

VMware Cloud Director 10.2.2 リリース ノート

VMware Cloud Director 10.2.2 | 2021 年 4 月 8 日 | ビルド 17855679 (インストールされているビルド 17855680)

このリリースノートの追加事項や更新事項を確認してください。

このドキュメントの内容

- [新機能](#)
- [システム要件とインストール](#)
- [ドキュメント](#)
- [VMware Cloud Director 10.2.x の以前のリリース](#)
- [解決した問題](#)
- [既知の問題](#)

新機能

VMware Cloud Director バージョン 10.2.2 には次の新機能が含まれています。

- **VMware Tanzu Mission Control は、VMware Cloud Director でプロビジョニングされた Tanzu Kubernetes クラスタをサポート** - VMware Cloud Director でプロビジョニングされた Kubernetes クラスタを Tanzu Mission Control に接続できます。その結果、クラスタは Tanzu Mission Control コンソールに表示されるようになります。既存のクラスタを VMware Tanzu Mission Control 組織に接続する方法については、『VMware Tanzu Mission Control 製品ドキュメント』の「[Attach an Existing Cluster](#)」を参照してください。
- **Tanzu Kubernetes クラスタ テナント ネットワークの隔離** - Tanzu Kubernetes クラスタは、クラスタが作成された同一の組織仮想データセンター内のワークロードからのみアクセスが可能になりました。必要に応じて、Tanzu Kubernetes クラスタ内の特定のサービスへの外部アクセスを手動で構成できます。詳細については、『VMware Cloud Director テナント ポータル ガイド』の「[Tanzu Kubernetes クラスタ内のサービスへの外部アクセスの構成](#)」を参照してください。
- **Tanzu Kubernetes クラスタ ポッドおよびサービスの CIDR の選択** - Tanzu Kubernetes クラスタの作成中に、Kubernetes サービスおよび Kubernetes ポッドの IP アドレス範囲を指定できます。詳細については、『VMware Cloud Director テナント ポータル ガイド』の「[Tanzu Kubernetes クラスタの作成](#)」を参照してください。
- **VMware Cloud Director で Tanzu Kubernetes クラスタとの通信に管理ネットワークを使用** - VMware Cloud Director 管理ネットワークは、クラウド インフラストラクチャを提供し、クライアント システムで VMware Cloud Director の管理タスクを実行するためのアクセスを提供するプライベートネットワークです。以前のリリースでは、Kubernetes サービス ネットワークが使用されます。
- **VMware Cloud Director アプライアンス SNMP エージェント** - ポーリング要求をリッスンするエージェントを構成できます。既存の Net-SNMP エージェントがある場合、VMware Cloud Director アプライアンスはアップグレー

ド時に Net-SNMP インストールを VMware-SNMP に置き換えます。VMware-SNMP セットアップ中に、VMware Cloud Director アプライアンスは、SNMP 処理に必要なファイアウォール ルールを動的に構成します。Net-SNMP で動作する既存のファイアウォール ルールは、アップグレードの前に削除する必要があります。詳細については、『VMware Cloud Director のインストール、構成、およびアップグレード』ガイドの「[VMware Cloud Director アプライアンス SNMP エージェントの構成](#)」を参照してください。

- **グローバル配置ポリシー** - サービス プロバイダは、VMware Cloud Director 環境内のすべての vCenter Server インスタンスおよびクラスターで効率的に機能する配置ポリシーを定義できます。1つの配置ポリシーは、1つ以上の vCenter Server インスタンスの複数のクラスターにまたがるホストを参照できます。基盤となるインフラストラクチャの境界を配置ポリシーのグローバルな論理構造の背後で抽象化することで、サービス プロバイダとテナントの双方で論理的なエクスペリエンスを実現します。この変更で、仮想マシンから vApp テンプレートが作成された際に配置ポリシーをキャプチャすることが可能になりました。作成された vApp テンプレートは、仮想マシンと vApp テンプレートが異なるプロバイダ仮想データセンターにある場合でも、元の仮想マシンからすべての配置ポリシーを継承します。ベスト プラクティスは、配置ポリシーに特徴的な命名規則を使用することです。詳細については、『VMware Cloud Director Service Provider Admin Portal ガイド』の「[グローバル仮想マシン配置ポリシーの作成](#)」を参照してください。
- **暗号化された仮想マシンでのゲストのカスタマイズ** - VMware Cloud Director 10.2.2 では、暗号化されたストレージで実行される仮想マシンのゲストのカスタマイズがサポートされるようになりました。
- **組織仮想データセンター テンプレート** - 仮想データセンター (VDC) テンプレートを作成して、テナント組織と共有し、組織管理者はこれを使用して VDC を作成できるようになりました。VMware Cloud Director 10.2.2 では、NSX-T ベースのネットワークと組織 VDC テンプレートの併用もサポートされます。
- **ストレージ ポリシーの更新** - サービス プロバイダは VMware Cloud Director のストレージ ポリシーを使用して、ゴールド、シルバー、ブロンズなどの階層化されたストレージ オファリングの作成や、専用ストレージのテナントへの提供も可能になりました。VMware Cloud Director エンティティをサポートするストレージ ポリシーの拡張により、ストレージ ポリシーの使用方法を柔軟に制御できるようになります。階層化されたストレージに加え、仮想マシン、コンテナ、Edge Gateway などを実行するための隔離されたストレージも可能になります。この更新で対処する一般的な使用事例は、クラスター間の共有ストレージが必要な場合や、実行中でないワークロードへの低コストストレージの提供が必要な場合です。たとえば、1つのストレージ ポリシーにすべての VMware Cloud Director エンティティを含めるのではなく、ストレージ ポリシーをすべての実行中の仮想マシンとコンテナ用のワークロードストレージ ポリシーに分割し、長期的なストレージ専用のカタログストレージポリシーにすることができます。低速または低コストの NFS オプションでカタログストレージポリシーをバックアップし、ワークロードストレージポリシーを vSAN で実行できます。
- **FIPS サポート** - 本リリースの VMware Cloud Director には、FIPS (Federal Information Processing Standards) のサポートが含まれるようになりました。VMware Cloud Director アプライアンスと Linux バイナリの両方を FIPS 対応モードで実行できます。FIPS モードはデフォルトで無効になっており、FIPS モードを有効にすると、VMware Cloud Director のパフォーマンスに影響することがあります。メトリック収集が構成されている場合、SSL 経由の Cassandra とのサーバおよびクライアント通信の構成を確認します。詳細については、『VMware Cloud Director のインストール、構成、およびアップグレード ガイド』の「[VMware Cloud Director アプライアンスでの FIPS モードの有効化/無効化](#)」を参照してください。または、Linux での VMware Cloud Director の有効化については、『VMware Cloud Director Service Provider Admin Portal ガイド』の「[サーバグループのセルでの FIPS モードの有効化](#)」を参照してください。
- **NSX-T Data Center によってバックアップされている組織 VDC での直接 VDC ネットワークのサポート** - サービス プロバイダは NSX-T Data Center によってバックアップされている VDC で直接組織 VDC ネットワークを作成できるようになりました。

