VMware Cloud Director 10.1 リリース ノート

VMware Cloud Director 10.1 | 2020 年 4 月 9 日 | ビルド 15967253（インストールされているビルド 15967236）

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

- このリリースの新機能
- セキュリティ
- 製品サポートに関する注意事項
- 以前のリリースからのアップグレード
- システム要件とインストール
- 解決した問題
- 既知の問題

このリリースの新機能

- このリリースの新機能および更新された機能については、VMware テクニカル ホワイト ペーパー『What's New with VMware vCloud Director 10.1』を参照してください。
- HTML5 ユーザー インターフェイスでの動作が次のように変更されました。
  以前の VMware Cloud Director バージョンで、HTML ユーザー インターフェイスの vApp アクション メニューを使用して、vApp を停止またはパワーオフすることができます。いずれの電源操作でも vApp のデプロイが解除されますが、vApp への影響が異なります。パワーオフ操作は、vApp 内仮想マシンの [起動と停止の順序] 設定には従いません。また、パワーオフ操作では、組織 VDC ネットワークからすべての仮想マシン NIC を切断し、vApp にデプロイされた Edge ゲートウェイを削除することにより、すべての vApp ネットワークのデプロイが解除されます。

  VMware Cloud Director 10.1 では、実行中の vApp でパワーオフ操作を実行しても、vApp および vApp 内の仮想マシンのデプロイは解除されずに vApp 内のすべての仮想マシンがパワーオフされます。仮想マシンの NIC の各ネットワークへの接続は維持され、すべての vApp Edge ゲートウェイのデプロイも維持されます。vApp 内の vApp および仮想マシンもデプロイされたままに

なります。vApp 内の各仮想マシンに対するパワーオフ アクションはアクティブなままであるため、仮想マシンのパワーオフに使用できます。このアクションによって、この仮想マシンのデプロイが解除されます。

vApp をパワーオフすると、パワーオフ操作は [起動と停止の順序] 設定で定義した起動順序に従います。その結果、仮想マシンは、起動に設定した順序とは逆の順序でパワーオフされます。[停止待機時間] 設定は、パワーオフ操作時には適用されません。vApp をパワーオフすると、vApp 内の仮想マシンの電源状態から取得した vApp の電源状態は [パワーオフ] と表示されます。

- VMware Cloud Director API 34.0 スキーマには、`numberOfCpus` 属性と `MemoryAllocationMB` 属性の定義が含まれています。

セキュリティ

- **警告:** バージョン 10.1 にアップグレードすると、VMware Cloud Director は常に、自身に接続されているすべてのインフラストラクチャ エンドポイントの証明書を検証します。これは、VMware Cloud Director での SSL 証明書の管理方法が変更されたためです。アップグレード前に証明書を VMware Cloud Director にインポートしていない場合は、vCenter Server と NSX の接続が、SSL 検証の問題が原因の接続エラーで失敗したと表示されることがあります。この場合、アップグレード後に、次の 2 つの方法のいずれかを実行できます。
  1. セル管理ツールで `trust-infrastructure-cert` コマンドを実行して、vCenter Server および NSX Manager インスタンスのすべてのインフラストラクチャ エンドポイントに自動的に接続して、これらの証明書を取得し、統合証明書ストアに格納します。「vSphere リソースからのエンドポイント証明書のインポート」を参照してください。
  2. Service Provider Admin Portal のユーザー インターフェイスで、vCenter Server と NSX の各インスタンスを選択し、証明書を受け入れるときに認証情報を再入力します。

- バージョン 10.1 以降では、サービス プロバイダとテナントは VMware Cloud Director API を使用してリモート サーバへの接続をテストし、サーバ ID を SSL ハンドシェイクの一部として検証できます。VMware Cloud Director ネットワーク接続を保護するには、接続テストに VMware Cloud Director API を使用しているテナントにアクセスできない内部ホストの拒否リストを構成します。拒否リストは、VMware Cloud Director のインストールまたはアップグレード後、テナントに VMware Cloud Director へのアクセス権を付与する前に構成します。「テスト接続の拒否リストの構成」を参照してください。
- すべての SSL 証明書を信頼する動作は VMware Cloud Director 10.1 で廃止されています。本リリースでは、vCenter Server と NSX の接続にこのオプションを使用することはできません。他の

