [NVMe コントローラ] を選択します。

結果

新規 NVMe コントローラが仮想マシンに追加されます。

次のステップ

仮想マシンにハード ディスクを追加して NVMe コントローラに割り当てることができます。

VMware Host Client での他の仮想マシン デバイスの構成

仮想マシンの CPU とメモリの構成、ハード ディスクと仮想ネットワーク アダプタの追加のほかに、DVD/CD-ROM ドライブ、フロッピー ドライブ、SCSI デバイスなどの仮想ハードウェアを追加および構成できます。また、仮想ウォッチドッグ タイマー (VWDT) デバイス、プリシジョン クロック デバイス、PCI デバイスを追加することもできます。

VMware Host Client での、仮想マシンへの CD または DVD ドライブの追加

クライアントまたはホスト上で物理ドライブを使用することも、ISO イメージを使用して CD/DVD ドライブを仮想マシンに追加することもできます。

ホスト上の USB CD/DVD ドライブでバックアップされる CD/DVD ドライブを追加する場合は、そのドライブを SCSI デバイスとして追加する必要があります。ESXi ホストでの SCSI デバイスのホット アドおよびホット リムーブはサポートされていません。

前提条件

仮想マシンをパワーオフします。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、ドロップダウン メニューから [CD/DVD ドライブ] を選択します。

4 [CD/DVD ドライブ] を展開し、オプションを選択します。

オプション	説明
物理ドライブの使用	a 場所として [クライアント デバイス] を選択します。 b [デバイス モード] ドロップダウン メニューから [CD-ROM のエミュレート] または [パススルー CD-ROM] を選択します。
ISO イメージの使用	a 場所として [データストア ISO ファイル] を選択します。 b イメージ ファイルのパスとファイル名を入力するか、[参照] をクリックしてファイルの場所に移動します。

5 仮想マシンの起動時に CD-ROM ドライブを接続しない場合は、[パワーオン時に接続] の選択を解除します。

6 仮想マシンでドライブが使用する仮想デバイス ノードを選択します。

7 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへのフロッピー ドライブの追加

物理フロッピー ドライブまたはフロッピー イメージを使用してフロッピー ドライブを仮想マシンに追加できます。

ESXi では、ホスト上の物理フロッピー ドライブによってバックアップされるフロッピー ドライブはサポートされていません。

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、ドロップダウン メニューから [フロッピー ドライブ] を選択します。

フロッピー ドライブがハードウェア リストに表示されます。

4 [フロッピー ドライブ] を展開し、使用するデバイスのタイプを選択します。

オプション	説明
クライアント デバイス	VMware Host Client へのアクセス元となるシステムの物理フロッピー デバイスまたは `.flp` フロッピー イメージにフロッピー デバイスを接続するには、このオプションを選択します。
既存のフロッピー イメージを使用	a ホストからアクセス可能なデータストア上にあるフロッピー ドライブの既存のイメージに仮想デバイスを接続するには、このオプションを選択します。 b [参照] をクリックし、フロッピー イメージを選択します。

5 （オプション） 仮想マシンのパワーオン時に接続するようにデバイスを構成するには、[パワーオン時に接続] を選択します。

6 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへの USB デバイスの追加

VMware Host Client を使用すると、仮想マシンに USB デバイスを追加できます。

前提条件

- USB コントローラがあることを確認します。 USB コントローラの仮想マシンへの追加を参照してください。
- 仮想マシンが配置されている ESXi ホストに物理 USB デバイスを接続して、このホストに USB デバイスを追加します。

注： 使用可能な USB デバイスが ESXi ホストにない場合は、USB デバイスを仮想マシンに追加できません。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、ドロップダウン メニューから [USB デバイス] を選択します。

仮想マシンで使用可能なハードウェア デバイスのリストに USB デバイスが表示されます。

4 [USB デバイス] ドロップダウン メニューから、仮想マシンに追加する USB デバイスを選択します。

5 [[保存]] をクリックします。

VMware Host Client での、仮想マシンへのサウンド コントローラの追加

VMware Host Client を使用すると、仮想マシンにサウンド コントローラを追加できます。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、ドロップダウン メニューから [サウンド コントローラ] を選択します。

仮想マシンで使用可能なハードウェア デバイスのリストにサウンド コントローラが表示されます。

4 [サウンド カード] ドロップダウン メニューから、仮想マシンに接続するサウンド コントローラを選択します。

5 [[保存]] をクリックします。

VMware Host Client でのパラレルおよびシリアル ポート構成

パラレル ポートおよびシリアル ポートは、周辺機器を仮想マシンに接続するためのインターフェイスです。仮想シリアル ポートは、物理シリアル ポートまたはホスト コンピュータ上のファイルに接続できます。また、2 台の仮想

マシンを直接接続したり、仮想マシンとホスト コンピュータ上のアプリケーションを接続する際にも使用できます。パラレル ポートとシリアル ポートを追加し、シリアル ポートの構成を変更できます。

VMware Host Client での、仮想マシンへのシリアル ポートの追加

仮想マシンは、最大で 4 つの仮想シリアル ポートを使用できます。仮想シリアル ポートは、物理シリアル ポートまたはホスト コンピュータ上のファイルに接続できます。また、ホスト側の名前付きパイプを使用することで、2 台の仮想マシンを直接接続するか、仮想マシンとホスト コンピュータ上のアプリケーションを接続することもできます。さらに、ポートまたは仮想シリアル ポート コンセントレータ (vSPC) URI を使用して、ネットワーク経由でシリアル ポートを接続することも可能です。

前提条件

- アクセスするポートのメディア タイプ、vSPC 接続、および当てはまる可能性があるすべての条件を理解してください。vSphere の仮想マシン管理 を参照してください。
- ネットワークを介してシリアル ポートを接続するには、ファイアウォールのルール セットを追加します。vSphere の仮想マシン管理 を参照してください。
- 必要な権限：仮想マシン.構成.デバイスの追加または削除

  仮想マシンをパワーオフします。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、[シリアル ポート] を選択します。

   シリアル ポートがハードウェア リストに表示されます。
4. ハードウェア リスト内でシリアル ポートを展開し、アクセスするメディア ポートのタイプを選択します。

オプション	説明
出力ファイルを使用	仮想シリアル ポートの出力を保存するホスト上のファイルの場所を参照します。
物理シリアル ポートを使用	ドロップダウン メニューからポートを選択します。
名前付きパイプを使用	a [パイプ名] フィールドに、パイプの名前を入力します。 b パイプの [近端] および [遠端] をドロップダウン メニューから選択します。
ネットワークの使用	a [方向] ドロップダウン メニューから、[サーバ] または [クライアント] を選択します。 b ポート URI を入力します。 この URI は、仮想マシンのシリアル ポートの接続先となるシリアル ポートのリモート エンドになります。 c 1 つの IP アドレスですべての仮想マシンにアクセスする手段として vSPC を使用する場合は、[仮想シリアル ポート コンセントレータの使用] を選択して、vSPC URI の場所を入力します。

5. （オプション） 仮想マシンのパワーオン時にパラレル ポート デバイスを接続しない場合は、[パワーオン時に接続] を選択解除します。

6 [[保存]] をクリックします。

例： 認証パラメータを使用しないクライアントまたはサーバへのシリアル ポート ネットワーク接続の確立

vSPC を使用せず、シリアル ポートが接続されている仮想マシンを `telnet://:12345` URI のサーバとして構成した場合、Linux または Windows オペレーティング システムから仮想マシンのシリアル ポートに接続できます。

```
telnet yourESXiServerIPAddress 12345
```

同様に、Linux システムのポート 23 (`telnet://yourLinuxBox:23`) で Telnet サーバを稼動する場合、仮想マシンをクライアント URI として設定します。

```
telnet://yourLinuxBox:23
```

仮想マシンは、ポート 23 で Linux システムへの接続を開始します。

VMware Host Client での、仮想マシンへのパラレル ポートの追加

仮想マシンにプリンタまたはスキャナなどの周辺デバイスを接続するには、パラレル ポートを使用できます。そのようなデバイスの出力はホスト コンピュータのファイルに送信されます。

注： ESXi4.1 またはそれ以前のバージョンのホストで稼動している仮想マシンにパラレル ポートを追加する場合は、ホスト上の物理パラレル ポートに出力を送信することも選択できます。このオプションは、ESXi5.0 以降のホスト バージョンでは使用できません。

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、[パラレル ポート] を選択します。

パラレル ポートがハードウェア リストに表示されます。

4 パラレル ポートを展開し、[接続] フィールドでファイルを作成するフォルダを参照します。

ファイル パスは [接続] テキスト ボックスに表示されます。

5 （オプション） 仮想マシンのパワーオン時に接続するようにデバイスを構成するには、[パワーオン時に接続] を選択します。

6 [[保存]] をクリックします。

仮想ウォッチドッグ タイマーの使用

仮想マシン内のシステム パフォーマンスに関する自立性を確保するために、仮想ウォッチドッグ タイマー (VWDT) デバイスを追加できます。ソフトウェアの問題またはエラーが原因でゲスト OS が応答を停止し、単独でリカバリできない場合、VWDT は事前定義された期間待機してからシステムを再起動します。

VWDT は、ゲスト OS、あるいは BIOS または EFI ファームウェアのいずれかを使用して起動できます。VWDT を BIOS または EFI ファームウェアで起動するように選択した場合、ゲスト OS が起動する前に VWDT が起動します。

VWDT は、クラスタ内の各仮想マシンで障害が発生した場合に個別にリカバリできる、ゲストベースのクラスタリング ソリューションで重要な役割を果たします。

VMware Host Client での、仮想ウォッチドッグ タイマー デバイスの仮想マシンへの追加

仮想ウォッチドッグ タイマー デバイスを仮想マシンに追加すると、長期間にわたって仮想マシンのゲスト OS で障害が発生しないようにすることができます。

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。
- 仮想マシンのゲスト OS が VWDT デバイスをサポートしていることを確認します。
- 仮想ハードウェアのバージョンが 17 であることを確認します。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[その他のデバイスの追加] を選択し、[ウォッチドッグ タイマー] をクリックします。

   ウォッチドッグ タイマー デバイスがハードウェア リストに表示されます。
4. （オプション）[BIOS/EFI ブートでの起動] を選択して、ウォッチドッグ タイマーを BIOS または EFI ファームウェアで起動します。

   このオプションを選択すると、ゲスト OS の前に VWDT デバイスが起動します。ゲスト OS の起動に時間がかかりすぎる場合、またはゲスト OS がウォッチドッグ タイマーをサポートしていない場合、このデバイスでは仮想マシンの再起動が継続されます。
5. [[保存]] をクリックします。

VMware Host Client での仮想マシンへのプレシジョン クロック デバイスの追加

プレシジョン クロックは、仮想マシン上で実行され、ホストのシステム時間を利用する仮想デバイスです。仮想マシンにプレシジョン クロックを追加することで、確実に時刻を同期し、高精度のタイムスタンプを作成できます。

前提条件

- 仮想マシンをパワーオフします。
- 仮想ハードウェアのバージョンが 17 であることを確認します。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。
- 仮想マシンに対する仮想マシン.構成.デバイス設定の変更権限を持っていることを確認します。

手順

1. VMware Host Client インベントリで、[仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[その他のデバイスの追加] をクリックし、[プレシジョン クロック]を選択します。

   プレシジョン クロック デバイスがハードウェア リストに表示されます。
4. （オプション） 時刻同期プロトコルを選択します。
5. [[保存]] をクリックします。

VMware Host Client での、仮想マシンへの PCI デバイスの追加

DirectPath I/O によって、仮想マシンのゲスト OS から、ホストに接続されている PCI または PCIe の物理デバイスに直接アクセスできます。このテクノロジーを利用することで、各仮想マシンを最大 16 個の物理 PCI デバイスに接続できます。動的 DirectPath I/O を使用して、複数の PCI パススルー デバイスを仮想マシンに割り当てることができます。vSphere 7.0 以降では、ベンダーとモデル名で PCI パススルー デバイスを識別できます。

注： PCI または PCIe パススルー デバイスを仮想マシンに追加すると、一部の仮想マシン操作を実行できなくなります。

ハードウェア ラベルの設定の詳細については、VMware Host Client でのハードウェア ラベルの変更を参照してください。

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンに対する仮想マシン.構成.デバイスの追加または削除権限を持っていることを確認します。
- PCI デバイスがホストに接続され、パススルーが使用可能になっていることを確認します。
- 仮想マシンに動的 PCI デバイスを追加する場合は、仮想ハードウェアのバージョンが 17 であることを確認します。

手順

1. VMware Host Client インベントリで、[仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[その他のデバイスの追加] をクリックし、デバイスを選択します。

オプション	操作
PCI デバイス	a [PCI デバイス] をクリックします。 新しいデバイスがハードウェア リストに表示されます。 b ドロップダウン メニューから、仮想マシンに接続する PCI デバイスを選択します。
動的 PCI デバイス	a [動的 PCI デバイス] をクリックします。 新しいデバイスがハードウェア リストに表示されます。 b [新規 PCI デバイス] を展開し、ドロップダウン メニューから、仮想マシンに接続する PCI パススルー デバイスを選択します。 PCI パススルー デバイスは、ベンダー、モデル名、およびハードウェアのラベルで識別できます。ハードウェア ラベルが使用されている場合は、括弧で囲まれて表示されます。 **注：** PCI デバイスを仮想マシンに追加すると、仮想マシンのメモリ サイズがすべて自動的に予約されます。

4 [[保存]] をクリックします。

VMware Host Client での仮想マシンのセキュリティ

仮想マシンで実行するゲスト OS は、物理システムと同じセキュリティ リスクに対して脆弱です。仮想環境内のセキュリティを向上させるために、ESXi ホストに仮想 Trusted Platform Module (vTPM) を追加することができます。また、最新の Windows 10 および Windows Server 2016 オペレーティング システムを実行する仮想マシンでは、仮想化ベース セキュリティ (VBS) を有効にすることもできます。仮想マシンに Virtual Intel® Software Guard Extensions (vSGX) を使用することで、ワークロードのセキュリティを強化できます。

VMware Host Client における仮想マシンの vSGX の有効化

エンクレーブの内容を開示および変更から保護するために、VMware Host Client の仮想マシンで vSGX を有効にすることができます。

vSGX による仮想マシンの保護

vSphere では、仮想マシンに対し vSGX を構成できます。最近の Intel 製 CPU の一部には、Intel® Software Guard Extension (Intel® SGX) と呼ばれるセキュリティ拡張機能が実装されています。Intel SGX では、エンクレーブと呼ばれるメモリのプライベート領域をユーザーレベルのコードで定義できます。Intel SGX により、エンクレーブの外部で実行されるコードがエンクレーブにアクセスできなくなり、その内容が開示または変更から保護されます。

ハードウェアで Intel SGX テクノロジーが使用可能な場合、vSGX により仮想マシンで SGX を使用できます。vSGX を使用するには、SGX 対応の CPU に ESXi ホストをインストールし、ESXi ホストの BIOS で SGX を有効にする必要があります。vSphere Client を使用して、仮想マシンで SGX を有効にすることができます。詳細については、『vSphere のセキュリティ』を参照してください。

一部の操作と機能は、SGX に対応していません。

- Storage vMotion での移行
- 仮想マシンのサスペンドまたはレジューム

- 仮想マシンのスナップショットの作成
- Fault Tolerance
- ゲストの整合性 (GI)（VMware AppDefense 1.0 のプラットフォーム基盤）の有効化

前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンで EFI ファームウェアが使用されていることを確認します。
- ESXi ホストがバージョン 7.0 以降であることを確認します。
- 仮想マシンのゲスト OS が、Linux、Windows 10（64 ビット）以降、または Windows Server 2016（64 ビット）以降であることを確認します。
- 仮想マシンに対する仮想マシン.構成.デバイス設定の変更権限を持っていることを確認します。
- SGX 対応の CPU に ESXi ホストがインストールされていて、ESXi ホストの BIOS で SGX が有効であることを確認します。サポートされている CPU の詳細については、https://kb.vmware.com/s/article/71367 を参照してください。

手順

1. VMware Host Client インベントリで、[仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想ハードウェア] タブで、[セキュリティ デバイス] を展開します。
4. [有効化] チェック ボックスを選択します。
5. [Enclave ページのキャッシュサイズ] で、テキスト ボックスに新しい値を入力し、ドロップダウン メニューからサイズを MB または GB 単位で選択します。

   注： Enclave ページのキャッシュ サイズは 2 の倍数にする必要があります。

6. [起動制御設定] ドロップダウン メニューから、適切なモードを選択します。

オプション	操作
ロック済み	Launch Enclave 構成を有効にします。 [Launch Enclave パブリック キー ハッシュ] で、有効な SHA256 ハッシュを入力します。 SHA256 ハッシュ キーには 64 文字を含める必要があります。
ロック解除済み	ゲスト OS の Launch Enclave 構成が有効になります。