- **自動スケーリング** – スケーリング グループは、テナントがワークロード グループで自動化された水平方向のスケールイン イベントおよびスケールアウト イベントを実行する際に使用できる新しい上位レベル オブジェクトです。自動スケール グループは、ソース vApp テンプレート、ロード バランサ ネットワーク、および CPU とメモリの使用に基づいてグループを拡大/縮小するルールのセットによって構成できます。VMware Cloud Director は、スケーリング グループ内の仮想マシンを自動的にスピンアップ/シャットダウンします。『VMware Cloud Director テナント ポータル ガイド』の「[自動スケール グループ](#)」ドキュメントを参照してください。
- **ガイド ツアーの更新** – サービス プロバイダはガイド ツアーをカスタムで構築し、システム管理者やテナントを対象に公開することができます。VMware Cloud Director 10.2.2 以降、ガイド ツアーは VMware GitHub リポジトリまたはカスタム GitHub リポジトリからダウンロードできます。
- **固定 T シャツ サイズの削除** – VMware Cloud Director 10.2.2 では、vCloud Director for Service Providers 9.0 以降使用可能な事前定義された仮想マシン サイズの使用がサポートされなくなりました。仮想マシンサイジングポリシー機能を使用して、事前定義されている仮想マシンのサイジングを行うことができます。

システム要件とインストール

システム要件とインストール手順の詳細については、「[VMware Cloud Director 10.2 リリース ノート](#)」を参照してください。

アプライアンスの構成とサイジングの詳細については、「[VMware Cloud Provider Pod Designer - VMware で検証されたクラウドプロバイダ向けの設計](#)」を参照してください。

デフォルトで有効になっているサポート対象の暗号スイート：

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

システム管理者は、セル管理ツールを使用して、デフォルトで無効になっている他のサポート対象暗号スイートを明示的に有効にすることができます。

備考：5.5-update-3e より前のリリースの vCenter Server および 4.2 より前のバージョンの ovftool で相互運用するには、VMware Cloud Director が TLS バージョン 1.0 をサポートする必要があります。セル管理ツールを使用すると、サポートされる SSL プロトコルや暗号化のセットを再構成することができます。『VMware Cloud Director インストール、構成、およびアップグレード ガイド』のセル管理ツールのセクションを参照してください。

VMware Cloud Director アプライアンスのデプロイ

VMware Cloud Director アプライアンスのデプロイ後に、vami_firstboot ファイルが自動的に削除されないことがあります。これが原因で、アプライアンスは次に電源入れ直したまたは再起動したときに再初期化されます。この問題を回避するには、デプロイ後にサーバグループ内の各アプライアンスで次の手順を実行します。

1. VMware Cloud Director アプライアンスにファイル /opt/vmware/etc/vami/flags/vami_firstboot があるかどうかを確認します。

2. ファイルがある場合は、次のコマンドを実行して削除します。

```
rm /opt/vmware/etc/vami/flags/vami_firstboot
```

ドキュメント

製品の完全なドキュメントセットを参照するには、「[VMware Cloud Director のドキュメント](#)」にアクセスしてください。

VMware Cloud Director 10.2.x の以前のリリース

[VMware Cloud Director 10.2.1 リリース ノート](#)

[VMware Cloud Director 10.2 リリース ノート](#)

