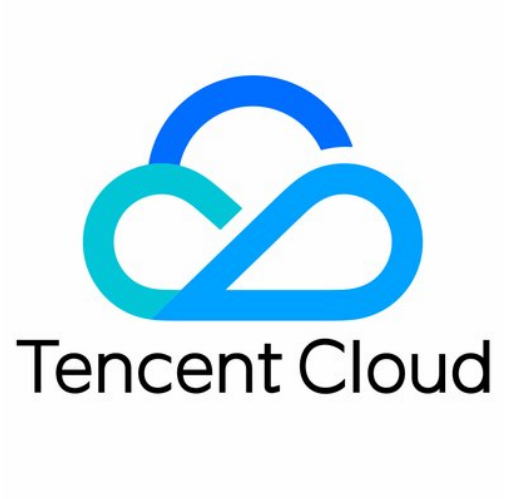
Tencent Kubernetes Engine

購入ガイド

製品ドキュメント



カタログ：

購入ガイド
コンテナクラスターの購入
TKE課金概要

最終更新日：：2022-03-31 15:04:01

課金項目

コンテナーサービスTKEを使用する時、製品の使用料金はクラスター管理料金とクラウド製品リソース料金から構成されます。

クラスター管理料金

> 注意：
> クラスター管理料金の正式な請求時間については、Tencent CloudのTKEが2022年3月21日10:00（北京時間）よりホスティングクラスター使用料金の請求を開始についてのお知らせをご参照ください。

クラスター管理料金**ホスティングクラスターのみに対して請求**。TKEによるホスティングクラスターは、高可用性・高性能・高拡張性・高安定性のフルホスティングパネルを提供し、 クラスターの構築や拡張などの操作を簡素化します。これにより、クラスターの管理やメンテナンスに手をかけず、コンテナー化したアプリケーションの開発に集中できるようになります。そのため、異なる構成のホスティングクラスターに対して、TKEはそれなりのクラスター管理料金を請求します。料金の詳細については、クラスター管理料金をご参照ください。

クラウド製品リソース料金

TKEの使用中に作成したほかのクラウド製品リソース（CVM、CBS、CLBなど）に対して、対応するクラウド製品の課金方式に従って料金を請求します。料金の詳細については、クラウド製品リソース料金をご参照ください。

クラスター管理料金(id:cluster)

課金モデル

TKEの課金方式は主に従量制課金（後払い）を採用します。

課金項目	課金モデル	支払方式	課金単位

課金項目	課金モデル	支払方式	課金単位
クラスター （個）	従量制課金	購入時 料金凍結、時間単位で請求	ドル/時間

製品価格

説明：

- ノードはKubnernetss Nodeを指し、CVMノード、BMノード、サードパーティノード、仮想ノードなどが含まれます。
- アイドル状態のクラスターに対して、クラスター管理料金を請求しません。

最大管理ノード数	価格 （ドル/時間）
5	0.02040816
20	0.06279435
50	0.11459969
100	0.19152276
200	0.40031397
500	0.8021978
1000	1.47252747
3000	2.44897959
5000	4.40188383

クラウド製品リソース料金

TKEの使用中に作成したほかのクラウド製品リソース（CVM、CBS、CLBなど）に対して、対応するクラウド製品の課金方式に従って料金を請求します。料金の詳細については、各製品の課金説明をご参照ください。

クラウド製品	課金説明
クラウドサーバー CVM	CVM課金モデル

クラウド製品	課金説明
クラウドディスク CBS	CBS価格一覧
ロードバランサー CLB	CLB課金説明

注意：
TKEはKubernetesベースの宣言式サービスです。TKEが作成したロードバランサーCLBやクラウドディスクCBSなどのIaaSサービスリソースを必要としなくなる場合、具体的なサービスリソース画面から削除するのではなく、TKEコンソールから該当するサービスリソースを削除してください。そうしない場合、TKEは削除されたサービスリソースを再作成し、関連の料金が請求されます。例えば、TKEにロードバランサーCLBサービスリソースがすでに作成されているとします。ロードバランサーコンソールからこのCLBインスタンスを削除すると、TKEは宣言式APIにより新しいCLBインスタンスを作成します。

購入説明

最終更新日：：2022-03-31 15:04:01

ご購入時の注意事項

説明：
ご購入時の注意事項に従わないためにサービスが利用できない場合、対応するサービス利用不可時間は、サービス利用不可時間として計上されません。詳しくは、TKEサービスレベル利用規約。

クラスターをご購入時に、クラスターパネルコンポネントの高負荷によるクラスター利用不可を回避するために、以下の推奨スペックを参考にして、業務に応じて適切なクラスター構成を選択してください。
例えば、1つのクラスターに50ノードをデプロイするが、Podを2000もデプロイする場合、最大管理ノードが50ではなく、100のクラスター構成を選択すべきです。

注意：PodにはNamespace配下のすべての状態のPodが含まれ、システムコンポーネント関連のPod（cni-agentなど）が含まれません。

最大管理ノード数	最大Pod数（推奨）	最大ConfigMap数（推奨）	最大CRD 数（推奨）
5	150	32	150
20	600	64	600
50	1500	128	1250
100	3000	256	2500
200	6000	512	5000
500	15000	1024	10000
1000	30000	2048	20000
3000	90000	4096	50000
5000	150000	6144	100000

リージョンとアベイラビリティーゾーン

最終更新日：：2022-03-31 15:04:01

リージョン

概要

リージョン（Region）とは、データセンターの物理的な場所です。Tencent Cloudでは、リージョンとリージョンの間は完全に分離されており、異なるリージョン間で最大限の安定性とフォールトトレランスが確保されます。アクセスの遅延を低減し、ダウンロード速度を向上させるためには、顧客に最も近いリージョンを選定することをお勧めします。