7. [[保存]] をクリックします。

VMware Host Client における仮想マシンの vSGX の無効化

仮想マシンで vSGX を無効にするために、VMware Host Client を使用できます。

手順

1. VMware Host Client インベントリで、[仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで、[セキュリティ デバイス] を展開します。

4 [有効化] チェック ボックスを選択解除し、[保存] をクリックします。

結果

vSGX が仮想マシンで無効になります。

VMware Host Client での仮想マシンからの vTPM デバイスの削除

Trusted Platform Module (TPM) は、プライベート キーや OS シークレットなどのホスト固有の機密情報を格納する特別なチップです。TPM チップは、暗号化タスクの実行やプラットフォームの一貫性の証明にも使用されます。VMware Host Client では、仮想マシンから vTPM デバイスを削除することのみが可能です。

仮想 TPM デバイスは、TPM 機能のソフトウェア エミュレーションです。仮想 TPM (vTPM) デバイスは、環境内の仮想マシンに追加できます。vTPM を実装する場合、ホストに物理 TPM チップは不要です。ESXi は vTPM デバイスを使用することで、vSphere 環境で TPM の機能を発揮します。

vTPM は、Windows 10 または Windows Server 2016 オペレーティング システムがインストールされた仮想マシンで利用できます。仮想マシンのハードウェア バージョンが 14 以降である必要があります。

仮想 TPM デバイスは、vCenter Server インスタンス内の仮想マシンにのみ追加できます。詳細については、『vSphere のセキュリティ』ドキュメントを参照してください。

VMware Host Client では、仮想マシンから仮想 TPM デバイスを削除することのみが可能です。

前提条件

- 仮想マシンのハードウェア バージョンが 14 以降である必要があります。
- ゲスト OS は、Windows 10 または Windows Server 2016 以降にする必要があります。
- 仮想マシンをパワーオフする必要があります。

手順

1 VMware Host Client インベントリ内で [仮想マシン] をクリックします。

2 リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。

3 [仮想ハードウェア] タブで TPM デバイスを検索し、[削除] アイコンをクリックします。

仮想 TPM デバイスが仮想マシンから削除されます。

4 [保存] をクリックして、ウィザードを終了します。

VMware Host Client での既存の仮想マシン上の仮想化ベース セキュリティの有効化または無効化

仮想化ベース セキュリティ (VBS) では、Microsoft Hyper-V ベースの仮想化テクノロジーを使用して、隔離された仮想化環境に Windows OS のコア サービスを分離します。この分離によって環境内の主要なサービスを操作できなくなるため、保護のレベルが強化されます。

サポート対象の Windows ゲスト OS の既存の仮想マシンで Microsoft の仮想化ベース セキュリティ (VBS) を有効または無効にすることで、仮想マシンのセキュリティ レベルを変更できます。

仮想マシンで VBS を有効にすると、VBS 機能のために Windows が必要とする仮想ハードウェアが自動的に有効になります。VBS を有効にすると、仮想マシンで Hyper-V のバリアントが起動し、Hyper-V のルート パーティション内で Windows が実行を開始します。

VBS は、Windows 10、Windows Server 2016 などの最新バージョンの Windows OS で使用可能です。VBS を仮想マシンで使用するには、仮想マシンの互換性が ESXi 6.7 以降である必要があります。

VMware Host Client では、仮想マシンの作成時に VBS を有効にできます。また、既存の仮想マシンの場合は VBS の有効と無効を切り替えることもできます。

前提条件

VBS を構成するプロセスでは、まず仮想マシンで VBS を有効にしてから、ゲスト OS で VBS を有効にします。

注： ハードウェア バージョン 14 未満で Windows 10、Windows Server 2016 および Windows Server 2019 用に構成された新規仮想マシンは、デフォルトでレガシー BIOS を使用して作成されます。仮想マシンのファームウェア タイプをレガシー BIOS から UEFI に変更する場合は、ゲスト OS を再インストールする必要があります。

仮想マシンで VBS を有効にするためには、ホストの TPM の検証が成功する必要があります。

VBS に Intel CPU を使用するには、vSphere 6.7 以降が必要です。仮想マシンは、ハードウェア バージョン 14 以降、および次のサポート対象ゲスト OS のいずれかを使用して作成されている必要があります。

- Windows 10（64 ビット）以降のリリース
- Windows Server 2016（64 ビット）以降のリリース

VBS に AMD CPU を使用するには、vSphere 7.0 Update 2 以降が必要です。仮想マシンは、ハードウェア バージョン 19 以降、および次のサポート対象ゲスト OS のいずれかを使用して作成されている必要があります。

- Windows 10（64 ビット）、バージョン 1809 以降のリリース
- Windows Server 2019（64 ビット）以降のリリース

VBS を有効にする前に、Windows 10 バージョン 1809、および Windows Server 2019 の最新のパッチをインストールしてください。

手順

1. VMware Host Client インベントリ内で [仮想マシン] をクリックします。
2. リスト内の仮想マシンを右クリックし、ポップアップ メニューから [設定の編集] を選択します。
3. [仮想マシン オプション] タブで、仮想マシンの VBS を有効または無効にします。
   - 仮想マシンで VBS を有効にするには、[仮想化ベースのセキュリティの有効化] チェック ボックスを選択します。

- 仮想マシンで VBS を無効にするには、[仮想化ベースのセキュリティの有効化] チェック ボックスを選択解除します。

VBS を有効にすると、いくつかのオプションが自動的に選択され、ウィザードで淡色表示になります。

4 [保存] をクリックして、ウィザードを終了します。

VMware Host Client でのストレージの管理

6

ESXi ホストに VMware Host Client を使用して接続している場合に、アダプタの構成、データストアの作成、ストレージ デバイス情報の表示など、さまざまなストレージ管理タスクを ESXi ホスト上で実行できます。

この章には、次のトピックが含まれています。

VMware Host Client のデータストア

データストアはファイル システムに似た論理コンテナで、各ストレージ デバイスに関する特定の情報が格納されており、仮想マシン ファイルを格納するための一貫したモデルを提供します。また、データストアを使用して、ISO イメージ、仮想マシン テンプレート、およびフロッピー イメージを格納できます。

使用するストレージのタイプによって、データストアは次のタイプに分けられます。

- 仮想マシン ファイル システム （VMFS）
- ネットワーク ファイル システム (NFS)

VMFS データストアの場合に限り、データストア作成後にキャパシティを拡張できます。

ブロック ストレージ デバイス、ファイバ チャネルと iSCSI、および NAS デバイスは、ハードウェア アクセラレーションをサポートします。

ハードウェア アクセラレーション機能により、ESXi ホストを互換性のあるストレージ システムと統合できます。ホストは、特定の仮想マシンとストレージ管理の操作をストレージ システムにオフロードできます。ストレージ ハードウェア アシストにより、ホストはこれらの操作をより短時間で実行できます。 また、CPU、メモリ、およびストレージ ファブリック バンド幅の使用量を削減できます。

詳細については、http://kb.vmware.com/kb/1021976 にある VMware のナレッジベースの記事を参照してください。

VMware Host Client でのデータストア情報の表示

VMware Host Client を使用して、ホストで使用できるデータストアを表示し、それらのプロパティを分析します。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックし、[データストア] をクリックします。

2 特定のデータストアの詳細情報を表示するには、リストからデータストアを選択します。

VMware Host Client での VMFS データストアの作成

VMFS データストアは、仮想マシンのリポジトリとして機能します。ファイバ チャネル、iSCSI、ローカル ストレージ デバイスなど、ホストが検出する SCSI ベースのストレージ デバイス上に、VMFS データストアを設定できます。[新しいデータストア] ウィザードを使用して、VMware Host Client でデータストアを作成できます。

前提条件

ストレージで必要なアダプタをインストールおよび構成する必要があります。アダプタを再スキャンして、新しく追加されたストレージ デバイスを検出します。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [新しいデータストア] をクリックします。

[新しいデータストア] ウィザードが開きます。

3 [作成タイプの選択] ページで、[新しい VMFS データストアの作成] を選択し、[次へ] をクリックします。

オプション	説明
新しい VMFS データストアの作成	ローカル ディスク デバイス上に新しい VMFS データストアを作成します。
既存の VMFS データストアにエクステントを追加します	別のディスクに新しいエクステントを追加して既存のデータストアのサイズを増やします。
既存の VMFS データストアのエクステントを拡張します	既存のデータストア エクステントのサイズを増やします。
NFS データストアのマウント	リモート NFS ボリュームをマウントして新しいデータストアを作成します。

4 [デバイスの選択] ページで、新しい VMFS パーティションを作成する場所を選択します。

a 新しいデータストアの名前を入力します。

b データストアを追加する先のデバイスを選択します。

リストには、使用可能な容量が十分にあるデバイスのみが表示されます。

c [次へ]をクリックします。

5 [パーティション分割オプションの選択] ページで、デバイスのパーティション分割方法を選択し、[次へ] をクリックします。

オプション	説明
[Use Full Disk（フル ディスクを使用）]	デバイス上で使用可能なすべての空き容量を示します。
[カスタム]	[空き容量] バーをクリックし、水平スクロール バーを使用してデバイスをパーティション分割します。

6 [設定の確認] ページで構成の詳細を確認し、[完了] をクリックします。

VMFS データストアのキャパシティの拡張

VMFS データストアでより多くの容量が必要な場合は、データストアのキャパシティを増やすことができます。データストア エクステントを拡張するか、エクステントを追加することにより、キャパシティを動的に増やすことができます。

次のいずれかの方法で、データストアのキャパシティを拡張します。

- データストア エクステントが拡張可能な場合、これを動的に拡張し、隣接するキャパシティを使用できるようにする基盤となるストレージ デバイスで、エクステントの直後に空き容量がある場合、そのエクステントは拡張可能だとみなされます。
- エクステントを動的に追加する。データストアでは、最小要件 2 TB のエクステントを最大 32 個に拡張することができます。これは単一のボリュームとして扱われます。複数のエクステントにまたがる VMFS データストアでは、任意のエクステントまたはすべてのエクステントを随時使用できます。次のエクステントを使用する前に、特定のエクステントの容量を使い切る必要はありません。

注： データストアが、アトミック テスト アンド セット (ATS) メカニズムとも呼ばれる Hardware Assisted Locking のみをサポートしている場合は、ATS 以外のデバイスに拡張することはできません。詳細については、#unique_185 を参照してください。

注： データストアが、アトミック テスト アンド セット (ATS) メカニズムとも呼ばれる Hardware Assisted Locking のみをサポートしている場合は、ATS 以外のデバイスに拡張することはできません。詳細については、『vSphere のストレージ』を参照してください。

VMware Host Client での既存の VMFS データストアの拡張

データストアに仮想マシンを追加する必要がある場合、またはデータストア上で実行している仮想マシンの容量を増やす必要がある場合、VMFS データストアの容量を動的に増加できます。

共有のデータストアにパワーオンされた仮想マシンがあり、完全に容量が使用されている場合、パワーオンされている仮想マシンが登録されているホストからのみ、データストアの容量を増加できます。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [新しいデータストア] をクリックします。

3 [作成タイプの選択] ページで、[既存の VMFS データストアにエクステントを追加します] をクリックし、[次へ] をクリックします。

4 [データストアの選択] ページで、展開するデータストアを選択し、[次へ] をクリックします。

5 [デバイスの選択] ページで、新規 VMFS パーティションを作成するデバイスを選択し、[次へ] をクリックします。

6 [パーティション分割オプションの選択] ページで、デバイスのパーティション分割方法を選択し、[次へ] をクリックします。

オプション	説明
[Use Full Disk（フル ディスクを使用）]	デバイス上で使用可能なすべての空き容量を示します。
[カスタム]	[空き容量] バーをクリックし、水平スクロール バーを使用してデバイスをパーティション分割します。

7 [設定の確認] ページで構成の詳細を確認し、[完了] をクリックします。

VMware Host Client でのネットワーク ファイル システム データストアのマウント

VMware Host Client で、仮想ディスクを格納するネットワーク ファイル システム (NFS) データストアを作成し、ISO イメージや仮想マシンなどを格納する中央のリポジトリとして使用することができます。ESXi に組み込まれた NFS クライアントは、TCP/IP 接続で NFS (Network File System) プロトコルを使用して、NAS サーバ上に存在する指定された NFS ボリュームにアクセスします。vSphere は、バージョン 3 および 4.1 の NFS プロトコルをサポートします。

ESXi ホストは、NFS ボリュームをマウントし、ストレージのニーズに応じてこのボリュームを使用することができます。

通常、NFS ボリュームまたはディレクトリは、ストレージ管理者によって作成され、NFS サーバからエクスポートされます。VMFS などのローカル ファイル システムで NFS ボリュームをフォーマットする必要はありません。代わりに、ボリュームを ESXi ホストに直接マウントし、VMFS データストアを使用する場合と同じ方法で仮想マシンを保存および起動します。

NFS は、NFS データストアに仮想ディスクを格納するほかに、ISO イメージや仮想マシンのテンプレートなどの中央リポジトリとして使用できます。ISO イメージ用のデータストアを使用する場合、仮想マシンの CD-ROM デバイスをデータストア上の ISO ファイルに接続できます。次に、その ISO ファイルからゲスト OS をインストールできます。

NFS ストレージを使用する場合は、NFS サーバの設定、ネットワーク、NFS データストアなどに関連する個別のガイドラインを参照してください。

手順

1 VMware Host Client での NFS データストアのマウント

[新しいデータストア] ウィザードを使用して、ネットワーク ファイル システム (NFS) データストアを VMware Host Client にマウントできます。

VMware Host Client での NFS データストアのマウント

[新しいデータストア] ウィザードを使用して、ネットワーク ファイル システム (NFS) データストアを VMware Host Client にマウントできます。

前提条件

NFS では、リモート サーバに格納されているデータへアクセスするためのネットワーク接続が必要であるため、NFS を構成するにはまず、VMkernel ネットワークを構成する必要があります。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [新しいデータストア] をクリックします。

[新しいデータストア] ウィザードが開きます。

3 [作成タイプの選択] ページで、[NFS データストアのマウント] をクリックし、[次へ] をクリックします。

4 [NFS マウントの詳細の指定] ページで、マウントする NFS の詳細を指定します。

a NFS データストアの名前を入力します。

b NFS サーバ名を入力します。

サーバ名については、IP アドレス、DNS 名、または NFS UUID で入力できます。

注： 異なるホスト上で同じ NFS ボリュームをマウントする場合、サーバ名とフォルダ名がホスト間で同一であることを確認してください。名前が一致しない場合、ホストは同じ NFS ボリュームを 2 つの異なるデータストアとして検出します。これによって、vMotion などの機能が失敗する場合があります。たとえば、1 つのホストでサーバ名を「**`filer`**」と入力し、別のホストで「**`filer.domain.com`**」と入力した場合に、このような不一致が見られます。

c NFS シェアを指定します。

d NFS バージョンを指定します。

e [次へ] をクリックします。

5 [設定の確認] ページで、NFS データストアの設定を確認し、[完了] をクリックします。

VMware Host Client でのデータストアのアンマウント

VMware Host Client でデータストアをアンマウントすると、そのデータストアの状態は変更されませんが、管理対象ホストのインベントリには表示されなくなります。マウントされたままの状態になっている別のホストでは、データストアは引き続き表示されます。

アンマウントの処理中は、データストアへの I/O が発生する可能性がある設定操作を行わないでください。

前提条件

注： データストアが vSphere HA ハートビートで使用されていないことを確認してください。vSphere HA ハートビートによってデータストアのアンマウントができなくなることはありません。ただし、データストアがハートビートのために使用されている場合、そのデータストアをアンマウントするとホストに障害が発生し、アクティブな仮想マシンがすべて再起動されることがあります。

データストアをアンマウントする前に、次の前提条件を満たしていることも確認してください。

- そのデータストア上に仮想マシンが存在しない。
- Storage DRS は、データストアを管理していない。
- そのデータストアに対して Storage I/O Control が無効になっている。

手順

1. VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。
2. リスト内でアンマウントするデータストアを右クリックし、[アンマウント] をクリックします。
3. データストアをアンマウントすることを確認します。

データストアのアンマウントまたは削除の失敗

データストアをアンマウントまたは削除しようとすると、操作が失敗します。

問題

データストアでファイルが開かれている場合、データストアをアンマウントまたは削除する操作は失敗します。このようなユーザー操作では、vSphere HA エージェントは開いているすべてのファイル、たとえばハートビート ファイルを閉じます。vCenter Server がエージェントにアクセスできない、またはエージェントが保留中の I/O をフラッシュしてファイルを閉じることができない場合、「ホスト「`{hostName}`」の HA エージェントは、データストア「`{dsName}`」でのファイル アクティビティの静止に失敗しました」という障害が発生します。

原因

アンマウントまたは削除するデータストアがハートビートに使用されている場合、vCenter Server はデータストアをハートビートから除外し、新しいデータストアを選択します。ただし、アクセスできない、つまり、ホストが隔離されているまたはネットワーク パーティション分割されている場合、エージェントは更新されたハートビート データストアを取得しません。このような場合、ハートビート ファイルは閉じられず、ユーザーの操作は失敗します。操作は、all paths down 状態などのストレージ障害が原因でデータストアがアクセス不可能である場合も失敗する可能性があります。