解決した問題

- **VMware Cloud Director 10.2.x にアップグレードした後、SSL で Cassandra に対して CMT コマンドを実行すると、エラー メッセージが表示されて失敗する**
cell-management-tool を使用して SSL で Cassandra を構成または再構成すると、操作が失敗してエラー メッセージが表示されます。
VCD の SSL コンテキストをロードできません。
- **New: 仮想マシンを無効にしてからドメインに参加すると、仮想マシンのハードウェア プロパティの更新に失敗し、エラー メッセージが表示される**
仮想マシンによるドメインへの参加を無効にすると、同じ仮想マシンのハードウェア プロパティの更新が失敗し、エラー メッセージが表示されます。
エラー: ドメイン参加が無効化されている場合、<Domain name> を提供しないでください。
- **New: 仮想マシンを有効にしてからドメインに参加すると、仮想マシンのハードウェア プロパティの更新に失敗し、エラー メッセージが表示される**
仮想マシンに [この仮想マシンを有効にしてドメインに参加] ゲスト カスタマイズを構成すると、同じ仮想マシンのハードウェア プロパティの更新が失敗し、エラー メッセージが表示されます。
エラー: <UUID> [ドメインへの参加] が選択されている場合、[ドメイン名]、[ユーザー名]、および [パスワード] を空にすることはできません
- **予約プール割り当てモデルを使用する組織 VDC で、テンプレートから vApp をインスタンス化すると、デプロイされている仮想マシンの構成が無効になる**
この問題は、非予約プール割り当てモデルを使用する VDC がカタログをバックアップする場合に発生します。
vApp テンプレートをそのカタログに保存し、予約プール割り当てモデルを使用した組織 VDC でそのカタログから vApp をインスタンス化すると、仮想マシンの構成のメモリ予約とメモリ制限が無効になります。
- **仮想マシンの展開解除直後に vApp から同じ仮想マシンの削除を試みると、エラー メッセージが表示されて失敗する**
VMware Cloud Director API を使用して、仮想マシンの展開解除直後に vApp から同じ仮想マシンを削除すると操作が失敗し、エラー メッセージが表示されます。
オブジェクトの削除に失敗しました。

- **インポートされた LDAP ユーザーにユーザー パスワードを変更する権限がないにもかかわらず、テナント ポータル ユーザー インターフェイスに [パスワードを変更] オプションが表示される**

VMware Cloud Director テナント ポータルで、インポートされた LDAP ユーザーが上位ナビゲーション バーに移動し、自分のユーザー名をクリックすると、ユーザーにユーザー パスワードを変更する権利がない場合でもドロップダウンメニューに [パスワードを変更] オプションが誤って表示されます。

- **直接組織 VDC ネットワークに接続されている vApp で、仮想マシンの NIC の IP モードを [固定 - IP プール] に設定できない**

直接組織 VDC ネットワークに接続されている vApp では、仮想マシンの NIC の IP モードを [固定 - IP プール] に設定できません。これは、直接ネットワークが複数のサブネットが含まれている外部ネットワークによってバックアップされ、最初のサブネットの IP プールが完全に使用された場合に発生します。別の NIC を仮想マシンに追加するか、または別の仮想マシンを vApp に追加し、IP モードを [固定 - IP プール] に設定すると、VMware Cloud Director では設定が適用されず、IP モードが [DHCP] に変更されます。

- **VMware Cloud Director 10.1.2 からバージョン 10.2.x へのアップグレードを試みると、不正確なエラーが報告される**

VMware Cloud Director 10.1.2 をバージョン 10.2.x にアップグレードすると、次の不正確なエラー メッセージが表示されます。

エラー：別のバージョンの VMware Cloud Director の RPM がすでにインストールされていますが、バージョンが認識されないため、このリリースからのアップグレードはサポートされません。このアップグレードは正常に実行されませんが、ユーザーはリスクを認識したうえで続行できます。

VMware Cloud Director ではバージョン 10.1.2 からバージョン 10.2.x へのアップグレードはサポートされているため、エラー メッセージは無視してもかまいません。

- **VMware Cloud Director アプライアンスを再起動すると、サービス API またはアプライアンス管理ユーザー インターフェイスから、vmware-vcd サービスが失敗状態であると報告されることがある**

VMware Cloud Director アプライアンスを再起動すると、サービス API またはアプライアンス管理ユーザー インターフェイスから、vmware-vcd サービスが失敗状態であると誤って報告されることがあります。これは OS ネットワーク スタックが使用可能になる前に、vmware-vcd サービスが起動を試行した場合に発生します。その結果、サービスは失敗状態になり、サービスが 1 つ以上のポートにバインドできなかったことを示すエラー メッセージが表示されます。その後、vcd-watchdog によって vmware-vcd サービスは正常に起動されますが、systemd サービス ステータスには反映されません。

- **プロバイダ VDC の Kubernetes ポリシーが参照するスーパーバイザー クラスタがプロバイダ VDC のプライマリ クラスタでない場合、このポリシーを VDC に公開できない**

複数のスーパーバイザー クラスタを含むプロバイダ VDC がある場合、プライマリ以外のスーパーバイザー クラスタを参照するプロバイダ VDC の Kubernetes ポリシーを公開すると、LMException エラーが発生して失敗します。

- **ストレージ ポッドまたはクラスタでストレージ ポリシーをバックアップしている、ストレージ ポリシーで VMware Cloud Director IOPS 制限を有効にできない**

Service Provider Admin Portal で、1 つ以上のストレージ ポッドまたはクラスタがストレージ ポリシーをバックアップしている場合に、[影響のある配置] フラグをオフにしても、そのストレージ ポリシーに VMware Cloud Director の IOPS 制限を有効にすることはできません。