次の表を表示するか、またはDescribeRegions APIを使用して、リージョンの完全なリストを表示できます。

特徴

- 異なるリージョン間のネットワークは完全に分離されており、異なるリージョン間のクラウド製品は、**デフォルトではプライベートネットワークを介して通信できません**。
  異なるリージョン間のクラウド製品は、パブリックネットワークIPでInternetにアクセスすることで通信できます。異なるプライベートネットワーク内のクラウド製品は、より高速で安定したCloud Connect Networkを介して通信できます。
- Cloud Load Balancerは現在、デフォルトでは、同一リージョン内のトラフィック転送をサポートします。リージョン間のバインディング機能をアクティブにすると、Cloud Load BalancerとCVMのクロスリージョンバインディングがサポートされます。

アベイラビリティーゾーン

概要

アベイラビリティーゾーンとは、Tencent Cloudが同一リージョン内で電源とネットワークが互いに独立している物理的なデータセンターです。ビジネスの持続性を確保し、アベイラビリティーゾーン間の障害を互いに隔離させ（大規模な災害または大規模な電源設備の障害を除く）、障害が広がらないようにすることを目的としています。独立したアベイラビリティーゾーンでインスタンスを起動することにより、ユーザーは単一障害点からアプリケーションを保護できます。
APIインターフェースを介して、アベイラビリティーゾーンの完全なリストを表示できます。

特徴

同じVPC内のクラウド製品は、プライベートネットワークを介して相互接続されているため、異なるアベイラビリティーゾーンにある場合でも、プライベートIPアドレスを直接使用してアクセスすることができます。

> 説明：
> プライベートネットワークの相互接続とは、同じアカウントでのリソースの相互接続を指します。異なるアカウントのリソースは、プライベートネットワークから完全に分離されています。

中国

リージョン	アベイラビリティーゾーン
華南地区（広州） ap-guangzhou	広州3区 ap-guangzhou-3
	広州4区 ap-guangzhou-4
	広州6区 ap-guangzhou-6
華東地区（上海） ap-shanghai	上海2区 ap-shanghai-2
	上海3区 ap-shanghai-3
	上海4区 ap-shanghai-4
	上海5区 ap-shanghai-5
華東地区（南京） ap-nanjing	南京1区 ap-nanjing-1
	南京2区 ap-nanjing-2
華北地区（北京） ap-beijing	北京3区 ap-beijing-3

	北京4区 ap-beijing-4
	北京5区 ap-beijing-5
	北京6区 ap-beijing-6
	北京7区 ap-beijing-7
西南地区（成都） ap-chengdu	成都1区 ap-chengdu-1
	成都2区 ap-chengdu-2
香港・マカオ・台湾リージョン（中国香港） ap-hongkong	香港2区（中国香港のノードは香港・マカオ・台湾地域をカバーできる） ap-hongkong-2

その他の国及び地域

リージョン	アベイラビリティーゾーン
東南アジア（シンガポール） ap-singapore	シンガポール1区（シンガポールのノードは東南アジア地域をカバーできる） ap-singapore-1
	シンガポール2区（シンガポールのノードは東南アジア地域をカバーできる） ap-singapore-2
東南アジア（ジャカルタ） ap-jakarta	ジャカルタ1区（ジャカルタのノードは東南アジア地域をカバーできる） ap-jakarta-1
北東アジア（ソウル） ap-seoul	ソウル1区（ソウルのノードは北東アジア地域をカバーできる） ap-seoul-1
	ソウル2区（ソウルのノードは北東アジア地域をカバーできる） ap-seoul-2
北東アジア（東京） ap-tokyo	東京2区（東京のノードアベイラビリティーゾーンは北東アジア地域をカバーする） ap-tokyo-2
南アジア太平洋（ムンバ	ムンバイ1区（ムンバイのノードは南アジア太平洋地域をカバーできる）

イ） ap-mumbai	ap-mumbai-1
	ムンバイ2区（ムンバイのノードは南アジア太平洋地域をカバーできる） ap-mumbai-2
東南アジア（バンコク） ap-bangkok	バンコク1区（バンコクノードは東南アジアパシフィック地域をカバーできる） ap-bangkok-1
北アメリカ地域（トロント） na-toronto	トロント1区（トロントのノードは北アメリカ地域をカバーできる） na-toronto-1
米国東部（バージニア） na-ashburn	バージニア1区（バージニアのノードは米国東部をカバーできる） na-ashburn-1
	バージニア2区（バージニアのノードは米国東部をカバーできる） na-ashburn-2
欧州地区（フランクフルト） eu-frankfurt	フランクフルト1区（フランクフルトのノードはヨーロッパ地域をカバーできる） eu-frankfurt-1
欧州リージョン（モスクワ） eu-moscow	モスクワ1区（モスクワのノードはヨーロッパ地域をカバーできる） eu-moscow-1

リージョンとアベイラビリティーゾーンを選択する方法

リージョンとアベイラビリティーゾーンを選択する際に、以下の要因を考慮する必要があります。

- CVMインスタンスの所在地、ユーザーおよびターゲットユーザーの地理的な場所。
  アクセス遅延を削減し、アクセス速度を向上させるためには、CVMを購入する際に、ユーザーに最も近いリージョンを選択することをお勧めします。
- CVMと他のクラウド製品との関係。
  他のクラウド製品を選択する場合は、各クラウド製品がプライベートネットワークを介して相互に通信できるように、なるべく同じリージョンと同じアベイラビリティーゾーンに配置することをお勧めします。これにより、アクセス遅延を削減し、アクセス速度を向上させることができます。
- 高可用性とフォールトトレランス。
  VPCが1つしかない場合でも、単一障害点が生じることを回避して、災害復旧を実現するために、ビジネスを異なるアベイラビリティーゾーンにデプロイすることをお勧めします。
- 異なるアベイラビリティーゾーン間では、ネットワーク遅延が発生する可能性がありますので、実際のビジネス要件に応じて検討し、高可用性と低遅延の最適なバランスを見つけることをお勧めします。

