البنية التحتية السحابية المرنة لجوجل

التحجيم والأتمتة

Elastic Google Cloud Infrastructure

Scaling and Automation

- ملف مختصر للمقرر – Elastic Google Cloud Infrastructure: Scaling and Automation

- ملف مختصر للتجارب – Elastic Google Cloud Infrastructure: Scaling and Automation

- ملف مختصر للأختبارات – Elastic Google Cloud Infrastructure: Scaling and Automation

- نبذه عن المقرر الرابع: البنية التحتية السحابية المرنة لجوجل: التحجيم والأتمتة – Elastic Google Cloud Infrastructure: Scaling and Automation

- تقدم هذه الدورة التدريبية السريعة عند الطلب للمشاركين البنية التحتية الشاملة والمرنة وخدمات النظام الأساسي التي تقدمها Google Cloud.
- من خلال مجموعة من محاضرات الفيديو والعروض التوضيحية والمختبرات العملية ، يستكشف المشاركون وينشرون عناصر الحل ، بما في ذلك الشبكات المتصلة بأمان ، وموازنة الأحمال ، والموازنة التلقائية ، وأتمتة البنية التحتية والخدمات المدارة.

مرحبا بك في البنية التحتية السحابية المرنة: التحجيم والأتمتة

- **مرحبًا بك في** Elastic Cloud Infrastructure: Scaling and Automation.
- **ركزت المحاضرة التي شاهدتها للتو على ثلاث دورات في الهندسة المعمارية.**
- **تقدم لك هذه الدورات التدريبية البنية التحتية الشاملة والمرنة وخدمات النظام الأساسي التي توفرها** Google Cloud، **مع التركيز على** Compute Engine:

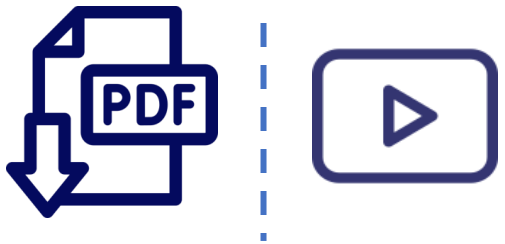
1. **البنية التحتية السحابية الأساسية: الأساس**
2. **البنية التحتية السحابية الأساسية: الخدمات الأساسية**
3. **البنية التحتية السحابية المرنة: التحجيم والأتمتة (هذه الدورة)**

- مرحبا بك في البنية التحتية السحابية المرنة: التحجيم والأتمتة

- تعتمد هذه الدورة التدريبية على البنية الأساسية السحابية الأساسية: دورة الخدمات الأساسية وتعزز دراستك للهندسة المعمارية باستخدام Compute Engine.
- في هذه الدورة التدريبية ، نبدأ بالانتقال إلى الخيارات المختلفة لربط الشبكات لتمكينك من توصيل بنيتك الأساسية بـ Google Cloud.
- بعد ذلك ، سننتقل إلى خدمات موازنة التحميل والموازنة التلقائية في Google Cloud، والتي سيتعين عليك استكشافها مباشرةً.
- بعد ذلك ، سنغطي خدمات أتمتة البنية التحتية مثل Terraform، بحيث يمكنك أتمتة نشر خدمات البنية التحتية السحابية من Google.أخيرًا ، سنتحدث عن الخدمات المدارة الأخرى التي قد ترغب في الاستفادة منها في Google Cloud.
- فيما يلي وحدات الدورة:
- ربط الشبكات - موازنة الحمل والتحكم الذاتي - أتمتة البنية التحتية - الخدمات المدارة.
- استمتع بهذه الدورة!

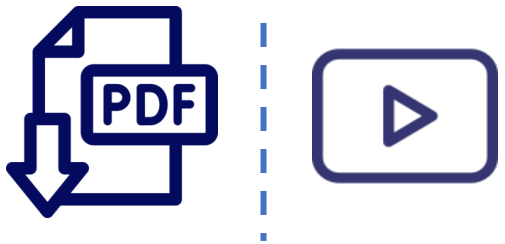
نظرة عامة عن الوحدة

- مرحبًا ، أنا بريانكا فيرجاديا ، محامية مطوّري برامج Google Cloud.
- في هذه الوحدة ، نركز على ربط الشبكات.
- تتطلب التطبيقات وأعباء العمل المختلفة حلول اتصال مختلفة بالشبكة. لهذا السبب تدعم Google طرقًا متعددة لتوصيل بنيتك الأساسية بـ GCP.
- في هذه الوحدة ، سنركز على منتجات الاتصال الهجين الخاصة بـ GCP وهي Cloud VPN و Cloud Interconnect و Peering.
- سننظر أيضًا في خيارات مشاركة شبكة VPC داخل GCP.
- لنبدأ بالحديث عن Cloud VPN حتى تتمكن من استكشافها في المختبر.



سحابة VPN

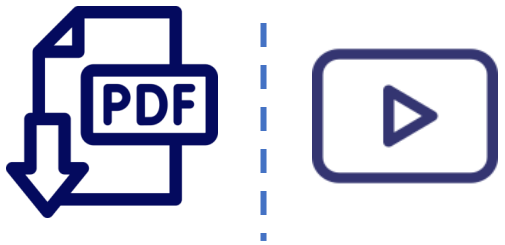
- تقوم Cloud VPN بشكل آمن بتوصيل شبكتك المحلية بشبكة Google Cloud VPC الخاصة بك من خلال نفق IPsec VPN.
- يتم تشفير حركة المرور بين الشبكتين بواسطة بوابة VPN واحدة ، ثم يتم فك تشفيرها بواسطة بوابة VPN الأخرى.
- يحمي هذا بياناتك أثناء انتقالها عبر الإنترنت العام ، ولهذا السبب تعد Cloud VPN مفيدة لاتصالات البيانات ذات الحجم المنخفض.
- كخدمة مُدارة ، توفر Cloud VPN اتفاقية مستوى خدمة (SLA) توفر خدمة 99.9٪ وتدعم VPN من موقع إلى موقع والمسارات الثابتة والديناميكية وأصفار IKEv1 و IKEv2.
- لا تدعم Cloud VPN حالات الاستخدام حيث تحتاج أجهزة الكمبيوتر العميلة إلى "الاتصال" بشبكة VPN باستخدام برنامج VPN للعميل.
- أيضًا ، يتم تكوين المسارات الديناميكية باستخدام Cloud Router، والتي سنغطيها باختصار.



- سحابة VPN

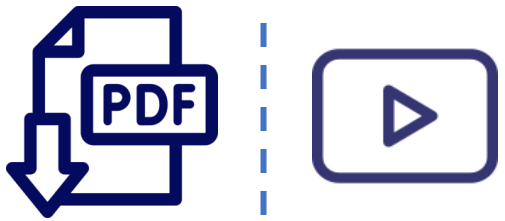
- لمزيد من المعلومات حول اتفاقية مستوى الخدمة وهذه الميزات.
- يرجى الرجوع إلى ارتباط التوثيق. نظرة عامة على Cloud VPN: https://cloud.google.com/vpn/docs/concepts/overview

  دعني أتصفح مثالاً على Cloud VPN.
- يوضح هذا الرسم التخطيطي اتصال VPN كلاسيكي بين VPC والشبكة المحلية.
- تحتوي شبكة VPC الخاصة بك على شبكات فرعية في الشرق الأوسط والولايات المتحدة والغرب 1 ، مع موارد Google Cloud في كل من تلك المناطق.
- هذه الموارد قادرة على الاتصال باستخدام عناوين IP الداخلية الخاصة بها لأن التوجيه داخل الشبكة يتم تكوينه تلقائيًا (على افتراض أن قواعد جدار الحماية تسمح بالاتصال).



سحابة VPN

- الآن ، من أجل الاتصال بشبكتك المحلية ومواردها ، تحتاج إلى تكوين بوابة Cloud VPN الخاصة بك وبوابة VPN المحلية وأنفاق VPN.
- بوابة Cloud VPN هي مورد إقليمي يستخدم عنوان IP خارجي إقليمي.
- يمكن أن تكون بوابة VPN المحلية الخاصة بك جهازًا ماديًا في مركز البيانات الخاص بك أو عرض VPN فعلي أو قائم على البرامج في شبكة مزود خدمة سحابي آخر. تحتوي بوابة VPN هذه أيضًا على عنوان IP خارجي. يقوم نفق VPN بعد ذلك بتوصيل بوابات VPN الخاصة بك ويعمل كوسيط افتراضي يتم من خلاله تمرير حركة المرور المشفرة. من أجل إنشاء اتصال بين بوابتين للشبكة الافتراضية الخاصة ، يجب عليك إنشاء أنفاق VPN يحدد كل نفق الاتصال من منظور بوابته ، ولا يمكن لحركة المرور المرور إلا عند إنشاء زوج من الأنفاق ، الآن ، هناك شيء واحد يجب تذكره عند استخدام Cloud VPN
- وهو أن الحد الأقصى لوحدة الإرسال. أو MTU، لبوابة VPN المحلية الخاصة بك.
- لا يمكن أن تكون أكبر من 1460 بايت. هذا بسبب تشفير الحزم وتغليفها.



- سحابة VPN

- لمزيد من المعلومات حول اعتبار MTU هذا ، يرجى الرجوع إلى ارتباط التوثيق في موارد الدورة التدريبية.
- [اعتبارات MTU: https://cloud.google.com/vpn/docs/concepts/mtu-considerations بالإضافة إلى Classic VPN، تقدم Google Cloud أيضًا نوعًا ثانيًا من بوابة Cloud VPN، HA VPN. HA VPN هو حل Cloud VPN عالي التوفر يتيح لك الاتصال الآمن بشبكتك المحلية بشبكة Virtual Private Cloud (VPC) من خلال اتصال IPsec VPN في منطقة واحدة.
- توفر HA VPN اتفاقية مستوى خدمة (SLA) تبلغ 99.99٪ من توفر الخدمة. لضمان توفر اتفاقية مستوى الخدمة بنسبة 99.99٪ للاتصالات HA VPN، يجب عليك تكوين نفقين أو أربعة أنفاق بشكل صحيح من بوابة HA VPN إلى بوابة VPN النظيرة أو إلى بوابة HA VPN أخرى.
- عند إنشاء بوابة HA VPN، تختار Google Cloud تلقائيًا عنواني IP خارجيين.

- سحابة VPN

- واحد لكل من العدد الثابت لواجهتين. يتم اختيار كل عنوان IP تلقائيًا من مجموعة عناوين فريدة لدعم الإتاحة العالية. تدعم كل واجهة من واجهات بوابة HA VPNأنفاق متعددة. يمكنك أيضًا إنشاء عدة بوابات HA VPN، عندما تحذف بوابة HA VPN، تقوم Google Cloud بإصدار عناوين IP لإعادة استخدامها.
- يمكنك تكوين بوابة HA VPN بواجهة نشطة واحدة وعنوان IP خارجي واحد ؛ ومع ذلك ، لا يوفر هذا التكوين توفر خدمة SLA بنسبة 99.99٪. يجب أن تستخدم أنفاق VPN المتصلة ببوابات HA VPN التوجيه الديناميكي (BGP) اعتمادًا على طريقة تكوين أولويات المسار لأنفاق HA VPN، يمكنك إنشاء تكوين توجيه نشط / نشط أو نشط / خامل.

سحابة VPN

- تدعم HA VPN VPN من موقع إلى موقع في أحد الهياكل أو سيناريوهات التكوين التالية الموصى بها: بوابة HA VPN للأجهزة VPN النظيرة بوابة HA VPN إلى Amazon Web Services (AWS) بوابة خاصة افتراضية اثنان HA VPN متصلان بكل منهما أخرى دعنا نستكشف هذه التكوينات بمزيد من التفصيل. هناك ثلاثة تكوينات نموذجية لبوابة النظراء لـ HA VPN.
- بوابة HA VPN لجهازي VPN منفصلين ، لكل منهما عنوان IP الخاص به ، وبوابة HA VPN لجهاز VPN واحد يستخدم عنواني IP منفصلين وبوابة HA VPN لجهاز VPN نظير يستخدم عنوان IP واحد.
- دعنا نسير من خلال مثال. في هذا الهيكل ، تتصل بوابة HA VPN واحدة بجهازين نظير. يحتوي كل جهاز نظير على واجهة واحدة وعنوان IP خارجي واحد. تستخدم بوابة HA VPN نفقين ، نفق واحد لكل جهاز نظير. إذا كانت البوابة من جانب النظير تعتمد على الأجهزة ، فإن وجود بوابة ثانية من جانب النظير يوفر التكرار وتجاوز الفشل على هذا الجانب من الاتصال.
- تتيح لك البوابة المادية الثانية أخذ إحدى البوابات
- في وضع عدم الاتصال لترقيات البرامج أو عمليات الصيانة المجدولة الأخرى.

- سحابة VPN

- كما أنه يحميك في حالة حدوث عطل في أحد الأجهزة.
- في Google Cloud، يأخذ REDUNDANCY_TYPE لهذا التكوين القيمة TWO_IPS_REDUNDANCY.
- يوفر المثال الموضح هنا توفرًا بنسبة 99.99٪. عند تكوين بوابة VPN خارجية من HA VPN إلى Amazon Web Services (AWS)، يمكنك استخدام بوابة عبور أو بوابة خاصة افتراضية. تدعم بوابة النقل فقط التوجيه متعدد المسارات بتكلفة متساوية (ECMP) عند التمكين ، تقوم ECMP بتوزيع حركة المرور بالتساوي عبر الأنفاق النشطة. دعونا نلقي نظرة على مثال. في هذا الهيكل ، توجد ثلاثة مكونات رئيسية للبوابة لإعداد هذا التكوين. بوابة HA VPN في Google Cloud بواجهتين ، وبوابتين خاصتين افتراضية من AWS، والتي تتصل ببوابة HA VPN الخاصة بك ، ومورد بوابة VPN خارجي في Google Cloud يمثل بوابة AWSالخاصة الافتراضية.
- يوفر هذا المورد معلومات إلى Google Cloud حول بوابة AWS الخاصة بك.
- يستخدم تكوين AWS المدعوم ما مجموعه أربعة أنفاق.


سحابة VPN

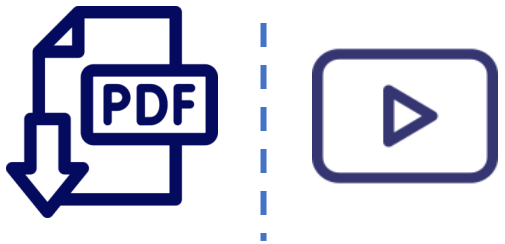
- نفقان من بوابة خاصة افتراضية AWS واحدة إلى واجهة واحدة لبوابة HA VPN، ونفقان من بوابة AWS الافتراضية الخاصة الأخرى إلى الواجهة الأخرى لبوابة HA VPN يمكنك توصيل شبكتي Google Cloud VPC معًا باستخدام بوابة HA VPN في كل شبكة.
- يوفر التكوين الموضح توفرًا بنسبة 99.99٪. من منظور كل بوابة HA VPN، تقوم بإنشاء نفقين. تقوم بتوصيل الواجهة 0 على بوابة HA VPNواحدة بالواجهة 0 على HA VPN الأخرى ، والواجهة 1 على بوابة HA VPN واحدة للواجهة 1 على HA VPN الأخرى.
- لمزيد من المعلومات حول HA VPN والانتقال إلى HA VPN، راجع روابط الوثائق في موارد الدورة التدريبية.
- [طبولوجيا] https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies الانتقال Cloud VPN: إلى https://cloud.google.com/network-connectivity/docs/vpn / how-to / move-to-ha-vpn HA VPN: ذكرنا سابقًا أن Cloud VPN يدعم كلا من المسارات الثابتة والديناميكية.
- من أجل استخدام المسارات الديناميكية ، تحتاج إلى تكوين الموجهات السحابية.