- **テナントポータル**のユーザーインターフェイスからサブスクライブされているカタログの **[公開設定]** を更新した後、このカタログを同期すると、「401 Unauthorized」エラーが発生して失敗する
テナントポータル
- **vApp** で仮想マシンのリストを開いて、**[複数選択]** オプションを有効にすると、**[アクション]** メニューが使用できなくなる
vApp で仮想マシンのリストを開いて、**[複数選択]** オプションを有効にすると、**[アクション]** メニューが使用できなくなります。複数の仮想マシンを選択することはできますが、これらの仮想マシンでアクションを同時に実行することはできません。
- **複数選択グリッド**をフィルタリングするときに、別のページに移動すると、フィルタリングされた項目が表示されなくなる
複数選択グリッドで結果をフィルタリングしたときに、使用できるページが複数ある場合は、フィルタ結果の次のページ以降に何も表示されません。この問題は、リストから複数の項目を選択してフィルタリングした場合（たとえば、組織 VDC にストレージポリシーを追加したり、vApp または仮想マシンをユーザーやグループで共有したりした場合）に、ダイアログボックス内で発生します。
- **vApp ユーザー**がテンプレートから vApp を作成する際に、「操作は拒否されました」というエラーメッセージが表示される
割り当てられているユーザーロールが vApp ユーザーである場合、テンプレートから vApp を作成する際に、vApp 内の仮想マシンの仮想マシンサイジングポリシーをカスタマイズすると、「操作は拒否されました」というメッセージが表示されます。この問題は、vApp ユーザーロールでは vApp をテンプレートからインスタンス化できますが、このロールには仮想マシンのメモリ、CPU、またはハードディスクをカスタマイズできる権限が含まれていないために発生します。サイジングポリシーを変更することで、仮想マシンのメモリまたは CPU を変更します。
- **Kubernetes Container Clusters** プラグインで、ロード中にデータグリッドに何も表示されない場合がある
Kubernetes Container Clusters プラグインでは、ロード中のスピナーが表示されないため、ロード中に一部のデータグリッドには何も表示されません。
- **VMware Cloud Director API** を使用してホストを取得すると、numOfCpusLogical パラメータに対して正しくない値が返される
GET /admin/extension/host/{id} API 呼び出しを実行してホストを取得すると、NumOfCpusLogical フィールドに論理 CPU ではなく、物理 CPU の数が表示されます。
この問題は本リリースで、NumOfCpusLogical フィールドを廃止し、次の 2 つの新しいフィールドを出力の本文に追加することで修正されています。
NumOfCpuCoresPhysical
NumOfCpuCoresLogical
- **VMware Cloud Director** で CPU 使用量が急増し、システムの速度が低下する
一部の VMware Cloud Director セルでは、vcloud サービスによる高い CPU 使用量が示されます。CPU 使用量が高いとセルのパフォーマンスが低下し、一部のタスクが失敗します。
- **暗号化された仮想マシン**でゲストのカスタマイズを実行できない

仮想マシンを仮想マシン暗号化機能を持つストレージ ポリシーと関連付ける場合、仮想マシンでゲストのカスタマイズを有効にすると、ゲストのカスタマイズ構成が適用されません。

- **NSX-T ポリシーベースの IPsec VPN を無効にすると、操作が失敗してエラー メッセージが表示される**
HTML5 ユーザー インターフェイスまたは VMware Cloud Director API を使用して NSX-T ポリシーベースの IPsec VPN を無効にすると、操作が失敗し、「エラー コード 500090」というエラー メッセージが表示されます。
- **仮想マシンをテンプレートからインスタンス化すると、ネットワーク アダプタ タイプの構成が正しい仮想マシンがデプロイされない**
仮想マシンをテンプレートからインスタンス化すると、デプロイされた仮想マシンではネットワーク アダプタ タイプの正しい構成が保持されません。
- **複数セルの VMware Cloud Director インストールで、サブスクリブされているカタログの同期がタイムアウトになる**
外部カタログからサブスクリブされているカタログへのコンテンツの自動ダウンロードを無効にすると、カタログの同期が 1% でフリーズし、タイムアウトになります。
- **グループ継承ロールを持つ LDAP ユーザーを使用する際に VMware Cloud Director にログインすると失敗する**
ロールを LDAP グループから継承する LDAP ユーザーとしてログインすると、ログイン操作が失敗して、認証エラー エラー メッセージが表示されます。
- **VMware Cloud Director が開いているすべてのブラウザセッションからログオフする**
複数のウィンドウまたはタブで HTML5 ユーザー インターフェイスを開き、それらのすべてで [アイドルセッション タイムアウト] 構成で指定した時間を超えてアクティブでない場合、VMware Cloud Director は開いているすべてのセッションからログオフします。
- **Chrome ブラウザの使用時に、全データストアのリストのデータストア名をクリックしてもデータストア詳細ページが開かない**
VMware Cloud Director Service Provider ポータルを Chrome で開くと、全データストアのリストのデータストア名をクリックしてもデータストア詳細ページが開きません。
- **セキュリティ グループの名前と説明を更新すると、既存のメンバーがグループから削除される**
セキュリティ グループの名前または説明を更新すると、既存のメンバーがグループから削除されます。
- **[OVF ファイルからの vApp の作成] ウィザードに、VMware Cloud Director テナント ポータルに戻るリンクとして製品名とベンダー名が表示される**
vApp を OVF パッケージから作成すると、ウィザードの [詳細の確認] ページに製品名とベンダー名が VMware Cloud Director テナント ポータルへのリンクとして表示されます。
- **OVA からの vApp の作成が失敗して、「タイムアウト」メッセージが表示される**
OVA ファイルが 8 GB を超えると、この OVA ファイルからの vApp の作成が失敗し、「タイムアウト」エラー メッセージが表示されます。
- **[グループの編集] ウィザードに使用可能なテナント ロールがすべて表示されない**
組織が 15 を超えるテナント ロールから構成されている場合でも、[グループの編集] ウィザードの [ロール] ドロップダウン メニューに表示されるのは 15 ロールのみです。