すべての接続でも、すべての証明書を信頼する動作は廃止されています。VMware Cloud Director 10.1 より後のバージョンではサポート対象外になる予定です。システム管理者はこの移行への対応が必要になります。

- VMware Cloud Director システムの組織で LDAP を使用する場合は、ユーザー インターフェイスの Trust On First Use ダイアログを使用するか、API を使用して証明書をアップロードします。
- このオプションのすべての使用を監査し、ユーザー インターフェイスまたは API を使用して適切な証明書を提供します。
- テナントに変更を通知します。**[すべての証明書を承認]** オプションを有効にしたカスタム LDAP を使用しているすべてのテナントは、この設定から移行する必要があります。テナントは、ユーザー インターフェイスの Trust On First Use ダイアログを使用するか、API を使用して証明書をアップロードすることができます。

アップデートされたオープン ソース パッケージ

- `jackson-databind` がバージョン 2.9.10.1 にアップデートされました。
- `jre` が 1.8.0u231 にアップデートされました。
- `openssl` がバージョン 1.0.2u にアップデートされました。
- `xstream` がバージョン 1.4.11.1 にアップデートされました。

製品サポートに関する注意事項

VMware Cloud Director 10.1 は vSphere 7.0 および NSX-T Data Center 3.0 をサポートしていません。現在、相互運用性の認証が進行中で、vSphere 7.0 と NSX-T 3.0 Data Center は VMware Cloud Director 10.1 のマイナー パッチ リリースでサポートされる予定です。

NSX-T Data Center の VRF-Lite Tier-0 ゲートウェイでバッキングされる外部ネットワークはサポートされません。

販売終了およびサポート終了に関する警告

- SQL Server データベースはサポートされなくなりました。PostgreSQL データベースのみがサポートされています。
- Oracle Linux は、VMware Cloud Director アプリケーションをインストールするホスト OS としてサポートされなくなりました。
- VMware Cloud Director API バージョン 20 以前はサポートされていません。

- VMware Cloud Director API バージョン 27.0 ~ 29.0 は、VMware Cloud Director 10.1 以降はサポート対象外になるため、廃止されます。
- VMware Cloud Director API バージョン 30.0 は廃止されました。
- Flex ベースのユーザー インターフェイスは製品から削除され、サポートされなくなりました。
- `/api/sessions` API ログイン エンドポイントは VMware Cloud Director API バージョン 33.0/VMware Cloud Director 10.0 で廃止され、以降の VMware Cloud Director リリースでサポートされなくなります。サービス プロバイダおよびテナントの VMware Cloud Director へのアクセス用に、個別の VMware Cloud Director OpenAPI ログイン エンドポイントを使用することができます。
- API `/cloud/server_status` は、HTTP と HTTPS の両プロトコルで廃止され、以降のリリースで削除されます。HTTP と HTTPS の両プロトコルには、`/api/server_status` を使用する必要があります。
- リセット アクション `/ldap/action/resetLdapCertificate` および `/ldap/action/resetLdapKeyStore` は、VMware Cloud Director 10.1 での SSL 証明書の格納および処理方法が理由で VMware Cloud Director API バージョン 34.0 から削除されています。`/cloudapi/1.0.0/ssl/trustedCertificates` エンドポイントを使用して、証明書の信頼を解除する必要があります。
- 更新アクション `/ldap/action/updateLdapCertificate` および `/ldap/action/updateLdapKeyStore` は廃止され、以降のリリースではサポートされなくなります。VMware Cloud Director では、LDAP 証明書 `/cloudapi/1.0.0/ssl/trustedCertificates` の信頼性のために新しいエンドポイントが導入されています。
- vSphere では、SAML IDP としての vSphere SSO は廃止されています。SAML IDP として vSphere SSO を使用するように設定されたすべての VMware Cloud Director 環境は、別の外部 SAML IDP に移行する必要があります。今後の vSphere および VMware Cloud Director リリースで、この IDP の使用はサポートされなくなります。
- DSA および DSS 証明書では、使用できる推奨暗号スイートがなくなるため、これらの証明書はサポートされなくなります。

今後のサポート終了のお知らせ

- VMware Cloud Director API 34.0 (VMware Cloud Director 10.1) に含まれている API は現在廃止のものが増加しているため、以降のリリースでは削除される予定です。『VMware Cloud Director API プログラミング ガイド』を参照してください。