سحابة VPN

- يمكن لـ Cloud Router إدارة المسارات لنفق Cloud VPN باستخدام بروتوكول Border Gateway Protocol أو BGP,
- تسمح طريقة التوجيه هذه بتحديث المسارات وتبادلها دون تغيير تكوين النفق.
- على سبيل المثال ، يوضح هذا الرسم التخطيطي شبكتين فرعيتين إقليميتين مختلفتين في شبكة VPC، وهما Test and Prod.
- تحتوي الشبكة المحلية على 29 شبكة فرعية ، والشبكتان متصلتان عبر أنفاق Cloud VPN.
- الآن ، كيف ستتعامل مع إضافة شبكات فرعية جديدة؟ على سبيل المثال ، كيف يمكنك إضافة شبكة فرعية "Staging"جديدة في شبكة Google Cloud وشبكة فرعية محلية جديدة 10.0.30.0/24 للتعامل مع حركة المرور المتزايدة في مركز البيانات الخاص بك؟ لنشر تغييرات تكوين الشبكة تلقائيًا ، يستخدم نفق VPN جهاز التوجيه السحابي لإنشاء جلسة BGP بين VPC وبوابة VPN المحلية ، والتي يجب أن تدعم BGP.

- سحابة VPN

- ثم يتم الإعلان عن الشبكات الفرعية الجديدة بسلاسة بين الشبكات.
- هذا يعني أنه يمكن للحالات في الشبكات الفرعية الجديدة أن تبدأ في إرسال واستقبال حركة المرور على الفور ، كما ستستكشف في الدرس القادم.
- لإعداد BGP، يجب تعيين عنوان IP إضافي لكل نهاية نفق VPN.
- يجب أن يكون هذان العنوانان IP عبارة عن عناوين P امحلية للارتباط ، تنتمي إلى نطاق عناوين 169.254.0.0/16 IP هذه العناوين ليست جزءًا من مساحة عنوان IP لأي من الشبكتين وتستخدم حصريًا لإنشاء BG



HA VPN

- HA VPN **كبوابة** VPN **بديلة للشبكة السحابية**
- **بالإضافة إلى** Classic VPN، **تقدم** Google Cloud **أيضًا نوعًا ثانيًا من بوابة** Cloud VPN، HA VPN
- HA VPN **هو حل** Cloud VPN **عالي التوفر يتيح لك الاتصال بأمان شبكة محلية إلى شبكة** Virtual Private Cloud (VPC) **الخاصة بك من خلال** IPsec VPN **اتصال في منطقة واحدة.**
- **توفر** HA VPN **اتفاقية مستوى خدمة** (SLA) **تبلغ** 99.99٪ **من توفر الخدمة.**
- **لمزيد من المعلومات حول** HA VPN، **ارجع إلى وثائق هياكل** Cloud VPN
- **للحصول على معلومات حول الانتقال إلى** HA VPN، **راجع الانتقال إلى** HA VPN

- **مقدمة المختبر: تكوين Google Cloud HA VPN**

- **دعونا نطبق ما قمنا بتغطيته للتو. في هذا المعمل ، تقوم بإنشاء VPC عالمي يسمى vpc-demo، مع شبكتين فرعيتين مخصصتين في us-east1 و us-central1.**
- **في VPC هذا ، يمكنك إضافة مثيل Compute Engine في كل منطقة.**
- **يمكنك بعد ذلك إنشاء VPC ثاني يسمى محليًا لمحاكاة مركز البيانات المحلي للعميل.**
- **في VPC الثاني هذا ، يمكنك إضافة شبكة فرعية في المنطقة us-central1 ومثيل Compute Engine يعمل في هذه المنطقة.**
- **أخيرًا ، يمكنك إضافة HA VPN وجهاز توجيه سحابي في كل VPC وتشغيل نفقين من كل بوابة HA VPN قبل اختبار التكوين للتحقق من 99.99٪ SLA.**

معمل – LAB: تكوين Google Cloud HA VPN

- في هذا التمرين المعملي ، تقوم بإنشاء أنفاق VPN بين شبكتين في مناطق منفصلة بحيث يمكن لجهاز افتراضي في إحدى الشبكات اختبار اتصال جهاز افتراضي في الشبكة الأخرى عبر عنوان IP الداخلي الخاص به.
- نصائح لمختبرات الدورة التدريبية
- احصل على أقصى استفادة من Coursera و Qwiklabs من خلال تجربة نصائحنا أدناه.
- تجنب الخلط بين الحساب والتصفح الخاص.
- أغلق هذه الصفحة وسجل الدخول مرة أخرى إلى Coursera في وضع التصفح المتخفي قبل الانتقال.
- عند العودة إلى هذه الدورة التدريبية وصفحة الإرشادات المعملية ، انقر فوق "فتح الأداة" للمتابعة.
- تجنب الخلط بين الحساب والتصفح الخاص.

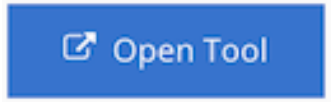
- **معمل** – LAB: **تكوين** Google Cloud HA VPN

- **باستخدام وضع التصفح المتخفي ، يضمن ذلك عدم استخدامك لحساب** Google **الخاص بك عن طريق الخطأ (بما في ذلك** Gmail**) أثناء الوصول إلى** Google Cloud Console.
- **يمنع هذا أيضًا** Qwiklabs **من تسجيل خروجك من حسابات** Google **الخاصة بك.**
- **الإرشادات التفصيلية لاستخدام وضع التصفح المتخفي في** Google Chrome **متوفرة هنا.**
- **اعتمادًا على المستعرض الخاص بك ، قد يُطلق على وضع التصفح المتخفي أيضًا اسم الاستعراض الخاص أو استعراض** InPrivate.

- **معمل** – LAB: **تكوين** Google Cloud HA VPN

- **لضمان الانتهاء من المختبر تم وضع علامة عليه في كورسيرا:**

1. **قم بالوصول إلى كل معمل فردي بالنقر فوق فتح الأداة في كورسيرا**



2. **أكمل المختبر في** Qwiklabs
3. **انقر على "إنهاء المعمل" في** Qwiklabs

4. **أغلق نافذة أو علامة تبويب متصفح** Qwiklabs

- **معمل** – LAB: **تكوين** Google Cloud HA VPN

- **للتفاعل مع المتعلمين الآخرين:**

إذا كنت تواجه أي صعوبة في المعامل ، فنحن نشجعك على النشر عنها في منتديات المناقشة الخاصة بهذه الدورة التدريبية. إذا لم تكن لديك مشاكل مع المعامل ، ففكر في تصفح منتديات المناقشة للحصول على فرص لمساعدة زملائك المتعلمين.

- **لتقديم طلب دعم:**

إذا كنت تواجه مشكلات فنية مع المختبرات أو التصنيف ، فيرجى إرسال طلب دعم هنا:

https://qwiklab.zendesk.com/hc/en-us/requests/new

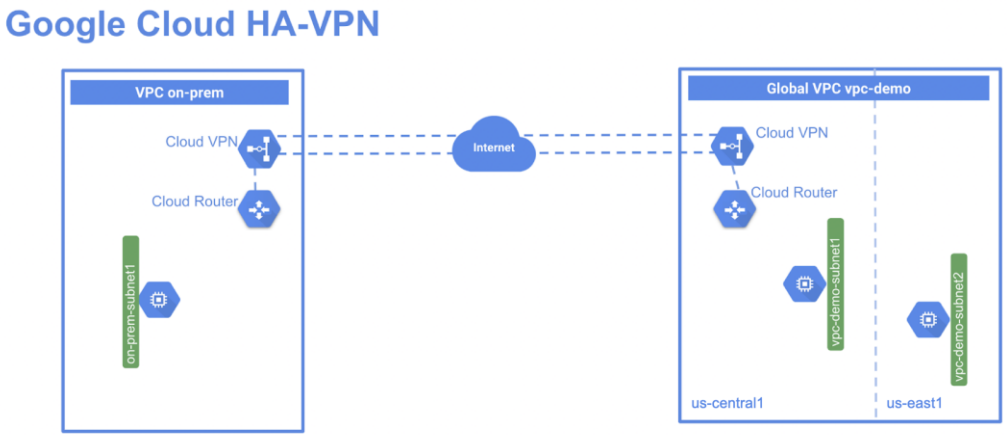
- **معمل** – LAB: – Configuring Google Cloud HA VPN

- HA VPN **هو حل** Cloud VPN **عالي التوفر** (HA) **يتيح لك الاتصال الآمن بشبكتك المحلية بشبكة** VPC **الخاصة بك من خلال اتصال** IPsec VPN **في منطقة واحدة.**
- **توفر** HA VPN **اتفاقية مستوى خدمة** (SLA) **تبلغ** 99.99٪ **من توفر الخدمة.**

- HA VPN **هو حل إقليمي لكل حل** VPN، VPC.
- **تحتوي بوابات** HA VPN **على واجهتين ، لكل منهما عنوان** IP **العام الخاص به.**
- **عندما تقوم بإنشاء بوابة** HA VPN، **يتم اختيار عنوانين** IP **عامين تلقائيًا من مجموعات عناوين مختلفة. عندما يتم تكوين** HA VPN **بنفقين ، توفر** Cloud VPN **وقت تشغيل متوفر بنسبة** 99.99٪.

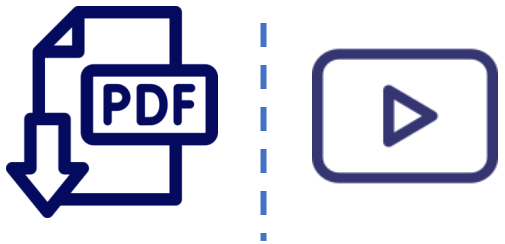
معمل – LAB: - Configuring Google Cloud HA VPN

- في هذا المعمل ، تقوم بإنشاء VPC عالمي يسمى vpc-demo، مع شبكتين فرعيتين مخصصتين في us-east1 و us-central1 في VPC هذا ، يمكنك إضافة مثيل Compute Engine في كل منطقة.
- يمكنك بعد ذلك إنشاء VPC ثاني يسمى محليًا لمحاكاة مركز البيانات المحلي للعميل.
- في VPC الثاني هذا ، يمكنك إضافة شبكة فرعية في المنطقة us-central1 ومثيل Compute Engine يعمل في هذه المنطقة.
- أخيرًا ، يمكنك إضافة HA VPN وجهاز توجيه سحابي في كل VPC وتشغيل نفقين من كل بوابة HA VPN قبل اختبار التكوين للتحقق من SLA ٪99.99.



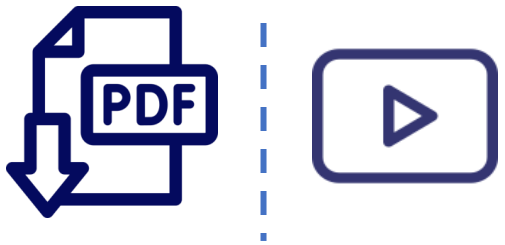
الترابط السحابي والتناظر

- بعد ذلك ، دعنا نتحدث عن خدمات Cloud Interconnect and Peering تتوفر خدمات Cloud Interconnect و Peering مختلفة لربط بنيتك التحتية بشبكة Google يمكن تقسيم هذه الخدمات إلى اتصالات مخصصة مقابل اتصالات مشتركة وطبقة من الآيتين بطبقة ثلاثة اتصالات. الخدمات هي Direct Peering، و Carrier Peering، و Interconnect، و Partner Interconnect.
- توفر الاتصالات المخصصة اتصالاً مباشرًا بشبكة Google ، لكن الاتصالات المشتركة توفر اتصالاً بشبكة Google من خلال شريك.
- تستخدم الوصلة ذات الطبقتين شبكة محلية ظاهرية (VLAN) تقوم بالتوصيل مباشرة إلى بيئة GCP الخاصة بك ، مما يوفر الاتصال بعناوين IP الداخلية في مساحة عنوان RFC 1918 ، توفر اتصالات الطبقة الثلاث الوصول إلى خدمات G Suite و YouTube و Google Cloud APIs باستخدام عناوين IP العامة.



الترابط السحابي والتناظر

- الآن كما أوضحت سابقًا ، تقدم Google أيضًا خدمة الشبكة الافتراضية الخاصة الخاصة بها والتي تسمى Cloud VPN.
- تستخدم هذه الخدمة الإنترنت العام ولكن حركة المرور مشفرة وتوفر الوصول إلى عناوين IP الداخلية.
- هذا هو السبب في أن Cloud VPN هو إضافة مفيدة إلى Direct Peering و Carrier Peering.
- اسمحوا لي أن أشرح خدمات Cloud Interconnect و Peering بشكل منفصل أولاً ثم سأقدم بعض الإرشادات حول اختيار الاتصال الصحيح.

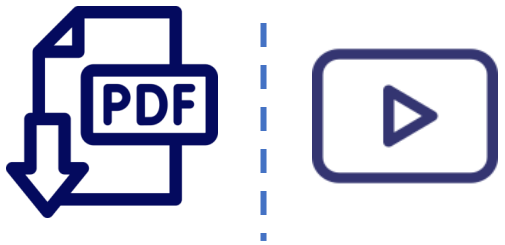


الترابط السحابي

- يوفر Interconnect المخصص اتصالات مادية مباشرة بين شبكتك المحلية وشبكة Google يمكّنك هذا من نقل كمية كبيرة من البيانات بين الشبكات ، مما قد يكون أكثر فعالية من حيث التكلفة من شراء نطاق ترددي إضافي عبر الإنترنت العام. من أجل استخدام الاتصال البيني المخصص ، تحتاج إلى توفير اتصال متقاطع بين شبكة Google وجهاز التوجيه الخاص بك في مرفق مشترك في الموقع ، كما هو موضح في هذا الرسم البياني. لتبادل المسارات بين الشبكات ، يمكنك تكوين جلسة BGP عبر الاتصال البيني بين جهاز التوجيه السحابي والموجه الداخلي. سيسمح هذا لحركة مرور المستخدم من الشبكة المحلية بالوصول إلى موارد GCP على شبكة VPC والعكس صحيح.
- يمكن تكوين الاتصال الداخلي المخصص لتقديم اتفاقية مستوى خدمة (SLA)بنسبة 99.9 بالمائة أو 99.99 بالمائة لوقت التشغيل.