注： VMFS データストアを削除すると、インベントリ内のすべてのホストからデータストアが削除されます。このため、アクセスできない、またはデータストアにアクセスできない vSphere HA クラスタにホストがある場合、操作は失敗します。

解決方法

データストアがアクセス可能で、影響を受けるホストにアクセスできることを確認します。

VMware Host Client でのデータストア ファイル ブラウザの使用

データストア ファイル ブラウザを使用して、データストアのコンテンツを管理します。データストアへのファイルのアップロード、システムへのデータストア ファイルのダウンロード、データストア フォルダまたはファイルの移動とコピー、新しいデータストア ディレクトリの作成など、さまざまなタスクを実行できます。

VMware Host Client でのデータストアへのファイルのアップロード

データストア ファイル ブラウザを使用して、ホスト上のデータストアにファイルをアップロードします。

注： Virtual Volumes は、仮想データストアへのファイルの直接アップロードをサポートしません。先に仮想データストアにフォルダを作成してから、フォルダにファイルをアップロードする必要があります。

データストアは、仮想マシンのファイルのストレージとして従来どおりに使用するだけでなく、仮想マシン関連のデータやファイルの保存にも使用できます。たとえば、オペレーティング システムの ISO イメージをローカル コンピュータからホストのデータストアにアップロードできます。これらのイメージを使用して新しい仮想マシンにゲスト OS をインストールします。

前提条件

必要な権限：データストア.データストアの参照

手順

1. VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。
2. [データストア ブラウザ] をクリックします。
3. ファイルを保存するデータストアを選択します。
4. （オプション）[ディレクトリの作成] をクリックして、ファイルを保存する新しいデータストア ディレクトリを作成します。
5. 保存先フォルダを選択し、[アップロード] をクリックします。
6. ローカル コンピュータからアップロードするアイテムを特定し、[開く] をクリックします。

   選択したデータストアにファイルがアップロードされます。
7. （オプション）データストア ファイル ブラウザを更新し、アップロードしたファイルがリストにあることを確認します。
8. [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client でのデータストアからシステムへのファイルのダウンロード

管理対象のホスト上で使用可能なデータストアのファイルをローカル システムにダウンロードするには、データストア ファイル ブラウザを使用します。

前提条件

必要な権限：データストア.データストアの参照

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [データストア ブラウザ] をクリックします。

3 ターゲット データストアを選択します。

4 ダウンロードするファイルが格納されているフォルダをクリックします。

そのフォルダ内で使用可能なファイルが表示されます。

5 ダウンロードするファイルをクリックします。

6 [ダウンロード] をクリックします。

ファイルがシステムにダウンロードされます。

7 [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client でのデータストアからのファイルの削除

不要になったファイルをデータストアから永久に削除することができます。

前提条件

必要な権限：データストア.データストアの参照

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [データストア ブラウザ] をクリックします。

3 ターゲット データストアを選択します。

4 削除するファイルが格納されているフォルダを選択します。

そのフォルダ内で使用可能なファイルが表示されます。

5 データストアから削除するファイルをクリックし、[削除] をクリックし、再度 [削除] をクリックします。

6 [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client でのデータストア フォルダまたはファイルの移動

データストア ファイル ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所に、ファイルまたはフォルダを移動します。

注： 仮想ディスク ファイルは、フォーマット変換することなく移動およびコピーされます。移動元のホストとはタイプが異なるホスト上のデータストアに仮想ディスクを移動する場合は、仮想ディスクを使用する前に、仮想ディスクの変換が必要になることがあります。

前提条件

必要な権限：データストア.データストアの参照

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [データストア ブラウザ] をクリックします。

3 ターゲット データストアを選択します。

4 別の場所に移動するファイルまたはフォルダを選択し、[移動] をクリックします。

5 移動先の場所を選択し、[移動] をクリックします。

6 [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client でのデータストア フォルダまたはファイルのコピー

データストア ファイル ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所にフォルダまたはファイルをコピーします。

注： 仮想ディスク ファイルは、フォーマット変換することなく移動およびコピーされます。移動元のホストとはタイプが異なるホスト上のデータストアに仮想ディスクを移動する場合は、仮想ディスクの変換が必要になることがあります。

前提条件

必要な権限：データストア.データストアの参照

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [データストア ブラウザ] をクリックします。

3 ターゲット データストアを選択します。

4 別の場所に移動するファイルまたはフォルダを選択し、[コピー] をクリックします。

5 移動先の場所を選択し、[コピー] をクリックします。

6 [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client での新しいデータストア ディレクトリの作成

ファイルを特定の場所に保存する必要がある場合は、新しいデータストア ディレクトリを作成できます。

前提条件

必要な権限：データストア.データストアの参照

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 [データストア ブラウザ] をクリックします。

3 [ディレクトリの作成] をクリックします。

4 ターゲット データストアを選択します。

5 （オプション） 新規ディレクトリの名前を入力します。

6 [ディレクトリの作成] をクリックします。

7 [閉じる] をクリックしてファイル ブラウザを終了します。

VMware Host Client でのデータストア名の変更

VMware Host Client で、データストアの表示名を変更できます。

注： ホストを vCenter Server で管理している場合、VMware Host Client からデータストアの名前を変更することはできません。名前の変更は、ホストを管理している vCenter Server インスタンスからのみ実行できます。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 リスト内のデータストアを右クリックし、ドロップダウン メニューから [名前の変更] を選択します。

3 データストアの新しい名前を入力し、[保存] をクリックして変更を適用します。

4 （オプション） [更新] をクリックして、使用可能なデータストアのリストに新しいデータストア名が表示されるのを確認します。

VMware Host Client での VMFS データストアの削除

再署名せずにマウントされたコピーなど、あらゆるタイプの VMFS データストアを削除できます。データストアを削除すると、そのデータストアおよびそのデータストアと関連付けられているすべてのファイルがホストから削除されます。

注： データストアの削除操作により、仮想マシンに関連する、データストア上のすべてのファイルが永久に削除されます。アンマウントしなくてもデータストアを削除することはできますが、最初にデータストアをアンマウントすることをお勧めします。

前提条件

すべての仮想マシンをデータストアから削除します。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [データストア] の順にクリックします。

2 リスト内のデータストアを右クリックし、ドロップダウン メニューから [削除] を選択します。

3 [確認] をクリックしてデータストアを削除します。

VMware Host Client でのストレージのシン プロビジョニング

ESXi では、アレイ レベルと仮想ディスク レベルという、2 つのモデルのシン プロビジョニングを使用できます。

シン プロビジョニングは、オンデマンドで柔軟にストレージ容量を割り当てることによって、ストレージ利用を最適化する方法です。シン プロビジョニングは、シック プロビジョニングと呼ばれる従来のモデルと対照的なものです。シック プロビジョニングを使用すると、将来のストレージの必要性を事前に予測して大量のストレージ容量が提供されます。ただし、容量は未使用のままとなり、ストレージのキャパシティを十分に利用できない場合があります。

VMware シン プロビジョニング機能は、データストアおよびストレージ アレイ レベルでストレージを十分に利用できない問題を解消するのに役立ちます。

VMware Host Client でシン プロビジョニングされた仮想ディスクの作成

ストレージ容量を節約するために、シン プロビジョニング仮想ディスクを作成することができます。シン プロビジョニング仮想ディスクは、最初は小さく、必要なディスク容量が増加するにつれて拡大します。シン ディスクは、ディスク レベルのシン プロビジョニングに対応したデータストアのみに作成できます。

次の手順では、新しい仮想マシンを作成すると想定します。詳細については、『VMware Host Client での仮想マシンの作成』を参照してください。

手順

1. VMware Host Client インベントリ内で [ホスト] を右クリックし、[仮想マシンの作成/登録] を選択します。

   [新規仮想マシン] ウィザードが開きます。
2. 新規仮想マシンをホスト上に追加する方法を選択し、[次へ] をクリックします。
3. 仮想マシンの名前を入力します。
4. 仮想マシンの互換性を [互換性] ドロップダウン メニューから選択します。
5. [ゲスト OS バージョン] ドロップダウン メニューからゲスト OS のバージョンを選択し、[次へ] をクリックします。
6. [新規仮想マシン] ウィザードの [ストレージの選択] ページに表示されるアクセス可能なデータストアのリストから、仮想マシンの構成ファイルおよびすべての仮想ディスクを置くデータストアを選択します。
7. [仮想ハードウェア] タブで、[ハード ディスク] を展開します。
8. [ディスク プロビジョニング] で [シン プロビジョニング] ラジオ ボタンを選択し、[次へ] をクリックします。
9. [新規仮想マシン] ウィザードの [設定の確認] ページで、仮想マシンの構成設定を確認し、[終了] をクリックして設定を保存します。

VMware Host Client での仮想マシン ストレージ リソースの表示

VMware Host Client で、仮想マシン用にデータストアのストレージ容量がどのように割り当てられているかを表示できます。

[リソース消費] には、構成ファイル、ログ ファイル、スナップショット、仮想ディスクなどの仮想マシン ファイルが占有しているデータストア容量が表示されます。仮想マシンが実行中の場合、使用済みストレージ容量にはスワップ ファイルも含まれます。

シン ディスクを持つ仮想マシンでは、実際のストレージ使用量は仮想ディスクのサイズよりも小さい場合があります。

手順

1 VMware Host Client インベントリ内で仮想マシンをクリックします。

2 仮想マシンのサマリ ページの右下の領域で、リソース消費に関する情報を確認します。

VMware Host Client での仮想マシンのディスク フォーマットの判別

仮想ディスクがシック フォーマットかシン フォーマットかを判別できます。

手順

1 VMware Host Client インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。

2 [仮想ハードウェア] タブで、[ハード ディスク] を展開します。

[タイプ] テキスト ボックスに仮想ディスクのフォーマットが表示されます。

VMware Host Client でのストレージ アダプタの管理

VMware Host Client を使用してホストまたは vCenter Server に接続する場合、各種の iSCSI コンポーネントの設定など、ストレージ アダプタでさまざまなタスクを実行できます。

VMware Host Client 環境で管理しているホストで iSCSI を有効にすると、新しいネットワーク ポート バインド、固定ターゲットおよび動的ターゲットの設定と追加、CHAP 認証の管理、およびホスト ストレージでのさまざまな設定を詳細に行うことができます。

VMware Host Client でのストレージ アダプタの表示

ホストが使用するストレージ アダプタと関連情報を表示します。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックし、[アダプタ] をクリックします。

そのホストが使用できるすべてのストレージ アダプタが、[アダプタ] に一覧表示されます。

2 特定のアダプタの詳細を表示するには、リストからアダプタを選択します。

VMware Host Client でのソフトウェア iSCSI アダプタの構成

ソフトウェア ベースの iSCSI を実装すると、標準の NIC を使用して、ホストを IP ネットワーク上のリモート iSCSI ターゲットに接続できます。ESXi に組み込まれたソフトウェア iSCSI アダプタは、ネットワーク スタックを介して物理 NIC と通信します。

注： ソフトウェア iSCSI アダプタを使用する前に、ネットワークを設定し、アダプタを有効にし、CHAP などのパラメータを設定する必要があります。

iSCSI アダプタ設定のワークフローには、次の手順が含まれます。

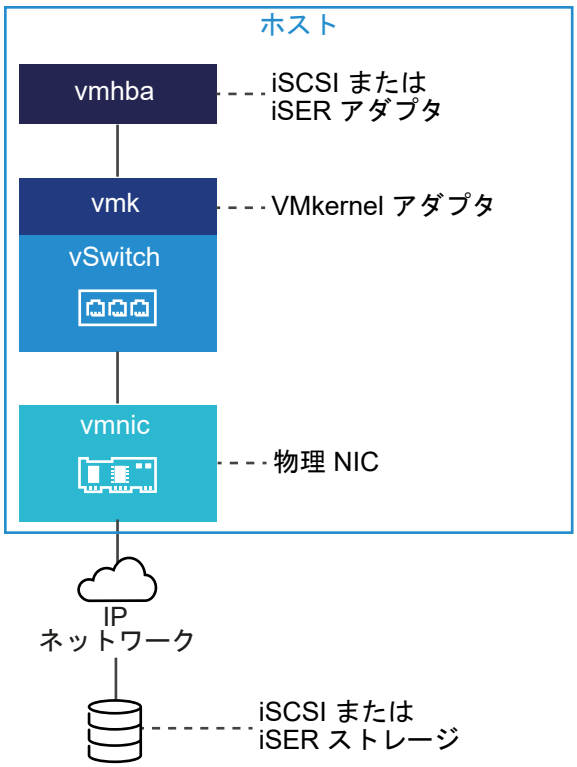
- ホスト上の iSCSI の有効化。 VMware Host Client での ESXi ホスト用 iSCSI の有効化を参照してください。
- ポート バインドの追加。 VMware Host Client でのポート バインドの追加 を参照してください。

- ポート バインドの削除。 VMware Host Client でのポート バインドの削除 を参照してください。

iSCSI および iSER 用ネットワークの設定

特定のタイプの iSCSI アダプタは、VMkernel ネットワークに依存します。これらのアダプタには、ソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタと、VMware iSCSI over RDMA (iSER) アダプタが含まれます。環境にこれらのアダプタのいずれかが含まれている場合は、iSCSI または iSER コンポーネントと物理ネットワーク アダプタの間のトラフィックの接続を構成する必要があります。

ネットワーク接続の構成には、各物理ネットワーク アダプタへの仮想 VMkernel アダプタの作成が含まれます。各仮想および物理ネットワーク アダプタ間で 1:1 のマッピングを使用します。その際に、VMkernel アダプタを適切な iSCSI または iSER アダプタと関連付けます。このプロセスをポート バインドと呼びます。



ポート バインドを設定するときは、次のルールに準拠します。

- ソフトウェア iSCSI アダプタは、ホストで使用可能な物理 NIC で接続できます。
- 依存型 iSCSI アダプタを接続する場合は、必ず固有の物理 NIC へ接続する必要があります。
- RDMA 対応のネットワーク アダプタにのみ、iSER アダプタを接続する必要があります。

ソフトウェア iSCSI でのネットワーク接続の使用時機と方法に関する特別の考慮事項については、http://kb.vmware.com/kb/2038869 にある VMware ナレッジ ベースの記事を参照してください。

VMware Host Client での ESXi ホスト用 iSCSI の有効化

VMware Host Client 環境でホストの iSCSI を有効にし、CHAP 認証、ネットワーク ポート バインド、固定ターゲット、動的ターゲット、さまざまな詳細設定などのストレージ アダプタのパラメータを設定します。

手順

1 VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。

2 [有効] ラジオ ボタンを選択します。

3 （オプション） 変更するパラメータとコンポーネントを設定します。

4 [構成の保存] をクリックします。

ソフトウェア iSCSI とのネットワーク通信設定のベスト プラクティス

ソフトウェア iSCSI とのネットワーク通信を設定する際には、次のベスト プラクティスを考慮してください。

ソフトウェア iSCSI ポートのバインド

ESXi ホスト上のソフトウェア iSCSI イニシエータを 1 つ以上の VMkernel ポートにバインドすると、バインドされたポートのみを使用して iSCSI トラフィックがやり取りされるようになります。バインドされていないポートは iSCSI トラフィックに使用されません。

ポートのバインドを設定すると、バインドされたすべてのポートから、設定されたすべてのターゲット ポータルへの iSCSI セッションが iSCSI イニシエータにより確立されます。

次の例を参照してください。

VMkernel ポート	ターゲット ポータル	iSCSI セッション
バインドされた VMkernel ポート x 2	ターゲット ポータル x 2	4 つのセッション（2 x 2）
バインドされた VMkernel ポート x 4	ターゲット ポータル x 1	4 つのセッション（4 x 1）
バインドされた VMkernel ポート x 2	ターゲット ポータル x 4	8 つのセッション（2 x 4）

注： ポートのバインドを使用する場合は、すべての VMkernel ポートからすべてのターゲット ポータルに到達可能であることを確認してください。到達可能でない場合は、iSCSI セッションの確立に失敗する可能性があります。その結果、再スキャン処理に予想以上の時間がかかる場合があります。

ポートのバインドを使用しない場合

ポートのバインドを使用しない場合は、ESXi ネットワーク レイヤーのルーティング テーブルに従って最適な VMkernel ポートが選択されます。ホストはこのポートを使用してターゲット ポータルとの iSCSI セッションを確立します。ポートのバインドを使用しない場合、確立されるセッションは、1 つのターゲット ポータルにつき 1 つのみです。