以前のリリースからのアップグレード

VMware Cloud Director 10.1 へのアップグレード、アップグレードおよび移行パス、およびワークフローの詳細については、「VMware Cloud Director アプライアンスのアップグレードと移行」または「Linux での vCloud Director のアップグレード」を参照してください。

システム要件とインストール

ポートとプロトコル

VMware Cloud Director 10.1 で使用されるネットワーク ポートおよびプロトコルの詳細については、「VMware のポートとプロトコル」を参照してください。

互換性マトリックス

次の内容に関する情報については、VMware 製品相互運用性マトリックスを参照してください。

- 他の VMware プラットフォームとの VMware Cloud Director の相互運用性
- サポート対象の VMware Cloud Director データベース

サポート対象の VMware Cloud Director サーバ オペレーティング システム

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

サポート対象の AMQP サーバ

VMware Cloud Director は AMQP を使用して、拡張サービス、オブジェクト エクステンション、および通知で使用されるメッセージ バスを提供します。本リリースの VMware Cloud Director では、RabbitMQ バージョン 3.7.9 または 3.8.2 が必要です。

詳細については、『VMware Cloud Director インストール、構成およびアップグレード ガイド』を参照してください。

履歴メトリック データを格納するためのサポート対象データベース

VMware Cloud Director が仮想マシンのパフォーマンスおよびリソース使用量について収集するメトリックを格納するように VMware Cloud Director のインストールを構成できます。履歴メトリックのデー

タは、Cassandra データベースに格納されます。VMware Cloud Director は、Cassandra バージョン 3.x をサポートします。

詳細については、『VMware Cloud Director インストール、構成およびアップグレード ガイド』を参照してください。

ディスク容量の要件

各 VMware Cloud Director サーバに、インストールとログ ファイル用として約 2,100 MB の空き容量が必要です。

メモリ要件

メモリ要件については、『VMware Cloud Director インストール、構成、およびアップグレード ガイド』を参照してください。

CPU 要件

VMware Cloud Director は、CPU バウンド アプリケーションです。該当する vSphere バージョンに合わせた CPU オーバーコミット ガイドラインを順守する必要があります。仮想化環境では、VMware Cloud Director で使用可能なコアの数に関係なく、物理 CPU に対する vCPU の比率は、過剰なオーバーコミットが発生しない適切な数にする必要があります。

必須の Linux ソフトウェア パッケージ

各 VMware Cloud Director サーバには、いくつかの共通の Linux ソフトウェア パッケージがインストールされている必要があります。これらのパッケージは、通常、オペレーティング システム ソフトウェアと一緒にデフォルトでインストールされます。欠落しているパッケージがあると、インストーラは診断メッセージを表示して失敗します。

```
alsa-lib
bash
chkconfig
coreutils
findutils
glibc
grep
initscripts
krb5-libs
libgcc
libICE
libSM
libstdc++
libX11
libXau
libXdmcp
libXext
libXi
libXt
libXtst
module-init-tools
net-tools
pciutils
procps
redhat-lsb
sed
tar
wget
which
```

インストーラで必要とするパッケージに加えて、ネットワーク接続を構成したり、SSL 証明書を作成したりする手順では、Linux `nslookup` コマンドを使用する必要があります。これは、Linux bind-utils パ

ッケージで入手できます。

サポート対象の LDAP サーバ

次の LDAP サービスから VMware Cloud Director にユーザーとグループをインポートできます。

プラットフォーム	LDAP サービス	認証方式
Windows Server 2012	Active Directory	シンプル、シンプル SSL
Windows Server 2016	Active Directory	シンプル、シンプル SSL
Linux	OpenLDAP	シンプル、シンプル SSL

サポートされるセキュリティ プロトコルおよび暗号化スイート

VMware Cloud Director では、クライアント接続が安全である必要があります。SSL バージョン 3 および TLS バージョン 1.0 と 1.1 にはセキュリティ上の重大な脆弱性があることがわかっており、クライアント接続の確立時にサーバが使用を提供するデフォルトのプロトコル セットには含まれていません。システム管理者は、他のプロトコルと暗号スイートを有効に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。次のセキュリティ プロトコルがサポートされます。

