Alibaba Cloud
CSK 容器服#Kubernetes版

お知らせ

Document Version20191114

目次

1 脆弱性の修正：kubectl cp に関連する CVE-2019-11249

数か月前、**kubectl cp** に関連する脆弱性 **CVE-2019-11246** が公開されました。 **Kubernetes** は、**kubectl cp** に関連する新たな脆弱性 **CVE-2019-11249** を発表しました。 この脆弱性により、攻撃者は **kubectl cp** コマンドを実行することでディレクトリトラバーサルが可能になり、**TAR** パッケージに保存された悪意あるファイルを、ホスト上の任意のパスに書き込むことができます。 このプロセスは、ユーザーのシステム権限によってのみ制限されます。 **kubectl** クライアントのバージョンを安全なバージョンにアップグレードすることを推奨します。 脆弱性 **CVE-2019-11249** の詳細は、「*#unique_2*」をご参照ください。

2 Container Service Swarm のサポート終了について

Alibaba Cloud は **2019** 年 **12** 月 **31** 日で、**Container Service Swarm** の技術サポートを終了します。 ただし、**Container Service Kubernetes** は引き続きご使用いただけるため、安定した信頼性の高いエンタープライズクラスのサービスをご利用できます。 次の情報に従って、事前にアプリケーションを移行することを推奨します。

1. **2019** 年 **7** 月 **1** 日から、**Container Service** コンソールで **Swarm** クラスターを作成できません。 特別な要件がある場合は、チケットを起票し、サポートセンターへお問い合わせください
2. **2019** 年 **12** 月 **31** 日から、**Swarm** クラスターに関連するコンソール機能とドキュメントがオフラインになります。 **API** アクションを呼び出すことで、既存の **Swarm** クラスターを管理できます。

Swarm クラスターから **Kubernetes** クラスターにアプリケーションを移行する方法については、「移行ソリューションの概要」をご参照ください。

3 Cloud Controller Manager のアップグレード

v1.9.3.105-gfd4e547-aliyun

- アノテーション設定が有効にならなかったバグを修正しました。
- **SLB** コンソールに **SLB** インスタンスの名前を変更できる機能を追加しました。 **Cloud Controller Manager (CCM) V1.9.3.10** 以前を使用して作成された **SLB** インスタンスの名前を変更する場合は、まずマネージャにタグを追加する必要があります。 詳しくは、「*#unique_5*」をご参照ください。

Container Service コンソールを使用して、 **Cloud Controller Manager** を最新バージョンにアップグレードすることを推奨します。

4 ACK セキュリティポリシーのアップグレードに関する通知

2019 年 **4** 月 **17** 日より、**Kubernetes** クラスターへのアクセスに必要な権限を管理するための **ACK** のセキュリティポリシーがアップグレードされました。 このリリース以降、アップグレードされたセキュリティポリシーでは、必要な権限を付与されていない **RAM** ユーザーによって実行されるクラスターのアクセスを拒否します。 つまり、**RAM** ユーザーは、必要なアクセス権限が付与されている **Kubernetes** クラスターにのみアクセスできます。

対応するクラスターにアクセスするには、管理下にあるすべての **RAM** ユーザーに、必要な **RAM** 権限を付与する必要があります。 詳細は、「*#unique_7*」 をご参照ください。

5 脆弱性修正: CVE-2019-1002101

この更新プログラムで修正された脆弱性では、ファイルとディレクトリをコンテナーとの間でコピーするために使用される `kubectl cp` コマンドを通して不具合が発生しました。 具体的には、この脆弱性により、攻撃者は、シンボリックリンクヘッダーを含む悪意のある **tar** パッケージを、イメージまたは実行中のコンテナーに埋め込むことが可能になります。 **tar** パッケージが抽出されるプロセス中に、シンボリックリンクヘッダーと同じ名前を共有するディレクトリに格納されているファイルが変更または監視されます。

この脆弱性は、**kubectl V1.11.9**、**V1.12.7**、**V1.13.5**、および **V1.14.0** で修正されました。 **kubectl** のこれらのバージョンのいずれかを使用する必要があります。 詳しくは、「*kubectl のインストールと設定*」をご参照ください。

6 マルチゾーン Kubernetes クラスターへのディスクのマウントに失敗するバグを修正

- **2019** 年 **1** 月 **28** 日以降に作成されたマルチゾーン **Kubernetes** クラスターは、このバグの影響を受けません。
- **2019** 年 **1** 月 **28** 日より前に作成されたマルチゾーン **Kubernetes** クラスターの場合、**ACK** はこのバグの解決策を提供しており、ディスクをクラスターにマウントできます。 詳細は、「*#unique_10*」 をご参照ください。

7 サーバーレス Kubernetes クラスターをサポートする ECI インスタンスの課金に関するお知らせ

2019 年 1 月 22 日以降、サーバーレス Kubernetes クラスターのサポートに使用される ECI インスタンスには料金が発生します。 詳細は、「*#unique_12*」 をご参照ください。

8 脆弱性修正:Kubernetes ダッシュボードの脆弱性 CVE-2018-18264

この修正された脆弱性は、**V1.10** 以前の **Kubernetes** ダッシュボードで発見されました。 この脆弱性により、攻撃者が **ID** 認証をバイパスすることができ、ダッシュボードのログインアカウントを使用して、クラスター内のシークレットを読み取ることができました。 詳細については、「*CVE-2018-18264* の脆弱性の修正」をご参照ください。