- **組織 VDC ネットワークを削除した後、Edge Gateway のファイアウォール ルールの更新に失敗し、エラー メッセージが表示される**

Edge Gateway のファイアウォール ルールで使用されている組織 VDC ネットワークを削除すると、同じ Edge Gateway の別のファイアウォール ルールの後続の更新に失敗し、エラー メッセージが表示されます。

値が `??virtualwire-xx??` の Edge ファイアウォール ソース/ターゲット タイプは、VMware Cloud Director では認識されず、サポートされません。
- **[ルールの編集] ウィザードの [保存] ボタンがグレーアウトされ、ファイアウォール ルールを更新できない**

NSX-T Data Center ファイアウォール ルールが [拒否] アクションを使用するように構成されている場合、HTML5 ユーザー インターフェイスでファイアウォール ルールを更新すると、[ファイアウォールの編集] ウィザードの [保存] ボタンがグレーアウトされます。
- **vApp のパワーオンに失敗して「無効な状態」エラー メッセージが表示される**

vApp のパワーオンに 3 分以上かかると、操作が失敗し、「無効な状態」エラー メッセージが表示されます。
- **VDC テンプレートを使用してデプロイされた VDC に対し NSX Edge Gateway の内部インターフェイスが切断される**

VMware Cloud Director API を使用して、経路指定ネットワークの構成を含む VDC テンプレートから新しい VDC を作成すると、デプロイされている NSX Edge の内部インターフェイスが切断されます。
- **[Edge Gateway の作成] ウィザードで組織 VDC に使用可能な 15 個を超える Edge クラスタを表示できない**

15 個を超える Edge クラスタで構成されている組織仮想データセンターで、新しい Edge Gateway をデプロイすると、[Edge Gateway の作成] ウィザードの [Edge クラスタ] ページには Edge クラスタ が 15 個まで表示されません。
- **[Edge クラスタ割り当ての編集] のデータ グリッドが空白で表示される**

Edge Gateway をデータセンター グループに追加すると、[Edge クラスタ割り当ての編集] ウィザードのデータ グリッドが空白で表示されます。
- **vRealize Orchestrator ワークフローの実行ウィザードに、VDC 名ではなく VDC の URL が表示される**

VMware Cloud Director で、vRealize Orchestrator ワークフローを開始すると、[サービスの実行] ウィザードに仮想データセンター名ではなく仮想データセンターの URL が表示されます。
- **VMware Cloud Director 10.2 にアップグレードした後、サービス監視でコンソール プロキシ エンドポイントが使用不可と報告される**

vCloud Director 9.7 から VMware Cloud Director 10.2 にアップグレードした後、ロード バランサ サービス監視でコンソール プロキシ エンドポイントが [使用不可] と報告され、セルへのアクセスの試みが失敗し、ERR_CONNECTION_REFUSED エラー メッセージが表示されます。
- **仮想マシンを無効にしてドメインに参加させると、同じ仮想マシンで一部の操作が失敗し、「ドメイン参加が無効化されている場合、DomainName を提供しないでください」というエラー メッセージが表示される**

ゲストのカスタマイズ [この仮想マシンを有効にしてドメインに参加] を仮想マシンで有効にし、後で無効にすると、仮想マシンの名前変更、または vApp への追加が、エラー メッセージとともに失敗します。

ドメイン参加が無効化されている場合、DomainName を提供しないでください

既知の問題

- **New:** NetApp ストレージアレイから NFS データストアをマウントすると、VMware Cloud Director アプライアンスの初期構成中にエラー メッセージを表示して失敗する

VMware Cloud Director アプライアンスの初期構成中に、NetApp ストレージアレイから NFS データストアを構成すると、次のエラーメッセージが表示されて操作は失敗します。

NFS のバックエンド検証が次のエラーで失敗しました: 不明なユーザーによって所有されています。

回避策: VMware Cloud Director Appliance API を使用して VMware Cloud Director アプライアンスを構成します。

- **New:** VMware Cloud Director のインストール中にカスタマー エクスペリエンス向上プログラム (CEIP) を無効にした後でも、ステータスが **Enabled** になる

VMware Cloud Director のインストール中に、CEIP に参加するオプションを無効にすると、インストールの完了後に CEIP のステータスがアクティブになります。

回避策: [\[VMware カスタマー エクスペリエンス向上プログラムへの参加または離脱\]](#) の手順に従って、CEIP を無効にします。

- **New:** ブラウザで [LDAP] ページを更新しても、同じページに戻らない

Service Provider Admin Portal では、ブラウザで [LDAP] ページを更新すると、[LDAP] ページには戻らず、プロバイダ ページに移動します。