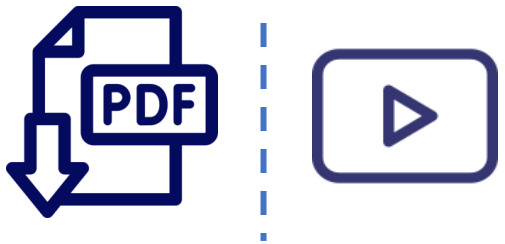
الترابط السحابي

- راجع وثائق Dedicated Interconnect للحصول على تفاصيل حول كيفية تحقيق اتفاقيات مستوى الخدمة هذه. من أجل استخدام Dedicated Interconnect، يجب أن تلبي شبكتك فعليًا شبكة Google في منشأة مدعومة مشتركة الموقع. تُظهر هذه الخريطة الموقع حيث يمكنك إنشاء اتصالات مخصصة. للحصول على قائمة كاملة بهذه المواقع ، راجع قسم الارتباط لهذا الفيديو. الآن ، قد تنظر إلى هذه الخريطة وتقول ، حسنًا ، أنا لست قريبًا من أحد هذه المواقع. هذا عندما تريد التفكير في Partner Interconnect.
- يوفر Partner Interconnect الاتصال بين شبكتك المحلية وشبكة VPC الخاصة بك من خلال مزود خدمة مدعوم. يكون هذا مفيدًا إذا كان مركز البيانات الخاص بك في الموقع الفعلي الذي لا يمكنه الوصول إلى مرفق موقع مشترك مخصص للربط البيني



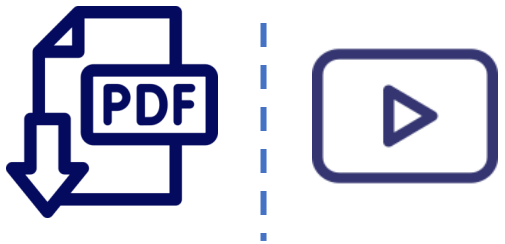
- **الترابط السحابي**

- **أو إذا كانت احتياجات البيانات الخاصة بك لا تضمن اتصالاً داخليًا مخصصًا. من أجل استخدام** Partner Interconnect**، فأنت تعمل مع مزود خدمة مدعوم لتوصيل** VPC **والشبكات المحلية. للحصول على قائمة كاملة بمقدمي الخدمات ، راجع قسم الارتباط في هذا الفيديو. يمتلك مقدمو الخدمة هؤلاء اتصالات فعلية حالية بشبكة** Google **التي يوفرونها لعملائهم لاستخدامها. بعد إنشاء اتصال بمزود الخدمة ، يمكنك طلب اتصال** Partner Interconnect **من مزود الخدمة الخاص بك ، ثم إنشاء جلسة** BGP **بين جهاز التوجيه السحابي والموجه المحلي لبدء تمرير حركة المرور بين الشبكات الخاصة بك. نحن مقدمو الخدمة الذين يعملون. يمكن تكوين** Partner Interconnect **لتقديم 99.9 بالمائة أو 99.99 بالمائة من وقت التشغيل** SLA **بين** Google**ومقدم الخدمة. راجع وثائق** Partner Interconnect**للحصول على تفاصيل حول كيفية تحقيق اتفاقيات مستوى الخدمة هذه. اسمحوا لي أن أقارن خيارات** Interconnect **التي ناقشناها للتو.**



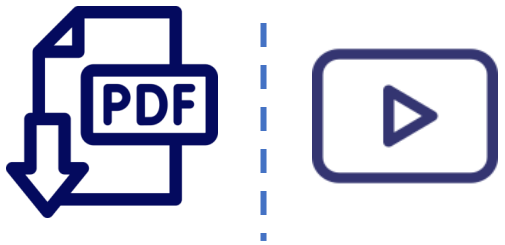
الترابط السحابي

- توفر كل هذه الخيارات إمكانية الوصول إلى عنوان IP الداخلي بين الموارد في شبكتك المحلية وشبكة VPC الخاصة بك. الاختلافات الرئيسية هي سعة الاتصال ومتطلبات استخدام الخدمة. تتمتع أنفاق IPsec VPN التي تقدمها Cloud VPN بسعة 1.5-3 جيجابت في الثانية لكل نفق وتتطلب جهاز VPN على شبكتك المحلية. تنطبق سعة 1.5 جيجابت في الثانية على حركة المرور التي تعبر الإنترنت العام ، وتنطبق السعة الثالثة جيجابت في الثانية على حركة المرور التي تعبر ارتباط تناظري مباشر. يمكنك تكوين عدة أنفاق إذا كنت تريد توسيع نطاق هذه السعة. يتمتع Interconnect المخصص بسعة 10 جيجابت في الثانية لكل ارتباط ويتطلب منك اتصالاً في موقع مشترك تدعمه Google.
- يمكن أن يكون لديك ما يصل إلى ثمانية روابط لتحقيق مضاعفات 10 جيجابت في الثانية ، ولكن 10 جيجابت في الثانية هي الحد الأدنى للسعة. اعتبارًا من هذا التسجيل.



الترابط السحابي

- هناك ميزة تجريبية توفر 100 جيجابت في الثانية لكل رابط بحد أقصى رابطين. ضع في اعتبارك أن الميزات الموجودة في الإصدار التجريبي لا تغطيها أي اتفاقية مستوى خدمة (SLA) أو سياسات الإيقاف ، وقد تخضع لتغييرات غير متوافقة مع الإصدارات السابقة.
- تبلغ قدرة Partner Interconnect من 50 ميجابت في الثانية إلى 10 جيجابت في الثانية لكل اتصال ، وتعتمد المتطلبات على مزود الخدمة.
- توصيتي هي أن تبدأ مع أنفاق VPN عندما تحتاج إلى اتصال على مستوى المؤسسة بـ GCP، قم بالتبديل إلى Dedicated Interconnect أو Partner Interconnect، اعتمادًا على قربك من مرفق الموقع المشترك ومتطلبات السعة الخاصة بك.



التناظر

- دعنا نتحدث عن خدمات التناظر السحابية وهي Direct Peering و Carrier Peering تكون هذه الخدمات مفيدة عندما تطلب الوصول إلى خصائص Google السحابية و Google تتيح لك إنشاء اتصال نظير مباشر بين شبكة عملك وشبكة Google.
- باستخدام هذا الاتصال ، ستتمكن من تبادل حركة المرور على الإنترنت بين شبكتك وشبكة Google في أحد مواقع شبكة الحافة الواسعة النطاق في Googles يتم المعالجة المباشرة مع Google عن طريق تبادل مسار BGP بين Google والكيان المناظير.
- بعد وجود اتصال مباشر بين النظراء ، يمكنك استخدامه للوصول إلى جميع خدمات Google، بما في ذلك المجموعة الكاملة من منتجات Google cloud platform على عكس التوصيل البيني المخصص ، لا يوجد لدى Direct Peering اتفاقية مستوى الخدمة (SLA) من أجل استخدام التناظر المباشر ، تحتاج إلى تلبية متطلبات التناظر في قسم الروابط في هذا الفيديو.
- نقاط التواجد في نظام تحديد المواقع العالمي (GPS) أو نقاط التواجد (PoP)
- هي المكان الذي تتصل فيه شبكة Google ببقية الإنترنت عبر التناظر.

التناظر

- نقاط الاتصال موجودة في أكثر من 90 تبادلًا للإنترنت وفي أكثر من 100 مرفق ربط حول العالم. لمزيد من المعلومات حول نقاط التبادل والتسهيلات هذه ، أوصي بالاطلاع على إدخالات قاعدة بيانات التناظرية من Google والمرتبطة أسفل هذا الفيديو. إذا نظرت إلى هذه الخريطة وقلت ، مرحبًا ، أنا لست قريبًا من أحد هذه المواقع ، فستحتاج إلى التفكير في Carrier Peering ، إذا كنت تحتاج إلى الوصول إلى البنية التحتية العامة لـ Google ولا يمكنك تلبية متطلبات التناظر الخاصة بـ Google، فيمكنك الاتصال بشريك Carrier Peering ، اعمل مباشرةً مع مزود الخدمة للحصول على الاتصال الذي تحتاجه وفهم متطلبات الشركاء.
- للحصول على قائمة كاملة بمقدمي الخدمات المتاحين ، راجع قسم الروابط في هذا الفيديو. الآن تمامًا مثل Direct Peering، لا تمتلك Carrier Pearing أيضًا اتفاقية مستوى الخدمة (SLA)اسمحوا لي أن أقارن خيارات التناظر التي ناقشناها للتو. توفر كل هذه الخيارات الوصول إلى عنوان PP العام لجميع خدمات Google ، الاختلافات الرئيسية هي السعة
- ومتطلبات استخدام الخدمة ، تتمتع تقنية Direct Peering بسعة 10 جيجابت في الثانية لكل رابط
- وتتطلب منك اتصالاً في نقطة وجود حافة GCP نظير الناقل والقدرة والمتطلبات.
- حقًا ، اعتمادًا على مزود الخدمة الذي تعمل معه.

اختيار الاتصال

- الآن وقد ناقشنا جميع خدمات التجميع المختلفة ، دعني أساعدك في تحديد الخدمة الأفضل التي تلبي احتياجات الاتصال الهجين لديك. لقد بدأت هذا الدرس بتقديم خمس طرق مختلفة لربط بنيتك الأساسية بـ GCP لقد قسمت الخدمات إلى اتصالات مخصصة مقابل اتصالات مشتركة ، وطبقة 2 مقابل اتصالات طبقة ثالثة. هناك طريقة أخرى لتنظيم هذه الخدمات وهي عن طريق خدمات التوصيل البيني والخدمات المماثلة. توفر خدمات التوصيل البيني وصولاً مباشرًا إلى عناوين IP الخاصة بـ RFC1918 في VPC الخاص بك باستخدام اتفاقية مستوى الخدمة.
- في المقابل ، توفر خدمات التناظر الوصول إلى عناوين IP العامة لـ Google فقط بدون اتفاقية مستوى الخدمة. هناك طريقة أخرى لاختيار الخدمة المناسبة التي تلبي احتياجاتك وهي استخدام مخطط التدفق.
- اسمح لي بتوجيهك عبر هذا المخطط من الأعلى باستخدام الافتراضات التي تريد توسيع بنيتك التحتية إلى السحابة.

اختيار الاتصال

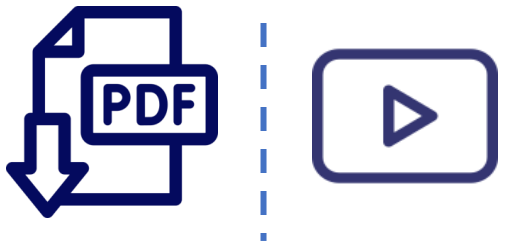
- اسأل نفسك عما إذا كنت بحاجة إلى توسيع شبكتك لخدمات G Suite أو YouTube أو Google Cloud APIs.
- إذا قمت بذلك ، فاختر إحدى خدمات التناظر. إذا كان بإمكانك تلبية متطلبات التناظر المباشر من Google، فاختر التناظر المباشر ، وإلا فاختر التناظر الناقل.
- إذا لم تكن بحاجة إلى توسيع شبكتك لخدمات G Suite أو Google Cloud APIs، ولكنك ترغب في توسيع مدى وصول شبكتك إلى GCP، فأنت تريد اختيار إحدى خدمات Interconnect.
- إذا لم تتمكن من مقابلة Google في إحدى منشآتها ذات الموقع المشترك ، فاختر Cloud VPN أو الاتصال البيني للشريك.
- سيعتمد هذا الاختيار على عرض النطاق الترددي ومتطلبات التشفير جنبًا إلى جنب مع الغرض من الاتصال.
- على وجه التحديد ، إذا كانت لديك احتياجات متواضعة للنطاق الترددي.
- فسنستخدم الاتصال لفترات قصيرة وتجارب ونطلب قناة مشفرة ، ونختار Cloud VPN.

- اختيار الاتصال

- وإلا اختر اتصال الشريك.
- إذا كان بإمكانك مقابلة Google في إحدى منشآتها ذات الموقع المشترك ، فيمكنك الانتقال إلى الاتصال البيني المخصص.
- ومع ذلك ، إذا لم تتمكن من توفير آلية التشفير الخاصة بك لحركة المرور الحساسة ، أو تشعر أن اتصال 10 جيجابت في الثانية كبير جدًا ، أو تريد الوصول إلى سحابات متعددة ، فستحتاج إلى التفكير في VPN السحابي أو الاتصال البيني الشريك بدلاً من ذلك.

مشتركة VPC و VPC Peering

- دعنا ننقل انتباهنا من الاتصال الهجين إلى شبكات VPC المشتركة. في أبسط بيئة سحابية ، قد يكون لمشروع واحد شبكة VPC واحدة تغطي العديد من المناطق مع مثيلات VM التي تستضيف تطبيقات كبيرة ومعقدة للغاية.
- ومع ذلك ، تنشر العديد من المؤسسات بشكل عام عدة مشاريع منفصلة مع شبكات VPC وشبكات فرعية متعددة.
- في هذا الدرس ، سنغطي تهيئتين لمشاركة شبكات VPC عبر مشاريع GCP.
- أولاً ، سننتقل إلى VPC المشترك ، والذي يسمح لك بمشاركة شبكة عبر العديد من المشاريع في مؤسسة GCP الخاصة بك.
- ثم سننتقل إلى نظير شبكة VPC، والذي يسمح لك بتكوين اتصالات خاصة عبر المشاريع في نفس المؤسسات أو مؤسسات مختلفة.
- يسمح VPC المشترك للمؤسسة بتوصيل الموارد من مشاريع متعددة بشبكة VPC مشتركة ، يسمح هذا للموارد بالتواصل مع بعضها البعض بشكل آمن وفعال باستخدام عناوين IP الداخلية من تلك الشبكة.
- مثال في هذا الرسم التخطيطي توجد شبكة واحدة تنتمي إلى مشروع خدمة تطبيق الويب.



مشتركة VPC و VPC Peering

- تتم مشاركة هذه الشبكة مع ثلاثة مشاريع أخرى ، وهي خدمة التوصية وخدمة التخصيص وخدمة التحليلات.
- يحتوي كل مشروع من مشاريع الخدمة هذه على مثيلات موجودة في نفس الشبكة مثل خادم تطبيق الويب وتسمح بالاتصال الخاص بهذا الخادم باستخدام عناوين IP الداخلية.
- يتصل خادم تطبيق الويب بالعملاء والمحليين باستخدام عنوان IP الخارجي للخادم. على النقيض من ذلك ، لا يمكن الوصول إلى خدمات الواجهة الخلفية خارجيًا لأنها تتواصل فقط باستخدام عناوين IP الداخلية.
- عند استخدام VPC المشترك ، فإنك تقوم بتعيين مشروع كمشروع مضيف وإرفاق مشروع خدمة آخر أو أكثر به. في هذه الحالة ، يكون مشروع خدمة تطبيقات الويب هو المشروع المضيف والمشاريع الثلاثة الأخرى هي مشاريع الخدمة. تسمى شبكة VPC الإجمالية شبكة VPC المشتركة.
- على النقيض من ذلك ، تتيح شبكة VPC اتصال RFC 1918 الخاص عبر شبكتي VPC.
- بغض النظر عما إذا كانت تنتمي إلى نفس المشروع أو نفس المؤسسة.

مشتركة VPC و VPC Peering

- الآن ، تذكر أن كل شبكة VPC سيكون لها قواعد جدار حماية تحدد حركة المرور المسموح بها أو المرفوضة بين الشبكات. على سبيل المثال ، في هذا الرسم البياني ، توجد منظمتان تمثلان مستهلكًا ومنتجًا على التوالي. لكل مؤسسة عقدة مؤسسية خاصة بها ، وشبكة VPC، ومثيلات الآلة الافتراضية ، ومسؤول الشبكة ، ومسؤول المثيل.
- من أجل إنشاء شبكة VPC بشكل ناجح ، يحتاج مسؤول شبكة المنتج إلى محض شبكة المنتج مع شبكة المستهلك ويحتاج مسؤول شبكة المستهلك إلى إقران شبكة المستهلك بشبكة المنتج. عندما يتم إنشاء كل من وصلات التناظر ، تصبح جلسة نظير شبكة VPC نشطة ويتم تبادل المسارات.
- يسمح هذا لمثيلات الجهاز الظاهري بالاتصال بشكل خاص باستخدام عناوين IP الداخلية الخاصة بها. التناظر الشبكي VPC هو نهج لامركزي أو موزع لشبكات متعددة المشاريع.
- نظرًا لأن كل شبكة VPC قد تظل تحت سيطرة مجموعات المسؤولين المنفصلة
- وتحتفظ بجدار الحماية العالمي وجداول التوجيه الخاصة بها.

