VMware Cloud Director 10.2 リリース ノート

VMware Cloud Director 10.2 | 2020 年 10 月 15 日 | ビルド 17029810（インストールされているビルド 17008054）

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

VMware Cloud Director バージョン 10.2 には次の新機能が含まれています。

- **NSX-T Advanced と同等な機能：** NSX Advanced Load Balancer (Avi)、分散ファイアウォール、VRF-Lite、クロス VDC ネットワーク、IPv6、同じネットワーク上のデュアル スタック (IPv4/IPv6)、SLAAC、DHCPv6、CVDS (vSphere 7.0/NSX-T 3.0)、L2VPN（API のみ）
- **Tanzu ランタイム vSphere with Kubernetes を使用して、VMware Cloud Director で最新のアプリケーションをサポート：**Kubernetes クラスタを管理および使用するためのプロバイダおよびテナント ユーザー インターフェイス
- **VMware Cloud Director 仮想アプライアンスの機能強化：**初期導入時のユーザー入力の検証、スタンバイ セルを効率的に作成することで、セルのリストアを簡素化
- **ストレージの機能強化：**プロバイダおよびテナントのディスク レベルの IOPS 制御、共有ディスク
- **セキュリティの機能強化：**「セキュリティ」セクションを参照してください
- **ユーザー インターフェイスの機能強化：**簡易検索、アドバイザリ、証明書の管理
- **プラットフォームの拡張性の機能強化**
- **スケールの機能強化：**『VMware Configuration Maximums』を参照してください

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、「What's New in VMware Cloud Director 10.2」を参照してください。

VMware Cloud Director アドオン ソリューションの最新のリリース ノートについては、次のリンクを参照してください。

- Container Service Extension 3.0
- Object Storage Extension 2.0
- App Launchpad 2.0
- Terraform

- Tenant App 2.5

セキュリティ

VMware Cloud Director 10.2 仮想アプライアンスには、この Photon Security Advisory までアップデートされた Photon OS が付属しています。

VMware Cloud Director 10.2 は、PKCS12 キーストアをサポートしています。PKCS12 形式のキーストアは、VMware Cloud Director のネットワーク接続とデータベース接続を構成するとき、またはセル管理ツールを使用して証明書を生成または置換するときに使用できます。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。

製品サポートに関する注意事項

TKG クラスタ ノードは隔離されています。ただし、TKG クラスタによって公開されるサービスは、サービス仮想 IP アドレスまたはエンドポイントへのネットワーク アクセス権を持つすべてのユーザーがアクセス可能で、サービス独自の認証および承認メカニズムによって保護されています。 認証はワークロードへのアクセスをセキュリティで保護する唯一の方法であるため、入力方向サービスでは TLS などの暗号化されたトラフィックのみを許可することを強く推奨します。

販売終了およびサポート終了に関する警告

- VMware Cloud Director API バージョン 29 以前はサポートされていません。
- VMware Cloud Director API バージョン 30 および 31 は廃止されました。
- VMware Cloud Director API バージョン 30 は次のリリースで使用できなくなります。
- `/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 以降で廃止され、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 プロトコルと HTTPS プロトコルの両方で廃止されています。`/cloud/server_status` は、以降の VMware Cloud Director リリースで削除される予定です。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 `/amqp/action/resetAmqpCertificate` および `/amqp/action/resetAmqpKeyStore` は、VMware Cloud Director 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 35.0 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 `/amqp/action/updateAmqpCertificate` および `/amqp/action/updateLdapKeyStore` は廃止されています。これらのアクションは、以降の VMware Cloud Director リリースで削除される予定です。AMQP 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を使用できます。
- 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 以降で削

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、以降のリリースではサポート対象外のため、廃止になります。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。次の 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。

以前のリリースからのアップグレード

VMware Cloud Director 10.2 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 10.2 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 Ports and Protocols」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
- NSX Advanced Load Balancer (Avi) - 現在、Cloud Director のこのリリースでは、NSX Advanced Load Balancer (Avi) バージョン 20.1.1 のみがサポートされています