- 他の国または地域のCVMインスタンスにアクセスする必要がある場合は、他の国または地域のCVMを選択することをお勧めします。中国本土のCVMインスタンスを使用して、他の国や地域のサーバーにアクセスする場合、ネットワーク遅延が大幅に増加する可能性があります。ご利用はお勧めしません。

リソースの可用性

次の表は、グローバル、リージョン、アベイラビリティーゾーンに固有のTencent Cloudリソースを示しています。

```
&lt;table>
<tbody><tr><th>リソース</th><th>リソース ID形式<br>&lt;リソースの略語>-8桁の数字と文字</th><th>タイプ</th><th>説明</th></tr>
</tbody><tbody>
<tr>
<td>ユーザーアカウント</td>
<td>制限なし</td>
<td>グローバルに一意の識別子</td>
<td>ユーザーは同じアカウントを使用して、Tencent Cloudのグローバルリソースにアクセスできます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/213/6092">SSHキー</a> </td>
<td>skey-xxxxxxxx</td>
<td>グローバル</td>
<td>ユーザーはSSHキーを使用して、アカウント下の任意のリージョンのCVMをバインドできます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/213/4939">CVMインスタンス</a> </td>
<td>ins-xxxxxxxx</td>
<td>単一のアベイラビリティーゾーンでのみ利用可能</td>
<td>ユーザーは特定のアベイラビリティーゾーンでのみCVMインスタンスを作成できます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/213/4941">カスタマイズイメージ</a> </td>
<td>img-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>ユーザーはインスタンスのカスタムイメージを作成でき、また、同じリージョン内の異なるアベイラビリティーゾーンで使用できます。他のリージョンで使用する必要がある場合は、イメージのコピー機能を利用して、カスタムイメージを他のリージョンにコピーしてください。</td>
</tr>
<tr>
```

```
<td> <a href="https://intl.cloud.tencent.com/document/product/213/5733">EIP</a>
</td>
<td>eip-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>EIPは、同じリージョン内のインスタンスにのみ関連付けることができます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/213/12452">セキュリティグループ</a> </td>
<td>sg-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>セキュリティグループは、同じリージョン内のインスタンスにのみ関連付けることができます。Tencent Cloudは、ユーザーに3つのデフォルトのセキュリティグループを自動的に作成します。</td>
</tr>
<tr>
<td> <a href="https://cloud.tencent.com/document/product/362">Cloud Block Storage</a> </td>
<td>disk-xxxxxxxx</td>
<td>単一のアベイラビリティーゾーンでのみ利用可能</td>
<td>ユーザーは、特定のアベイラビリティーゾーンでのみCloud Block Storageを作成でき、また、同じアベイラビリティーゾーンのインスタンスにマウントできます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/362/31638">スナップショット</a> </td>
<td>snap-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>特定のCloud Block Storageにスナップショットを作成した後、ユーザーは対象リージョンで作成されたスナップショットを使用して、他の操作（クラウドディスクの作成など）を行うことができます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/214/524">Cloud Load Balancer</a> </td>
<td>clb-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>Cloud Load Balancerは、同じリージョン内の異なるアベイラビリティーゾーンのCVMにバインドして、トラフィックを転送することができます。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/215/535">Virtual Private Cloud</a> </td>
<td>vpc-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>VPCは特定のリージョンに作成され、異なるアベイラビリティーゾーンで同じVPCに属するリソースを作成できます。</td>
</tr>
```

```
<tr><td> <a href="https://intl.cloud.tencent.com/document/product/215/535#.E5.AD.90.E7.BD.91">サブネット</a> </td>
<td>subnet-xxxxxxxx</td>
<td>単一のアベイラビリティーゾーンでのみ利用可能</td>
<td>ユーザーは、異なるアベイラビリティーゾーン間でサブネットを作成することができません。</td>
</tr>
<tr>
<td> <a href="https://intl.cloud.tencent.com/document/product/215/31810">ルートテーブル</a> </td>
<td>rtb-xxxxxxxx</td>
<td>単一リージョンの複数のアベイラビリティーゾーンで利用可能</td>
<td>ユーザーは、ルーティングテーブルを作成するときに特定のVPCを指定する必要があります。</td>
</tr>
</tbody>
```

関連する操作

インスタンスを他のアベイラビリティーゾーンに移行する

すでに起動されたインスタンスは、アベイラビリティーゾーンを変更できませんが、ユーザは他の方法でインスタンスを他のアベイラビリティーゾーンに移行させることができます。元のインスタンスからカスタムイメージを作成し、カスタムイメージを使用して新しいアベイラビリティーゾーンでインスタンスを起動し、新しいインスタンスの設定を更新します。