- TLS バージョン 1.2
- TLS バージョン 1.1（デフォルトで無効)
- TLS バージョン 1.0（デフォルトで無効)

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_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

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。

サポートされるブラウザ

VMware Cloud Director は、次のブラウザの最新および以前のメジャー リリースと互換性があります。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11

サポートされるゲスト OS と仮想ハードウェアのバージョン

VMware Cloud Director では、各リソース プールをバッキングする ESXi ホストでサポートされる、すべてのゲスト OS と仮想ハードウェア バージョンがサポートされます。

VMware Cloud Director WebMKS 2.1.1

VMware Cloud Director WebMKS 2.1.1 コンソールでは、次のサポートが追加されています。

- Google Chrome と Windows 版 Mozilla Firefox の PrintScreen キー。
- Windows および macOS の Windows キー。Windows キーを押す操作をシミュレートするには、Windows OS で Ctrl+Windows を押すか、macOS で Ctrl+Command を押します。
- Google Chrome および Mozilla Firefox での自動キーボード レイアウト検出。

解決した問題

- **2 つの VMware Cloud Director アプライアンス サイトを関連付けると、オブジェクトがサイト間で表示されなくなる**
  サイトに組織、組織 VDC、vApp、仮想マシンなどのオブジェクトがある場合は、サイトの関連付けを作成したときに、現在のサイトからこれらのオブジェクトを表示できません。HTML 5 ユーザー インターフェイスには、他の関連付けられたサイトからのオブジェクトのみが表示されます。この問題は、VMware Cloud Director アプライアンスの `/etc/hosts` ファイルの内容が正しくないため、マルチサイト ファンアウト通信中に発生します。

- **仮想マシンのサイジング ポリシーの更新がメモリ割り当てエラーで失敗する**
  割り当てプール VDC を Flex 組織 VDC に変換すると、vCloud Director は変換前の割り当てプール VDC の最大ポリシー情報を保持します。割り当てプール VDC で定義されている予約よりも

CPU またはメモリの予約が多く確保されている場合、「仮想マシンの予約、制限、または共有の設定が無効です」エラーで失敗します。

- **複数セル環境のプライマリ セルでタスクを静止または一時停止しても、定期タスクがセカンダリ セルで再開しない**
  複数セル環境でプライマリ セルを静止または一時停止すると、プライマリ セルのバックグラウンドで実行されている定期タスクが、セカンダリ セルで再開しません。

- **データ サービスが有効になっているホストベースのストレージ ポリシーが設定された仮想マシンから、別のホストベースのストレージ ポリシーが設定された仮想マシンにクローンを作成すると、エラーで失敗する**
  IOPS や仮想マシンの暗号化などのホストベースのルールが有効になっているストレージ ポリシーが設定された仮想マシンを作成する場合に、仮想マシンのクローンを作成して、ターゲット仮想マシンのストレージ ポリシーを変更すると、「クローン操作中は、データ サービス機能を使用して仮想マシン ストレージ ポリシーを変更または適用することができません。」というエラーが表示されて失敗します。データ サービス機能を使用する仮想マシン ストレージ ポリシーは、クローン作成操作が完了してから、仮想マシンがパワーオンされるまでの間に、プロビジョニング済みの仮想マシンに割り当てることができます。

- **グローバル テナント ロール vApp 作成者が、テンプレートやメディアのアップロードと作成に必要な権限を持っていない場合でも実行できる**
  グローバル テナント ロール vApp 作成者には、デフォルトで「マイ クラウドからの vApp を追加」権限があります。この権限とテンプレート/メディア: 作成/アップロード権限は単一の操作を共有しているため、VMware Cloud Director は誤って テンプレート/メディア: 作成/アップロード権限も vApp 作成者ロールに付与します。

  この問題は修正されています。vApp 作成者ロールに引き続きテンプレート/メディア: 作成/アップロード権限を持たせる場合は、サービス プロバイダは vApp 作成者グローバル ロールに権限を追加して組織に公開できます。

- **新しく作成した仮想マシンが組織 VDC のデフォルト ストレージ ポリシーにデプロイされる**
  vCloud Director テナント ポータルで新しいスタンドアロン仮想マシンを作成するときに、ストレージ ポリシーを指定するオプションが表示されません。その結果、作成された仮想マシンは、組織 VDC のデフォルトのストレージ ポリシーを使用してデプロイされます。

