ロックダウン モード

概要

このセクションでは、ロックダウン モードの概要を説明します。ロックダウン モードは、ホストへのアクセス許可を制限することにより、ESXi ホストのセキュリティを強化するために使用されます。このモードを有効にすると、ESXi ホストには vCenter Server または Direct Console ユーザインターフェイス（DCUI）からのみアクセスできます。ロックダウン モードの有効化は、どのユーザがホスト サービスへのアクセスを認可されるかに影響します。

（注） ロックダウン モードが有効になり、root または administrator@vsphere.local、 またはその他のユーザが例外ユーザ リストに含まれていない場合、これらのユーザは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

表 *1:* ロックダウン モードの動作

サービス	通常モード	通常のロックダウン モード	厳密なロックダウン モード
vSphere Web サービス API	すべてのユーザ（権限に基づく）	vCenter（vpxuser） 例外にユーザが含まれます（権限に基づく）。	vCenter（vpxuser） 例外にユーザが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）

サービス	通常モード	通常のロックダウン モード	厳密なロックダウン モード
CIM プロバイダー	ホスト上の管理者権限を持つユーザ。	vCenter（vpxuser） 例外にユーザが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）	vCenter（vpxuser） 例外にユーザが含まれます（権限に基づく）。 vCloud Director（vslauser、該当する場合）
Direct Console UI（DCUI）	ホスト上の管理者権限を持つユーザおよびDCUI 内のユーザ。アクセスの詳細オプション。	DCUI アクセス詳細オプションで定義されたユーザ。 例外にホスト上の管理者権限を持つユーザが含まれます。	DCUI サービスが停止します。
ESXi シェル （イネーブルな場合）	ホスト上の管理者権限を持つユーザ。	DCUI アクセス詳細オプションで定義されたユーザ。 例外にホスト上の管理者権限を持つユーザが含まれます。	DCUI アクセス詳細オプションで定義されたユーザ。 例外にホスト上の管理者権限を持つユーザが含まれます。
SSH（イネーブルな場合）	ホスト上の管理者権限を持つユーザ。	DCUI アクセス詳細オプションで定義されたユーザ。 例外にホスト上の管理者権限を持つユーザが含まれます。	DCUI アクセス詳細オプションで定義されたユーザ。 例外にホスト上の管理者権限を持つユーザが含まれます。

- ロックダウン モードの有効化または無効化 （2 ページ）
- ロックダウン モードのトラブルシューティング （3 ページ）

ロックダウン モードの有効化または無効化

このセクションでは、DCUI から、または vSphere Web Client からロックダウン モードを有効または無効にする方法について説明します。

（注） ロックダウン モードが有効になり、root または administrator@vsphere.local、 またはその他のユーザが例外ユーザ リストに含まれていない場合、これらのユーザは ESX への SSH 接続が許可されません。同様に、何らかの理由によりホストが vCenter から削除された場合、vCenter にホストを再び追加することは許可されません。

DCUI からのロックダウン モードの有効化または無効化：

ステップ 1 ESXi ホストに直接にログインします。
ステップ 2 ホストで Direct Console ユーザ インターフェイス（DCUI）を開きます。
ステップ 3 初期設定用の **F2 キー**を押します。
ステップ 4 [ロックダウン モードの設定（Configure Lockdown Mode）] の設定を切り替えるには **Enter** を押します。
ステップ 5 VSphere Web Client のインベントリでホストを特定します。

vSphere Web Client からのロックダウンモードの有効化または無効化：

ステップ 1 VSphere Web Client のインベントリでホストを特定します。
ステップ 2 [**Manage**] タブをクリックし、[Settings] をクリックします。
ステップ 3 [System] で、**[Security profile]** を選択します。
ステップ 4 [Lockdown Mode] パネルで、**[Edit]**をクリックします。
ステップ 5 **[ロックダウン モード（Lockdown Mode）]** をクリックして、いずれかのロックダウン モード オプションを選択します。

ロックダウン モードのトラブルシューティング

ロックダウンモードでエラーダイアログボックスが表示されたりソフトウェアのアップグレードが失敗したりする場合は、次のいずれかのシナリオに応じて以下の解決オプションを実行してください。

- 少なくとも 1 つのホストがロックダウン モードである。
- アップグレードの進行中にホストがロックダウン モードである。

少なくとも 1 つのホストがロックダウン モードである場合：

1. アップグレード前の検証でホスト ロックダウン モードをチェックします。
2. 状態を検出し、エラーをスローしてクラスタのアップグレードを中止します。

3. ロックダウン モードを無効にして、アップグレードを再試行します。

アップグレードの進行中にホストがロックダウン モードである場合：

ステップ 1 ホストをアップグレードする前に、ホスト ロックダウン モードをチェックします。
ステップ 2 状態を検出してエラーを送出し、アップグレードに失敗します。
ステップ 3 ロックダウン モードを無効にして、アップグレードを再試行します。

展開フェーズでの vCenter へのホスト追加エラー

HX インストール中のロックダウンの検証は、「root」ユーザーを使用した ESXi ホストの SSH アクセシビリティ チェックです。例外リストにルート ユーザーを追加すると、ロックダウン モードの展開検証チェックがバイパスされます。この場合、展開フェーズで vCenter にホストが追加されると、そのホストは失敗し、HX のインストールも失敗します。

展開フェーズで vCenter にホストを追加すると失敗し、エラー メッセージ「**vCenter のホストを追加できません**」が表示されます。

ロックダウン モードのステータスを確認し、無効にして、「root」ユーザーを例外から削除します。