1. 現在のインスタンスからカスタムイメージを作成します。詳細については、カスタムイメージをご参照ください。
2. 現在のインスタンスの ネットワーク環境 がプライベートネットワークであり、かつ移行後も現在のプライベートIPアドレスを保持する必要がある場合、ユーザーはまず現在のアベイラビリティーゾーンのサブネットを削除し、その後、新しいアベイラビリティーゾーンに元のサブネットと同一のIPアドレスの範囲でサブネットを作成することができます。削除できるのは、使用可能なインスタンスを含まないサブネットのみであることに注意する必要があります。以上より、現在のサブネット内のすべてのインスタンスを新しいサブネットに移動する必要があります。
3. さきほど作成したカスタムイメージを使用して、新しいアベイラビリティーゾーンに新しいインスタンスを作成します。ユーザは、元のインスタンスと同じタイプと設定を選択できるか、新しいインスタンスタイプと設定を選択できます。詳細については、インスタンスの作成をご参照ください。
4. 元のインスタンスがすでにElastic IPアドレスに関連付けられている場合、古いインスタンスとの関連付けを解除してから、新しいインスタンスに関連付ける必要があります。詳細については、EIPをご参照ください。
5. （オプション）元のCVMインスタンスが従量課金タイプの場合、元のインスタンスを終了することができます。詳細については、インスタンスの終了をご参照ください。

イメージを他のリージョンにコピーする

インスタンスの起動や表示などの操作は、リージョン属性があります。起動する必要のあるインスタンスのイメージが対象リージョンに存在しない場合、イメージを対象リージョンにコピーする必要があります。詳細については、イメージのコピーをご参照ください。

クラスター割り当て量購入制限

最終更新日：：2022-03-31 15:04:01

各ユーザーに対して、Tencent CloudのTKEクラスターは地域ごとに固定したクォーターを割り当てています。

TKE クォーター制限

ユーザーごとに購入できるTKEクォーターはデフォルトでは以下となります。より多くのクォーター項目が必要である場合、クォーター申請チケット でクォーターを申請することができます。

> 注意：
> 2019年10月21日より、ユーザークラスターがサポートする5000未満の最大ノードクォーターは、すべて5000に調整されました。

クォーター項目	デフォルト値	参照可能なエントリ	クォーター拡張可否
単一地域配下のクラスター	5	TKE 概要画面の右下側	はい
単一クラスター配下のノード	5000		
単一地域配下のイメージネームスペース	10		
単一地域配下のイメージリポジトリ	500		
単一イメージ配下のイメージバージョン	100		

CVMクォーター制限

Tencent CloudのTKEによって生成されたCVMは、CVMの購入制限にかけられます。詳しくは、CVM購入制約をご参照ください。ユーザーごとに購入できるCVMクォーターはデフォルトでは以下のとおりとなります。より多くのクォーター項目が必要である場合、クォーター申請チケット でクォーターを申請することができます。

クォーター項目	デフォルト値	参照可能なエントリ	クォーター拡張可否
単一利用可能リージョン配下の従量制課金CVM	30台または60台	CVM 概要画面-各地域のリソース	はい

クラスター設定制限

説明：
クラスター設定制限は、クラスターの規模を制限しており、現在変更不可です。

設定項目	アドレス範囲	影響範囲	参照可能なエリート	変更可否
VPC ネットワーク-サブネットワーク	カスタム設定	当該サブネットワークに追加できるノード数	クラスターに対応するVPCサブネットワーク一覧-利用可能なIP数	• 変更不可 • 新規サブネットワーク利用可能
コンテナーのネットワークセグメントCIDR	カスタム設定	• クラスター内部の最大ノード数 • クラスター内部の最大service数 • ノードごとの最大Pod数	クラスター基本情報画面-コンテナーのネットワークセグメント	変更不可

リソース制限の説明

2021年1月13日より、Tencent CloudのTKEシステムは、ノード数（nodeNum）が5以下（0 < nodeNum ≤ 5）、また、ノード数が5より大きいが20未満（5 < nodeNum < 20）のクラスターにおけるネームスペースに自動的に一連のリソースクォーターを適用します。これらのクォーターはリムーブ不可であり、クラスターにデプロイされたアプリケーションの潜在バグからクラスターパネルを保護し、その安定性を確保します。

これらのクォーターを確認する場合、以下のコマンドを実行します。

```
kubectl get resourcequota tke-default-quota -o yaml
```

指定されたネームスペースの `tke-default-quota` オブジェクトを確認する場合、 `--namespace` オプションを使用し、ネームスペースを指定してください。

具体的なクォーター制限は以下の通りです：

クラスター規模	クォーター制限
0 < nodeNum ≤ 5	総数の制限 Pod：4000，configMap：3000，CustomResourceDefinition(CRD)：4000
5 < nodeNum < 20	総数の制限 Pod：8000，configMap：6000，CustomResourceDefinition(CRD)：8000
20 ≤ nodeNum	制限なし

特殊な運用シーンでクォーターを調整する必要がある場合、チケットの提出で申請してください。

コンテナノードハードディスクの設定

最終更新日：：2022-03-31 15:04:01

説明

TKEがクラスターを作成または拡張する時、業務需要に合わせて、コンテナーノードのシステムディスクのタイプとサイズ、データディスクのタイプとサイズを設定し、異なるタイプのディスクを選択することができます。

アドバイス

1.コンテナーのディレクトリがシステムディスクに格納されるため、50Gのシステムディスクを作成することを推奨します。
2.システムディスクに何か要求がある場合、クラスターを初期化する時、dockerのディレクトリをデータディスクに移行することを推奨します。

TKEノードパブリックネットワークIPの説明

最終更新日：：2022-04-07 11:12:42

パブリックネットワークから直接業務セキュリティにアクセスできないが、パブリックネットワークへのアクセスができるようにするという要望がある場合、Tencent CloudのNATゲートウェイをご利用ください。以下でNATゲートウェイを使用してパブリックネットワークにアクセスする方法をご紹介します。

パブリックネットワークIP

デフォルトでは、クラスターを作成する時、クラスターのノードにパブリックネットワークIP
を割り当てます。割り当てられたパブリックネットワークIPは以下の役割を果たします：