回避策: なし。

- **New:** 組織の LDAP 同期設定を編集できない

VMware Cloud Director Service Provider Admin Portal の [LDAP 同期設定] タブで、[編集] をクリックしても動作せず、組織の LDAP 設定を編集できません。

回避策: なし。

- **New:** VMware Cloud Director で LDAP 同期の開始時刻の値が正しく表示されない

VMware Cloud Director Service Provider Admin Portal で、[LDAP 同期] ページの [同期の開始時刻] に、構成した日時ではなくページを開いた日時が表示されます。

回避策: なし。

- **New:** 予約プール仮想データセンターを Flex 組織仮想データセンターに変換すると、仮想マシンが非準拠になる
予約プール割り当てモデルを使用する組織仮想データセンターで、一部の仮想マシンに CPU とメモリのゼロ以外の予約、CPU とメモリの無制限でない構成、またはその両方がある場合、Flex 組織仮想データセンターに変換した後でこれらの仮想マシンは非準拠になります。仮想マシンを再び準拠状態にしようと試みると、システムは予約と制限に関して誤ったポリシーを適用して、CPU およびメモリの予約をゼロに設定し、制限を [制限なし] に設定します。

回避策:

1. システム管理者が、正しい構成の仮想マシンサイジングポリシーを作成する必要があります。
2. システム管理者が、変換後の Flex 組織仮想データセンターに新しい仮想マシンサイジングポリシーを発行する必要があります。
3. テナントは、VMware Cloud Director API または VMware Cloud Director テナントポータルを使用して、Flex 組織 VDC 内の既存の仮想マシンに仮想マシンサイジングポリシーを割り当てることができます。

- **New:** FIPS モードが有効な場合に vRealize Orchestrator を統合すると、無効なパラメータに関連するエラーが発生して操作が失敗する

FIPS モードを有効にすると、VMware Cloud Director と vRealize Orchestrator 間の統合が機能しなくなります。

VMware Cloud Director ユーザー インターフェイスが「VRO 要求パラメータが無効です」エラーを返します。API 呼び出しを行うと、次のエラーが返されます。

```
Caused by: java.lang.IllegalArgumentException: 'param' arg cannot be null at
org.bouncycastle.jcajce.provider.ProvJKS$JKSKeyStoreSpi.engineLoad(Unknown Source) at
java.base/java.security.KeyStore.load(KeyStore.java:1513) at
com.vmware.vim.install.impl.CertificateGetter.createKeyStore(CertificateGetter.java:128) at
com.vmware.vim.install.impl.AdminServiceAccess.(AdminServiceAccess.java:157) at
com.vmware.vim.install.impl.AdminServiceAccess.createDiscover(AdminServiceAccess.java:238) at
com.vmware.vim.install.impl.RegistrationProviderImpl.(RegistrationProviderImpl.java:56) at
com.vmware.vim.install.RegistrationProviderFactory.getRegistrationProvider(RegistrationProviderFactory.java:143)
at com.vmware.vcloud.vro.client.connection.STSClient.getRegistrationProvider(STSClient.java:126) ...136 more
```

回避策: なし。

- **New:** VMware Cloud Director API 呼び出しで vCenter Server 情報を取得すると、UUID ではなく URL が返される

この問題は、VMware Cloud Director バージョン 10.2.1 以前への最初の登録に失敗した vCenter Server インスタンスで発生します。これらの vCenter Server インスタンスに対し、API 呼び出しを行って vCenter Server 情報を取得すると、VMware Cloud Director API が誤って想定された UUID ではなく URL を返します。

回避策: vCenter Server インスタンスを VMware Cloud Director に再接続します。

- **New:** VMware Cloud Director が HTML5 ユーザー インターフェイスからログオフするまでの時間が、アイドルセッションタイムアウト構成で指定した時間を超える

VMware Cloud Director は HTML5 ユーザー インターフェイスからログオフするまでに、アイドルセッションタイムアウト構成で指定した時間の 2 倍の時間を要します。

回避策: ウィンドウを最小化するか、同じウィンドウ内の別のタブに切り替える必要があります。

- **New:** vCenter Server 7.0 Update 2a または Update 2b にアップグレードした後、Tanzu Kubernetes Grid クラスタを作成できない

基盤となる vCenter Server のバージョンが 7.0 Update 2a または Update 2b の場合、Kubernetes Container Clusters プラグインを使用した Tanzu Kubernetes Grid クラスタの作成に失敗します。

回避策: なし。

- **New:** セルを VMware Cloud Director 10.2.2 にアップグレードする前に特定の証明書およびトラストストア ファイルを削除しないと、セルが動作しなくなる

certificates.bak、proxycertificates.bak、および truststore.bak ファイルがセルの /opt/vmware/vcloud-director/etc/ フォルダにある場合、バージョン 10.2.2 へのアップグレード後、セルが動作しなくなります。ログに次のエラーが記録されます。

```
cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.pem': No such file or directory
cp: cannot stat '/opt/vmware/vcloud-director/etc/proxycertificates.key': No such file or directory
```

回避策: /opt/vmware/vcloud-director/bin/configure を実行します。

- **New: OpenSSL で生成された PKCS8 ファイルを VMware Cloud Director アプライアンスに FIPS モードでアップロードしようとする、エラーが発生して失敗する**