既知の問題

- **New: Microsoft Internet Explorer 11 を使用していると仮想マシンの Web コンソールを開くことができない**
  Microsoft Internet Explorer 11 を使用して仮想マシンのコンソールに接続すると空白のウィンドウが開き、仮想マシン コンソールにアクセスできません。

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：テナント ポータル ユーザー インターフェイスで、アフィニティ ルールまたは非アフィニティ ルールを作成するときに、必須チェック ボックスを選択解除してもルールの構成に影響しない**
  テナント ポータル ユーザー インターフェイスでアフィニティ ルールまたは非アフィニティ ルールを作成するときに、必須チェック ボックスを選択解除しても、ルールの構成には影響しません。アフィニティ ルールと非アフィニティ ルールは常に必須です。つまり、ルールを満たせない場合、ルールに追加された仮想マシンはパワーオンしません。

  回避策：なし。

- **NEW：VMware Cloud Director API を使用して vApp に対してクエリを実行すると、numberOfCpus および MemoryAllocationMB 属性のフィールドが空の状態で返される**
  VMware Cloud Director API 33.0 以前のバージョンを使用して vApp REST API クエリを実行すると、REST API レスポンス本文から、`numberOfCpus` および `MemoryAllocationMB` 属性のフィールドが空の状態で返されます。これは、API スキーマに `numberOfCpus` および `MemoryAllocationMB` 属性の定義が含まれていないために発生します。

  回避策：vApp に対するクエリには VMware Cloud Director API 34.0 を使用します。

- **NEW：NSX-T Edge Gateway に NAT ルールを追加しようとすると失敗する**

NSX-T Edge Gateway に NAT ルールを追加しようとすると、「新しい値と廃止された値が再配布のためにまとめて更新されました。エラー コード 503266」というエラーが表示されて失敗します。

回避策：NSX-T Data Center ポリシー API を使用して、NSX-T Edge Gateway が接続されている外部ネットワークの再配布設定を更新します。

1. NSX-T Edge Gateway が接続されている外部ネットワークをバッキングする Tier-0 ルーターの ID をメモします。
   - GET 要求を実行して、環境内の Tier-0 ルーターのリストを取得します。
     `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s`
   - リストを調べて、表示名で Tier-0 を特定します。この表示名は、VMware Cloud Director ユーザー インターフェイスの外部ネットワークの全般情報タブに表示される Tier-0 ルーターの名前と一致します。
2. 外部ネットワーク（`Tier-0` ゲートウェイ）を手動で更新します。
   - GET 要求を実行して、ルーター上の `localeServices` のリストを取得します。
     `GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services`
     応答として 1 つのロケール サービスが返されます。
   - `localeService ID` をコピーし、GET 要求を実行して調べます。

     ```
     GET <nsxtmanagerurl>/policy/api/v1/infra/tier-0s/<TIER-0 ID>/locale-services/<LocaleServiceId>.
     ```

     応答では、ロケール サービスのプロパティのリストが返されます。

     ```
     {
       "route_redistribution_config": {
         "bgp_enabled": true,
         "enabled": true,
         "redistribution_rules": [
           {
             "name": "some-name",
             "route_redistribution_types": [
               "TIER1_DNS_FORWARDER_IP",
               "TIER1_NAT",
               "TIER1_STATIC"
             ]
           }
         ]
       },
       ...
     }
     ```

   - 次のように応答を変更します。

     ```
     {
       "route_redistribution_config": null,
       "route_redistribution_types": [
         "TIER1_DNS_FORWARDER_IP",
         "TIER1_NAT",
     ```

```
    "TIER1_STATIC"
  ],
  ...
}
```

  - 変更されたプロパティを使用して PUT 要求を実行し、Tier-0 ルーターの `localeService` を更新します。

- **New: ターゲット ストレージ コンテナがデータストア クラスタである場合、別のクラスタに仮想マシンを再配置すると失敗する**
  ターゲット ストレージ コンテナがデータストア クラスタである場合に、仮想マシンを別のクラスタに再配置する操作を実行すると、`NO_FEASIBLE_PLACEMENT_SOLUTION` エラーが発生して移行は失敗します。VMware Cloud Director のログに `invalidProperty = spec.host` という Storage DRS 起動エラーが記録されます。

