

VMware Cloud Director 10.2.2.3 リリース ノート

VMware Cloud Director 10.2.2.3

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

ヴィ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

Copyright © 2023 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

- 1 概要 4
- 2 新機能 5
- 3 システム要件とインストール 6
- 4 ドキュメント 7
- 5 VMware Cloud Director 10.2.x の以前のリリース 8
- 6 既知の問題 9

概要

1

VMware Cloud Director 10.2.2.3 | 2022 年 4 月 14 日 | ビルド 19585218 (インストールされているビルド 19580548)
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。

新機能

2

VMware Cloud Director 10.2.2.3 パッチ リリースでは、CVE-2022-22966 が解決されています。詳細については、<https://www.vmware.com/security/advisories> を参照してください。

システム要件とインストール

3

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。

ドキュメント

4

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

5

[VMware Cloud Director 10.2.2.2 リリース ノート](#)

[VMware Cloud Director 10.2.2.1a リリース ノート](#)

[VMware Cloud Director 10.2.2.1 リリース ノート](#)

[VMware Cloud Director 10.2.2 リリース ノート](#)

[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](#)

- **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。

- **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。

- **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 :

- a 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。
- b 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。
- c 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。

- **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 間の統合が機能しくなくなります。VMware Cloud Director のユーザー インターフェイスでは「**Invalid VRO request params**」というエラーが返ります。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.ja
va:238) at com.vmware.vim.install.impl.RegistrationProviderImpl.
(RegistrationProviderImpl.java:56) at
com.vmware.vim.install.RegistrationProviderFactory.getRegistrationProvider(Registra
tionProviderFactory.java:143) at
com.vmware.vcloud.vro.client.connection.STSClient.getRegistrationProvider(STSClient
.java:126) ... 136 more

```

回避策：なし。

- **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。

- **FIPS モードを使用時に、OpenSSL で生成された PKCS8 ファイルのアップロードがエラーで失敗する**

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、「Bad request: org.bouncycastle.pkcs.PKCSException: unable to read encrypted data: ... not available: No such algorithm: ...」エラーまたは「salt must be at least 128 bits」エラーでアップロードが失敗します。

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atalog 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。プラグインを無効にする方法については、「[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。Name must start with a letter and only contain alphanumeric or hyphen (-) characters. (Max 128 characters)。

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して表示されます。

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。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。

- **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、VMware Cloud Director 10.2.x サイトにログインするか、vCenter Server インスタンスを VMware Cloud Director 10.2.x サイトに登録しても、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、「Named disk encryption is not supported in this version of vCenter Server.」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。詳細については、[「https://support.mozilla.org/ja-JP/」](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することはできません。"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 10.2.x にアップグレードした後、Cassandra から SSL 証明書をインポートすると、cell-management-tool がエラー メッセージを表示して失敗する**

cell-management-tool を使用して Cassandra から SSL をインポートすると、操作が失敗して次のエラーメッセージが表示されます。

```
Unable to load VCD's SSL context.
```

回避策：VMware Cloud Director Service Provider Admin Portal を使用して Cassandra から SSL をインポートします。詳細については、「[信頼された証明書のインポート](#)」を参照してください。

- **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い場合は、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。