OpenSSL は FIPS 準拠のプライベート キーを生成できません。VMware Cloud Director が FIPS モードで、OpenSSL を使用して生成された PKCS8 ファイルをアップロードすると、アップロードは失敗し、「不正な要求: org.bouncycastle.pkcs.PKCSException: 暗号化されたデータを読み取ることができません: ... 使用できません: アルゴリズムがありません: ...」というエラーまたは「salt は 128 ビット以下にする必要があります」というエラーが表示されます。

回避策: PKCS8 ファイルをアップロードするには、FIPS モードを無効にします。

- **アップグレード後、VMware Cloud Director アプライアンス管理ユーザー インターフェイスの [システム構成] 画面が表示されない**

VMware Cloud Director アプライアンスをバージョン 10.2.2 にアップグレードした後、アプライアンス管理ユーザー インターフェイスの新しい [システム構成] 画面が表示されません。

回避策: この問題を回避して再発を防ぐには、ブラウザのキャッシュをクリアします。

- **Kubernetes Container Clusters プラグインを使用して Tanzu Kubernetes クラスタを作成すると失敗する**

Kubernetes Container Clusters プラグインを使用して Tanzu Kubernetes クラスタを作成する場合は、Kubernetes のバージョンを選択する必要があります。ドロップダウンメニューのバージョンの中には、バックアップしている vSphere インフラストラクチャと互換性のないものがあります。互換性のないバージョンを選択すると、クラスタの作成が失敗します。

回避策: 失敗したクラスタのレコードを削除し、互換性のある Tanzu Kubernetes バージョンを使用して再試行してください。Tanzu Kubernetes と vSphere の非互換性の詳細については、「[vSphere with Tanzu 環境の更新](#)」を参照してください。

。

- **組織内にサブスクリプションされているカタログがある場合、VMware Cloud Director をアップグレードすると、カタログの同期に失敗する**

アップグレード後、組織内にサブスクリプションされているカタログがある場合、VMware Cloud Director は公開されたエンドポイント証明書を自動的に信頼しません。証明書を信頼していない場合、コンテンツ ライブラリの同期に失敗します。

回避策: 各カタログ サブスクリプションの証明書を手動で信頼します。カタログ サブスクリプションの設定を編集する際、[初回使用時に信頼する (TOFU)] ダイアログが表示され、リモート カタログ証明書を信頼するように求められます。

証明書の信頼に必要な権限を持っていない場合は、組織管理者に確認します。

- **VMware Cloud Director をアップグレードして、Tanzu Kubernetes クラスタの作成を有効にすると、自動生成されたポリシーが使用不能になり、ポリシーを作成または公開できなくなる**

VMware Cloud Director をバージョン 10.2.2 に、vCenter Server をバージョン 7.0.0d 以降にアップグレードし、スーパーバイザー クラスタによってバックアップされるプロバイダ仮想データセンター (VDC) を作成すると、VMware Cloud Director で VDC の横に Kubernetes のアイコンが表示されます。ただし、新しいプロバイダ仮想データセンターには自動生成された Kubernetes ポリシーがありません。Kubernetes ポリシーを作成するか、組織仮想データセンターに公開しようとしても、使用可能なマシン クラスはありません。

回避策: 対応する Kubernetes エンドポイント証明書を手動で信頼します。VMware のナレッジベースの記事 [83583](#) を参照してください。

- **Setup DRaaS and Migration プラグインが、VMware Cloud Director ユーザー インターフェイスの上部のナビゲーション バーに 2 回表示される**

この問題は、vCloud Availability 4.0.0 が VMware Cloud Director Availability 4.0.0 にブランド変更されたため、2つのプラグインが存在することが原因で発生します。VMware Cloud Director は vCloud Availability 4.0.0 プラグインを自動的に無効にしません。古いバージョンと新しいバージョンが、[\[詳細\]](#) の下の上部のナビゲーション バーに Setup DRaaS and Migration プラグインとして表示されます。

回避策: vCloud Availability 4.0.0 プラグインを無効にします。プラグインの無効化については、[「プラグインの有効化/無効化」](#) を参照してください。

- **ラテン文字以外の文字を含む Kubernetes クラスタ名を入力すると、[新規クラスタの作成] ウィザードの [次へ] ボタンが無効になる**

Kubernetes Container Clusters プラグインは、ラテン文字のみをサポートしています。ラテン文字以外の文字を入力すると、次のエラーが表示されます。名前は文字で開始する必要があり、英数字またはハイフン (-) のみを使用できます。(最大 128 文字)。

回避策: なし。

- **TKGI クラスタのサイズを変更すると、データ グリッド内の一部の値が空白または該当なしとして表示される**
VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) クラスタのサイズを変更すると、データ グリッドビューの組織と仮想データセンターのクラスタの値が空白または該当なしと表示されます。

回避策: なし。

- **優先順位を使用してアドバイザリをフィルタリングすると、内部サーバエラーが発生する**

VMware Cloud Director API を使用してアドバイザリに優先順位フィルタを適用すると、エラー メッセージが表示されて操作が失敗します。

```
"minorErrorCode": "INTERNAL_SERVER_ERROR" "message": "[ d0ec01b3-019f-4ed2-a012-1f7f5e33cb7f ] java.lang.String cannot be cast to java.lang.Integer"
```