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 7
- CentOS 8
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8

VMware Cloud Director アプライアンスのデプロイ

VMware OVF Tool を使用して VMware Cloud Director アプライアンス 10.2 を OVF テンプレートとしてデプロイする場合は、バージョン 10.2 に新しく追加された、次のパラメータを含める必要があります。 `--X:enableHiddenProperties`このパ

ラメータを含めない場合は、「`Property vcloudapp.nfs_mount.VMware_vCloud_Director` はユーザーが構成することはできません。」というエラーが発生して、VMware OVF Tool は失敗します。
「VMware OVF Tool を使用した VMware Cloud Director アプライアンスのデプロイ」を参照してください。

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 3.8.x 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 は、Apache Cassandra バージョン 3.11.*x* をサポートします。

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

備考： Internet Explorer 11 は VMware Cloud Director 10.2 以降ではサポートされていません。Microsoft Edge またはサポートされている別のブラウザを使用できます。Internet Explorer 11 を使用する必要がある場合は、別のブラウザを使用でき

るようになるまで、VMware Cloud Director バージョン 10.0.x または 10.1.x を使用することを検討してください。

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

- **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、次のエラーが発生して失敗します。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。

- **クラスタ間で仮想マシンを移動すると、ターゲット ストレージ コンテナがデータストア クラスタの場合は失敗する**
  クラスタ間で仮想マシンを移動すると、ターゲット ストレージ コンテナがデータストア クラスタの場合は失敗します。ログに次のエラーが記録されます。

  ```
  2020-05-18 15:51:12,083 | ERROR | task-service-activity-pool-23 | SdrsPlacementManagerImpl | SDRS invocation error | requestId=eaa593e5-e051-4423-ac02-97ad09a39f4c,request=POST https://bos1-vcd-sp-static-203-38.eng.vmware.com/api/vApp/vm-c2b0ee1f-02f1-4377-8852-a9711c2a571e/action/reconfigureVm,requestTime=1589817067877,remoteAddress=10.150.203.38:32049,userAgent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 ...,accept=application/*+xml;version 3 4.0 vcd=6e36bc7a-3850-4f2a-a057-d96758ef5fbe,task=1e8217b8-88f1-41f8-8292-1bb6178b0b3e activity=(com.vmware.vcloud.backendbase.management.system.TaskActivity,urn:uuid:1e8217b8-88f1-41f8-8292-1bb6178b0b3e) (vmodl.fault.InvalidArgument) { faultCause = null, faultMessage = null, invalidProperty = spec.host }
  ```

- **「初回ログイン時に root パスワードを期限切れにする」設定を有効にしている場合、アプライアンスをデプロイできない**
  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` ログに次のエラーが記録されます。
  ```
  Invoking postgresauth script ... sudo: Account or password is expired, reset your password and try again Changing password for root. sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper sudo: unable to change expired password: Authentication token manipulation error cp: cannot stat '/var/vmware/vpostgres/current/.ssh/id_rsa': No such file or directory chown: cannot access '/opt/vmware/vcloud-director/id_rsa': No such file or directory [ERROR] postgresauth script failed to execute.
  ```

- **VMware Cloud Director テナント ポータルで、仮想マシンに、仮想データセンター (VDC) の場所に基づいた高度なフィルタリングを適用すると機能しない**
  VMware Cloud Director テナント ポータルのユーザー インターフェイスで、VDC の場所に基づく高度なフィルタリングを使用して仮想マシンをフィルタリングすると、エラーが発生して検索は失敗します。

既知の問題

- **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：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：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：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：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、バッキングしている 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。

- **New：ストレージ ポッドまたはクラスタでストレージ ポリシーをバッキングしていると、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 ポリシーをバッキングしている場合に、**[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。