- パブリックネットワークIPでクラスターのノードマシンにログインします。
- パブリックネットワークIPでパブリックネットワークサービスにアクセスします。

パブリックネットワーク帯域幅

パブリックネットワークサービスを作成する時、パブリックネットワークロードバランサーが使用するのはノードの帯域幅とトラフィックです。パブリックネットワークサービスを提供する場合、ノードにパブリックネットワーク帯域幅があることを確保する必要があります。業務がパブリックネットワークを必要としなければ、パブリックネットワーク帯域幅を購入しなくても構いません。

NATゲートウェイ

CVMはElastic IPアドレスをバインドしません。Internetにアクセスするすべてのトラフィックは NATゲートウェイ経由で転送されます。このソリューションでは、CVMがInternetにアクセスするトラフィックは、内部ネットワーク経由でNATゲートウェイに転送されるため、CVM購入時のパブリックネットワークの帯域幅に制限されません。また、NATゲートウェイが生じたネットワークトラフィックはCVMのパブリックネットワークのアウトバンドを占有しません。NATゲートウェイ経由でInternetにアクセスするには、以下を実施してください：

ステップ1：NATゲートウェイを作成します

1. VPCコンソールにログインし、左側のナビゲーションバーで【 NAT Gateway】をクリックします。
2. 「NATゲートウェイ」管理画面で、**Create**をクリックします。
3. 表示された「Create an NAT Gateway 」ウィンドウに、以下のパラメータを記入します。

- ゲートウェイ名：カスタム。
- 所属ネットワーク：NATゲートウェイサービスのプライベートネットワークを選択します。
- ゲートウェイタイプ：必要に応じて選択してください。ゲートウェイタイプは作成後にも変更可能です。
- アウトバンド帯域幅上限：必要に応じて選択します。
- Elastic IP：NATゲートウェイにElastic IPを割り当てます。既存Elastic IPを選択するか新規購入してElastic IPを割り当ててください。

4. **Create **をクリックして、NATゲートウェイの作成を完了します。

> 注意：
> NATゲートウェイ作成時にリース料金は1時間凍結されます。

ステップ2：関連サブネットワークが関連付けられたルーティングテーブルを設定します

> 説明：
> NATゲートウェイを作成した後、サブネットのトラフィックをNATゲートウェイに転送するように、VPCコンソールのルーティングテーブル画面でルーティングルールを設定する必要があります。

1. 左側のナビゲーションバーで【Route Table】をクリックします。
2. ルーティングテーブル一覧で、Internetにアクセスするサブネットワークが関連付けられたルーティングテーブルのID/名前をクリックして、ルーティングテーブルの詳細画面に入ります。
3. 「Routing Policy」欄で、「+ New routing policies」をクリックします。
4. 表示された「Add routing」ウィンドウに、** Destinationを記入し、Next Hop TypeにNAT gateway、 Next Hop**に作成したNATゲートウェイのIDを指定します。
5. **OK**をクリックします。
   上記のように設定した後、このルーティングテーブルに関連付けられたサブネットワークにおけるCVMがIntenetにアクセスするトラフィックはNATゲートウェイに転送されます。

その他のソリューション

案1：Elastic IPアドレスを使用します

CVMはElastic IPアドレスだけをバインドし、NATゲートウェイを使用しません。この案では、CVMがInternetにアクセスするすべてのトラフィックは、Elastic IPアドレス経由で転送され、CVM購入時のパブリックネットワークの帯域幅に制限されます。パブリックネットワークへのアクセスによって生じた料金は、CVMネットワーク課金

モデルによって計算されます。
使用方法：Elastic IPアドレス使用手引書をご参照ください。

案2：NATゲートウェイとastic IPアドレス両方を使用します

NATゲートウェイとastic IPアドレス両方を使用する案では、CVMからInternetへのアクセスによって生じたすべてのトラフィックは、内部ネットワーク経由でNATゲートウェイに転送されます。返されたパケットもNATゲートウェイ経由でCVMに転送されます。この部分のトラフィックは、CVM購入時のパブリックネットワークの帯域幅に制限されません。NATゲートウェイが生じたネットワークトラフィックはCVMのパブリックネットワークのアウトバンドを占有しません。InternetからのトラフィックがCVMのElastic IPアドレスにアクセスする場合、CVMが返したパケットは全部Elastic IPアドレス経由で転送され、生じたパブリックネットワークのアウトバンドトラフィックは、CVM購入時のパブリックネットワークの帯域幅に制限されます。パブリックネットワークへのアクセスによって生じた料金は、CVMネットワーク課金モデルによって計算されます。

> 注意：
> ご利用中のアカウントで帯域幅パックによる帯域共有機能をアクティブ化した場合、NATゲートウェイが生じたアウトバンドトラフィックは帯域幅パック全体に基づき計算されます(0.12ドル/GBのネットワークトラフィック料金を重複して請求しません）。NATゲートウェイの高いアウトバンドによって多額な帯域幅パック料金が生じることを防ぐために、NATゲートウェイのアウトバンドに制限をかけることを推奨します。

TKEセキュリティグループの設定

最終更新日：：2022-03-31 15:04:02

セキュリティはみんなが関心を持っている問題です。Tencent Cloudは、セキュリティを製品設計上の最も重要な要因とし、製品にセキュリティ隔離を厳しく要求します。TKEもこれを重要視しています。Tencent Cloudの基幹ネットワークは十分なセキュリティメカニズムを提供しています。TKEの基幹ネットワークは、より豊富なネットワーク機能を提供するTencent Cloudバーチャルプライベートクラウド VPC を採用します。本書では、TKEでセキュリティグループを使用するベストプラクティスを紹介することで、セキュリティポリシーの選択に協力します。