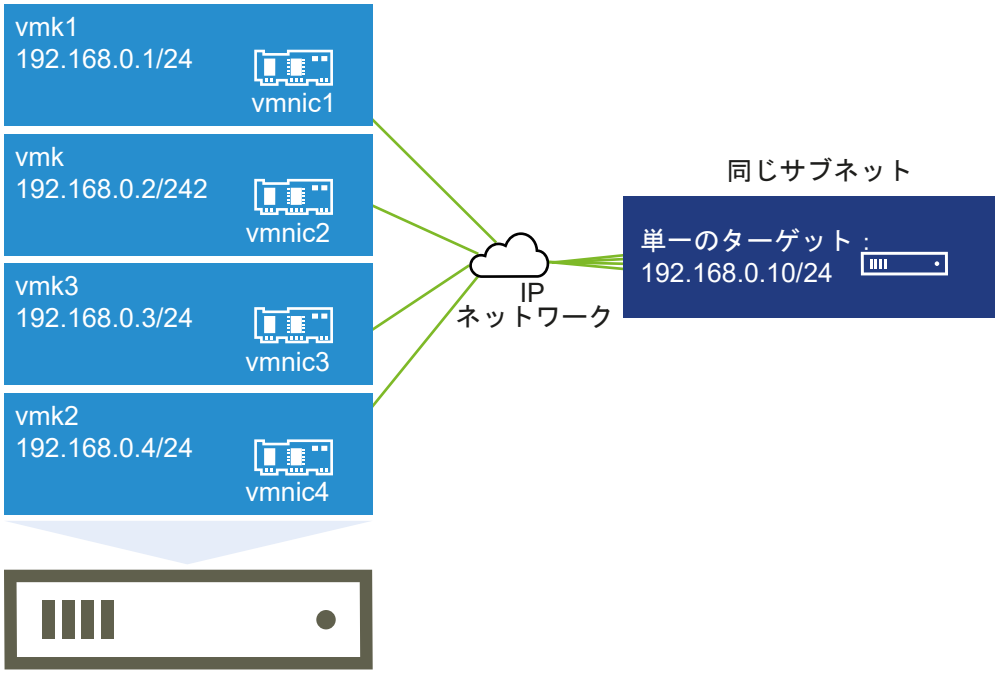
次の例を参照してください。

VMkernel ポート	ターゲット ポータル	iSCSI セッション
バインドされていない VMkernel ポート x 2	ターゲット ポータル x 2	2 つのセッション
バインドされていない VMkernel ポート x 4	ターゲット ポータル x 1	1 つのセッション
バインドされていない VMkernel ポート x 2	ターゲット ポータル x 4	4 つのセッション

ソフトウェア iSCSI でのマルチパスの使用

例 1：ネットワーク ポータルが 1 つだけの場合の iSCSI ターゲットへのマルチパス

ターゲットにネットワーク ポータルが 1 つしか存在しない場合は、ESXi ホストで複数の VMkernel ポートを追加し、それらのポートを iSCSI イニシエータにバインドすることで複数のパスを作成できます。

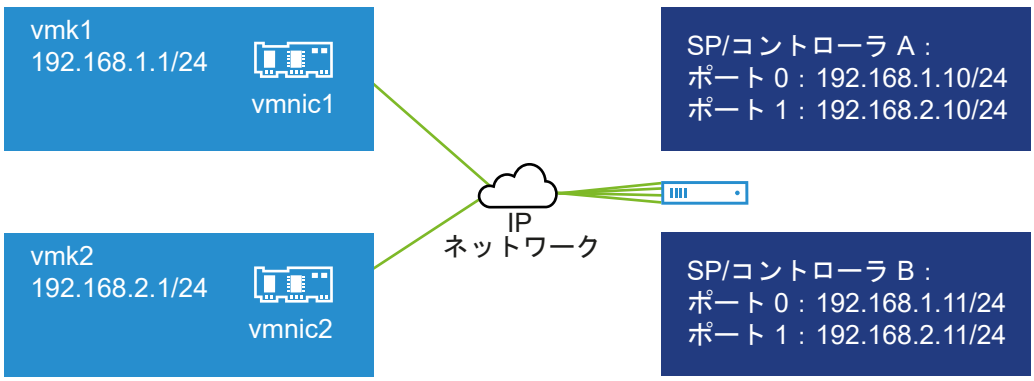


この例では、すべてのイニシエータ ポートとターゲット ポータルが同じサブネットに属しています。また、バインドされているすべてのポートを通じてターゲットに到達できます。VMkernel ポートが 4 つ、ターゲット ポータルが 1 つ存在するため、合計 4 つのパスが作成されます。

ポートのバインドを使用しない場合、作成されるパスは 1 つのみです。

例 2：VMkernel ポートが異なるサブネットに属す場合のマルチパス

異なる IP サブネットに属す複数のポートとターゲット ポータルを設定することで、複数のパスを作成できます。イニシエータとターゲット ポートを異なるサブネットに分けておくと、特定のポートを経由するパスが ESXi により作成されます。ポートのバインドを設定するにはすべてのイニシエータとターゲット ポートが同じサブネットに属している必要があるため、この構成ではポートのバインドを使用しません。



3 つのポートがすべて同じサブネットに属しているため、ESXi はコントローラ A とコントローラ B のポート 0 に接続する際に vmk1 を選択します。同様に、コントローラ A とコントローラ B のポート 1 に接続する際には vmk2 が選択されます。この構成では NIC チーミングを使用できます。

合計 4 つのパスが作成されます。

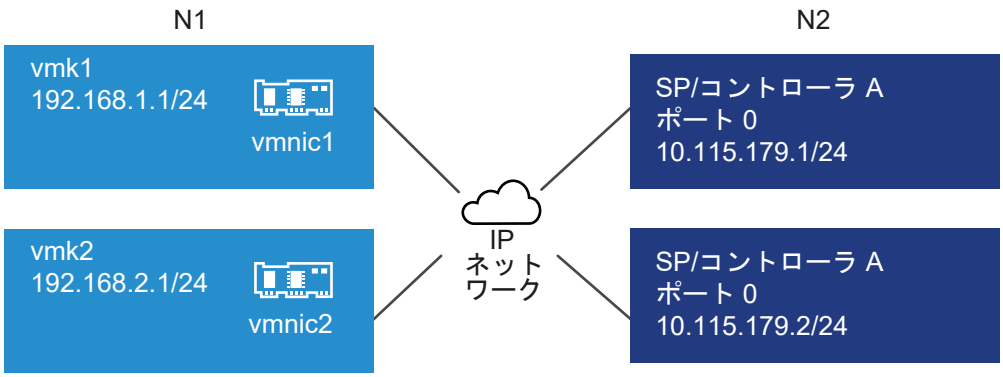
パス	説明
パス 1	vmk1 とコントローラ A のポート 0
パス 2	vmk1 とコントローラ B のポート 0
パス 3	vmk2 とコントローラ A のポート 1
パス 4	vmk2 とコントローラ B のポート 1

ソフトウェア iSCSI によるルーティング

iSCSI トラフィック用のスタティック ルートを追加するには、`esxcli` コマンドを使用します。スタティック ルートを設定すると、異なるサブネットに属すイニシエータとターゲット ポートの間で通信を行えるようになります。

例 1：ポートのバインドを使用する場合のスタティック ルートの使用例

この例では、バインドされるすべての VMkernel ポートを 1 つのサブネット (N1) に残し、すべてのターゲット ポータルを別のサブネット (N2) に設定します。その後、ターゲット サブネット (N2) のスタティック ルートを追加できます。

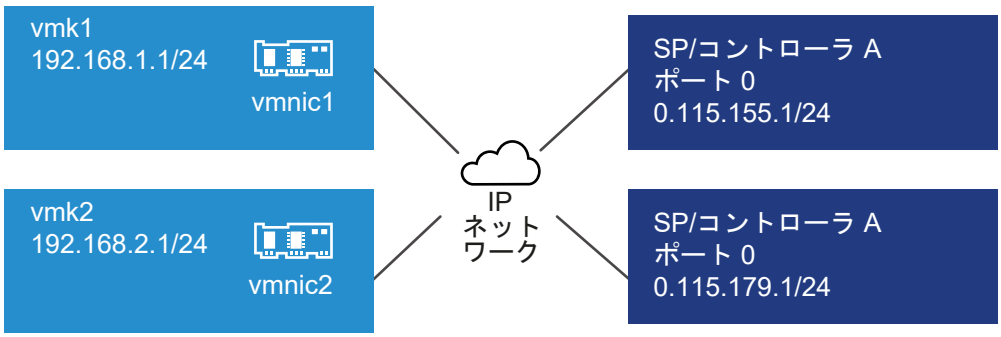


次のコマンドを使用します。

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

例 2：複数のパスを作成する場合のスタティック ルートの使用例

この構成では、異なるサブネットを使用するときにスタティック ルートを使用します。この構成では、ポートのバインドを使用できません。



vmk1 と vmk2 を別々のサブネット（192.168.1.0 と 192.168.2.0）に設定します。ターゲット ポータルも別々のサブネット（10.115.155.0 と 10.155.179.0）に属しています。

vmk1 から 10.115.155.0 のスタティック ルートを追加できます。vmk1 からゲートウェイに到達可能であることを確認してください。

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.155.0/24
```

その後、vmk2 から 10.115.179.0 のスタティック ルートを追加できます。vmk2 からゲートウェイに到達可能であることを確認してください。

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network
10.115.179.0/24
```

コントローラ A のポート 0 に接続する際には vmk1 が使用されます。

コントローラ B のポート 0 に接続する際には vmk2 が使用されます。

例 3：vmkernel ポートごとに異なるゲートウェイを使用する場合のルーティング

vSphere 6.5 以降では、VMkernel ポートごとに異なるゲートウェイを設定できます。DHCP を使用して VMkernel ポートの IP アドレス設定を取得する場合は、DHCP を使用してゲートウェイ情報も取得できます。

VMkernel ポートごとのゲートウェイ情報を表示するには、次のコマンドを使用します。

```
# esxcli network ip interface ipv4 address list
```

```
Name  IPv4 Address    IPv4 Netmask   IPv4 Broadcast  Address Type  Gateway         DHCP DNS
----  --------------  -------------  --------------  ------------  --------------  --------
vmk0  10.115.155.122  255.255.252.0  10.115.155.255  DHCP          10.115.155.253      true
vmk1  10.115.179.209  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
vmk2  10.115.179.146  255.255.252.0  10.115.179.255  DHCP          10.115.179.253      true
```

VMkernel ポートごとに異なるゲートウェイを使用する場合は、ポートのバインドを使用して異なるサブネットに属すターゲットに到達できます。

VMware Host Client でのポート バインドの追加

VMware Host Client を使用して、iSCSI アダプタとホスト上の VMkernel アダプタをバインドします。

前提条件

- ホスト上の各物理ネットワーク アダプタ用に、仮想 VMkernel アダプタを作成します。複数の VMkernel アダプタを使用する場合は、正しいネットワーク ポリシーを設定してください。
- 必要な権限：ホスト.構成.ストレージ パーティション構成

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. [ネットワーク ポートのバインド] セクションで、[ポート バインドの追加] をクリックします。
3. iSCSI アダプタとバインドする VMkernel アダプタを選択します。

   注： VMkernel アダプタのネットワーク ポリシーがバインド要件に準拠していることを確認してください。

   ソフトウェア iSCSI アダプタは、1 つ以上の VMkernel アダプタにバインドできます。依存型ハードウェア iSCSI アダプタの場合は、正しい物理 NIC と関連付けられた VMkernel アダプタを 1 つのみ使用できます。
4. [選択] をクリックします。
5. [構成の保存] をクリックします。

VMware Host Client でのポート バインドの削除

ホスト上の iSCSI 構成を編集して、ポート バインドを削除します。

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. [ネットワーク ポートのバインド] セクションで、リストから VMkernel NIC を選択します。
3. [ポート バインドの削除] をクリックします。
4. [構成の保存] をクリックします。

VMware Host Client での動的ターゲットの設定

iSCSI アダプタがネットワーク上のアクセス可能なストレージ リソースを特定できるように、ターゲット検出アドレスを設定する必要があります。ESXi ホストは、動的および静的な検出方法をサポートしています。動的検出では、イニシエータが特定の iSCSI ストレージ システムに接続するたびに、SendTargets 要求が iSCSI システムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供します。

SendTargets 検出とも呼ばれます。イニシエータが指定された iSCSI サーバに接続するたびに、イニシエータはターゲットの SendTargets 要求をサーバに送信します。サーバは、使用可能なターゲットのリストをイニシエータに提供することで応答します。これらのターゲットの名前および IP アドレスは、[静的検出] タブに表示されます。動的検出で追加された静的ターゲットを削除する場合、このターゲットは、次回の再スキャン実行時、iSCSI アダプタのリセット時、またはホストの再起動時にリストに戻すことができます。

注： ESXi は、ソフトウェア iSCSI および依存型ハードウェア iSCSI を使用して、指定した iSCSI サーバ アドレスの IP ファミリに基づいてターゲット アドレスをフィルタリングします。アドレスが IPv4 の場合、iSCSI サーバからの SendTargets 応答で取得される可能性のある IPv6 アドレスは除外されます。iSCSI サーバを指定するために DNS 名が使用されている場合や、iSCSI サーバからの SendTargets 応答に DNS 名が含まれている場合、ESXi は、DNS ルックアップで最初に解決されたエントリの IP ファミリを使用します。

動的検出の設定では、新しい iSCSI システムのみを追加できます。既存の iSCSI システムの IP アドレス、DNS 名、またはポート番号は変更できません。パラメータを変更するには、既存のシステムを削除してから新しく追加します。

前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. [動的ターゲットの追加] をクリックします。

   新しい動的ターゲットがリストに表示されます。
3. 新しい動的ターゲットに対しアドレスを追加するには、リストのターゲットをクリックして、アドレスを入力します。
4. （オプション） 新しい動的ターゲットのポート番号を変更するには、ターゲットの [ポート] テキスト ボックスをクリックして、新しいポート番号を入力します。
5. （オプション） 動的ターゲット設定を編集するには、使用可能なターゲットのリストから新しいターゲットを選択して、[設定の編集] をクリックし、変更するパラメータを設定して、[保存] をクリックします。
6. （オプション） 特定のターゲットを削除するには、該当のターゲットを選択して [動的ターゲットの削除] をクリックします。

   ターゲットが既存の動的ターゲットのリストに表示されなくなります。
7. [構成の保存] をクリックします。

VMware Host Client での固定ターゲットの設定

iSCSI イニシエータで静的検出を使用して、ターゲットに関する情報を手動で入力できます。

静的検出の設定では、新しい iSCSI ターゲットのみを追加できます。既存のターゲットの IP アドレス、DNS 名、iSCSI ターゲット名、またはポート番号は変更できません。これを変更するには、既存のターゲットを削除して新しいターゲットを追加します。

動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。iSCSI アダプタは、提供したターゲットのリストを使用して、iSCSI サーバに接続して通信します。

前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. [固定ターゲットの追加] をクリックします。

   新しい固定ターゲットがリストに表示されます。
3. 新しい固定ターゲットに対し名前を追加するには、リスト内のターゲットをクリックして、名前を入力します。
4. 新しい固定ターゲットに対しアドレスを追加するには、リストのターゲットをクリックして、アドレスを入力します。
5. （オプション） 新しい固定ターゲットのポート番号を変更するには、ターゲット [ポート] テキスト ボックスをクリックして、新しいポート番号を入力します。
6. （オプション） 固定ターゲット設定を編集するには、使用可能なターゲットのリストから新しいターゲットを選択して、[設定の編集] をクリックし、変更するパラメータを設定して、[保存] をクリックします。
7. （オプション） 特定のターゲットを削除するには、該当のターゲットを選択して [固定ターゲットの削除] をクリックします。

   ターゲットが既存の固定ターゲットのリストに表示されなくなります。
8. [構成の保存] をクリックします。

VMware Host Client での iSCSI の詳細設定の編集

iSCSI の詳細設定では、ヘッダ ダイジェスト、データ ダイジェスト、ARP リダイレクト、遅延 ACK などのパラメータを制御します。通常、割り当てられた定義済みの値でホストは正しく動作するので、これらの設定を変更する必要はありません。

注意： VMware サポート チームとの支援を受けて作業しているか、iSCSI の詳細設定で指定する値についての十分な情報がある場合を除き、この詳細設定を変更しないでください。

前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. [詳細設定] をクリックして、設定のリスト全体を表示します。
3. 変更するパラメータを編集し、[構成の保存] をクリックします。

VMware Host Client での iSCSI アダプタ用 CHAP 認証の設定

すべてのターゲットが、イニシエータ レベルで、同一の CHAP 名および CHAP シークレットを iSCSI イニシエータから受け取るように設定できます。デフォルトでは、すべての検出アドレスまたは固定ターゲットは、イニシエータ レベルで設定された CHAP パラメータを継承します。

CHAP 名は 511 文字未満の英数字、CHAP シークレットは 255 文字未満の英数字である必要があります。一部のアダプタでは、この上限の値がさらに小さい場合があります。たとえば、QLogic アダプタの上限値は、CHAP 名では 255 文字、CHAP シークレットでは 100 文字です。