回避策: すべてのアドバイザリを取得して、手動でフィルタリングします。詳細については、[VMware Cloud Director OpenAPI](#) のドキュメントを参照してください。

- **API ドキュメントに、アドバイザリの優先順位の並べ替え順に関する誤った説明が表示される**

アドバイザリ モデル オブジェクトには、作成する各アドバイザリの緊急度を指定するための優先順位フィールドが含まれています。アドバイザリ API のドキュメントには、優先順位が降順で表示されていると誤って記載されています。VMware Cloud Director API ドキュメントには、アドバイザリの優先順位が昇順で表示されています。

回避策: なし。

- **NFS のダウンタイムによって VMware Cloud Director アプライアンスのクラスタ機能が誤動作することがある**
NFS に空きがない、読み取り専用になっているなどの理由で NFS が使用できない場合、アプライアンスのクラスタ機能は誤動作を開始します。NFS が停止している、またはアクセスできない場合、HTML5 ユーザー インターフェイスは応答しません。影響を受ける可能性のあるその他の機能として、障害が発生したプライマリセル

のフェンス、スイッチオーバー、スタンバイセルの昇格などがあります。NFS 共有ストレージを正しく設定する方法については、「[VMware Cloud Director アプライアンスに対する転送サーバストレージの準備](#)」を参照してください。

回避策:

- NFS の状態を read-only にならないように修正します。
- NFS 共有に空きがない場合は、クリーンアップします。
- **マルチサイト環境で vCenter Server および NSX のリソースを追加しているときにエンドポイントを信頼した場合、統合証明書ストレージ領域にエンドポイントが追加されない**

マルチサイト環境で、HTML5 ユーザー インターフェイスを使用して vCloud Director 10.0 サイトにログインするか、vCenter Server インスタンスを vCloud Director 10.0 サイトに登録しようとしても、VMware Cloud Director はエンドポイントを統合証明書ストレージ領域に追加しません。

回避策:

- 証明書を VMware Cloud Director 10.1 サイトにインポートするには、API を使用します。
- 証明書管理機能をトリガするには、VMware Cloud Director 10.1 サイトの SP Admin Portal に移動し、サービスの **[編集]** ダイアログに移動して、**[保存]** をクリックします。
- **vCenter Server バージョン 6.5 以前で名前付きディスクを暗号化しようと試みると、エラーが発生して失敗する**
vCenter Server インスタンス バージョン 6.5 以前の場合、新規または既存の名前付きディスクを暗号化が有効になっているポリシーに関連付けると、操作が失敗し、「このバージョンの vCenter Server では、名前付きディスクの暗号化はサポートされていません。」というエラーが表示されます。

回避策: なし。

- **Firefox で VMware Cloud Director Service Provider Admin Portal を使用している場合に、テナント ネットワーク画面をロードできない**

Firefox で VMware Cloud Director Service Provider Admin Portal を使用すると、組織仮想データセンターの **[ファイアウォールの管理]** 画面などのテナント ネットワーク画面の読み込みに失敗することがあります。この問題は、Firefox ブラウザでサードパーティ Cookie をブロックするように設定していると発生します。

回避策: Firefox ブラウザで、サードパーティの Cookie を許可するよう設定します。詳細については、「<https://support.mozilla.org/ja-JP/>」に移動し、ナレッジベースの記事「**Cookie が無効にされていると表示される**」を参照してください。

- **VMware vSphere Storage APIs Array Integration (VAAI) 対応 NFS アレイ上、または vSphere Virtual Volumes (VVols) 上に作成されている高速プロビジョニングされた仮想マシンを統合できない**

ネイティブ スナップショットが使用されている場合、高速プロビジョニングされた仮想マシンのインプレイス統合はサポートされません。VAAI 対応データストアおよび VVols では、ネイティブ スナップショットが常に使用されます。高速プロビジョニングされた仮想マシンがこれらのいずれかのストレージ コンテナにデプロイされている場合、その仮想マシンを統合することはできません。

回避策: "VAAI 対応 NFS または VVols を使用する組織仮想データセンターで高速プロビジョニングを有効にしてはいけません。"VAAI または VVol のデータストアにスナップショットを持つ仮想マシンを統合するには、その仮想マシンを別のストレージ コンテナに再配置します。

- **権限のセットが必須でない組織管理者ロールに対して、[ログの有効化] トグルが有効になっている**
ロールに**システム ログの構成**権限がない場合でも、**組織管理者**ロールが割り当てられたユーザーに対し、**[ログの有効化]** トグルが有効になっています。

回避策: この問題は、VMware Cloud Director 10.2.2.1 パッチ リリースで修正されています。

- **VMware Cloud Director API を使用して、テンプレートから仮想マシンを作成するときに、デフォルトのストレージ ポリシーを指定しなかった場合、テンプレートに対してストレージ ポリシーが設定されていなければ、新しく作成された仮想マシンは、ソース テンプレート自体のストレージ ポリシーを使用する**

VMware Cloud Director API を使用して、テンプレートから仮想マシンを作成するときに、デフォルトのストレージ ポリシーを指定しなかった場合、テンプレートに対してストレージ ポリシーが設定されていなければ、新しく作成された仮想マシンは、デプロイ先の**組織仮想データセンター**のストレージ ポリシーは使用せずに、ソース テンプレート自体のストレージ ポリシーを使用します。

回避策: なし。