セキュリティグループ

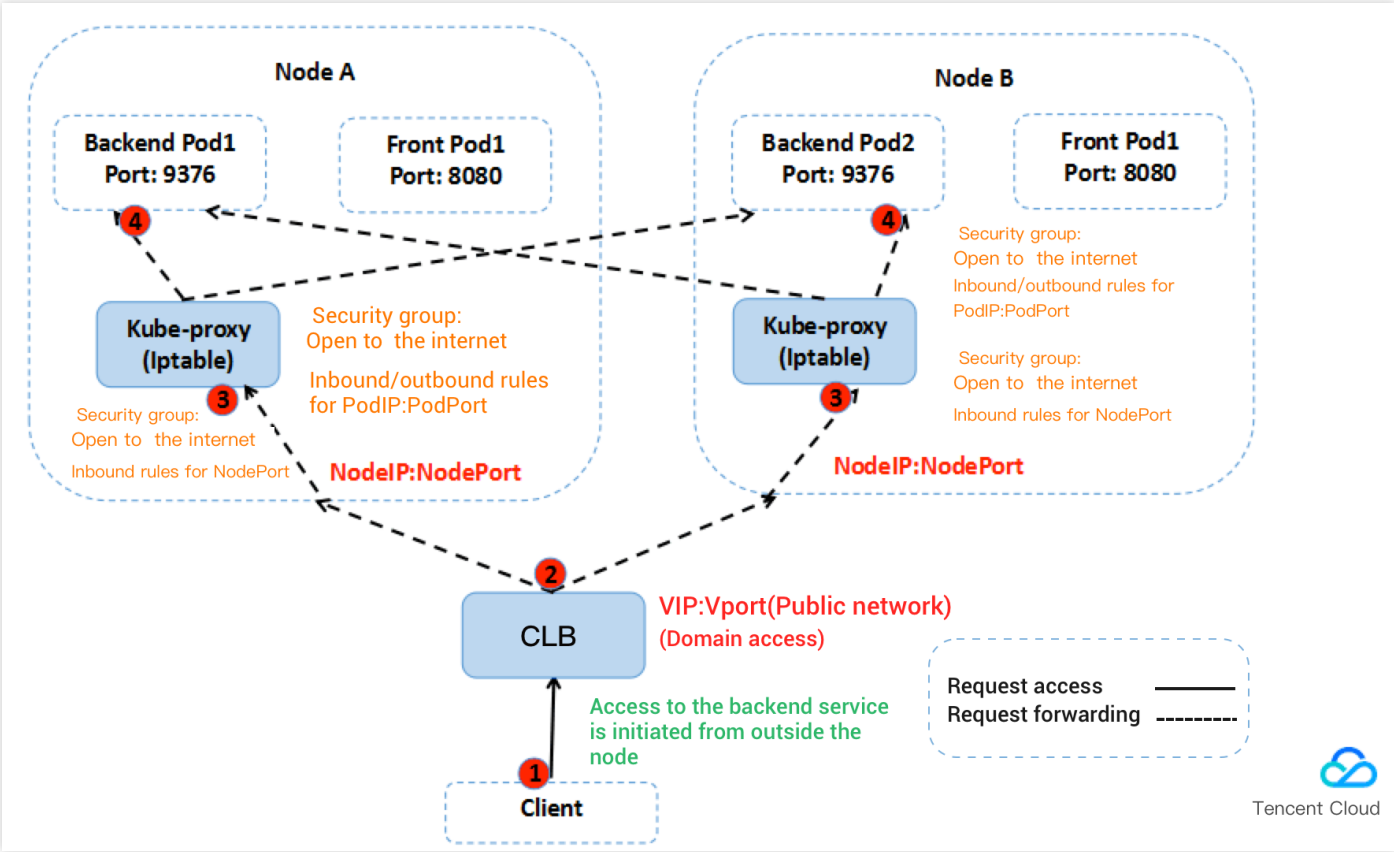
セキュリティグループは状態付きのパケットフィルタリング型仮想ファイアウォールであり、1台または複数台のCVMのネットワークアクセス制御を設定するために使用され、Tencent Cloudによって提供される重要なネットワークセキュリティ隔離の手段です。セキュリティグループの詳細は、セキュリティグループをご参照ください。

TKEを使用しセキュリティグループを選択する時検討すべきのポイント

- コンテナークラスターにおいて、サービスインスタンスが分散式にデプロイされるため、異なるサービスインスタンスはクラスターのノードに分散されます。同一クラスター配下のホストを同じセキュリティにバインドし、クラスターのセキュリティグループにほかのCVMを追加しないことを推奨します。
- 外部に対して、セキュリティは必要最小限の権限を付与します。
- 以下のTKE使用規則を適用する必要があります。
- コンテナーインスタンスネットワークとクラスターノードネットワークへのアクセスを許可します
  サービスがホストノードにアクセスする時、Kube-proxyモジュールが設定したiptables規則に従って、リクエストをサービスの任意1つのインスタンスに転送します。サービスのインスタンスがほかのノードに存在する可能性があるため、ノードをまたがったアクセスが行われます。例えば、アクセスするデスティネーションIPに、サービスインスタンスIP、クラスター上のほかのノードIP、ノード上のクラスターのcbr0ブリッジIPがある場合、- 対向側のノードでコンテナーインスタンスネットワークとクラスターノードネットワークへのアクセスを許可する必要があります。
- 同一VPCにおける異なるクラスターがお互いアクセスする場合、対応するクラスターのコンテナーネットワークとノードネットワークへのアクセスを許可する必要があります。
- SSHによるノードへのログインが必要な場合、22ポートを開放する必要があります。
- ノードの30000 - 32768ポートを開放します。
  アクセル経路で、ロードバランサーを介してパケットをコンテナークラスターのNodeIP：NodePortに転送して