  回避策：この問題を回避するには、管理者レベルのアクセス権が必要です。

  1. vCenter Server で、IOPS を有効にするすべてのストレージ ポッドからストレージ ポリシー タグを削除して、ストレージ ポリシーを更新します。
  2. VMware Cloud Director で **[影響のある配置]** をオフにして、ストレージ ポリシーで VMware Cloud Director の IOPS を有効にします。
  3. vCenter Server で、タグをストレージ ポッドに再接続し、ストレージ ポリシーを更新します。
- **New：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。**
  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。

  回避策：なし。

- **New：スタンドアローン仮想マシンの NIC 設定を編集できない**
  スタンドアロン仮想マシンの NIC 設定を更新することはできません。[編集] をクリックして仮想マシンの NIC 設定を開くと、[設定] 画面は開きますが、応答しなくなります。

  回避策：
  1.スタンドアロン仮想マシンを vApp に変換します。
  2.vApp の NIC 設定を編集します。
  3.vApp をスタンドアロン仮想マシンに再度変換します。

- **New：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 権限がありません」エラーが発生して失敗します。この問題は、カタログの設定を更新すると、既存のパスワードが削除され、null に設定されるために発生します。

  回避策：カタログの **[公開設定]** を更新し、テナント ポータルのユーザー インターフェイスからパスワードを再設定します。

- **New：VMware Cloud Director をバージョン 10.1.2 からバージョン 10.2 にアップグレードすると、不正確なエラーが報告される**
  VMware Cloud Director をバージョン 10.1.2 からバージョン 10.2 にアップグレードすると、次のような不正確なエラー 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 のバージョン 10.1.2 から 10.2 へのアップグレードはサポートされているため、エラー メッセージは無視する必要があります。

回避策：このエラーは無視してください。

- **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。

  回避策：

  1. `systemctl reset-failed vmware-vcd.service` を実行します。
  2. `systemctl start vmware-vcd.service` を実行します。
- **組織内にサブスクライブ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、組織内にサブスクライブ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 に、vCenter Server をバージョン 7.0.0d 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キング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：Kubernetes エンドポイント証明書を手動で信頼します。詳細な手順については、https://kb.vmware.com/s/article/80996 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 プラグインを手動で無効にします。

- **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。

  回避策：プロバイダ VDC が 1 つのスーパーバイザー クラスタによってバッキングされ、そのクラスタがプライマリ クラスタであることを確認します。プロバイダ VDC は、ホスト クラスタとスーパーバイザー クラスタによってバッキングできますが、スーパーバイザー クラスタはプライマリである必要があります。

- **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。

- **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。

  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。

- **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。

  回避策：グリッドのいずれかの列のサイズを変更します。

- **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 を使用している場合に、アドバイザリに優先順位フィルタを適用すると、エラーが発生して失敗します。

  ```
  "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。

- **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、優先順位が降順で並べ替えら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。

- **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。

- **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。

- **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。

- **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。

- **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 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。

- **vCloud Director 10.0 からアップグレードした後、ゲスト OS のカスタマイズと IPv6 接続が有効になっている Linux テンプレートから新しくデプロイした仮想マシンで、ネットワーク接続の問題が発生する**
  vCloud Director 10.0 からアップグレードした後、バージョン 10.0 で作成した Linux 仮想マシン テンプレートを使用して新しい仮想マシンをデプロイし、ゲスト OS のカスタマイズと IPv6 接続を有効にすると、デプロイされた仮想マシンでネットワーク接続の問題が発生します。この問題は、デプロイ プロセスによって仮想マシンの `/etc/hosts` ファイルに `VM_DOMAIN_NAME` パラメータと `VM_HOST_NAME` パラメータのエントリが重複して作成されるため、発生することがあります。

  回避策：仮想マシンの `/etc/hosts` ファイルから、`VM_DOMAIN_NAME` と `VM_HOST_NAME` の重複するエントリを削除します。

- **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。