前提条件

- ソフトウェアまたは依存型ハードウェア iSCSI に対し CHAP パラメータを設定する前に、通常の片方向の CHAP 認証、または双方向の相互 CHAP 認証のどちらを設定するか決定します。独立型ハードウェア iSCSI アダプタは、双方向の CHAP 認証をサポートしません。
  - 片方向の CHAP では、ターゲットがイニシエータを認証します。
  - 相互 CHAP では、ターゲットおよびイニシエータの両方が互いを認証します。CHAP と相互 CHAP にそれぞれ異なるシークレットを使用します。

  CHAP パラメータを設定するときには、それらのパラメータがストレージ側のパラメータと一致するようにします。
- 必要な権限：ホスト.構成.ストレージ パーティション構成

手順

1. VMware Host Client インベントリ内で [ストレージ] > [アダプタ] > [iSCSI の構成] の順にクリックします。
2. 片方向の CHAP を設定するには、[CHAP 認証] を展開して、すべてのパラメータを表示します。
   a. CHAP のセキュリティ レベルを選択します。
   b. CHAP 名を入力します。

      入力する名前が、ストレージ側で設定した名前と一致するようにします。
   c. 認証に使用する片方向の CHAP シークレットを入力します。ストレージ側で入力するのと同じシークレットを使用してください。
3. 相互 CHAP を設定するには、片方向の CHAP 用のオプションとして [CHAP を使用] を選択します。[相互 CHAP 認証] を展開して、すべてのパラメータを表示します。
   a. [CHAP を使用する] を選択します。
   b. 相互 CHAP 名を入力します。
   c. 相互 CHAP シークレットを入力します。

      片方向の CHAP と相互 CHAP にそれぞれ異なるシークレットを使用します。
4. [構成の保存] をクリックします。

結果

iSCSI アダプタの認証設定を変更する場合、新しい iSCSI セッションでは更新された認証情報のみを使用します。強制再認証などの外的な要因で接続が失われるか、アダプタの iSCSI ターゲットを削除して追加しない限り、既存のセッションは継続します。

VMware Host Client でのストレージ デバイスの管理

VMware Host Client を使用して、管理対象 ESXi ホストがアクセスするローカル ストレージ デバイスおよびネットワーク ストレージ デバイスを管理できます。

VMware Host Client でのストレージ デバイスの表示

ホストで使用可能なすべてのストレージ デバイスを表示します。サードパーティ製のマルチパス プラグインを使用している場合は、プラグインを介して使用できるストレージ デバイスもリストに表示されます。

[ストレージ デバイス] ビューでは、ホストのストレージ デバイスの一覧表示、それらの情報の分析、プロパティの修正を行うことができます。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックし、[デバイス] をクリックします。

そのホストが使用できるすべてのストレージ デバイスが、[デバイス] に一覧表示されます。

2 特定のデバイスの詳細情報を表示するには、リストからデバイスを選択します。

VMware Host Client での、デバイス パーティション テーブルのクリア

VMware Host Client を使用して ESXi ホストにログインする場合、そのホストからアクセスできるディスク デバイスのパーティション テーブルをクリアできます。

前提条件

デバイスが起動ディスク、VMFS データストア、または vSAN として ESXi で使用されていないことを確認します。

手順

1 VMware Host Client で [ストレージ] をクリックし、[デバイス] をクリックします。

2 リスト内のデバイスを右クリックし、[パーティション テーブルをクリア] をクリックし、[はい] をクリックします。

パーティション テーブルを変更すると、データが失われる場合があります。

VMware Host Client での個々のデバイス パーティションの編集

ESXi ホストに VMware Host Client でログインすると、パーティション エディタを使用して、デバイスの個々のパーティションを削除できます。

前提条件

デバイスが起動ディスク、VMFS データストア、または vSAN として ESXi で使用されていないことを確認します。

手順

1 VMware Host Client で [ストレージ] をクリックし、[デバイス] をクリックします。

2 リスト内のデバイスを右クリックし、[パーティションの編集] をクリックします。

3 パーティションを選択し、[パーティションの削除] をクリックします。

4 （オプション） [リセット] をクリックして、元のパーティションをリストアします。

5 [パーティションの保存] をクリックします。

6 パーティションを変更することを確認します。

永続的なメモリの管理

ESXi 6.7 以降では、不揮発性メモリ (NVM) または永続的なメモリ (PMEM) と呼ばれる、最新のコンピュータ メモリ テクノロジーをサポートしています。PMEM は、揮発性メモリの高速データ転送と、従来型ストレージのパーシステンスおよび耐障害性を併せ持っています。PMEM デバイスでは、アクセス時の遅延が低く抑えられ、再起動または電源の停止中でも格納されたデータが保持されます。

ホストの永続的なメモリ リソースの使用量のモード

ホストに物理的な PMEM デバイスを追加すると、ESXi は PMEM リソースを検出し、ホスト上で稼動する仮想マシンにホストのローカル PMEM データストアとして公開します。ゲスト OS によっては、仮想マシンから PMEM リソースに直接アクセスできます。

各ホストには、ホストのすべての PMEM リソースをプールして表示するローカルの PMEM データストアを 1 台のみ配置できます。

永続的なメモリは、メモリとストレージの両方の特性を兼ね備えています。そのため、仮想マシンは、ESXi ホストの PMEM リソースをメモリ（仮想 NVDIMM デバイス経由）またはストレージ（仮想 PMEM ハードディスク経由）として使用できます。

ホストのローカル PMEM データストアは、すべての直接アクセスした NVDIMM デバイスと仮想 PMEM ハードディスクを格納します。

仮想 PMEM (vPMEM)

このモードでは、ゲスト OS が PMEM に対応している場合、仮想マシンは、ホストの物理 PMEM リソースに直接アクセスできるため、リソースを標準的なバイト アドレス指定が可能なメモリとして使用できます。

仮想マシンは、PMEM への直接アクセスに NVDIMM (virtual non-volatile dual in-line memory modules) を使用します。NVDIMM は メモリ デバイスの一種で、通常のメモリ チャネルに搭載されますが、不揮発性メモリが含まれています。vSphere 6.7 では、仮想 NVDIMM は新しいタイプのデバイスで、ホストの物理 PMEM 領域を指します。1 台の仮想マシンには、最大 64 個の NVDIMM デバイスを割り当てることができます。各 NVDIMM デバイスは、ホストのローカル PMEM データストアに格納されます。

注： 仮想マシンに NVDIMM デバイスを追加するには、仮想マシンがハードウェア バージョン 14 で、ゲスト OS が永続的なメモリをサポートしている必要があります。ゲスト OS が PMEM に対応していない場合でも、PMEM を使用できますが、仮想マシンに NVDIMM デバイスを追加することはできません。

仮想 PMEM ディスク (vPMemDisk)

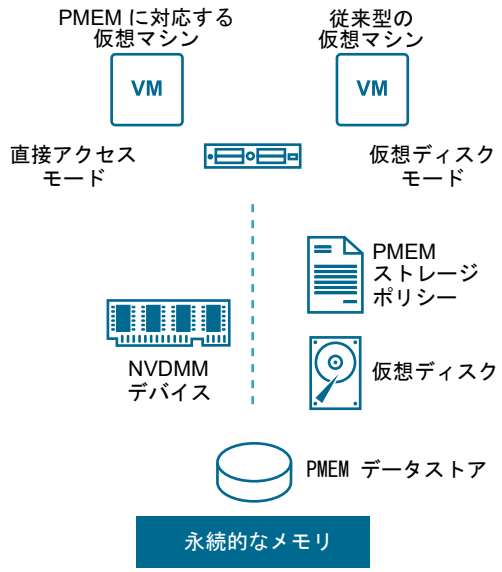
このモードでは、仮想マシンがホストの PMEM リソースに直接アクセスすることはありません。

仮想マシンに仮想 PMEM ハード ディスクを追加する必要があります。仮想 PMEM ハード ディスクは、PMEM ストレージ ポリシーが適用される従来型の SCSI ディスクです。ポリシーにより、ハード ディスクがホストのローカル PMEM データストアに自動的に配置されます。

このモードの使用については、仮想マシンのハードウェア バージョンおよびゲスト OS に要件はありません。

注： ゲスト OS が PMEM に対応していない場合、仮想マシンは vPMemDisk を介してのみ PMEM を使用できます。

次の図は、永続的なメモリのコンポーネントがどのように相互作用するかを示しています。



NVDIMM または仮想の永続的なメモリ ディスクを使用する仮想マシンを構成および管理する方法については、『vSphere のリソース管理』ドキュメントを参照してください。

PMEM データストアの構造

VMware Host Client ユーザー インターフェイスでは、ホスト - ローカル PMEM データストアの複雑な構造に関する情報が提供されます。この情報を分析し、トラブルシューティングや管理のために使用するには、複雑な構造に関する概念に精通する必要があります。

モジュール

VMware Host Client ユーザー インターフェイスでは、モジュールは、ホストのマザーボードに接続されている物理 NVDIMM を表します。

VMware Host Client では、各モジュールの健全性ステータスを確認し、健全でない NVDIMM モジュールを識別できます。

インターリーブ セット

インタリーブ セットは、1 つまたは複数のモジュールの論理グループです。インターリーブ セットは、物理 DIMM 間で情報を分散する方法と、ESXi がモジュールから情報を読み取る方法を示します。ESXi は各インタリーブ セットから順番に読み取るため、インタリーブ セットを使用するとメモリのスループットが向上します。

たとえば、1 つのインタリーブ セットが 2 つのモジュールで構成されている場合、ESXi は 2 つの物理 DIMM から並行して情報を読み取り、その後、次のインタリーブ セットに進みます。

VMware Host Client ユーザー インターフェイスでは、NVDIMM のインタリーブ セットのグループ化の方法についての情報を確認できます。

ネームスペース

名前空間とは、NVDIMM 内で連続したアドレスを持つメモリ領域です。名前空間は、複数のインタリーブ セットにまたがることができます。PMEM データストアは、名前空間の上に構築されます。

VMware Host Client では、各名前空間の容量、健全性ステータス、場所 ID を表示できます。

VMware Host Client でのモジュール、インタリーブ セット、および名前空間に関する情報の表示

VMware Host Client では、ホストのローカル PMEM データストアのモジュール、インタリーブ セット、および名前空間に関する情報を表示できます。そのため、健全でないモジュールを簡単に識別し、トラブルシューティングを実行することができます。

ホストのローカル PMEM データストアでは、ほとんどの従来のデータストア管理タスクを実行することができません。ただし、トラブルシューティングの目的で、モジュール、インタリーブ セット、および名前空間に関する情報を使用できます。

前提条件

ホストに少なくとも 1 つの物理 NVDIMM デバイスがあることを確認します。

手順

1 [ナビゲータ] ペインで、[ストレージ] をクリックします。

2 [永続的なメモリ] タブで、ホストのローカル PMEM データストアに関する情報を表示します。

- PMEM データストアを構成する NVDIMM に関する情報を表示するには、[モジュール] をクリックします。
- NVDIMM での名前空間に関する情報を表示するには、[名前空間] をクリックします。
- モジュールすなわち物理 NVDIMM がインタリーブ セットにどのようにグループ化されているかを確認するには、[インタリーブ セット] をクリックします。

VMware Host Client での、名前空間の削除

VMware Host Client では、ESXi によって作成された名前空間ではなく、ホスト マシンに以前にインストールされた OS によって作成された名前空間を削除できます。

前提条件

- ホストをメンテナンス モードに切り替えます。
- 名前空間のコンテンツが後で必要になる可能性がある場合には、コンテンツをバックアップします。

手順

1 VMware Host Client で、[ストレージ] をクリックします。

2 [永続的なメモリ] タブで、[名前空間] をクリックします。

3 （オプション） 名前空間のリストで、[状態] 列を確認して、ESXi が現在使用している名前空間を特定します。

容量を解放するには、状態が [使用中] の名前空間を削除する必要があります。

4 名前空間を選択し、[削除] アイコンをクリックします。

重要： 名前空間を削除すると、データストア上の容量が解放されますが、ホストを再起動した後にのみ空き容量を使用できます。

5 ホストを再起動するには、[ホストの再起動] アイコンをクリックします。

結果

選択した名前空間が PMEM データストアから削除されます。ESXi は、PMEM データストアで使用できる新しい名前空間を自動的に作成します。新しい名前空間は、削除されたものと同じ容量、タイプ、およびロケーション ID を持ちます。

VMware Host Client でのストレージの監視

VMware Host Client で、管理対象 ESXi ホストのストレージの健全性を監視できます。管理対象のホスト上で、さまざまなデータストア、ストレージ アダプタ、およびストレージ デバイスと関連付けられているイベントやタスクを表示することもできます。

VMware Host Client でのデータストアの監視

VMware Host Client で、データストアの健全性や、そのデータストアと関連付けられているイベントおよびタスクを監視できます。VSphere 6.5 Update 1 以降で、vSphere Client の vSAN サービスを有効にした後でも、vSAN 環境を監視できます。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックします。

2 [データストア] をクリックします。

3 リスト内のデータストアをクリックします。

VMware Host Client インベントリ内でそのデータストアが展開します。

4 データストア名の下の [監視] をクリックします。

5 （オプション）そのデータストアと関連付けられているイベントを表示するには、[イベント] をクリックします。

6 （オプション） ホストの vSAN 環境の構成パラメータを表示するには、[vSAN] をクリックします。

7 （オプション） このデータストアにあるホストを表示するには、[ホスト] をクリックします。

8 （オプション）[パフォーマンス サービス]、[ネットワーク]、[物理ディスク]、[データ]、[クラスタ]、[制限] などのさまざまなパラメータのステータスの詳細を表示するには、[健全性] をクリックします。

VMware Host Client での vSAN の監視

VMware Host Client を使用して、ESXi ホストの vSAN 環境を監視できます。

vSAN の概念

VMware vSAN では、仮想マシンの共有ストレージをソフトウェア ベースで作成する方法を使用します。ESXi ホストのローカルの物理ストレージ リソースを仮想化し、サービス品質要件に沿って仮想マシンとアプリケーションに分割して割り当てることができる、ストレージのプールに変換します。vSAN は ESXi ハイパーバイザーに直接実装されます。

vSAN は、ハイブリッドのクラスタまたはオールフラッシュのクラスタのいずれかに構成できます。ハイブリッドのクラスタでは、キャッシュ レイヤーにフラッシュ デバイスが使用され、ストレージ キャパシティ レイヤーに磁気ディスクが使用されます。 オールフラッシュのクラスタでは、キャッシュとキャパシティの両方でフラッシュ デバイスが使用されます。

vSAN は、既存のホスト クラスタで、または新しく作成するクラスタで、有効にできます。vSAN は、すべてのローカル キャパシティ デバイスを、vSAN クラスタのすべてのホストによって共有される単一のデータストアに集約します。データストアは、キャパシティ デバイスまたはキャパシティ デバイスが搭載されているホストをクラスタに追加することにより、拡張することができます。 vSAN のベスト プラクティスとして、クラスタのすべての ESXi ホストが、すべてのクラスタ メンバーと同様または同一の構成にすることをお勧めします。これにはストレージ構成も含まれます。この一貫した構成により、クラスタ内のすべてのデバイスおよびホストで、仮想マシンのストレージ コンポーネントが分散されます。ローカル デバイスを持たないホストでも、vSAN データストアに仮想マシンを参加させて実行することができます。

ホストがローカル ストレージ デバイスを vSAN データストアに提供する場合、フラッシュ キャッシュ用に少なくとも 1 個のデバイスを提供し、キャパシティ用に少なくとも 1 個のデバイスを提供する必要があります。キャパシティ デバイスはデータ ディスクとも呼ばれます。

提供元のホスト上のデバイスは、1 つ以上のディスク グループを形成します。各ディスク グループには、1 つのフラッシュ キャッシュ デバイスと、恒久的ストレージ用の 1 つまたは複数のキャパシティ デバイスが含まれています。各ホストは、複数のディスク グループを使用するように構成できます。

vSAN クラスタの設計およびサイジングに関するベスト プラクティス、容量の考慮事項、および一般的な推奨事項については、『VMware vSAN 設計とサイジングのガイド』を参照してください。

vSAN の特性

このトピックでは、vSAN とそのクラスタ、およびデータストアに適用される特性を概説します。

vSAN は、お使いの環境に数多くののメリットを提供します。

表 6-1. vSAN の機能

サポートされている機能	説明
共有ストレージ サポート	vSAN は、HA、vMotion、および DRS など、共有ストレージが必要な VMware 機能をサポートしています。たとえば、ホストの負荷が高くなると、DRS はクラスタ内の他のホストに仮想マシンを移行できます。
オンディスク フォーマット	vSAN のオンディスク仮想ファイル フォーマットは、vSAN クラスタごとに拡張性の高いスナップショットとクローン管理サポートを提供します。vSAN クラスタごとにサポートされる仮想マシン スナップショットとクローンの数については、『構成の上限』ドキュメントを参照してください。
オールフラッシュ構成とハイブリッド構成	vSAN は、オールフラッシュまたはハイブリッド クラスタで構成できます。
フォールト ドメイン	vSAN は、vSAN クラスタがデータセンターの複数のラックまたはブレード サーバ シャーシにまたがる場合に、ラックまたはシャーシの障害からホストを保護するフォールト ドメイン構成をサポートしています。
iSCSI ターゲット サービス	vSAN iSCSI ターゲット サービスを使用すると、vSAN クラスタ外のホストおよび物理ワークロードが vSAN データストアにアクセスできます。
ストレッチ クラスタ	vSAN は 2 つの地理的な場所にまたがるストレッチ クラスタをサポートします。
Windows Server Failover Clustering (WSFC) のサポート	vSAN 6.7 Update 3 以降のリリースでは、共有ディスクへのアクセスをノード間で調停するために、Windows Server Failover Clustering (WSFC) で要求される仮想ディスク レベルでの SCSI-3 Persistent Reservations (SCSI3-PR) がサポートされます。SCSI-3 PR がサポートされることにより、vSAN データストアでネイティブに仮想マシン間で共有されているディスク リソースを使用して WSFC を構成できます。 現在、以下の構成がサポートされています。 ■ クラスタあたり最大 6 個のアプリケーション ノード。 ■ ノードあたり最大 64 台の共有仮想ディスク。 **注：** vSAN では、Microsoft Windows Server 2012 以降で実行される Microsoft SQL Server 2012 以降の動作が確認済みです。
vSAN Health Service	vSAN Health Service には、クラスタ コンポーネントの問題の原因を監視、トラブルシューティング、診断し、潜在的なリスクを識別する事前構成済みの健全性チェック テストが含まれています。