ください。そのうち、NodeIPはクラスター上の任意のノードのホストIPであり、NodePortはサービス作成時にコンテナークラスターがデフォルトでサービスに割り当てたポートです。NodePortの範囲は30000 - 32768です。

下図ではパブリックネットワークからサービスにアクセスすることを例とします：



TKEのデフォルトセキュリティグループ規則

ノードのデフォルトセキュリティグループ規則

クラスターノード間の通信には一部のポートを開放する必要があります。無効なセキュリティグループをバインドすることによってクラスターの作成に失敗することを防ぐために、TKEはデフォルトのセキュリティグループ設定規則を用意しています。具体的には、下表をご参照ください：

> 注意：
> 現在のデフォルトセキュリティグループが業務需要を満足できず、このセキュリティグループにバインドされるクラスターをすでに作成している場合、セキュリティグループ規則管理を参照し、このセキュリティグループに対して、確認や変更などを行ってください。

インバンド規則

プロトコル規則	ポート	ソース	ポリシー	備考
ALL	ALL	コンテナーネットワーク CIDR	許可	コンテナーネットワークにおけるPod間通信の許可
ALL	ALL	クラスターネットワーク CIDR	許可	クラスターネットワークにおけるノード間通信の許可
tcp	22	0.0.0.0/0	許可	SSHログインポートの開放
tcp	30000 - 32768	0.0.0.0/0	許可	MasterとWorkerのノード間通信の許可
udp	30000 - 32768	0.0.0.0/0	許可	MasterとWorkerのノード間通信の許可
icmp	-	0.0.0.0/0	許可	ICMPプロトコルの許可、Ping対応

アウトバウンド規則

プロトコル規則	ポート	ソース	ポリシー
ALL	ALL	0.0.0.0/0	許可

説明：

- アウトバンド規則をカスタマイズする場合、ノードネットワークセグメントとコンテナーネットワークセグメントへのアクセスを許可する必要があります。
- コンテナーノードでこの規則を設定すれば、異なる方法でクラスターにおけるサービスにアクセスできます。
- クラスターにおけるサービスへのアクセス方法については、Service管理サービスへのアクセス方法をご参照ください。

独立クラスターMasterのデフォルトセキュリティグループ規則

独立クラスターを作成する時、デフォルトではMasterにTKEデフォルトセキュリティグループをバインドします。これは、クラスター作成後に、MasterとNodeが通信できないリスクやServiceにアクセスできないリスクを減らすためです。デフォルトのセキュリティグループ設定規則については、下表をご参照ください：

説明：

作成したセキュリティグループの権限はTKEサービスロールが継承します。詳しくは、サービスがロールに権限を付与する説明をご参照ください。

インバンド規則

プロトコル	ポート	ネットワークセグメント	ポリシー	備考
ICMP	ALL	0.0.0.0/0	許可	Ping対応
TCP	30000 - 32768	クラスターネットワークCIDR	許可	Masterと Workerの ノード間 通信の許可
UDP	30000 - 32768	クラスターネットワークCIDR	許可	Masterと Workerの ノード間 通信の許可
TCP	60001,60002,10250,2380,2379,53,17443,50055,443,61678	クラスターネットワークCIDR	許可	API Server通信の許可
TCP	60001,60002,10250,2380,2379,53,17443	コンテナーネットワークCIDR	許可	API Server通信の許可
TCP	30000 - 32768	コンテナーネットワークCIDR	許可	Service 通信の許可
UDP	30000 - 32768	コンテナーネットワークCIDR	許可	Service 通信の許可
UDP	53	コンテナーネットワークCIDR	許可	CoreDN 通信の許可
UDP	53	クラスターネットワークCIDR	許可	CoreDN 通信の許可

アウトバウンド規則

プロトコル規則	ポート	ソース	ポリシー
ALL	ALL	0.0.0.0/0	許可

クラスターの追加リソースが所属するプロジェクトの説明

最終更新日：：2022-03-31 15:04:02

クラスタ追加リソースが所属するプロジェクトの説明

概要

プロジェクトごとに財務清算などを行う場合、以下をお読みください：

1. クラスターにはプロジェクト属性がありません。クラスター内部のCVMやロードバランサーなどのリソースにはプロジェクト属性があります。
2. クラスターの追加リソースが所属するプロジェクト：当該クラスターに追加したリソースだけを当該プロジェクトの配下とします。

アドバイス

1. クラスターにおけるすべてのリソースを同一プロジェクトの配下とすることを推奨します
2. クラスターにおけるCVMを異なるプロジェクトに分散させる場合、CVMコンソールでプロジェクトを移行する必要があります。
3. CVMの所属するプロジェクトが異なる場合、CVMが所属する「セキュリティグループインスタンス」も異なるため、同じクラスターにおけるCVMの「セキュリティグループルール」を統一することを推奨します。

課金概要

最終更新日：：2022-03-31 15:04:02

TKE課金説明

現時点では、TKEのご利用自体は無料ですが、実際に使用されたクラウドリソースに応じて料金を請求します。TKE利用時に以下の製品が使用される場合があります。詳しくは、具体的な製品の課金説明をご参照ください。

- CVM課金モデル
- CBS価格一覧
- ロードバランサー課金説明

> 注意：
> TKEはKubernetesベースの宣言式サービスです。TKEが作成したロードバランサーCLBやクラウドディスクCBSなどのIaaSサービスリソースを必要としなくなる場合、具体的なサービスリソース画面から削除するのではなく、TKEコンソールから該当するサービスリソースを削除してください。そうしない場合、TKEは削除されたサービスリソースを再作成し、関連の料金が請求されます。例えば、TKEにロードバランサーCLBサービスリソースがすでに作成されているとします。ロードバランサーコンソールからこのCLBインスタンスを削除すると、TKEは宣言式APIにより新しいCLBインスタンスを作成します。