  回避策:

  1.vSphere Client を使用してターゲット データストア クラスタで Storage DRS を無効にするか、VMware Cloud Director API を使用して再配置先のストレージをデータストアに変更します。

  2.失敗した操作を再試行します。

- **NEW: 初回ログイン時に root パスワードを期限切れにする設定を有効にすると、VMware Cloud Director アプライアンスのデプロイに失敗する**
  [初回ログイン時に root パスワードを期限切れにする] 設定が有効なアプライアンスをデプロイすると、デプロイは失敗し、`/opt/vmware/var/log/firstboot` ログ ファイルに次のエラーが記録されます。

  ```
  [ERROR] postgresauth script failed to execute.
  ```

  回避策: **[初回ログイン時に root パスワードを期限切れにする]** 設定を無効にし、8 文字以上で、1 つ以上の大文字、1 つ以上の小文字、1 つ以上の数字、1 つ以上の特殊文字を含む初期 root パスワードを指定します。

- **NEW: 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」というメッセージが表示されることがある**
  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 を変更できます。

  回避策: なし。

- **NEW: 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 共有に空きがない、または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が誤動作する可能性があります。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。
- **NEW: 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いるときに、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 が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。
- **NEW: vCenter Server バージョン 6.5 以前で名前付きディスクを暗号化すると、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。

- **NEW: VMware Cloud Director バージョン 10.0 と 10.1 のマルチサイト混在環境で vCenter Server および NSX の接続に対する証明書の信頼が、ローカル サイトのオブジェクトに対してのみ機能する**
  VMware Cloud Director バージョン 10.0 と 10.1 を含むマルチサイト環境が互いに関連付けられている場合、いずれかのサイトにログインすると、他方のサイトで vCenter Server または NSX Manager インスタンスを登録できません。

回避策：vCenter Server または NSX Manager インスタンスを登録するサイトにログインし、登録プロセスを開始します。

- **NEW：VMware Cloud Director テナント ポータルで、[アプリケーション] タブの仮想マシンの詳細なフィルタリング オプションからデータセンター別に仮想マシンをフィルタリングできない**

  VMware Cloud Director テナント ポータルで、上部のナビゲーション バーの [アプリケーション] タブの下にある仮想マシンに移動し、[詳細フィルタ] オプションからデータセンター別に仮想マシンをフィルタリングすると、以下のようなエラーが表示されます：不正な要求: 不明なプロパティ名 `vdcName` です。

  回避策：上部のナビゲーションバーで、**[データセンター]** を選択し、内部の仮想マシンを表示するデータセンターを選択します。

- **NEW：拡張機能サービスで VMware Cloud Director からの RabbitMQ メッセージが処理されない**

  RabbitMQ に依存する拡張機能サービスでは、ヘッダーに新しい一時的な名前があるため、メッセージからヘッダー `notification.type` を取得できません。VMware Cloud Director 10.1.0 のヘッダー名は `notification.operationType` です。

  回避策：拡張機能サービスで VMware Cloud Director からの RabbitMQ メッセージを処理しており、`notification.type` ヘッダーを使用している場合は、変更する必要があります。notification.type ヘッダーを使用できない場合、拡張機能サービスはヘッダー `notification.operationType` から値を取得する必要があります。この変更は、バージョン 10.1.0 の場合にのみ必要です。

- **VMware Cloud Director Service Provider Admin Portal で、組織仮想データセンターの削除がエラーで失敗する**

  VMware Cloud Director Service Provider Admin Portal で、組織 VDC に Edge ゲートウェイを追加し、ゲートウェイでの VMware Cloud Director 分散ルーティングを有効にしている場合、組織 VDC の削除を試行すると、「組織 VDC ネットワークを削除できません」というエラーメッセージが表示されて失敗します。

  回避策:

  1. API を使用して、組織 VDC に関連付けられている組織 VDC ネットワークと Edge ゲートウェイを削除します。
  2. API を使用して、組織 VDC を削除します。

- **レガシー API ログイン エンドポイントへのプロバイダ アクセスを無効にすると、vCloud Usage Meter や vCloud Availability for VMware Cloud Director など、システム管理者のログインを利**