表 6-1. vSAN の機能 （続き）

サポートされている機能	説明
vSAN パフォーマンス サービス	vSAN パフォーマンス サービスには、IOPS、スループット、遅延、および輻輳の監視に使用される統計チャートが含まれています。vSAN クラスタ、ホスト、ディスク グループ、ディスク、および仮想マシンのパフォーマンスを監視できます。
組み込みの vSphere ストレージ機能	vSAN は、従来から VMFS および NFS ストレージとともに使用されている vSphere のデータ管理機能が組み込まれています。これらの機能には、スナップショット、リンク クローン、vSphere Replication が含まれます。
仮想マシン ストレージ ポリシー	vSAN では、仮想マシン ストレージ ポリシーと連携して、仮想マシン中心のストレージ管理をサポートしています。 仮想マシンのデプロイ中にストレージ ポリシーを割り当てない場合は、vSAN のデフォルト ストレージ ポリシーが自動的に仮想マシンに割り当てられます。
迅速なプロビジョニング	vSAN では、仮想マシンの作成中およびデプロイ中に、vCenter Server® で迅速にストレージをプロビジョニングできます。
デデュープおよび圧縮	vSAN はブロックレベルのデデュープおよび圧縮を実行してストレージ容量を節約します。vSAN オールフラッシュ クラスタでデデュープおよび圧縮を有効にすると、各ディスク グループ内の冗長なデータが削減されます。デデュープと圧縮の設定はクラスタ全体に行いますが、これらの機能はディスク グループ単位で適用されます。圧縮のみの vSAN はディスク単位で適用されます。
保存データの暗号化	vSAN では、保存データの暗号化が提供されます。データの暗号化は、デデュープなどの他のすべての処理が実行された後に行われます。保存データの暗号化を行うと、クラスタからデバイスが削除された場合に備えて、ストレージ デバイス上のデータが保護されます。
SDK サポート	VMware vSAN SDK for Java は、VMware vSphere Management SDK の拡張機能です。これには、開発者が vSAN のインストール、構成、監視、およびトラブルシューティングを自動化する際にに役立つドキュメント、ライブラリ、およびコード サンプルが含まれています。

VMware Host Client の vSAN を監視します。

VMware Host Client を使用して、ESXi ホストの vSAN 環境を監視できます。

前提条件

vSAN に関連するデータストアの画面を表示するには、vSphere Client で vSAN サービスを有効にしておく必要があります。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックします。

2 [データストア] タブで [vSAN データストア] をクリックします。

VMware Host Client ナビゲータで、vSAN データストアが展開されます。

3 [監視] をクリックします。

ユーザー インターフェイスに [vSAN]、[ホスト]、および [健全性] タブが表示されます。

オプション	説明
[vSAN]	現在のホストの構成が表示されます。要求モードと重複解除の設定を編集できます。次に関する設定も表示できます。 ■ 暗号化 - vSAN は vSAN データストア全体の情報の暗号化をサポートします。 ■ iSCSI サービス - iSCSI サービスを介した追加サービスです。 ■ パフォーマンス サービス - データストアの動作に関するデータを収集します。たとえば、読み書き操作の速度です。
[ホスト]	vSAN サーバにあるすべてのホストのリストを、ホストの IP アドレスと、ホストが属するフォルト ドメインと共に表示します。
[健全性]	[健全性] タブには、グループごとに編成したテストが含まれています。次のグループが表示されます。 ■ パフォーマンス サービス ■ ネットワーク ■ 物理ディスク ■ データ ■ クラスタ ■ 制限 各グループには、エラー、警告、不明、良好を表すステータス アイコンが付いています。グループのステータスは、そのグループに属するテストの最も重大な状態を表します。テストとその説明を表示するには、対象となるグループの右上隅にある展開アイコンをクリックします。展開されたカードから、グループに属するすべてのテストやテストの実行結果を確認できるほか、各テストでのシステムの調査対象に関する詳細情報を得られます。

4 監視する vSAN パラメータを選択します。

vSAN データストアの設定の編集

現在のホストの誤った構成状態を解消する必要がある場合は、vSAN データストアの設定を編集できます。

vSAN データストアの [要求モード] と [重複解除] の設定のみを編集できます。これらの変更は、現在のホストでのみ有効です。vSAN クラスタに参加している他のホストには同期されません。

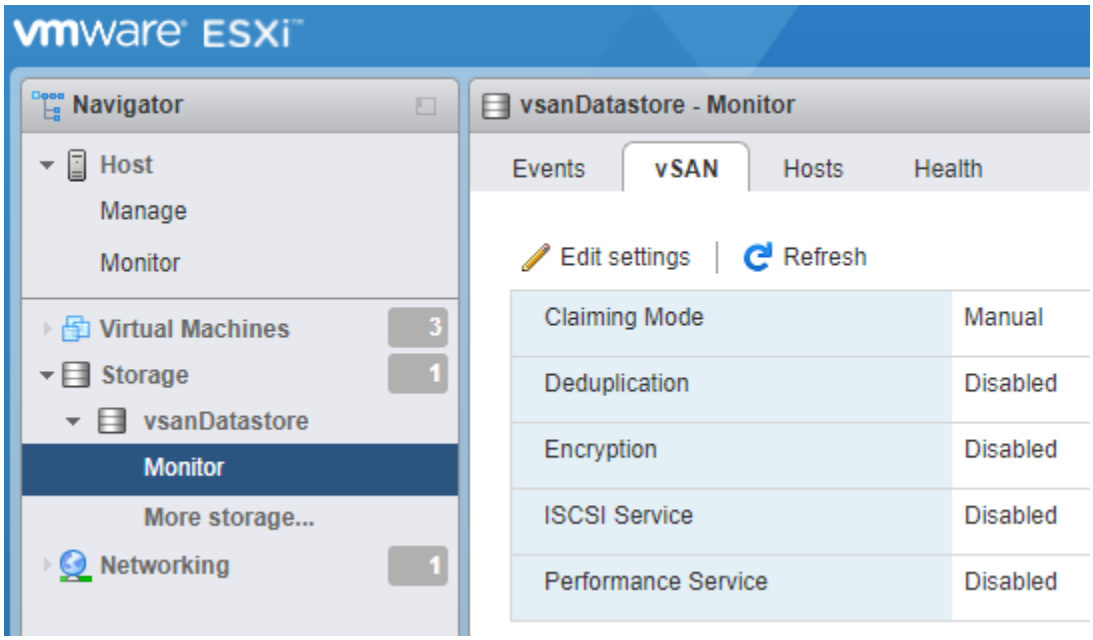
注： これらの設定は、トラブルシューティングにのみ使用します。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックします。

2 [データストア] タブで、テーブルから vSAN データストアをクリックします。

3 [監視] をクリックし、[vSAN] タブをクリックします。



4 [設定の編集] をクリックします。

[設定の編集] ダイアログ ボックスが開きます。

5 設定を変更します。[要求モード] から [自動] または [手動] を選択します。

オプション	操作
要求モード	a [要求モード] から [自動] または [手動] を選択します。 ■ [自動] を選択する場合、すべてのディスクを自動的に取得し、1 つのグループまたは同じサイズの複数のグループにそれらを要求します。 **注：** [自動] モードは廃止されました。vSAN のほとんどの機能と互換性がないハイブリッド ディスク グループのみを要求できます。 ■ [手動] を選択する場合は、グループ内のディスクを手動で編成し、vSphere Web Client を使用して再要求する必要があります。たとえば、手動要求モードは、vCenter Server が使用できない場合に適した選択です。
重複解除	a [重複解除] に [有効] または [無効] を選択します。

6 [保存] をクリックします。

VMware Host Client でのストレージの更新操作および再スキャン操作の実行

データストア、ストレージ デバイス、およびストレージ アダプタを更新すると、VMware Host Client に表示されるリストとストレージ情報が更新されます。この処理では、データストアのキャパシティなどの情報が更新されます。ストレージ管理作業を実行したり、SAN 構成を変更したりすると、ストレージの再スキャンが必要になる場合があります。

VMware Host Client でのアダプタの再スキャンの実行

SAN 構成を変更し、これらの変更が特定のアダプタを介してアクセスしているストレージに対してのみ限定される場合、このアダプタだけの再スキャンを実行します。アダプタを再スキャンすると、そのアダプタで使用可能な新しい LUN が検出されます。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックし、[アダプタ] をクリックします。

2 [再スキャン] をクリックします。

VMware Host Client でのデバイスの再スキャンの実行

デバイスを再スキャンすると、そのデバイスで使用可能な新しい VMFS ボリュームが検出されます。

手順

1 VMware Host Client インベントリ内で [ストレージ] をクリックし、[デバイス] をクリックします。

2 [再スキャン] をクリックします。

VMware Host Client でのスキャンするストレージ デバイスの数の変更

ESXi ホストのスキャンする LUN ID の範囲は、0 から 16,383 までです。ESXi は、16,383 より大きい LUN ID は無視します。設定可能な `Disk.MaxLUN` パラメータを使用して、スキャンされる LUN ID の範囲を管理します。パラメータのデフォルト値は 1024 です。

また、`Disk.MaxLUN` パラメータは、SCSI ターゲットが REPORT_LUNS を使用した直接検出をサポートしていない場合に、SCSI スキャン コードが個々の INQUIRY コマンドを使用して検出を試みる LUN の数を指定します。

`Disk.MaxLUN` パラメータは、必要に応じて変更できます。たとえば使用している環境に、LUN ID が 1 から 100 の少数のストレージ デバイスがある場合は、値を 101 に設定します。その結果、REPORT_LUNS をサポートしていないターゲット上でデバイス検出スピードを上げることができます。この値を小さくすると、再スキャンの時間と起動時間を短縮できます。ただし、ストレージ デバイスを再スキャンする時間は、ストレージ システムのタイプや、ストレージ システムの負荷など、いくつかの要因によって異なる場合があります。

また、1023 より大きな LUN ID を環境内で使用しているときは、このパラメータの値を増やさなければならない場合があります。

手順

1 VMware Host Client インベントリ内で [管理] をクリックし、[詳細設定] をクリックします。

2 `Disk.MaxLUN` までスクロール ダウンします。

3 `Disk.MaxLUN` を右クリックし、[編集オプション] をクリックします。

4 新しい値を入力し、[保存] をクリックします。

SCSI スキャン コードは、入力した値より小さい ID の LUN をスキャンします。

たとえば、0 ～ 100 の LUN ID を検出するには、`Disk.MaxLUN` を 101 に設定してください。

VMware Host Client のネットワーク 7

ESXi ホストに VMware Host Client を使用して接続している場合に、vSphere 標準スイッチ、ポート グループ、物理 NIC、VMkernel NIC、および TCP/IP スタックを表示および構成できます。

この章には、次のトピックが含まれています。

VMware Host Client でのポート グループの管理

ポート グループ設定を管理すると、トラフィック管理の設定、ネットワーク セキュリティの強化、パフォーマンスの向上が可能になります。VMware Host Client を使用することで、ポート グループを追加および削除できます。また、ポート グループ情報の確認のほか、NIC チーミングやトラフィック シェーピングなどのポート グループ設定の編集も実行できます。

VMware Host Client でのポート グループ情報の表示

VMware Host Client で、ポート グループ構成、ネットワーク詳細、仮想スイッチ トポロジ、NIC チーミング ポリシー、オフロード ポリシー、およびセキュリティ ポリシーに関する情報を表示できます。

手順

1. VMware Host Client インベントリ内で [ネットワーク] をクリックし、[ポート グループ] をクリックします。
2. 使用可能なポート グループのリストで、アイテムをクリックします。

   ネットワーク詳細、仮想スイッチ トポロジ、NIC チーミング ポリシー、オフロード ポリシー、およびセキュリティ ポリシーに関する情報が表示されます。

VMware Host Client での仮想スイッチ ポート グループの追加

VMware Host Client で、仮想スイッチにポート グループを追加できます。ポート グループにより、仮想マシンにネットワークが提供されます。

手順

1 VMware Host Client インベントリで [ネットワーク] を右クリックし、ポップアップ メニューの [ポート グループの追加] をクリックします。

2 新しいポート グループの名前を入力します。

3 ポート グループでの VLAN 処理を構成するための VLAN ID を設定します。

VLAN ID は、ポート グループでの VLAN タギング モードも反映します。

VLAN タギング モード	VLAN ID	説明
外部スイッチ タギング（EST）	0	仮想スイッチは、VLAN に関連付けられたトラフィックは渡しません。
仮想スイッチ タギング（VST）	1 から 4094 へ	仮想スイッチは、入力したタグでトラフィックをタグ付けします。
仮想ゲスト タギング（VGT）	4095	仮想マシンは VLAN を処理します。仮想スイッチは、すべての VLAN からのトラフィックを許可します。

4 ドロップダウン メニューから仮想スイッチを選択します。

5 [セキュリティ] を展開して、無差別モード、MAC アドレスの変更、偽装転送で、有効にするオプションを選択します。

6 [追加] をクリックします。

ポート グループが作成されます。

7 （オプション） [更新] をクリックして、新しいポート グループをリストに表示します。

VMware Host Client でのポート グループ設定の編集

VMware Host Client でネットワーク セキュリティを強化し、ネットワーク パフォーマンスを向上するために、ポート グループ名、VLAN ID、仮想スイッチなどの、さまざまなポート グループ設定を編集できます。また、セキュリティ、NIC チーミング、トラフィック シェーピングのコンポーネントも設定できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] > [ポート グループ] をクリックします。

2 編集するポート グループをリスト内で右クリックし、[設定の編集] を選択します。

3 （オプション） 新しいポート グループ名を入力します。

4 （オプション） VLAN ID の新しい値を入力します。

VLAN ID は、ポート グループでの VLAN タギング モードを反映します。

VLAN タギング モード	VLAN ID	説明
外部スイッチ タギング（EST）	0	仮想スイッチは、VLAN に関連付けられたトラフィックは渡しません。
仮想スイッチ タギング（VST）	1 から 4094 へ	仮想スイッチは、入力したタグでトラフィックをタグ付けします。
仮想ゲスト タギング（VGT）	4095	仮想マシンは VLAN を処理します。仮想スイッチは、すべての VLAN からのトラフィックを許可します。

5 （オプション） ドロップダウン メニューから仮想スイッチを選択します。

6 （オプション）［セキュリティ］を展開して、vSwitch のセキュリティ ポリシーの例外を拒否、承諾、継承するかを選択します。

オプション	説明
無差別モード	■ [拒否]。ゲスト アダプタを無差別モードに設定しても、アダプタが受信するフレームには影響しません。 ■ [承諾]。ゲスト アダプタを無差別モードに設定すると、アダプタの接続先であるポート グループの VLAN ポリシーで許可され、vSphere Distributed Switch を通過したすべてのフレームが検出されます。 ■ [vSwitch から継承]。ゲスト アダプタを無差別モードに設定すると、関連付けられた仮想スイッチの設定が継承されます。
MAC アドレス変更	■ [拒否]。[MAC アドレス変更] を [拒否] に設定した状態で、アダプタの MAC アドレスが `.vmx` 構成ファイルに設定された MAC アドレス以外の値にゲスト OS によって変更されると、すべての受信フレームが破棄されます。 ゲスト OS によって `.vmx` 構成ファイル内の MAC アドレスに一致するよう、MAC アドレスが再度変更されると、受信フレームの伝送が再開されます。 ■ [承諾]。ゲスト OS から MAC アドレスを変更すると、意図したように、新しい MAC アドレスへのフレームが受信されるようになります。 ■ [vSwitch から継承]。[MAC アドレス変更] を [vSwitch から継承] に設定すると、MAC アドレスは関連付けられた仮想スイッチの MAC アドレスに変更されます。
偽装転送	■ [拒否]。送信元の MAC アドレスが、アダプタに設定されている MAC アドレスと異なる場合、すべての送信フレームが破棄されます。 ■ [承諾]。フィルタリングは実行されず、送信フレームはすべて伝送されます。 ■ [vSwitch から継承]。送信フレーム設定は、関連付けられた仮想スイッチから継承されます。