مشتركة VPC و VPC Peering

- تاريخيًا ، كانت مثل هذه المشاريع تنظر في عناوين IP الخارجية أو شبكات VPN لتسهيل الاتصال الخاص بين شبكات VPC.
- ومع ذلك ، فإن نظير شبكة VPC لا يتحمل عيوب زمن انتقال الشبكة والأمان والتكلفة الموجودة عند استخدام عناوين IP الخارجية أو شبكات VPN.
- الآن بعد أن تحدثنا عن نظير شبكة VPC و VPC المشتركة ، اسمح لي بمقارنة كل من هذه التكوينات لمساعدتك في تحديد أيهما مناسب لموقف معين. إذا كنت ترغب في تكوين اتصال خاص بين شبكات VPC في مؤسسات مختلفة ، فيجب عليك استخدام نظير شبكة VPC، حيث يعمل VPC المشترك فقط داخل نفس المؤسسة.
- بشكل مشابه إلى حد ما ، إذا كنت ترغب في تكوين اتصال خاص بين شبكات VPC في نفس المشروع ، فيجب عليك استخدام نظارة شبكة VPC.

- **مشتركة** VPC و VPC Peering

- هذا لا يعني أن الشبكات يجب أن تكون في نفس المشروع ، ولكن يمكن أن تكون ، VPC المشتركة تعمل فقط عبر المشاريع.
- في رأيي ، يتمثل الاختلاف الأكبر بين التكوينين في نماذج إدارة الشبكة.
- VPC المشتركة هي نهج مركزي لشبكات متعددة المشاريع.
- لأن الأمن وسياسة الشبكة تحدث في شبكة VPC المعينة الفردية.
- على النقيض من ذلك ، فإن نظير شبكة VPC هو نهج لامركزي ، لأن كل شبكة VPC يمكن أن تظل تحت سيطرة مجموعات المسؤولين المنفصلة وتحافظ على جدار الحماية العالمي وجداول التوجيه الخاصة بها.

- **ما هو الغرض من الشبكات الخاصة الافتراضية (VPN)؟**
  - إنها طريقة لاكتشاف الدخلاء على حافة حدود الشبكة.
  - تسمى شبكات VPN أيضًا قوائم التحكم في الوصول ، أو قوائم ACL، وهي تحد من الوصول إلى الشبكة.
  - لتمكين طريقة اتصال آمنة (نفق) لتوصيل بيئتين موثوقتين من خلال بيئة غير موثوق بها ، مثل الإنترنت.
  - الغرض الرئيسي هو تشفير البيانات بحيث يمكن تخزينها بتنسيق مشفر.

- **ما هي خدمة Google Cloud Interconnect التي تتطلب اتصالاً في موقع مشترك في Google Cloud وتوفر 10 جيجابت في الثانية لكل رابط؟**
  - التناظر المباشر
  - التناظر الناقل
  - ربط الشريك
  - ربط مخصص
  - Cloud VPN

- **إذا لم تتمكن من تلبية متطلبات التناظر من Google، فما خدمة الاتصال بالشبكة التي يجب أن تختارها للاتصال بـ Google Workspaceو YouTube؟**
  - التناظر المباشر
  - ربط مخصص
  - ربط الشريك
  - التناظر الناقل

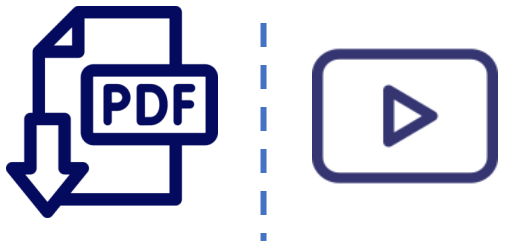
- **أي من الأساليب التالية للتواصل متعدد المشاريع يستخدم نموذج إدارة شبكة مركزية؟**
  - التناظر شبكة VPC
  - مشترك VPC
  - Cloud VPN

مراجعة الوحدة

- في هذه الوحدة ، نظرنا في خمس طرق مختلفة لربط بنيتك التحتية بـ GCP وهي Dedicated Interconnect و Partner Interconnect و Cloud VPN و Direct Peering و Carrier Peering.
- كما قدمت لك بعض الإرشادات حول كيفية الاختيار بين الخدمات المختلفة.
- تذكر ، قد تبدأ في استخدام خدمة واحدة وعندما تتغير متطلباتك أو تفتح مرافق الموقع المشترك الجديدة ، يمكنك التبديل إلى خدمة مختلفة.
- لقد قدمت لك أيضًا نظرة عامة موجزة عن نظير شبكة VPC و VPC المشتركة وهما تكوينان لمشاركة شبكات VPC عبر مشاريع GCP.

نظرة عامة عن الوحدة

- في هذه الوحدة ، نركز على موازنة الحمل والموازنة التلقائية. يمنحك Cloud Load Balancing القدرة على توزيع موارد الحوسبة المتوازنة في مناطق فردية أو متعددة لتلبية متطلبات التوافر العالية ، ووضع مواردك خلف عنوان IPواحد لأي بث ، ولتوسيع نطاق مواردك أو خفضها باستخدام القياس التلقائي الذكي. باستخدام Cloud Load Balancing، يمكنك تقديم المحتوى في أقرب مكان ممكن للمستخدمين على نظام يمكنه الرد على أكثر من مليون استفسار في الثانية.
- Cloud Load Balancing عبارة عن خدمة موزعة بالكامل ومدارة بواسطة البرامج. لا يعتمد على المثيل أو الجهاز ، لذلك لا تحتاج إلى إدارة البنية التحتية المادية لموازنة الحمل. يقدم GCP أنواعًا مختلفة من موازنات الأحمال التي يمكن تقسيمها إلى فئتين ، عالمية وإقليمية. موازين التحميل العام هي HTTP، و HTTPS، ووكيل SSL، وموازن تحميل بروكسي TCP.

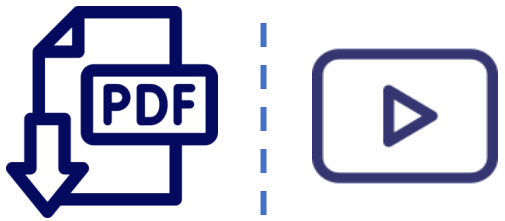


نظرة عامة عن الوحدة

- تعمل موازنات الأحمال هذه على الاستفادة من واجهات Google الأمامية ، وهي أنظمة موزعة معرّفة بالبرمجيات تقع في نقطة تواجد Googleويتم توزيعها عالميًا. لذلك ، تريد استخدام موازن تحميل عام عندما يتم توزيع المستخدمين والطبعات بشكل عام ، ويحتاج المستخدمون لديك إلى الوصول إلى نفس التطبيق والمحتوى ، وتريد توفير الوصول باستخدام عنوان IPواحد لكل بث.
موازنات التحميل الإقليمية هي موازين التحميل الداخلي والشبكة ، وتقوم بتوزيع حركة المرور على المثيلات الموجودة في منطقة GCPواحدة. يستخدم موازن التحميل الداخلي Andromeda، وهو مكدس المحاكاة الافتراضية للشبكة المعرفة بالبرمجيات في GCP، ويستخدم موازن تحميل الشبكة Maglev، وهو نظام برمجي كبير وموزع.
- يوجد أيضًا موازن تحميل داخلي آخر لحركة مرور HTTP و HTTPS موازن التحميل السادس هو موازن تحميل إقليمي للطبقة 7 قائم على الوكيل.
- والذي يمكّنك من تشغيل خدماتك وتوسيع نطاقها خلف عنوان IP خاص لموازنة التحميل.

نظرة عامة عن الوحدة

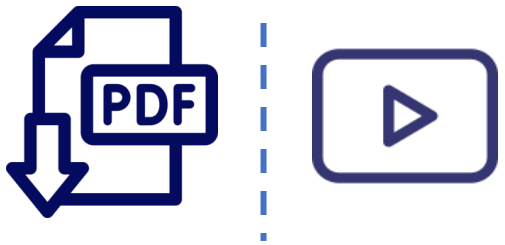
- لا يمكن الوصول إليه إلا في منطقة موازن التحميل في شبكة VPC الخاصة بك. في هذه الوحدة ، سنغطي الأنواع المختلفة لموازنات التحميل المتوفرة في GCP.
- سننتقل أيضًا إلى مجموعات المثيلات المُدارة وتكوينات القياس التلقائي الخاصة بها ، والتي يمكن استخدامها بواسطة تكوينات موازنة التحميل هذه.
- سوف تستكشف العديد من الميزات والخدمات المغطاة عبر معملين لهذه الوحدة.
- وسأنهي الأمور من خلال مساعدتك في تحديد موازن تحميل GCP الذي يلبي احتياجاتك بشكل أفضل.
- لنبدأ بالحديث عن مجموعات المثيل المُدارة.



الملف تفاعلي قم بالنقر على الأيقونة

مجموعات المثيل المُدارة

- مجموعة المثيلات المُدارة هي مجموعة مثيلات VM متطابقة تتحكم فيها ككيان واحد باستخدام قالب مثيل. يمكنك بسهولة تحديث جميع المثيلات في المجموعة عن طريق تحديد قالب جديد في تحديث متجدد. أيضًا ، عندما تتطلب تطبيقاتك موارد حساب إضافية ، يمكن لمجموعات المثيلات المُدارة التوسع تلقائيًا إلى عدد المثيلات في المجموعة. يمكن لمجموعات المثيلات المُدارة العمل مع خدمات موازنة التحميل لتوزيع حركة مرور الشبكة على جميع الطبعات في المجموعة. إذا توقف مثيل في المجموعة أو سحق أو تم حذفه من خلال إجراء آخر غير أوامر مجموعة المثيل ، فإن مجموعة المثيل المُدارة تعيد إنشاء المثيل تلقائيًا حتى تتمكن من استئناف مهام المعالجة الخاصة بها.
- يستخدم المثيل المعاد إنشاؤه نفس الاسم ونفس قالب المثيل مثل المثيل السابق. يمكن لمجموعات المثيل المُدارة تحديد المثيلات غير الصحية وإعادة إنشائها تلقائيًا في مجموعة لضمان تشغيل جميع المثيلات على النحو الأمثل.

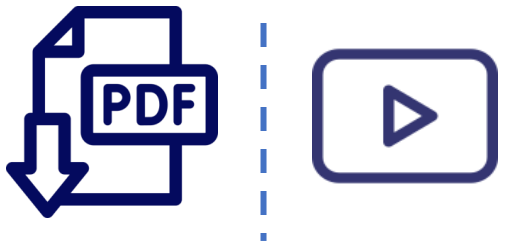


مجموعات المثيل المُدارة

- يوصى عمومًا بمجموعات المثيلات الإقليمية المُدارة عبر مجموعات المثيلات المُدارة من قبل المنطقة لأنها تسمح لك بتوزيع حمل التطبيق عبر مناطق متعددة بدلاً من حصر تطبيقك في منطقة واحدة أو جعلك تدير مجموعات مثيلات متعددة عبر مناطق مختلفة. يحمي هذا النسخ المتماثل من حالات فشل المنطقة والسيناريوهات غير المتوقعة حيث تتعطل مجموعة كاملة من الحالات في منطقة واحدة. إذا حدث ذلك ، يمكن لتطبيقك متابعة خدمة حركة المرور من المثيلات التي تعمل في منطقة أخرى في نفس المنطقة. لإنشاء مجموعة مثيل مُدارة ، تحتاج أولاً إلى إنشاء قالب مثيل. بعد ذلك ، ستنشئ مجموعة مثيل مُدارة من Nمثيلات محددة. يقوم مدير مجموعة المثيل تلقائيًا بتعبئة مجموعة المثيل استنادًا إلى قالب المثيل.
- يمكنك بسهولة إنشاء قوالب مثيل باستخدام وحدة التحكم السحابية. يشبه مربع حوار قالب المثيل ويعمل تمامًا مثل إنشاء مثيل ، باستثناء أنه يتم تسجيل الاختيارات بحيث يمكن تكرارها.
- .

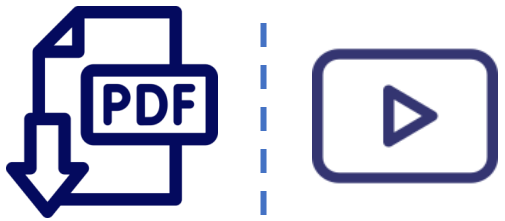
مجموعات المثيل المُدارة

- عند إنشاء مجموعة مثيل ، فإنك تحدد القواعد المحددة لمجموعة المثيل هذه.
- أولاً ، عليك أن تقرر نوع مجموعة المثيلات المُدارة التي تريد إنشاءها. يمكنك استخدام مجموعات المثيلات المُدارة للخدمة عديمة الحالة أو أحمال العمل المجمعة ، مثل الواجهة الأمامية لموقع الويب أو معالجة الصور من قائمة انتظار ، أو للتطبيقات ذات الحالة ، مثل قواعد البيانات أو التطبيقات القديمة.
- ثانيًا ، قم بتوفير اسم لمجموعة المثيل.
- ثالثًا ، حدد ما إذا كانت مجموعة المثيل ستكون مفردة أو متعددة المناطق وأين ستكون هذه المواقع. يمكنك اختياريًا تقديم تفاصيل تعيين اسم المنفذ.



مجموعات المثيل المُدارة

- رابعًا ، حدد قالب المثيل الذي تريد استخدامه.
- خامسًا ، حدد ما إذا كنت تريد التوسع التلقائي وتحت أي ظروف.
- أخيرًا ، ضع في اعتبارك إنشاء فحص صحي لتحديد الحالات السليمة والتي يجب أن تتلقى زيارات.
- بشكل أساسي ، تقوم بإنشاء أجهزة افتراضية ، لكنك تطبق المزيد من القواعد على مجموعة المثيل تلك.



الفحص الذاتي والفحوصات الصحية

- اسمحوا لي أن أقدم مزيدًا من التفاصيل حول تحجيم الفنان والفحوصات الصحية لمجموعة المثيلات المُدارة. كما ذكرت سابقًا ، توفر مجموعات المثيلات المُدارة إمكانات تحجيم تلقائية تتيح لك إضافة مثيلات أو إزالتها تلقائيًا من مجموعة مثيلات مُدارة. بناء على زيادة أو نقصان الحمل. يساعد القياس التلقائي تطبيقاتك بأمان على التعامل مع الزيادة في حركة المرور وتقليل التكاليف عندما تكون الحاجة إلى الموارد أقل. لقد حددت للتو سياسة القياس التلقائي ويقوم جهاز القياس التلقائي بإجراء القياس التلقائي بناءً على الحمل المقاس. تشمل سياسات القياس التلقائي المطبقة التوسع استنادًا إلى استخدام وحدة المعالجة المركزية أو سعة موازنة الحمل أو مقاييس المراقبة أو عن طريق أعباء العمل القائمة على قائمة الانتظار مثل انتفاخات السحابة.
- على سبيل المثال ، لنفترض أن لديك حالتين تستخدمان وحدة المعالجة المركزية بنسبة 100٪ و 85٪ كما هو موضح في هذه الشريحة.
- إذا كان استخدام وحدة المعالجة المركزية المستهدفة هو 75٪ .