用するすべての API 統合が機能を停止する

vCloud Director 10.0 以降では、サービス プロバイダおよびテナントから VMware Cloud Director へのアクセスに個別の VMware Cloud Director OpenAPI ログイン エンドポイントを使用できます。サービス プロバイダからレガシー `/api/sessions` エンドポイントへのアクセスが無効になっている場合は、vCloud Usage Meter や vCloud Availability for VMware Cloud Director など、VMware Cloud Director と統合された製品が機能を停止します。これらの製品を引き続き動作させるには、パッチを適用する必要があります。

この問題は、システム管理者にのみ影響します。テナント ログインは影響を受けません。

回避策：セル管理ツールを使用して、サービス プロバイダからレガシー `/api/sessions` エンドポイントへのアクセスを再度有効にします。

- **VDC の予約保証値を変更すると、再起動しても、既存の仮想マシンが適切に更新されない**

  システムのデフォルト ポリシーが設定された Flex 組織 VDC があり、この VDC 上のパワーオン状態の仮想マシンにデフォルトのサイジング ポリシーが設定されている場合に、VDC のリソース保証値を大きくすると、既存の仮想マシンのリソース予約は更新されず、非準拠とマークされることもありません。この問題は、レガシー VDC 割り当てモデルを Flex 割り当てモデルに変換したことで既存の仮想マシンが Flex 組織 VDC の新しいデフォルト ポリシーに準拠しなくなった場合にも発生します。

  回避策:

  1. 仮想マシン識別子を見つけるには、VMware Cloud Director テナント ポータルで仮想マシンの [詳細] 画面に移動します。URL に識別子が表示されます。
     `https://Cloud_Director_IP_address_or_host_name/tenant/.../vm-Identifier/general`
  2. VMware Cloud Director ユーザー インターフェイスに非準拠の仮想マシンを表示するには、VMware Cloud Director API を使用して、仮想マシンに対する明示的なコンプライアンス チェックを実行します。
     `POST: https://VCD_IP_Address/api/vApp/vm-Identifier/action/checkComputePolicyCompliance`
  3. ポリシーを再適用してリソース予約を再構成するには、VMware Cloud Director テナント ポータルで、非準拠仮想マシンに対して **[仮想マシンを準拠させる]** をクリックします。
- **VMware Cloud Director に、専用 vCenter Server インスタンス内の実行中の仮想マシン数と仮想マシンの総数、および CPU とメモリの統計情報が正しく表示されない**

  専用 vCenter Server インスタンスがバージョン 6.0 Update 3i 以前、6.5 Update 2 以前、または 6.7 Update 1 以前の場合は、VMware Cloud Director に、vCenter Server インスタンス内の実行中の仮想マシン数、仮想マシンの総数、および CPU とメモリの統計情報に関する情報が正しく表示されません。vSphere 環境に仮想マシンが置かれている場合でも、テナント ポータルの専用 vCenter Server のタイルと、Service Provider Admin Portal の専用 vCenter Server の情報に、実行中の仮想マシンと仮想マシンの総数が両方ともゼロと表示されます。

回避策：vCenter Server インスタンスをバージョン 6.0 Update 3j、6.5 Update 3、6.7 Update 2 以降にアップグレードします。

- **パワーオン状態にある仮想マシンのコンピューティング ポリシーを変更すると失敗することがある**
  パワーオン状態にある仮想マシンのコンピューティング ポリシーを変更する際に、仮想マシン グループまたは論理仮想マシン グループが含まれるプロバイダ VDC コンピューティング ポリシーに新しいコンピューティング ポリシーが関連付けられていると、エラーが発生します。次のエラー メッセージが表示されます。基盤システムのエラー: `com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`。

  回避策：仮想マシンをパワーオフしてから、操作をやり直してください。

- **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の 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。

- **VMware Cloud Director 10.1 では、vRealize Orchestrator ワークフローの入力パラメータのリストのみがサポートされる**
  VMware Cloud Director 10.1 では、以下の vRealize Orchestrator ワークフローの入力パラメータがサポートされます。

  - `boolean`
  - `sdkObject`
  - `secureString`
  - `number`
  - `mimeAttachment`
  - `properties`
  - `date`
  - `composite`
  - `regex`
  - `encryptedString`
  - `array`

  回避策：なし

- **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。

- **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。