7 （オプション）［NIC チーミング］を展開して、次のコンポーネントを設定します。

オプション	説明
ロード バランシング	アップリンクの選択方法を指定します。 ■ ［vSwitch から継承］。関連付けられた仮想スイッチで指定したアップリンクを選択します。 ■ ［IP ハッシュに基づいたルート］。各パケットの発信元と宛先の IP アドレスのハッシュに基づいてアップリンクを選択します。IP 以外のパケットの場合は、すべてそれらのオフセットを使用してハッシュを計算します。 ■ ［発信元 MAC ハッシュに基づいたルート］。送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。 ■ ［発信元ポート ID に基づいたルート］。発信元ポート ID に基づいたアップリンクを選択します。 ■ ［明示的なフェイルオーバー順序を使用］。アクティブ アダプタのリストからフェイルオーバーの検知基準を満たした最上位のアップリンクを常に使用します。 **注：** IP ベースのチーミングでは、EtherChannel で物理スイッチを構成する必要があります。その他のすべてのオプションでは、EtherChannel を無効にする必要があります。
ネットワークのフェイルオーバー検出	フェイルオーバーの検出に使用する方法を選択します。 ■ ■ ［vSwitch から継承］。関連付けられた仮想スイッチの個別の設定が継承されます。 ■ ［リンク状態のみ］。ネットワーク アダプタが提供するリンク ステータスのみに依存します。このオプションでは、ケーブルの抜けや物理スイッチの電源障害などの障害は検出されますが、スパニング ツリーによる物理スイッチ ポートのブロック、物理スイッチ ポートの誤った VLAN への構成、物理スイッチの反対側のケーブルの抜けなどの構成エラーは検出されません。 ■ ［ビーコンのみ］。リンクの障害を確認するには、リンク ステータスを確認するほか、チーミングされたすべての NIC にビーコンの検知の送信して listen します。これにより、［リンク状態のみ］では検出できない障害の多くを検出できます。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、ビーコンの検知を使用しないでください。
スイッチへの通知	フェイルオーバーが発生した場合にスイッチに通知するかどうかを、［はい］、［いいえ］、［vSwitch から継承］の中から選択します。 ［はい］を選択すると、仮想 NIC が分散スイッチに接続される場合、またはフェイルオーバーイベントによって、その仮想 NIC のトラフィックがチーム内の別の物理 NIC を経由する場合には、ネットワークを介して通知が送信され、物理スイッチの検索テーブルを更新します。ほとんどの場合、この処理によって、フェイルオーバーの発生および vMotion での移行の遅延が最小に抑制されます。 **注：** ポート グループを使用する仮想マシンが、Microsoft NLB （Network Load Balancing） をユニキャスト モードで使用している場合は、このオプションを使用しないでください。NLB がマルチキャスト モードで稼動している場合は、そのような問題はありません。

オプション	説明
フェイルバック	[はい]、[いいえ]、[vSwitch から継承] のいずれかを選択して、フェイルバックを無効または有効にします。 このオプションは、障害から復旧したあとで、物理アダプタをどのようにアクティブ モードに戻すかを決定します。フェイスバックをデフォルト設定の [はい] に設定すると、アダプタは復旧したあとすぐにアクティブ モードに戻り、そのスロットを引き継いだスタンバイ アダプタがある場合は、これを置き換えます。フェイルバックを [いいえ] に設定すると、故障したアダプタは、その時点でアクティブな別のアダプタが故障して交換が必要になるまで、復旧後もアクティブでない状態のままになります。
フェイルオーバーの順序	アップリンクのワークロードの分散方法を指定します。いくつかのアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際の緊急用にほかのアップリンクを確保しておく場合は、これらのアップリンクを異なるグループに分けて、この条件を設定します。 ■ [有効なアップリンク]。ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。 ■ [スタンバイ中のアップリンク]。有効なアダプタのいずれかの接続が利用できない場合に、このアップリンクを使用します。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、スタンバイ アップリンクを構成しないでください。ポート グループのいずれかのコンポーネントが、関連付けられた仮想スイッチの設定を継承するように設定されている場合は、フェイルオーバーの順番を設定できません。

8 （オプション） トラフィック シェーピングを設定するには、[トラフィック シェーピング] を展開して、[有効] をクリックし、次のパラメータを指定します。

オプション	説明
平均バンド幅	長期間にわたって平均化された、ポート全体で制限される毎秒ビット数、つまり、許容される平均的な負荷を設定します。
ピーク バンド幅	負荷の高いトラフィックの送受信時にポート全体で制限される最大の毎秒ビット数です。この値が、バースト時用の余剰分を使用しているときは常に、ポートが使用するバンド幅の上限になります。
バースト サイズ	バースト時に制限される最大バイト数です。このパラメータが設定されていると、ポートは割り当てられているすべてのバンド幅を使用しない場合に、バースト ボーナスを取得できます。ポートで、[平均バンド幅] で指定されているよりも多くのバンド幅が必要になると、バースト ボーナスが使用できる場合には、一時的にデータをより高速に転送できます。バースト ボーナスに累積でき、高速転送されるバイト数の上限をこのパラメータで設定します。

トラフィック シェーピング ポリシーは、仮想スイッチに接続された各仮想ネットワーク アダプタのトラフィックに適用されます。

9 [保存] をクリックして変更内容を適用します。

VMware Host Client での仮想スイッチ ポート グループの削除

ラベル付きの関連するネットワークが不要になった場合、仮想スイッチからポート グループを削除できます。

前提条件

削除するポート グループに接続されている、VMkernel NIC およびパワーオン状態の仮想マシンがないことを確認します。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[ポート グループ] タブをクリックします。

2 削除するポート グループを右クリックし、ポップアップ メニューから [削除] を選択します。

3 ポート グループを削除するには、[削除] をクリックします。

4 （オプション）[更新] をクリックして、ポート グループが削除されたことを確認します。

VMware Host Client での仮想スイッチの管理

VMware Host Client では、リンク検出、NIC チーミング、トラフィック シェーピングといった、さまざまな仮想スイッチ設定を行うことができます。

VMware Host Client での仮想スイッチ情報の表示

VMware Host Client で、構成、ネットワーク詳細、仮想スイッチ トポロジなど、仮想スイッチに関する情報を表示できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[仮想スイッチ] をクリックします。

2 使用可能な仮想スイッチのリストで、スイッチをクリックします。

仮想スイッチの構成、ネットワーク詳細、および仮想スイッチ トポロジに関する情報が表示されます。

VMware Host Client での、標準仮想スイッチの追加

VMware Host Client で、標準仮想スイッチを追加して、管理対象のホストおよびそのホスト上の仮想マシンにネットワーク接続を提供し、VMkernel トラフィックを処理することができます。作成する接続のタイプに応じて、VMkernel アダプタを備えた vSphere の標準スイッチの作成、既存の物理ネットワーク アダプタと新しいスイッチとの接続、または仮想マシン ポート グループを持つスイッチの作成ができます。

手順

1 VMware Host Client インベントリで [ネットワーク] を右クリックし、ポップアップ メニューの [標準 vSwitch の追加] をクリックします。

2 （オプション）[アップリンクの追加] をクリックして、新しい物理アップリンクを仮想スイッチに追加します。

3 仮想スイッチの名前を入力し、[仮想スイッチの作成] をクリックします。

4 仮想スイッチのアップリンクを選択します。

5 [リンクの検出] を展開して、仮想スイッチ モードのオプションを選択します。

操作	説明
待機	ESXi は、関連付けられた物理スイッチ ポートに関する情報を検出して表示しますが、スイッチ管理者は、vSphere の標準スイッチに関する情報を使用できません。
アドバタイズ	ESXi は vSphere の標準スイッチに関する情報をスイッチ管理者に提供しますが、物理スイッチに関する情報は検出および表示しません。
両方	ESXi は、関連付けられた物理スイッチに関する情報を検出して表示し、スイッチ管理者は、vSphere の標準スイッチに関する情報を使用できます。
なし	ESXi は、関連付けられた物理スイッチ ポートに関する情報を検出して表示しません。また、スイッチの管理者には、vSphere の標準スイッチに関する情報は提供されません。

6 [プロトコル] セクションで、ドロップダウン メニューから [Cisco Discovery Protocol] を選択します。

7 [セキュリティ] を展開して、無差別モード、MAC アドレスの変更、標準スイッチに接続された仮想マシンの偽造転送について承諾または拒否します。

オプション	説明
無差別モード	■ [拒否]。VM ネットワーク アダプタは、仮想マシン宛のフレームのみを受信します。 ■ [承諾]。仮想スイッチは、VM ネットワーク アダプタが接続されているポートのアクティブな VLAN ポリシーに従ってすべてのフレームを仮想マシンに転送します。 **注：** 無差別モードは、安全な操作ではありません。ファイアウォール、ポート スキャナ、侵入検知システムは、無差別モードで動作する必要があります。
MAC アドレス変更	■ [拒否]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレス（.vmx 構成ファイル内で設定）とは異なる値に変更すると、スイッチはアダプタへのすべての受信フレームをドロップします。 ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスに戻すと、仮想マシンは再びフレームを受信します。 ■ [承諾]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスとは異なる値に変更すると、スイッチは新しいアドレスへのフレームの通過を許可します。
偽装転送	■ [拒否]。スイッチは、仮想マシン アダプタからの送信フレームのうち、.vmx 構成ファイル内の送信元 MAC アドレスと異なるアドレスを持つフレームをすべてドロップします。 ■ [承諾]。スイッチはフィルタリングを実行せず、すべての送信フレームを許可します。

8 [追加] をクリックします。

VMware Host Client での標準仮想スイッチの削除

不要になった標準仮想スイッチは削除できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[仮想スイッチ] タブをクリックします。

2 リストから削除する仮想スイッチを右クリックし、[削除] をクリックします。

3 [はい] をクリックします。

VMware Host Client での、仮想スイッチへの物理アップリンクの追加

複数のアダプタを 1 つの vSphere 標準スイッチに接続して、NIC チーミングを設定できます。チームは、トラフィックを共有し、フェイルオーバーを可能にします。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[仮想スイッチ] をクリックします。

2 リスト内の仮想スイッチをクリックし、[アップリンクの追加] をクリックします。

3 使用可能なオプションから物理 NIC を選択します。

4 [[保存]] をクリックします。

VMware Host Client での仮想スイッチ設定の編集

VMware Host Client で、仮想スイッチ アップリンクなどの仮想スイッチ設定を編集できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[仮想スイッチ] をクリックします。

2 編集する仮想スイッチを右クリックし、[設定の編集] をクリックします。

3 （オプション）[アップリンクの追加] をクリックして、新しい物理アップリンクを仮想スイッチに追加します。

4 最大転送ユニット (MTU) を変更します。

MTU によって、単一パケットで転送されるペイロード データ量が増大するため、ジャンボ フレームが可能になり、ネットワークの効率性が向上します。

5 （オプション）[削除] アイコン（⊗）をクリックして、古いアップリンクを仮想スイッチから削除します。

6 [リンクの検出] を展開して、仮想スイッチ モードのオプションを選択します。

操作	説明
待機	ESXi は、関連付けられた物理スイッチ ポートに関する情報を検出して表示しますが、スイッチ管理者は、vSphere の標準スイッチに関する情報を使用できません。
アドバタイズ	ESXi は vSphere の標準スイッチに関する情報をスイッチ管理者に提供しますが、物理スイッチに関する情報を検出および表示しません。
両方	ESXi は、関連付けられた物理スイッチに関する情報を検出して表示し、スイッチ管理者は、vSphere の標準スイッチに関する情報を使用できます。
なし	ESXi は、関連付けられた物理スイッチ ポートに関する情報を検出して表示せず、スイッチ管理者は、vSphere の標準スイッチに関する情報を使用できません。

7 [プロトコル] セクションで、ドロップダウン メニューから [Cisco Discovery Protocol] を選択します。

8 [セキュリティ] を展開して、無差別モード、MAC アドレスの変更、標準スイッチに接続された仮想マシンの偽造転送について承諾または拒否します。

オプション	説明
無差別モード	■ [拒否]。VM ネットワーク アダプタは、仮想マシン宛のフレームのみを受信します。 ■ [承諾]。仮想スイッチは、VM ネットワーク アダプタが接続されているポートのアクティブな VLAN ポリシーに従ってすべてのフレームを仮想マシンに転送します。 **注：** 無差別モードは、安全な操作ではありません。ファイアウォール、ポート スキャナ、侵入検知システムは、無差別モードで動作する必要があります。
MAC アドレス変更	■ [拒否]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレス（.vmx 構成ファイル内で設定）とは異なる値に変更すると、スイッチはアダプタへのすべての受信フレームをドロップします。 ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスに戻すと、仮想マシンは再びフレームを受信します。 ■ [承諾]。ゲスト OS が仮想マシンの有効な MAC アドレスを VM ネットワーク アダプタの MAC アドレスとは異なる値に変更すると、スイッチは新しいアドレスへのフレームの通過を許可します。
偽装転送	■ [拒否]。スイッチは、仮想マシン アダプタからの送信フレームのうち、.vmx 構成ファイル内の送信元 MAC アドレスと異なるアドレスを持つフレームをすべてドロップします。 ■ [承諾]。スイッチはフィルタリングを実行せず、すべての送信フレームを許可します。

9 （オプション）[NIC チーミング] を展開して、次のコンポーネントを設定します。

オプション	説明
ロード バランシング	アップリンクの選択方法を指定します。 ■ [IP ハッシュに基づいたルート]。各パケットの発信元と宛先の IP アドレスのハッシュに基づいてアップリンクを選択します。IP 以外のパケットの場合は、すべてそれらのオフセットを使用してハッシュを計算します。 ■ [発信元 MAC ハッシュに基づいたルート]。送信元のイーサネットのハッシュに基づいて、アップリンクを選択します。 ■ [発信元ポート ID に基づいたルート]。発信元ポート ID に基づいたアップリンクを選択します。 ■ [明示的なフェイルオーバー順序を使用]。アクティブ アダプタのリストから、フェイルオーバーの検知基準を満たした最上位のアップリンクを常に使用します。 **注：** IP ベースのチーミングでは、EtherChannel で物理スイッチを構成する必要があります。その他のすべてのオプションでは、EtherChannel を無効にする必要があります。
ネットワークのフェイルオーバー検出	フェイルオーバーの検出に使用する方法を選択します。 ■ [リンク状態のみ]。ネットワーク アダプタが提供するリンク ステータスのみに依存します。このオプションでは、ケーブルの抜けや物理スイッチの電源障害などの障害は検出されますが、スパニング ツリーによる物理スイッチ ポートのブロック、物理スイッチ ポートの誤った VLAN への構成、物理スイッチの反対側のケーブルの抜けなどの構成エラーは検出されません。 ■ [ビーコンのみ]。チーム内のすべての NIC に対してビーコンの検知の送信および待機を行い、この情報とリンク ステータスを使用してリンク故障を確認します。これにより、リンク状態のみでは検出できない、前述の障害の多くを検出できます。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、ビーコンの検知を使用しないでください。
スイッチへの通知	[はい]、[いいえ]、[vSwitch から継承] のいずれかを選択して、フェイルオーバー時にスイッチに通知します。 [はい] を選択すると、フェイルオーバー イベントによって、仮想 NIC が Distributed Switch に接続される場合、または、その仮想 NIC のトラフィックがチーム内の別の物理 NIC を経由する可能性がある場合には、ネットワークを介して通知が送信され、物理スイッチの検索テーブルを更新します。ほぼすべての場合、この処理は、フェイルオーバーの発生および vMotion での移行の遅延を最小限に抑えるのに適しています。 **注：** ポート グループを使用する仮想マシンが、Microsoft NLB （Network Load Balancing） をユニキャスト モードで使用している場合は、このオプションを使用しないでください。NLB がマルチキャスト モードで稼動している場合は、そのような問題はありません。

オプション	説明
フェイルバック	[はい]、[いいえ]、[vSwitch から継承] のいずれかを選択して、フェイルバックを無効または有効にします。 このオプションは、障害から復旧したあとで、物理アダプタをどのようにアクティブ モードに戻すかを決定します。フェイルオーバーを [はい] （デフォルト） に設定すると、アダプタは、復旧後すぐにアクティブ モードに戻り、スロットを引き継いだスタンバイ アダプタがある場合はそれに取って代わります。フェイルバックを [いいえ] に設定すると、故障したアダプタは、その時点でアクティブな別のアダプタが故障して交換が必要になるまで、復旧後もアクティブでない状態のままになります。
フェイルオーバーの順序	アップリンクのワークロードの分散方法を指定します。いくつかのアップリンクを使用しつつ、使用中のアップリンクに障害が発生した際の緊急用にほかのアップリンクを確保しておく場合は、これらのアップリンクを異なるグループに分けて、この条件を設定します。 ■ [有効なアップリンク]。ネットワーク アダプタ接続が稼動中で有効な場合に、アップリンクを継続的に使用します。 ■ [スタンバイ中のアップリンク]。有効なアダプタのいずれかの接続が利用できない場合に、このアップリンクを使用します。 **注：** IP ハッシュに基づくロード バランシングを使用する場合は、スタンバイ アップリンクを構成しないでください。