الفحص الذاتي والفحوصات الصحية

- فإن أداة القياس التلقائي ستضيف مثيلاً آخر لتوزيع حمل وحدة المعالجة المركزية والبقاء أقل من 75٪ من استخدام وحدة المعالجة المركزية المستهدفة. وبالمثل ، إذا كان الحمل الإجمالي أقل بكثير من الهدف ، فسيقوم جهاز القياس التلقائي بإزالة المثيلات طالما أن ذلك يحافظ على الاستخدام الكلي أقل من الهدف. الآن قد تسأل نفسك كيف يمكنني مراقبة استخدام مجموعة المثيل الخاصة بي. عند النقر فوق مجموعة مثيل أو حتى جهاز افتراضي فردي ، يتم تقديم رسم بياني. بشكل افتراضي ، سترى استخدام وحدة المعالجة المركزية خلال الساعة الماضية ولكن يمكنك تغيير الإطار الزمني وتصور مقاييس أخرى مثل استخدام القرص والشبكة. هذه الرسوم البيانية مفيدة جدًا لمراقبة استخدام المثيلات الخاصة بك ولتحديد أفضل السبل لتكوين سياسة القياس التلقائي الخاصة بك لتلبية الطلبات المتغيرة.
- إذا كنت تراقب استخدام مثيلات الآلة الافتراضية الخاصة بك ومراقبة برنامج تشغيل المكدس.
- يمكنك حتى إعداد التنبيهات من خلال عدة قنوات إعلام.
- لمزيد من المعلومات حول القياس التلقائي. انظر قسم الروابط في هذا الفيديو.

الفحص الذاتي والفحوصات الصحية

- هناك تكوين مهم آخر لمجموعة مثيل مُدارة وموازن التحميل وهو فحص الصحة.
- الفحص الصحي مشابه جدًا لبرنامج تشغيل المكدس لتسجيل وقت التشغيل.
- ما عليك سوى تحديد منفذ البروتوكول والمعايير الصحية كما هو موضح في لقطة الشاشة. استنادًا إلى هذه التهيئة ، يحسب برنامج "شركاء Google المعتمدون" حالة صحية لكل حالة.
- تحدد المعايير الصحية عدد المرات التي يجب فيها التحقق مما إذا كانت الحالة صحية أم لا.
- هذه هي فترة الفحص. كم من الوقت لانتظار الرد. هذا هو الوقت المستقطع.
- كم عدد المحاولات الناجحة الحاسمة. هذه هي العتبة الصحية وعدد المحاولات الفاشلة الحاسمة.
- هذه هي العتبة غير الصحية. في المثال الموجود في هذه الشريحة.
- يجب أن يفشل فحص الصحة مرتين على مدار 15 ثانية قبل اعتبار المثيل غير صحي.

نظرة عامة على موازنة تحميل HTTP (S)

- الآن ، دعنا نتحدث عن HTTPS Load Balancing الذي يعمل في الطبقة السابعة من نموذج OSI.
- هذه هي طبقة التطبيق التي تتعامل مع المحتوى الفعلي لكل رسالة مما يسمح باتخاذ قرارات التوجيه بناءً على عنوان URL.
- توفر موازنة تحميل HTTPS في GCP موازنة تحميل شاملة لطلبات HTTPS المخصصة لمثيلاتك. هذا يعني أن تطبيقاتك متاحة لعملائك على أي عنوان IP واحد ، مما يبسط إعداد DNS الخاص بك.
- تعمل موازنة تحميل HTTPS على موازنة حركة مرور HTTP و HTTPS عبر مثيلات خلفية متعددة وعبر مناطق متعددة.
- يتم تحميل طلبات HTTP بشكل متوازن على المنفذ 80 أو 8080 ، ويتم موازنة تحميل طلبات HTTPS على المنفذ 443.
- تدعم موازنات التحميل هذه عملاء IPv4 و IPv6، وهي قابلة للتطوير ، ولا تتطلب تدفئة مسبقة ، وتمكّن التحميل المستند إلى المحتوى وعبر المناطق موازنة.

نظرة عامة على موازنة تحميل HTTP (S)

- يمكنك تكوين خرائطك الخاصة التي توجه بعض عناوين URL إلى مجموعة واحدة من الحالات وتوجه عناوين URL الأخرى إلى مثيلات أخرى.
- يتم توجيه الطلبات بشكل عام إلى مجموعة المثيلات الأقرب إلى المستخدم.
- إذا لم يكن لدى أقرب مجموعة مثيل سعة كافية ، فسيتم إرسال الطلب إلى أقرب مجموعة مثيل تالية لديها السعة.
- سوف تحصل على استكشاف معظم هذه الفوائد في المعمل الأول للوحدة.
- اسمحوا لي أن أتصفح البنية الكاملة لموازن تحميل HTTPS باستخدام هذا الرسم التخطيطي.
- تقوم قاعدة إعادة التوجيه العالمية بتوجيه الطلبات الواردة من الإنترنت إلى وكيل HTTP مستهدف.
- يتحقق وكيل HTTP الهدف من كل طلب مقابل خريطة عنوان URL.
- لتحديد الخدمة الخلفية المناسبة للطلب.

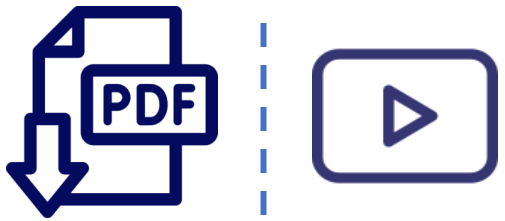
الملف تفاعلي قم بالنقر على الأيقونة

نظرة عامة على موازنة تحميل HTTP (S)

- على سبيل المثال ، يمكنك إرسال طلبات الصوت المائل www.example.com إلى خدمة خلفية واحدة ، والتي تحتوي على مثيلات مهيأة لتقديم ملفات صوتية ، وطلب www.example.com فيديو مائل إلى خدمة خلفية أخرى تحتوي على مثيلات تم تكوينها لتقديم ملفات الفيديو.
- تقوم خدمة الواجهة الخلفية بتوجيه كل طلب إلى خلفية مناسبة بناءً على حل منطقة السعة والمثيل الموجود للخلفيات المرفقة به.
- تحتوي خدمات الواجهة الخلفية على فحص صحي وتقارب الجلسة وإعداد المهلة وواحد أو أكثر من الخلفيات الخلفية. يسحب فحص الصحة المثيلات المرفقة بخدمة الواجهة الخلفية في فترات زمنية تم تكوينها.
- يُسمح للحالات التي تجتاز الفحص الصحي بتلقي طلبات جديدة. لا يتم إرسال طلبات الحالات غير الصحية حتى تعود إلى الحالة الصحية مرة أخرى.
- عادةً ما تستخدم موازنة تحميل HTTPS خوارزمية round robin لتوزيع الطلبات بين المثيلات المتاحة.

نظرة عامة على موازنة تحميل HTTP (S)

- يمكن تجاوز هذا بتقارب الجلسة. يحاول تقارب الجلسة إرسال جميع الطلبات من نفس العميل إلى نفس مثيل الجهاز الظاهري. تحتوي خدمات الواجهة الخلفية أيضًا على إعداد مهلة ، والذي يتم تعيينه على 30 ثانية بشكل افتراضي. هذا هو مقدار الوقت الذي ستنتظره خدمة الواجهة الخلفية على الواجهة الخلفية قبل اعتبار الطلب فاشلاً. هذه مهلة ثابتة وليست مهلة خاملة. إذا كنت تحتاج إلى اتصالات أطول عمراً ، فقم بتعيين هذه القيمة بشكل مناسب. تحتوي الخلفيات نفسها على مجموعة مثيل ، ووضع موازنة ، وعدد قياسي للقدرة. تحتوي مجموعة مثيل على مثيلات Virtual Machine.
- قد تكون مجموعة المثيلات مجموعة مثيل مُدارة مع أو بدون قياس تلقائي أو مجموعة مثيل غير مُدارة. يخبر وضع الموازنة نظام موازنة التحميل بكيفية تحديد متى تكون الواجهة الخلفية عند الاستخدام الكامل. إذا كانت الخلفيات القديمة لخدمة الواجهة الخلفية في منطقة ما قيد الاستخدام الكامل.



نظرة عامة على موازنة تحميل HTTP (S)

- يتم توجيه الطلبات الجديدة تلقائيًا إلى أقرب منطقة لا يزال بإمكانها التعامل مع الطلبات. يمكن أن يعتمد وضع الموازنة على استخدام وحدة المعالجة المركزية أو الطلبات في الثانية.
- يعد إعداد السعة عنصر تحكم إضافي يتفاعل مع إعداد وضع الموازنة. على سبيل المثال ، إذا كنت تريد عادةً أن تعمل مثيلاتك بحد أقصى 80 في المائة من استخدام وحدة المعالجة المركزية ، فستضبط وضع التوازن على 80 في المائة من استخدام وحدة المعالجة المركزية وقدرتك على 100 في المائة.
- إذا كنت ترغب في خفض استخدام المثيل إلى النصف ، فيمكنك ترك وضع التوازن عند 80 بالمائة من استخدام وحدة المعالجة المركزية وتعيين السعة على 50 بالمائة. الآن ، أي تغييرات على خدمات الواجهة الخلفية الخاصة بك ليست فورية.
- لذلك لا تتفاجأ إذا استغرق نشر التغييرات عبر الشبكة عدة دقائق.

- مثال: موازن تحميل HTTP

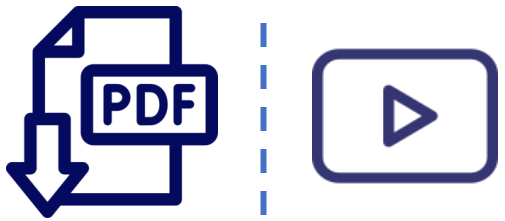
- اسمحوا لي أن أعمل من خلال موازن تحميل HTTP في العمل. يحتوي المشروع الموجود في هذه الشريحة على عنوان IP عالمي واحد ، ولكن يدخل المستخدمون إلى شبكة Google Cloud من موقعين مختلفين ، أحدهما في أمريكا الشمالية والآخر في أوروبا والشرق الأوسط وإفريقيا. أولاً ، تقوم قاعدة إعادة التوجيه العالمية بتوجيه الطلبات الواردة إلى وكيل HTTP المستهدف.
- يتحقق الوكيل من خريطة URL لتحديد الخدمة الخلفية المناسبة للطلب.
- في هذه الحالة ، نحن نخدم تطبيق سجل الزوار مع خدمة خلفية واحدة فقط.
- تحتوي الخدمة الخلفية على طرفين ، أحدهما في وسط الولايات المتحدة 1-أ ، والآخر في أوروبا الغربية 1-د. تتكون كل من هذه النهايات الخلفية من مجموعة مثيل مُدارة.
- الآن ، عندما يأتي طلب المستخدم ، تحدد خدمة موازنة التحميل الأصل التقريبي للطلب من عنوان IP المصدر.

- مثال: موازن تحميل HTTP

- تعرف خدمة موازنة التحميل أيضًا مواقع المثيلات المملوكة للخدمة الخلفية ، وسعتها الإجمالية واستخدامها الحالي الإجمالي. لذلك ، إذا كانت المثيلات الأقرب إلى المستخدم ذات سعة متاحة ، فسيتم إعادة توجيه الطلب إلى أقرب مجموعة من المثيلات. في مثالنا ، ستتم إعادة توجيه حركة المرور من المستخدم في أمريكا الشمالية إلى مجموعة المثيلات المُدارة في US Central 1-a، وسيتم توجيه حركة المرور من المستخدم في أوروبا والشرق الأوسط وإفريقيا إلى مجموعة المثيلات المُدارة في أوروبا الغربية 1- .d. إذا كان هناك العديد من المستخدمين في كل منطقة ، فسيتم توزيع الطلبات الواردة إلى المنطقة المحددة بالتساوي عبر جميع الخدمات الخلفية المتاحة والطبعات الموجودة في تلك المنطقة.
- في حالة عدم وجود مثيلات سليمة ، مع السعة المتاحة في منطقة معينة ، يقوم موازن التحميل بدلاً من ذلك بإرسال الطلب إلى أقرب منطقة تالية ذات سعة متاحة. لذلك.

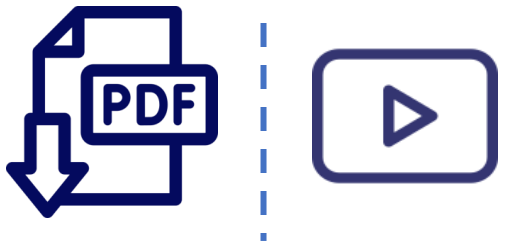
- مثال: موازن تحميل HTTP

- يمكن إعادة توجيه حركة المرور من مستخدم منطقة أوروبا والشرق الأوسط وإفريقيا إلى الواجهة الخلفية المركزية 1- aالأمريكية ، إذا كانت الواجهة الخلفية أوروبا الغربية 1-د لا تحتوي على سعة ، أو لا توجد بها حالات صحية على النحو الذي يحدده مدقق الصحة. يشار إلى هذا باسم موازنة التحميل عبر المناطق. مثال آخر ، لموازن تحميل HTTPS، هو موازن تحميل يعتمد على المحتوى.
- في هذه الحالة ، توجد خدمتان منفصلتان للجهة الخلفية تتعاملان مع حركة مرور الويب أو الفيديو.
- يتم تقسيم حركة المرور بواسطة موازن التحميل استنادًا إلى عنوان URL كما هو محدد في خريطة URL، إذا كان المستخدم يتنقل إلى مقطع فيديو مائل ، يتم إرسال حركة المرور إلى خدمة الفيديو الخلفية وإذا كان المستخدم يتنقل في أي مكان آخر ، فإن حركة المرور يتم إرساله إلى النهاية الخلفية لخدمة الويب.
- يتم تحقيق كل ذلك باستخدام عنوان IP عالمي واحد.



موازنة تحميل HTTP (S)

- يحتوي موازن تحميل HTTP (S) على نفس البنية الأساسية مثل موازن تحميل HTTP، ولكنه يختلف بالطرق التالية: يستخدم موازن تحميل HTTP (S) وكيل HTTPS مستهدفًا بدلاً من وكيل HTTP مستهدف.
- يتطلب موازن تحميل HTTP (S) تثبيت شهادة SSLموقعة مرة واحدة على الأقل على وكيل HTTPS الهدف لموازن التحميل.
- تنتهي جلسات SSL للعميل عند موازن التحميل. تدعم موازين تحميل HTTP (S) بروتوكول طبقة النقل QUIC. QUIC هو بروتوكول طبقة نقل يسمح ببدء اتصال العميل بشكل أسرع ، ويزيل حجب رأس الخط في التدفقات متعددة الإرسال ، ويدعم ترحيل الاتصال عندما يتغير عنوان IP الخاص بالعميل.
- لمزيد من المعلومات حول بروتوكول QUIC، راجع الارتباط الموجود في موارد الدورة التدريبية.
- لاستخدام HTTPS، يجب عليك إنشاء شهادة SSL واحدة على الأقل.
- يمكن استخدامها بواسطة الوكيل الهدف لموازن التحميل.



موازنة تحميل HTTP (S)

- يمكنك تكوين الخادم الوكيل المستهدف بما يصل إلى 15 شهادة SSL لكل شهادة SSL، تقوم أولاً بإنشاء مورد شهادة SSL، والذي يحتوي على معلومات شهادة SSL.
- تُستخدم موارد شهادة SSL فقط مع وكلاء موازنة التحميل مثل وكيل HTTPS المستهدف أو وكيل SSL المستهدف ، والذي سنناقشه لاحقًا في هذه الوحدة.
- تسمح لك حاويات الواجهة الخلفية باستخدام حاويات Google Cloud Storage مع موازنة تحميل HTTP (S).
- يستخدم موازن تحميل HTTP (S) خارجي مخطط URL لتوجيه حركة المرور من عناوين URL المحددة إما إلى خدمة خلفية أو حاوية خلفية.