EKS課金説明

EKSは、後払いの従量制課金モデルを採用し、実際に構成したリソースと使用時間に応じて料金を請求するため、事前に支払う必要がありません。詳しくは、イラスチッククラスター課金概要をご参照ください。

購入チャネル

最終更新日：：2022-03-31 15:04:02

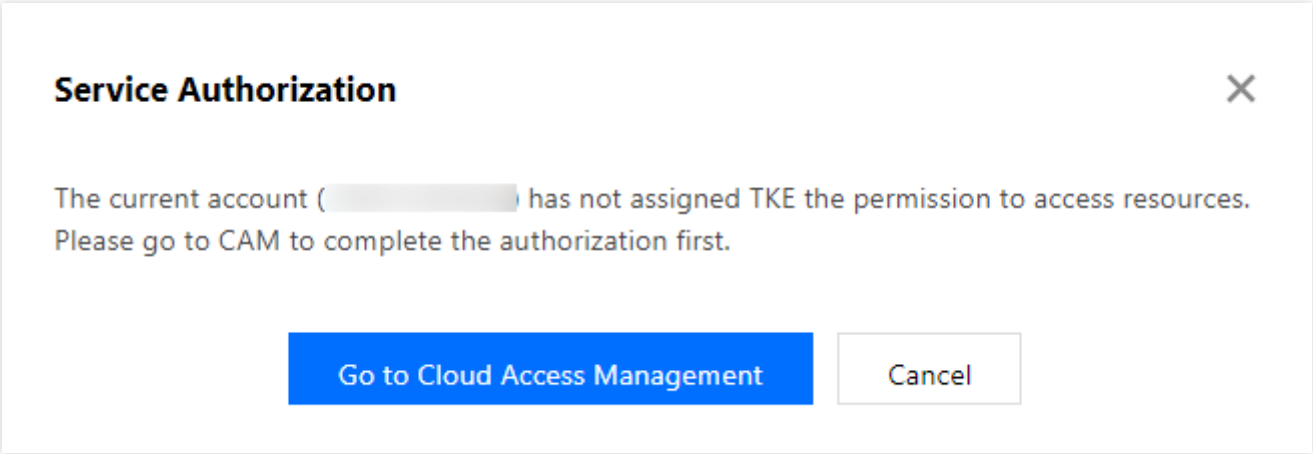
公式サイトでの購入

Tencent Cloud公式サイトにログインし、【製品】>【インフラ】>【コンテナー】>【TKE】の順に選択し、【今すぐ利用】をクリックして、TKEコンソールに入ります。初めてご利用の方は、以下の手順を参照しサービス認証を行ってから、TKE製品をご購入ください。

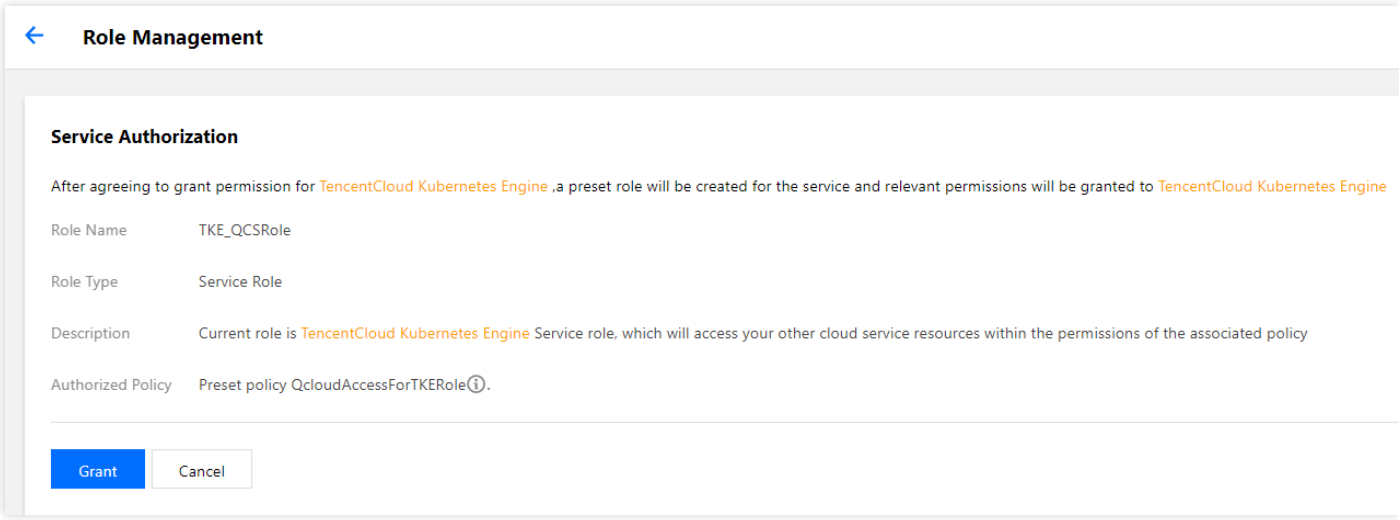
サービス認証

> 説明：
> すでにサービス認証が行われている場合、以下の手順をスキップしてください。

1. 表示された「サービス認証」ダイアログウィンドウ中の情報を確認して、【アクセス管理へ】をクリックします。下図の通りです：



2. 「ロール管理」画面で、ロール関連の情報を確認します。下図の通りです：



3. 【承認】をクリックすると、サービス認証が完了し、Tencent Cloud TKE購入画面で製品を購入できるようになります。