10 （オプション） トラフィック シェーピングを設定するには、[トラフィック シェーピング] を展開して、[有効] をクリックし、次のパラメータを指定します。

オプション	説明
平均バンド幅	長期間にわたって平均化された、ポート全体で許容される毎秒ビット数、つまり、許容される平均的な負荷を設定します。
ピーク バンド幅	負荷の高いトラフィックの送受信時にポート全体で許容される最大の毎秒ビット数です。この値が、バースト時用の余剰分を使用しているときは常に、ポートが使用するバンド幅の上限になります。
バースト サイズ	バースト時に許容する最大バイト数です。このパラメータを設定すると、割り当てられたバンド幅をすべて使用していない場合、ポートはバースト時用の余剰分を獲得できます。ポートに [平均バンド幅] で指定した値よりも多くのバンド幅が必要になると、バースト時用の余剰分が利用可能な場合は、一時的に高速でデータを転送できるようになります。このパラメータは、バースト時用の余剰分で累積可能なバイト数を上乗せし、高速転送を実現します。

トラフィック シェーピング ポリシーは、仮想スイッチに接続された各仮想ネットワーク アダプタのトラフィックに適用されます。

11 [[保存]] をクリックします。

VMware Host Client での物理ネットワーク アダプタの管理

物理アダプタを標準スイッチに割り当て、管理対象ホスト上の仮想マシンおよび VMkernel アダプタへの接続を提供します。

VMware Host Client での物理ネットワーク アダプタ情報の表示

VMware Host Client で、物理ネットワーク アダプタ (NIC) の構成および設定に関するさまざまな情報を表示できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[物理 NIC] をクリックします。

2 情報を表示するネットワーク アダプタをクリックします。

VMware Host Client での物理 NIC の編集

VMware Host Client を使用して、物理 NIC の速度を編集できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[物理 NIC] をクリックします。

2 編集する NIC をテーブル内で選択します。

3 [設定の編集] をクリックし、ドロップダウン メニューから速度を選択します。

4 [[保存]] をクリックします。

VMware Host Client での VMkernel ネットワーク アダプタの管理

VMware Host Client で、VMkernel ネットワーク アダプタ (NIC) の追加と削除、および VMkernel NIC 設定の表示と変更を実行できます。

VMware Host Client での VMkernel ネットワーク アダプタ情報の表示

VMware Host Client で、TCP/IP 構成、ネットワーク詳細、仮想スイッチ トポロジなど、VMkernel ネットワーク アダプタ (NIC) に関する情報を表示できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[VMkernel NIC] をクリックします。

2 リスト内の NIC をクリックして、構成およびトポロジの詳細を表示します。

VMware Host Client での、VMkernel ネットワーク アダプタの追加

VMkernel ネットワーク アダプタ(NIC) を VMware vSphere® Standard Edition™ スイッチに追加して、ホスト用のネットワーク接続を提供することができます。VMkernel NIC は、VMware vSphere® vMotion®、IP ストレージ、フォルト トレランス、ログ、vSAN などのシステム トラフィックも処理します。

手順

1 VMware Host Client インベントリ内で [ネットワーク] を右クリックし、[VMkernel NIC の追加] をクリックします。

2 [VMkernel NIC の追加] ダイアログ ボックスで、VMkernel アダプタを設定します。

オプション	説明
新規ポート グループのラベル	VMkernel NIC を追加すると、ポート グループも追加されます。このポート グループの名前を指定します。
VLAN ID	VLAN ID を入力して、使用する VMkernel アダプタのネットワーク トラフィック用の VLAN を指定します。
IP バージョン	IPv4、IPv6、またはその両方を選択します。 **注：** IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。

3 ドロップダウン メニューから仮想スイッチを選択します。

4 （オプション） IPv4 設定セクションを展開し、IP アドレスを取得する方法を選択します。

オプション	説明
DHCP を使用して IP 設定を取得します	IP 設定は自動的に取得されます。ネットワークには、DHCP サーバが存在する必要があります。
固定 IP 設定を使用	VMkernel アダプタの IPv4 アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。

5 （オプション） IPv6 設定セクションを展開し、IPv6 アドレスを取得する方法を選択します。

オプション	説明
DHCPv6	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
自動構成	ルーターの通知を使用して IPv6 アドレスを取得します。
固定 IPv6 アドレス	a [アドレスの追加] をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックスの長さを入力します。

6 ドロップダウン メニューから TCP/IP スタックを選択します。

VMkernel アダプタに TCP/IP スタックを設定した後で、その設定を変更することはできません。vMotion またはプロビジョニング TCP/IP スタックを選択する場合は、このスタックのみを使用して、ホストの vMotion またはプロビジョニング トラフィックを処理できます。デフォルト TCP/IP スタックの、vMotion 用のすべての VMkernel アダプタは、将来の vMotion セッションで無効になります。プロビジョニング TCP/IP スタックを使用する場合、デフォルト TCP/IP スタックの VMkernel アダプタは無効になり、一部の操作を実行することができません。このような操作には、仮想マシンのコールド移行、クローン作成、スナップショットの移行などのトラフィック プロビジョニングが含まれます。

7 （オプション） サービスを選択して、ホスト上でデフォルトの TCP/IP スタックを有効にします。

vMotion では、vMotion トラフィックを送信するネットワーク接続として、VMkernel アダプタが自身を別のホストにアドバタイズできます。デフォルト TCP/IP スタックの VMkernel アダプタで vMotion サービスを有効にしていない場合、または vMotion TCP/IP スタックを使用しているアダプタがない場合には、選択したホストへの vMotion による移行は実行できません。

8 選択内容を確認し、[作成] をクリックします。

VMware Host Client での VMkernel ネットワーク アダプタ設定の編集

VMkernel ネットワーク アダプタでサポートされているトラフィック タイプや、IPv4 または IPv6 アドレスの取得方法の変更が必要になる場合があります。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[VMkernel NIC] をクリックします。

2 ターゲットの標準スイッチ上にある VMkernel アダプタを選択し、[アクション] をクリックし、ドロップダウン メニューから [設定の編集] を選択します。

3 （オプション） VLAN ID を編集します。

VLAN ID は、VMkernel アダプタのネットワーク トラフィックが使用する VLAN を特定します。

4 （オプション） IP アドレスのバージョンを編集するには、IPv4、IPv6、またはその両方をドロップダウン メニューから選択します。

注： IPv6 オプションは IPv6 が有効になっていないホスト上には表示されません。

5 （オプション） IPv4 設定セクションを展開し、IP アドレスを取得する方法を選択します。

オプション	説明
DHCP を使用して IP 設定を取得します	IP 設定は自動的に取得されます。ネットワークには、DHCP サーバが存在する必要があります。
固定 IP 設定を使用	VMkernel アダプタの IPv4 アドレスおよびサブネット マスクを入力します。 IPv4 での VMkernel デフォルト ゲートウェイおよび DNS サーバのアドレスは、選択した TCP/IP スタックから取得されます。

6 （オプション） IPv6 設定セクションを展開し、IPv6 アドレスを取得する方法を選択します。

オプション	説明
DHCPv6	DHCP を使用して IPv6 アドレスを取得します。ネットワークには、DHCPv6 サーバが存在する必要があります。
自動構成	ルーターの通知を使用して IPv6 アドレスを取得します。
固定 IPv6 アドレス	a [アドレスの追加] をクリックして IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックスの長さを入力します。

7 （オプション） ホスト上のデフォルト TCP/IP スタックに対して有効または無効にするサービスを選択します。

vMotion では、vMotion トラフィックを送信するネットワーク接続として、VMkernel アダプタが自身を別のホストにアドバタイズできます。デフォルト TCP/IP スタックの VMkernel アダプタ対して vMotion サービスが有効化されていない場合、または vMotion TCP/IP スタックを使用しているアダプタがない場合には、選択したホストへの vMotion による移行は実行できません。

8 設定の変更内容を確認し、[保存] をクリックして変更を適用します。

VMware Host Client での VMkernel ネットワーク アダプタの削除

VMware Host Client で、不要になった VMkernel ネットワーク アダプタを削除できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[VMkernel NIC] をクリックします。

2 削除する VMkernel アダプタを右クリックし、[削除] をクリックします。

3 [確認] をクリックしてネットワーク アダプタを削除します。

VMware Host Client でのホストの TCP/IP スタック構成の表示

ホスト上の TCP/IP スタックの DNS およびルーティング構成を表示できます。IPv4 および IPv6 ルーティング テーブル、輻輳制御アルゴリズム、および許可される接続の最大数を表示することもできます。

手順

1 ホスト インベントリ内で [ネットワーク] をクリックし、[TCP/IP スタック] をクリックします。

2 リスト内のスタックをクリックします。

選択したスタックの構成設定が表示されます。

VMware Host Client での、ホストの TCP/IP スタックの構成の変更

ホスト上の TCP/IP スタックの DNS およびデフォルト ゲートウェイ構成を変更できます。輻輳制御アルゴリズム、接続の最大数、およびカスタム TCP/IP スタックの名前を変更することもできます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[TCP/IP スタック] をクリックします。

2 リストにあるスタックを右クリックし、[設定の編集] を選択します。

[TCP/IP 構成の編集: プロビジョニング スタック] ダイアログ ボックスが開きます。

3 この TCP/IP スタックにおける設定をホストが取得する方法を指定します。

- [次のアダプタから DHCP サービスを使用] ラジオ ボタンを選択し、TCP/IP スタックのデフォルトの設定構成を渡すアダプタを選択します。

- ［この TCP/IP スタックの設定を手動で構成］を選択して、設定構成を変更します。

オプション	説明
基本構成	**［ホスト名］** ローカル ホストの名前を編集します。 **［ドメイン名］** ドメイン名を編集します。 **［プライマリ DNS サーバ］** 優先 DNS サーバの IP アドレスを入力します。 **［セカンダリ DNS サーバ］** 代替 DNS サーバの IP アドレスを入力します。 **［ドメインの検索］** 非修飾のドメイン名を解決する際に DNS 検索で使用する DNS サフィックスを指定します。
ルーティング	IPv4 および IPv6 ゲートウェイ情報を編集します。 **注：** デフォルト ゲートウェイを削除すると、ホストへの接続が失われる可能性があります。
詳細設定	輻輳制御アルゴリズムおよび最大接続数を編集します。

4 ［[保存]］をクリックします。

VMware Host Client での ESXi ファイアウォールの構成

ESXi には、デフォルトで有効になっているファイアウォールが含まれています。インストール時、ESXi ファイアウォールは、受信トラフィックと送信トラフィックをブロックするように構成されています。ただし、ホストのセキュリティ プロファイルで有効化されているサービスのトラフィックは除外されます。

ファイアウォールのポートを開く場合は、外部からの攻撃や不正アクセスの危険にさらされる可能性があるため、ESXi ホストで実行されているサービスへのアクセスを制限することを検討します。認証済みのネットワークからのアクセスのみを許可するように ESXi ファイアウォールを構成してリスクを軽減します。

注： ファイアウォールは、ICMP (Internet Control Message Protocol) の ping と、DHCP および DNS（UDP のみ）クライアントとの通信も許可します。

VMware Host Client を使用した ESXi ファイアウォール設定の管理

VMware Host Client で ESXi ホストにログインすると、サービスまたは管理エージェントの受発信用ファイアウォール接続を構成できます。

注： 異なるサービスに重複するポート ルールが適用されている場合は、1 つのサービスを有効にすると、他のサービスも暗黙的に有効化されます。どの IP アドレスにホストの各サービスへのアクセスを許可するかを指定するとこの問題を回避できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックします。

2 [ファイアウォール ルール] をクリックします。

VMware Host Client により、アクティブな着信および発信接続や、それを対応するファイアウォール ポートのリストが表示されます。

3 一部のサービスでは、サービスの詳細を管理できます。サービスを右クリックし、ポップアップ メニューからオプションを選択します。

- 開始 ボタン、停止 ボタン、または 再起動 ボタンを使用して、一時的にサービスのステータスを変更します。
- 起動ポリシーを変更し、ホストおよびファイアウォール ポートでのサービスの起動および停止を構成するか、手動で設定します。

VMware Host Client を使用した、ESXi ホストの許可された IP アドレスの追加

デフォルトでは、各サービスのファイアウォールはすべての IP アドレスへのアクセスを許可します。トラフィックを制限するには、管理サブネットからのトラフィックだけを許可するように各サービスを構成します。環境で使用されないサービスがある場合には、それらの選択を解除することもできます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックし、[ファイアウォール ルール] をクリックします。

2 リスト内のサービスをクリックし、[設定の編集] をクリックします。

3 [許可された IP アドレス] セクションで、[次のネットワークからの接続のみを許可します] をクリックし、ホストに接続するネットワークの IP アドレスを入力します。

IP アドレスをコンマで区切ります。次のアドレス形式を使用できます。

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

4 [OK] をクリックします。

VMware Host Client でのネットワーク イベントおよびタスクの監視

管理対象の ESXi ホスト上のポート グループ、仮想スイッチ、物理ネットワーク アダプタ、VMkernel ネットワーク アダプタ、および TCP/IP スタックと関連付けられているイベントおよびタスクに関する詳細情報を表示できます。

VMware Host Client でのポート グループの監視

VMware Host Client で、ホスト上のポート グループのイベントとタスクを表示して、ポート グループのパフォーマンスを監視できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックします。

2 [ポート グループ] をクリックします。

3 リスト内のポート グループをクリックします。

そのポート グループが VMware Host Client インベントリ内で展開されます。

4 VMware Host Client インベントリ内で、ポート グループ名の下の [監視] をクリックします。

5 （オプション）[イベント] をクリックして、そのポート グループと関連付けられているイベントを表示します。

VMware Host Client での仮想スイッチの監視

VMware Host Client で、ホスト上の仮想スイッチのイベントとタスクを表示して、仮想スイッチのパフォーマンスを監視できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックします。

2 [仮想スイッチ] をクリックします。

3 リスト内の仮想スイッチをクリックします。

その仮想スイッチが VMware Host Client インベントリ内で展開されます。

4 VMware Host Client インベントリ内で、仮想マシン名の下の [監視] をクリックします。

5 （オプション）[イベント] をクリックして、その仮想スイッチと関連付けられているイベントを表示します。

VMware Host Client での物理ネットワーク アダプタの監視

VMware Host Client で、ホスト上の物理ネットワーク アダプタ (NIC) のイベントおよびタスクを表示して、その物理 NIC のパフォーマンスを監視できます。

手順

1 VMware Host Client インベントリ内で [ネットワーク] をクリックします。

2 [物理 NIC] をクリックします。

3 リスト内の物理ネットワーク アダプタをクリックします。

その物理ネットワーク アダプタが VMware Host Client インベントリ内で展開されます。

4 VMware Host Client インベントリ内で、物理ネットワーク アダプタ名の下の [監視] をクリックします。

5 （オプション）[イベント] をクリックして、その物理ネットワーク アダプタと関連付けられているイベントを表示します。

VMware Host Client での VMkernel ネットワーク アダプタの監視

VMware Host Client で、ホスト上の VMkernel ネットワーク アダプタのイベントおよびタスクを表示して、VMkernel ネットワーク アダプタのパフォーマンスを監視できます。

手順

1. VMware Host Client インベントリ内で [ネットワーク] をクリックします。
2. [VMkernel NIC] をクリックします。
3. リスト内の VMkernel ネットワーク アダプタをクリックします。

   その VMkernel ネットワーク アダプタが VMware Host Client インベントリ内で展開されます。
4. VMware Host Client インベントリ内で、VMkernel ネットワーク アダプタ名の下の [監視] をクリックします。
5. （オプション） [イベント] をクリックして、その VMkernel ネットワーク アダプタと関連付けられているイベントを表示します。

VMware Host Client での TCP/IP スタックの監視

VMware Host Client で、ホスト上の TCP/IP スタックのイベントとタスクを表示して、TCP/IP スタックのパフォーマンスを監視できます。

手順

1. VMware Host Client インベントリ内で [ネットワーク] をクリックします。
2. [TCP/IP スタック] をクリックします。
3. リスト内の TCP/IP スタックをクリックします。

   その TCP/IP スタックが VMware Host Client インベントリ内で展開されます。
4. VMware Host Client インベントリ内で、TCP/IP スタック名の下の [監視] をクリックします。
5. （オプション） その TCP/IP スタックと関連付けられているイベントを表示するには、[イベント] をクリックします。
6. （オプション） その TCP/IP スタックと関連付けられているタスクを表示するには、[タスク] をクリックします。