الملف تفاعلي قم بالنقر على الأيقونة

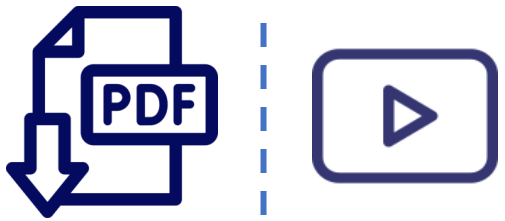
موازنة تحميل HTTP (S)

- إحدى حالات الاستخدام الشائعة هي: إرسال طلبات المحتوى الديناميكي ، مثل البيانات ، إلى خدمة الواجهة الخلفية ؛ وإرسال طلبات المحتوى الثابت ، مثل الصور ، إلى حاوية الخلفية. في هذا الرسم التخطيطي ، يرسل موازن التحميل حركة مرور بمسار / love-to-fetch / إلى حاوية تخزين Cloud في منطقة أوروبا الشمالية. تذهب جميع الطلبات الأخرى إلى حاوية التخزين السحابي في منطقة شرق الولايات المتحدة.
- بعد تكوين موازن تحميل مع حاويات الواجهة الخلفية ، يتم إرسال الطلبات إلى مسارات URL لتبدأ بـ / love-to-fetch / إلى حاوية التخزين السحابية في أوروبا الشمالية ، ويتم إرسال جميع الطلبات الأخرى إلى التخزين السحابي الأمريكي الشرقي دلو. مجموعة نقطة نهاية الشبكة ، أو NEG، هي كائن تكوين يحدد مجموعة من نقاط النهاية الخلفية أو الخدمات.
- حالة الاستخدام الشائعة لهذا التكوين هي نشر الخدمات في الحاويات.

الملف تفاعلي قم بالنقر على الأيقونة

موازنة تحميل HTTP (S)

- يمكنك أيضًا توزيع حركة المرور بطريقة دقيقة على التطبيقات التي تعمل على مثيلات الواجهة الخلفية. يمكنك استخدام NEGs كخلفية لبعض موازين التحميل ومع مدير المرور. تحدد NEGs الخاصة بالمناطق والإنترنت كيفية الوصول إلى نقاط النهاية ، وما إذا كان يمكن الوصول إليها ، وأين تقع. على عكس أنواع NEG هذه ، لا تحتوي NEGs التي لا تحتوي على خوادم على نقاط نهاية.
- تحتوي NEG النطاقية على نقطة نهاية واحدة أو أكثر يمكن أن تكون Compute Engine VMs أو الخدمات التي تعمل على الأجهزة الظاهرية ، يتم تحديد كل نقطة نهاية إما عن طريق عنوان IP أو IP: مجموعة المنافذ. يحتوي Internet NEG على نقطة نهاية واحدة تتم استضافتها خارج Google Cloud ، يتم تحديد نقطة النهاية هذه بواسطة اسم المضيف FQDN: أو IP: المنفذ ، يشير الاتصال الهجين NEG إلى خدمات مدير المرور التي تعمل خارج Google Cloud ، يشير NEG بدون خادم إلى خدمات Cloud Run و App Engine و Cloud Functions ، الموجودة في نفس المنطقة
- مثل NEG ، لمزيد من المعلومات حول استخدام NEGs.
- يرجى الاطلاع على الرابط الموجود في موارد الدورة التدريبية.



- مقدمة المختبر: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

  - دعنا نطبق ما قمنا بتغطيته للتو.
  - في هذا التمرين المعملي ، تقوم بتكوين موازن تحميل HTTP باستخدام القياس التلقائي.
  - على وجه التحديد ، يمكنك إنشاء مجموعتين من مجموعات المثيل المُدارة التي تعمل كخلفية في الولايات المتحدة المركزية الأولى وأوروبا الغربية الأولى.
  - ثم تقوم بإنشاء موازن تحميل واختبار الضغط عليه لإظهار موازنة الحمل الشاملة والقياس التلقائي.

- **معمل – LAB: تكوين موازن تحميل HTTP باستخدام القياس التلقائي**

  - في هذا التمرين المعملي ، تقوم بتكوين موازن تحميل HTTP.
  - بعد ذلك ، يمكنك الضغط على اختبار موازن التحميل لإظهار موازنة الحمل العامة والموازنة التلقائية.
  - نصائح لمختبرات الدورة التدريبية
  - احصل على أقصى استفادة من Coursera و Qwiklabs من خلال تجربة نصائحنا أدناه.
  - تجنب الخلط بين الحساب والتصفح الخاص.
  - أغلق هذه الصفحة وسجل الدخول مرة أخرى إلى Coursera في وضع التصفح المتخفي قبل الانتقال.
  - عند العودة إلى هذه الدورة التدريبية وصفحة الإرشادات المعملية ، انقر فوق "فتح الأداة" للمتابعة.
  - تجنب الخلط بين الحساب والتصفح الخاص.

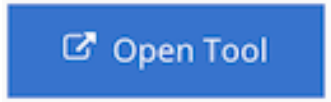
معمل – LAB: العمل مع الأجهزة الافتراضية

- باستخدام وضع التصفح المتخفي ، يضمن ذلك عدم استخدامك لحساب Google الخاص بك عن طريق الخطأ (بما في ذلك Gmail) أثناء الوصول إلى Google Cloud Console.
- يمنع هذا أيضًا Qwiklabs من تسجيل خروجك من حسابات Google الخاصة بك.
- الإرشادات التفصيلية لاستخدام وضع التصفح المتخفي في Google Chrome متوفرة هنا.
- اعتمادًا على المستعرض الخاص بك ، قد يُطلق على وضع التصفح المتخفي أيضًا اسم الاستعراض الخاص أو استعراض InPrivate.

- **معمل – LAB: العمل مع الأجهزة الافتراضية**

- **لضمان الانتهاء من المختبر تم وضع علامة عليه في كورسيرا:**

1. **قم بالوصول إلى كل معمل فردي بالنقر فوق فتح الأداة في كورسيرا**



2. **أكمل المختبر في** Qwiklabs
3. **انقر على "إنهاء المعمل" في** Qwiklabs

4. **أغلق نافذة أو علامة تبويب متصفح** Qwiklabs

- **معمل – LAB: العمل مع الأجهزة الافتراضية**

- **للتفاعل مع المتعلمين الآخرين:**

إذا كنت تواجه أي صعوبة في المعامل ، فنحن نشجعك على النشر عنها في منتديات المناقشة الخاصة بهذه الدورة التدريبية. إذا لم تكن لديك مشاكل مع المعامل ، ففكر في تصفح منتديات المناقشة للحصول على فرص لمساعدة زملائك المتعلمين.

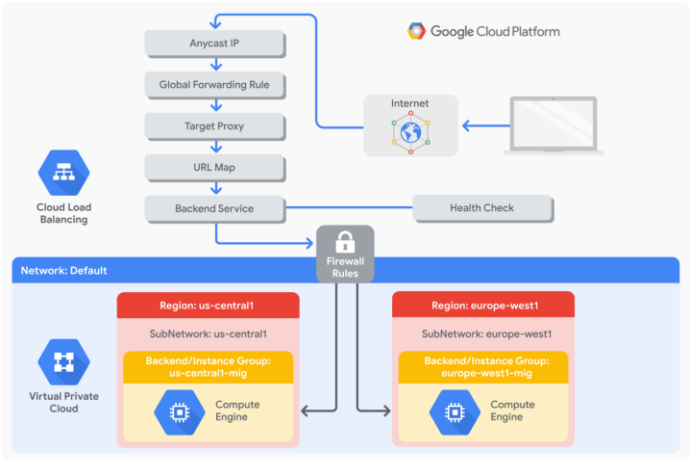
- **لتقديم طلب دعم:**

إذا كنت تواجه مشكلات فنية مع المختبرات أو التصنيف ، فيرجى إرسال طلب دعم هنا:

https://qwiklab.zendesk.com/hc/en-us/requests/new

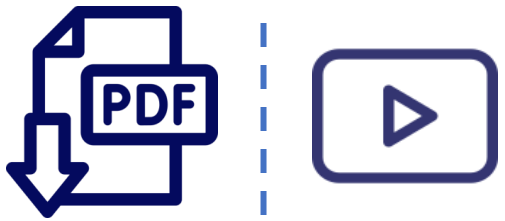
- **معمل** – LAB: Configuring an HTTP Load Balancer with Autoscaling

- **يتم تنفيذ موازنة تحميل** Google Cloud HTTP (S) **على حافة شبكة** Google **في نقاط تواجد** Google (POP) **حول العالم**.
- **تدخل حركة مرور المستخدم الموجهة إلى موازن تحميل** HTTP (S) **بروتوكول** POP **الأقرب للمستخدم ثم يتم موازنة التحميل عبر شبكة** Google **العالمية إلى أقرب واجهة خلفية لديها سعة متاحة كافية**.
- **في هذا التمرين المعملي ، تقوم بتكوين موازن تحميل** HTTP **كما هو موضح في الرسم التخطيطي أدناه**.
- **بعد ذلك ، يمكنك الضغط على اختبار موازن التحميل لإظهار موازنة الحمل العامة والموازنة التلقائية**.



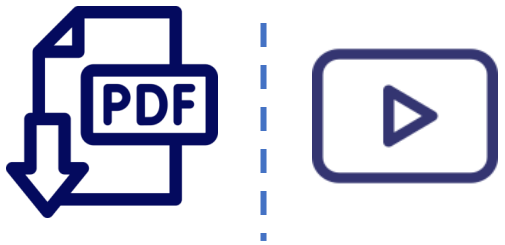
مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- في هذا التمرين المعملي ، قمت بتكوين HTTP Load Balancer مع الخلفيات في الولايات المتحدة المركزية وأوروبا الغربية. ثم تشدد على اختبار موازن التحميل باستخدام VM لإظهار موازنة الحمل العالمية والتوسيع التلقائي. يمكنك البقاء في جولة معملية ، ولكن تذكر أن واجهة مستخدم GCP يمكن أن تتغير ، لذلك قد تبدو بيئتك مختلفة قليلاً. إذن نحن هنا في وحدة تحكم GCP وأول شيء سأفعله هو تهيئة قواعد جدار الحماية HTTP وفحص الصحة. لذا اسمحوا لي أن أمضي قدمًا وأن أفعل ذلك بالانتقال إلى شبكة VPC، وعلى وجه التحديد ، قواعد جدار الحماية. لذلك ستلاحظ أن هناك بالفعل بعض قواعد جدار الحماية هنا لحركة مرور ICMP و RDP و SSH الداخلية.
- هذه هي التي تأتي دائمًا مع الشبكة الافتراضية. سنقوم الآن بإنشاء قاعدة جدار حماية للسماح لـ HTTP لذا اسمحوا لي أن أنشئ قاعدة جدار الحماية. سأقدم له اسمًا. سيكون للشبكة الافتراضية.
- سأحدد العلامات الهدف باستخدام خادم HTTP.



مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- وسيتعين علينا تحديد علامة الهدف هذه في مثيلاتنا لاحقًا. المصدر ، سأقوم بالتعيين على نطاقات IP وتعيينها من أي مكان. ثم يمكنني تحديد منفذ TCP إلى 80. هذا لـ HTTP ثم يمكننا النقر فوق "إنشاء". ثم سننشئ قاعدة جدار حماية مماثلة لمدقق الصحة لدينا. لذا يمكنني فعل ذلك أثناء إنشاء هذه القاعدة. مرة أخرى ، على نفس الشبكة ، سأستخدم نفس العلامات المستهدفة. لذلك فهو ينطبق فقط على الحالات التي تحتوي على هذه العلامة. الآن ، بالنسبة لنطاقات IP، سأكون أكثر تحديدًا. يتم توفير هذه في تعليمات المختبر لك ، ولكن هذه هي نطاقات IP للمدقق الصحي. الآن ، عند إدخالها ، تأكد من إدخال واحد أولاً. يمكنك النقر فوق "الفضاء" ويمكنك أن ترى أنه قد أقر بذلك. بعد ذلك ، يمكنك نسخ نطاق IP الآخر ولصقه ، ثم النقر فوقه ، ويمكنك أن ترى أنه تم التقاطه أيضًا. الآن ، بالنسبة للبروتوكول والمنافذ ، في هذه الحالة ، سنقوم فقط بتحديد كل بروتوكول TCP، ولكن يمكنك تضييق ذلك قليلاً اعتمادًا على نوع الفحص الصحي الذي تقوم به.



مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذا اسمحوا لي أن أنقر على "إنشاء" على ذلك. أثناء إنشاء هذه الصور ، يمكنني الآن إنشاء صورتي المخصصة.
- لذا سأذهب إلى Compute Engine.
- سنقوم بإنشاء VM سنسمي ذلك خادم الويب.
- سأقوم بذلك وأقوم بذلك. يمكنني ترك المنطقة مثل وسط الولايات المتحدة 1 ، المنطقة ، وسط الولايات المتحدة 1-أ.
- سأقوم الآن بتوسيع هذا الخيار هنا ، والإدارة ، والأمان ، والأقراص ، والشبكات ، والإيجار الوحيد. زوجان من الأشياء التي أريد القيام بها أولاً تحت الأقراص. أريد التأكد من عدم حذف هذا القرص عند حذف المثيل. هذا يعمل لأن هذه مجرد أقراص ثابتة ، فهي مجرد شبكة متصلة. على الشبكات ، سأقوم بتعريف علامة الشبكة ، خادم http، وسيكون هذا لشبكتنا الافتراضية. وبهذه الطريقة ، سيتم تطبيق جدران الحماية التي أنشأناها للتو على هذه الحالة.
- لذا اسمح لي بالمضي قدمًا والنقر على "إنشاء".
- بمجرد تشغيل هذا المثال ، سنقوم بتخصيصه عن طريق تثبيت بعض البرامج.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذلك سأنتظر فقط حتى يتم إنشاء المثيل. ذلك هو. يمكنني النقر فوق SSH سأقوم فقط بتشغيل الأوامر الموجودة في تعليمات المختبر. لذلك أولاً ، سأقوم فقط بتثبيت أنبوب Apache، وبعد ذلك سأبدأ خادم Apache بعد ذلك. سنقوم بالتحقق مرة أخرى من هذا الخادم من خلال الانتقال إلى عنوان IP الخارجي الذي لدينا هنا ، ولهذا السبب قمنا بإرفاق قاعدة جدار الحماية لعنوان IP الخارجي.
- لا نحتاج حقًا إلى قاعدة جدار الحماية لمدقق الصحة حتى الآن ، فسيكون ذلك لاحقًا لمثيلاتنا الخلفية ولم نقم بالفعل بتكوين هذا الفحص الصحي حتى الآن ، على أي حال. ها نحن ذا ، لا يزال الاتصال متصلاً ، لذا دعنا نعطيه بضع ثوانٍ. ها نحن ذا. سأقوم بلصق هذين الأمرين هناك.
- دع ذلك يجري.

- مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- ثم سأبدأ الخدمة. لذا دعني الآن أعود إلى وحدة التحكم وانقر على IP خارجي. هنا ، يمكننا رؤية صفحة Apache2 Debian الافتراضية. لذلك نرى أن هذا قد نجح. الآن ، أريد تعيين هذه الخدمة لبدء التشغيل. لذلك هناك أمر لذلك. لذا دعني أعود إلى محطة SSHوألصق في هذا الأمر. الآن ، سأعود إلى Compute Engine، وبالنسبة لخادم الويب ، سأختار إعادة التعيين. نعم ، أريد التأكد من أنني أفعل ذلك ، لذلك سأضغط على إعادة التعيين في هذا التأكيد. لذلك سيتوقف هذا الآن ويعيد تشغيل الجهاز. سأحتفظ بنفس عناوين IP ونفس قرص التمهيد الدائم ، ولكن يتم مسح الذاكرة بشكل أساسي. لذلك ، يجب أن تكون خدمات Apache متاحة بعد إعادة التعيين ، والتحديث ، يجب أن يكون أمر C الخاص بنا ناجحًا. لذلك يمكننا انتظار ذلك. لدينا خياران للتحقق من هذه الحالة.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- يمكننا الانتقال إلى عنوان IP الخارجي أو بمجرد نسخه احتياطيًا ، يمكننا إعادة SSH إلى المثيل وتشغيل أمر للتحقق من الحالة.
- إنه يخبرني أن خدمة Apache تعمل بالفعل. فلنجهز القرص الآن ، وسننشئ صورة مخصصة من ذلك القرص. لذا أولاً ، دعنا نخرج من جلسة SSH دعنا نتحقق مرة أخرى من أن المثيل الذي لدينا هنا يحتوي على قرص مرتبط ، وأن هذا القرص لا يتم حذفه عندما أحذف المثيل. يمكنني التحقق من ذلك بمجرد النقر على اسم المثيل. ثم سأقوم بالتمرير لأسفل إلى حيث يتحدث عن قرص التمهيد الخاص بي ، ها هو. تحت عند حذف المثيل ، فإنه يقول الاحتفاظ بالقرص. إذا لم يكن الأمر كذلك ، فيمكنني النقر فوق "تحرير" ويمكنني تغيير هذا السلوك. في حالتنا ، كل شيء على ما يرام ، لذلك سأقوم "بحذف" المثيل. هنا ، يسألني هل تريد أيضًا حذف هذا القرص الذي لن نفعله في حالتنا.
- لذلك سنقوم بحذف المثال. إذا ذهبت هنا إلى الأقراص ، يمكننا أن نرى أن لدينا القرص نفسه هنا.
- الآن ، يمكننا العودة إلى الحالات ، يمكننا الانتظار حتى يتم حذف هذا ولكن القرص سيبقى.
- إذن ما يمكننا فعله الآن هو المضي قدمًا وإنشاء صورة.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

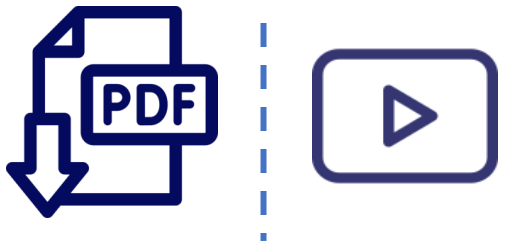
- لذلك سأضغط على قسم الصورة. هنا ، لدينا الصور المتوفرة. سأقوم بإنشاء صورتي المخصصة ، وإعطائها اسمًا. خادم الويب الخاص بي ، سنستخدمه كقرص مصدر ، ولكن يمكنك أن ترى أن هناك الكثير من الخيارات الأخرى مثل اللقطة ، يمكنك حتى القيام بذلك من قرص آخر أو من ملف التخزين السحابي. لذلك سأفعل ذلك من القرص. لدينا قرص واحد فقط متاح ، لذلك دعونا نختار ذلك. يمكننا الاحتفاظ بجميع الإعدادات الأخرى ، مثل التشفير والموقع ، ويمكنني النقر فوق "إنشاء". هذا الآن بصدد إنشاء صورة من هذا القرص. في هذه المرحلة ، يمكننا حتى حذف القرص نفسه بمجرد إنشاء تلك الصورة لأننا في الواقع نتحمل رسومًا مقابل القرص أثناء وجوده هناك. ولكن لأغراض المعمل ، يمكننا ترك ذلك حيث يتم تنظيف جميع مواردك في كل مشروع Qwiklabs تستخدمه.
- لذلك دعنا نمضي قدمًا ونقوم الآن بتكوين زر علامة تبويب المثيل وإنشاء مجموعات المثيل. لذا سأذهب إلى Compute Engine، وسنذهب إلى قوالب المثيل. سنقوم بإنشاء نموذج مثيل جديد وسأعطيه اسمًا ، قالب mywebserver

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- سنقوم بتغيير نوع الآلة إلى مايكرو. نحن فقط نقوم ببعض النماذج الصغيرة المتنوعة هنا. الآن ، الشيء المهم هو أنني بحاجة إلى تغيير قرص التمهيد لتحديد صورتي المخصصة. لذلك سأقوم بتغيير ذلك ، انتقل إلى الصور المخصصة ، وهنا لدي صورة خادم الويب الخاص بي من هذا المشروع. إذا كان لديك وصول إلى مشاريع أخرى ، فيمكنك أيضًا التقاط صورة من هناك. كل شيء معد. يمكنني اختيار الحجم وكذلك النوع من هذا. سأقوم فقط بترك هؤلاء والنقر فوق تحديد. الآن ، أحتاج أيضًا إلى التأكد من أن لدي علامات الشبكة الصحيحة. لذلك اسمحوا لي أن أذهب لتوسيع إدارة الأمن والاضطرابات. بالمناسبة ، يمكنك أن ترى أن واجهة المستخدم لقالب المثيل بالكامل تشبه إلى حد كبير قالب مثيل VM لأن كل ما تفعله هو أنك تقوم فقط بتعريف قواعد مثيلات VM، وبمجرد أن تتمكن من المجموعات من تلك ، استخدم كل هذه الإعدادات. لذلك هنا ، سأذهب إلى الشبكات ، وأختار الشبكة ، ويمكنني بعد ذلك التأكد من أن لديّ الشبكة الافتراضية.
- ثم أريد التأكد من أن لدي علامات الشبكة الخاصة بي.

- مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- حتى يتم تطبيق قواعد جدار الحماية التي أنشأناها في البداية على جميع المثيلات التي تم إنشاؤها من هذا القالب. لننتقل إلى إنشاء ، فلن يستغرق ذلك وقتًا طويلاً. ستقوم فقط بإنشاء قالب لا تنشئ أي حالات حتى الآن. في بعض الأحيان ، إذا نفد صبري ، فسأنقر فقط على "تحديث" ونرى أن لدينا كل شيء هنا. حتى الآن يمكنني النقر فوق مجموعة المثيل وإنشاء مجموعة المثيل الخاصة بي. لذلك سأبدأ بإنشاء مجموعة مثيل في us-central1، وستكون هذه منطقة متعددة أو إقليمية عبر المنطقة us-central1 يمكنني النظر في المناطق وربما إلغاء تحديد مناطق معينة أو تحديد المزيد من المناطق إذا أردت ذلك. سيستند هذا إلى النموذج الذي أنشأناه للتو. الآن ، القطعة المهمة هي أننا سنحصل على بعض التحجيم التلقائي. لذلك سنقوم بالتوسيع التلقائي. سنفعل ذلك على الاستخدام المتوازن لتحميل HTTP سيكون استيراد 80.



- مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

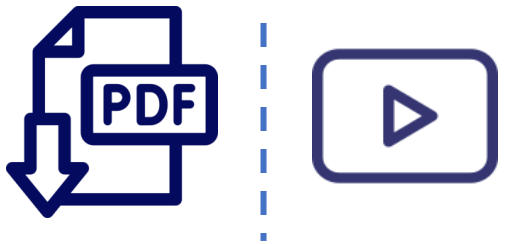
- نريد ما لا يقل عن مثيل واحد وخمسة على الأكثر. يمكننا ترك فترة التهدئة ويمكنك التمرير هنا لترى أنها تنتظر كل هذا الوقت قبل جمع المعلومات. لذلك لدينا بعض التهيئة لهذا المثال ، لذا فأنت تريد التأكد من أنه ينتظر على الأقل تلك 60 ثانية قبل أن يبدأ في البحث في ذلك. ثم يمكننا أيضًا الذهاب إلى الفحص الصحي. ليس لدينا واحد حتى الآن حتى نتمكن من إنشاء فحص صحي ويمكننا فقط تسميته بروتوكول فحص صحة HTTP يمكننا استخدام HTTP أو تركه كـ TCP 80 ما سيفعله هو أنه سيتحقق كل 10 ثوانٍ. سوف تنتظر خمس ثوانٍ بين وإذا كان هناك نجاحان متتاليان ، فهذا يعني النجاح ، ثلاث حالات فشل متتالية تعني أنه فشل ويعني أنه حالة غير صحية.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذا اسمحوا لي أن أنقر على حفظ وأكمل في ذلك. الآن هذا التأخير الأولي هنا يتعلق بالتمهيد ، لذا سنقوم بتعيين ذلك على 60 ثانية لفحص الصحة ، وبعد ذلك سأقوم بالنقر فوق إنشاء. الآن ، هذا يخبرني جيدًا ، أن القياس التلقائي لم يكتمل حقًا بعد لأننا لم نقم بإعداد موازنة تحميل HTTP، فلا بأس بذلك. نحن على وشك القيام بذلك. لذلك دعونا فقط انقر فوق "موافق". سنكرر نفس الشيء الآن لمجموعة المثيلات الخاصة بنا في europe-west1 لذا اسمحوا لي أن أحصل على هذا الاسم. ستكون أيضًا منطقة متعددة. من الواضح في هذه الحالة أن المنطقة هي أوروبا الغربية 1. نموذج المثيل نفسه. يعتمد التحجيم التلقائي أيضًا على منفذ HTTP 80، بحد أدنى واحد أو خمسة كحد أقصى ، يبرد ، والآن يمكننا فقط تحديد التحقق من الصحة. يبدو أنه لا يحتوي على هذا الفحص الصحي حتى الآن. يمكن أن يحدث هذا في الواقع إذا ذهبت إلى هذا بسرعة كبيرة. لنضغط على إلغاء.
- دعنا نعود. دعنا نرى ما إذا تم إنشاء مجموعة المثيل هذه.
- دعنا نحاول ذلك مرة أخرى ونرى ما إذا كان بإمكاننا إجراء هذا الفحص الصحي ، وهناك.
- حسنًا ، نحن سريعون جدًا لدرجة أنه يمكن أن يحدث ذلك بالتأكيد.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- دعني أتراجع ، أعد معلوماتي هنا ، مناطق متعددة ، أوروبا الغربية 1 ، قالبي. لست بحاجة إلى إنشاء واحدة. أريد فقط تحديد خمسة كحد أقصى وتعيين هذا التأخير الأولي مرة أخرى على 60. لا نريد الانتظار كل هذا الوقت للمختبر. سنقوم بالنقر فوق إنشاء HTTP وهو يعطينا مرة أخرى نفس التحذير الذي رأيناه للتو. حتى نتمكن من النقر فوق موافق. هنا يمكننا أن نرى إنشاء مجموعة المثيل هذه. يمكننا أيضًا الانتقال إلى مثيلات VM سنرى أن إحدى مجموعات المثيل قد أنشأت بالفعل مثيلاً. لذلك يمكنك أن ترى أنه يبدأ بهذا الاسم لمجموعة المثيل و MIG بالطريقة التي أضعها هنا ، هذا اختصار لمجموعة مثيلات مُدارة. يمكننا أن نرى التحجيم يحدث هنا. هذا واحد لديه بالفعل مثيل واحد. هذا مقياس من صفر إلى واحد.
- يمكنك بالفعل النقر هنا والحصول على الكثير من المعلومات. إذا ذهبت إلى المراقبة ، سترى استخدام وحدة المعالجة المركزية والتفاصيل والأعضاء.
- سيُظهر لنا أنه يتم توسيعه وعدده.



مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذلك يمكنك الحصول على الكثير من المعلومات إما بالانتقال إلى صفحة مجموعات المثيل أو مثيلات VM في كلتا الحالتين ، لدينا مثال واحد على الأقل في كل مجموعة.
- لذلك نحن مستعدون الآن لتكوين الخلفيات. لذلك دعونا نتحقق من هذه في الواقع. يمكننا الذهاب إلى قائمة التنقل ومثيل VM، نحن هنا بالفعل.
- يمكننا النظر في عناوين IP هذه. يمكنني النقر فوق كلاهما وسنرى أن كلاهما يحتوي على الصفحة الافتراضية لأعلى.
- هذا يثبت أن الصورة المخصصة التي أنشأناها سابقًا يتم الاستفادة منها هنا.
- لذلك قمنا بتثبيت كل تلك البرامج المخصصة ولدينا الآن ذلك.
- لذلك دعونا نقوم بتكوين موازن تحميل HTTP.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- سأذهب إلى قائمة التنقل ، وخدمات الشبكة ، وموازنة التحميل ، وإنشاء موازن تحميل. ستكون هذه موازين تحميل HTTP لبدء ذلك ، يمكنني اختيار ما إذا كانت واجهة الإنترنت أم داخلية فقط. لذا من الإنترنت إلى الأجهزة الافتراضية الخاصة بي ، نعم. انقر فوق متابعة. يمكنني تسميته ، موازن تحميل HTTP سأبدأ بتكوين الواجهة الخلفية. أريد إنشاء خدمة خلفية. سأعطيه اسمًا وسأحدد مجموعات المثيل. لنبدأ أولاً بـ us-central1، رقم المنفذ 80. سيكون وضع الموازنة هو المعدل. حد أقصى 50 طلبًا في الثانية ، سعة 100. لذلك فقط اتبع التعليمات المعملية هنا. لذلك ، فهذا يعني فقط أن موازن التحميل يحاول الاحتفاظ بكل حالة من الحالات التي ستحدث عند أو أقل من 50 طلبًا في الثانية.
- لذلك يمكنني النقر فوق "تم" وإضافة خلفية أخرى وهي الخلفية الوحيدة المتبقية. دعنا نسمع على سبيل المثال ، الاستخدام بمعدل استخدام وحدة المعالجة المركزية يبلغ 80 وسعة 100.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- وهذا يعني فقط أن تكوين القرص يعني أن توازن التحميل يحاول الحفاظ على كل مثيل لـ europe-west1 عند أو أقل من 80٪ من استخدام وحدة المعالجة المركزية. يمكنني أيضًا إرفاق هذا في الفحص الصحي هنا ، ثم النقر فوق إنشاء. الآن ، يمكنني تكوين المضيفين وقواعد المسار التي يمكن أن تحدد أن حركة مرور معينة يتم إرسالها إلى خلفيات أخرى اعتمادًا على عنوان URLلحركة المرور. لذلك يمكن إرسال خدمة الفيديو ربما إلى خلفية فيديو مقابل محتوى ثابت إلى خلفية ثابتة. نحن لا نستفيد من ذلك هنا. لذلك دعنا ننتقل إلى تكوين الواجهة الأمامية. يمكنني إعطائها اسمًا ولكني في الحقيقة أحتاج فقط إلى تحديد البروتوكول. نسخة IP، دعنا نبقيها سريعة الزوال ، المنفذ 80 ، انقر فوق تم ، ويمكننا مراجعته ووضع اللمسات الأخيرة عليه. إذن لدينا هنا الخلفية الخاصة بنا ، أمثالنا ، أو يجب أن أقول مجموعات المثيل لدينا ، وكذلك واجهتنا الأمامية. يمكنني أيضًا أن أضيف إذا عدت إلى هنا واجهة أمامية أخرى. لدي HTTP يمكننا أيضًا إضافة IPV6، لذلك دعونا نفعل ذلك. الآن يمكننا الانتهاء من ذلك.
- الآن علينا أن نحصل على واجهات أمامية وسنحصل على عنوانين IP.
- لذلك دعونا نمضي قدمًا وننشئ ذلك.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- بمجرد تشغيل ذلك ، يجب أن نرى عنوانين. سيكون العنوان في التنسيق السداسي العشري هو عنوان IPv6 الخاص بنا ، وستتمكن فقط من الانتقال إليه إذا كان اتصالك يسمح به بالفعل من حيث أنت.
- على سبيل المثال ، غالبًا ما تستخدم الهواتف المحمولة IPv6، لذا يمكنك محاولة توصيل العنوان بهاتفك الخلوي ومعرفة ما إذا كان بإمكانك الوصول إلى تلك الخلفيات.
- لذلك دعونا ننتظر حتى يتم التحميل.
- لذلك إذا قمت بالنقر فوق موازن التحميل الخاص بي ، فهذه هي الواجهة الأمامية ، وهي ليست جاهزة بعد.
- ذهبت إلى هنا ، ولكن أولاً ، دعنا نحدث وننتظر فقط أن تكون تلك الخدمة جاهزة ، وبعد ذلك يمكننا الدخول والحصول على مزيد من المعلومات عنها. لذلك أنا هنا ، لم يتم إعداد موازن التحميل. لم أستغرق سوى بضع ثوانٍ إضافية.
- حتى هنا يمكننا رؤية عناوين IP.
- مرة أخرى ، هذا هو IPv4، هذا هو IPv6.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذا فإن أول شيء يمكنني فعله هو أنه يمكنني في الواقع التنقل فقط إلى أولئك الذين يستخدمون المتصفح ، لأنني سمحت بحركة مرور HTTPمن أي مكان. لذا اسمحوا لي فقط بتوصيل ذلك بالمتصفح الخاص بي ، والانتقال بسرعة إلى IPv4 أتلقى بالفعل خطأ 404 ، ودليل المعمل يتحدث عن ذلك. لذلك اسمحوا لي أيضًا بفتح علامة تبويب أخرى ، واكتب عنوان IPv6، وتشغيل ذلك ، وتقول إنها لم تعثر على الخدمة بعد.
- لذا يتحدث دليل المختبر عن حقيقة أنه من الممكن أن تحصل على 404 أو 502 لبعض الوقت. لذا ما تريد القيام به هنا هو مجرد التحديث لبعض الوقت ، وما تفعله حقًا هو أنك تنتظر تطبيق هذا التكوين على جميع واجهات Google الأمامية. إذن هذا مرة أخرى ، يجب تطبيق أرصدة الحمل العالمية في كل مكان. لذا فإن التنفيذ الفعلي على الرغم من أن وحدة التحكم تبدو وكأن كل شيء جاهز ، قد تستغرق الخدمة أحيانًا بعض الوقت حتى يمكن الوصول إليها بالفعل.
- وقد يستغرق ذلك بضع دقائق ليتم إعدادها. لذا فقط اطلب التحديث عدة مرات.
- ودعنا ننتظر حتى يأتي ذلك. لذلك نحن هنا. أنا أبحث في عنوان IPv4.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لقد قمت بتحديث ذلك عدة مرات ، ويمكنني رؤية الواجهة الخلفية والتي كما نعلم ، يجب أن تكون صفحة Apache2 Debian الافتراضية ، وأنا أيضًا أتنقل إلى عنوان IPv6.
- في الواقع لدي حق الوصول إلى ذلك هنا. لذلك هذا يعمل كما هو متوقع. والآن بعد أن علمنا أن الواجهة الخلفية تعمل ، فقد حان الوقت لاختبارها. إذن ما سنفعله هو أننا سننشئ حالة أخرى الآن ، وننشئ فقط عددًا كبيرًا من حركة المرور إلى موازن التحميل ، ثم سنقوم بمراقبة حركة المرور هذه. لذا دعني أفتح علامة تبويب أخرى هنا ، لأنني أريد أن أكون قادرًا على العودة إلى موازن التحميل. سأقوم بإنشاء مثيل آخر الآن بالرجوع إلى Compute Engine، وإنشاء مثيل. سأحدد اسمًا ، فقط اختبار تحمّل. سأضع هذا في منطقة مختلفة تمامًا الآن. سأقوم باختيار غرب الولايات المتحدة 1. الآن ، فيما يتعلق بخلفياتي الخلفية ، لدي خلفية في US Central1 وخلفية في أوروبا الغربية 1.
- أقرب واجهة خلفية من هذا المثال الجديد الذي أقوم بإنشائه ستكون US Central1.
- لذلك نتخيل أنه يجب إعادة توجيه حركة المرور من غرب الولايات المتحدة إلى وسط الولايات المتحدة.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- سيكون هذا ما لم يكن الحمل مرتفعًا جدًا ، ودعنا نرى ما إذا كان بإمكاننا بالفعل كسر ذلك وإنشاء حمولة عالية حقًا ، بحيث يكون لدينا أيضًا حركة مرور تنتشر في المنطقة العربية التي أنشأناها. لذلك أريد تغيير قرص التمهيد. هنا ، دعنا بالفعل نختار الصورة المخصصة التي لدينا بالفعل. هناك حيث نحصل على مجموعة من البرامج المثبتة مسبقًا.
- ثم سأقوم بإنشاء ذلك ، وبمجرد الانتهاء من ذلك ، سأأخذ عنوان IP الخاص بميزان التحميل الخاص بنا. سأقوم بتخزين ذلك في متغير البيئة. سوف نتحقق منه للتأكد من أنه لدينا ، ومن ثم سنقوم بتحميله. لذلك دعونا ننتظر ظهور هذا المثال. مع أي مشروع جديد ، لديك دائمًا الكثير من المعلومات على الجانب الأيمن. من المفيد التحقق مما إذا كنت جديدًا على برنامج "شركاء Google المعتمدون". المثيل هو أعلى.
- اسمحوا لي أن أذهب SSH،
- ودعنا نخزن عنوان IP الآن ، أنا بحاجة إلى الاستيلاء على ذلك.
- لذا دعني أعود إلى هنا. سنستخدم عنوان IPv4.

- مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

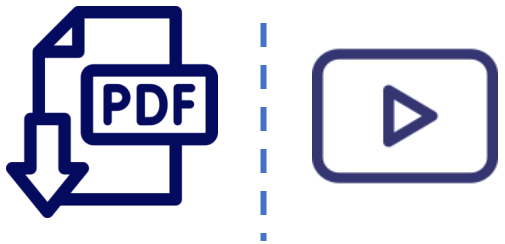
- واسمحوا لي أن أحصل على نسخة احتياطية من اختبار التحمل ، وأخزنها. هذا أيضًا تحقق ، وتأكد من تخزينه ، وهنا يمكننا رؤيته وهو يتطابق مع عنوان IP هذا. ذلك رائع. لنقم بتشغيل أمر لوضع حمل على موازن التحميل الخاص بنا. تمام. إذن هذا يستخدم Apache Bench، ولن يقيس هذا ، وسوف يعمل هذا الآن في الخلفية. والآن ما يمكنني فعله هو العودة إلى موازن التحميل الخاص بي ، والذي أنظر إليه الآن. إذا كنت أنظر بهذه الطريقة ، يمكنني في الواقع إلقاء نظرة مباشرة على الخلفية ، والنقر على الخلفيةHTTP ، وليس لدينا أي حركة مرور حتى الآن. يستغرق هذا بعض الوقت للتحديث هنا.
- يمكننا أن نرى الخلفيتين لدينا. يمكننا أن نرى أن أحدًا يقوم بتحجيم السعر ، والآخر يقوم بتوسيع نطاق استخدام وحدة المعالجة المركزية. بمجرد أن يكون لدينا الكثير من حركة المرور ، سيبدأ في الظهور هنا من أين تأتي هذه الحركة ، والمثال الذي ستذهب إليه. لذا ما نريد القيام به هو الانتظار هنا ، وتحديث هذه الصفحة لبضع دقائق.
- حتى نتمكن من رؤية بعض الزيارات التي يتم إنشاؤها.

مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- لذا اسمحوا لي أن أعود وأعود إلى هنا ، ولا توجد حركة مرور بعد. لذا دعنا ننتظر دقيقة أو دقيقتين ، ونرى ما يمكننا تصوره هنا. حسنا. لذلك استغرق هذا بضع ثوان فقط. لذلك نحن هنا.
- يمكننا أن نرى أن هناك الكثير من حركة المرور القادمة من أمريكا الشمالية ، وذلك لاختبارات الإجهاد الخاصة بي ، ويمكننا أن نرى أنها تتجه إلى US Central1 وهو الأقرب ، وهذا هو المكان الذي تتجه إليه معظم حركة المرور لدينا ، ومعظم الطلبات. ولكن لدينا أيضًا بعض حركة المرور التي تنتقل بالفعل إلى مثال أوروبا الغربية 1. لذلك يمكننا أن نرى أن لدينا موازنة حمولة عالمية هنا. ما يمكننا فعله الآن هو أنه يمكننا أيضًا مراقبة الخلفيات لمعرفة ما إذا كانت تتوسع بالفعل. لذلك إذا ذهبت إلى Compute Engine وقمت بالتحديث ، حسنًا ، يمكننا أن نرى بالفعل أن لدينا مجموعة أخرى من الخلفيات التي تحاول التعامل مع كل الزيادة المفاجئة في حركة المرور ، وأنا حقًا أؤكد اختبار هذا كثيرًا.
- إذا ذهبت إلى مجموعات المثيل ، فيمكننا الحصول على مزيد من المعلومات هنا.

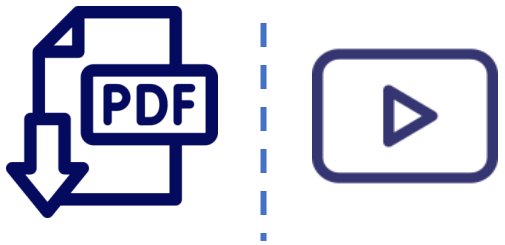
مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- إنه يقول أنه يواجه بالفعل مشكلة في عدد المثيلات التي حددتها ، الحد الأقصى هو خمسة.
- إذا ذهبنا إلى أوروبا الغربية 1 ، فيمكننا الحصول على مزيد من التفاصيل والمراقبة. لذلك فهو يوضح لنا كيف تم توسيع نطاقه ، وكيف يدير الحمل الذي يتم وضعه عليه. يمكننا أيضًا أن ننظر في US Central1، ونرى أن لدينا الآن ما يصل إلى خمس حالات بالفعل عبر مناطق مختلفة ، ويمكنني أيضًا الدخول في المراقبة هنا والحصول على مزيد من المعلومات ، وأرى ذلك عندما قمنا بالتوسع ، ولتحديث هذا قليلاً ، سنرى المزيد من الأمثلة هنا ، وسأتحدث أكثر عن السعة التي يمتلكها. يمكنني العودة إلى هنا ، والآن يمكننا أن نرى أن لدينا ، لأنني قدمت بالفعل الحد الأدنى جدًا من حركة المرور إلى Central1 الخاص بك ، فقط 50 طلبًا في الثانية ، لكنني أقوم بعمل 281 تقريبًا هنا.
- إذن لدينا الآن الكثير من حركة المرور الممتدة. لذا فهذه طريقة عرض جيدة حقًا للعودة إليها.
- لمراقبة موازن التحميل دائمًا.



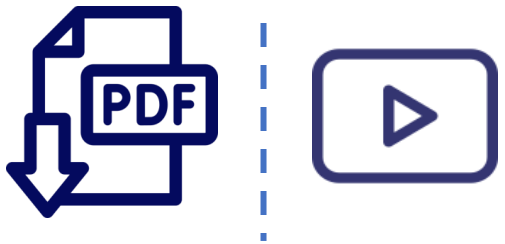
- مراجعة المعمل: تكوين موازن تحميل HTTP باستخدام القياس التلقائي

- بشكل متبادل ، يمكنك أيضًا استخدام تسجيل Stackdriver والمراقبة ، وإعداد التنبيهات ، وإعداد الأدوار.
- لذا ربما تحتاج إلى زيادة هذا الحد الأقصى وهو خمسة الآن.
- هذا حقا حد للتكلفة. قمت بتعيين ذلك بحيث لا تتجاوز التكلفة الخاصة بك أكثر من اللازم.
- لكن إذا كنت تقول ، "يا إلهي ، أنا بحاجة للعمل على هذا المرور." يمكن أن يكون لديك المزيد من الحالات.
- ربما تتعرض لهجوم في الواقع ، في تلك المرحلة يمكنك استخدام منتج يسمى Cloud AMR، ربما للسماح برفض عناوين IP معينة.
- لكن هذا حقًا كل ما نريد تحقيقه للمختبر.



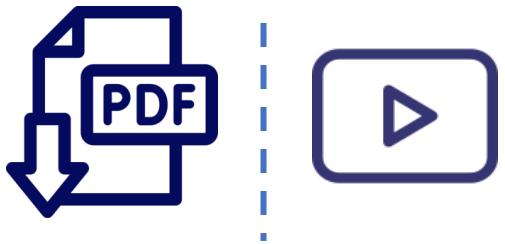
سحابة CDN

- تستخدم Cloud CDN، أو Content Delivery Network، نقاط تواجد Google الموزعة عالميًا للتخزين المؤقت لمحتوى HTTP (S) المتوازن التحميل بالقرب من المستخدمين. على وجه التحديد ، يمكن تخزين المحتوى مؤقتًا في عُقد CDN كما هو موضح في هذه الخريطة. يوجد أكثر من 90 موقعًا من مواقع التخزين المؤقت هذه منتشرة عبر المناطق الحضرية في آسيا والمحيط الهادئ والأمريكتين وأوروبا والشرق الأوسط وإفريقيا. للحصول على قائمة محدثة ، يرجى الرجوع إلى وثائق Cloud CDN.
- الآن ، لماذا يجب أن تفكر في استخدام Cloud CDN؟ حسنًا ، تقوم Cloud CDN بتخزين المحتوى مؤقتًا على حافة شبكة Google مما يوفر توصيلًا أسرع للمحتوى للمستخدمين مع تقليل تكاليف الخدمة. يمكنك تمكين Cloud CDN من خلال مربع اختيار بسيط عند إعداد خدمة الواجهة الخلفية لموازن تحميل HTTP (S)الخاص بك. لذلك من السهل تمكينك أنت والمستخدمين وفوائدهم ولكن كيف تقوم Cloud CDN بكل هذا؟
- دعنا نتصفح تدفق استجابة Cloud CDN بهذا الرسم التخطيطي.



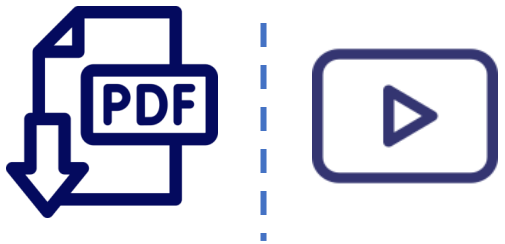
- سحابة CDN

- في هذا المثال ، يحتوي موازن تحميل HTTP (S) على نوعين من الخلفيات. توجد مجموعات مثيلات VM مُدارة في منطقتي us-central1 و asia-east1، وهناك دلو تخزين سحابي في شرق الولايات المتحدة 1.
- ستحدد خريطة URL الواجهة الخلفية لإرسال المحتوى إليها: يمكن استخدام حاوية التخزين السحابي لخدمة المحتوى الثابت ويمكن لمجموعات المثيل معالجة حركة مرور PHP الآن ، عندما يكون مستخدم في سان فرانسيسكو هو أول من يصل إلى جزء من المحتوى ، يرى موقع التخزين المؤقت في سان فرانسيسكو أنه لا يمكنه تلبية الطلب. هذا يسمى فقدان ذاكرة التخزين المؤقت. قد تحاول ذاكرة التخزين المؤقت الحصول على المحتوى من ذاكرة تخزين مؤقت قريبة ، على سبيل المثال إذا كان مستخدم في لوس أنجلوس قد وصل بالفعل إلى المحتوى.
- خلاف ذلك ، يتم إعادة توجيه الطلب إلى موازن تحميل HTTP (S).



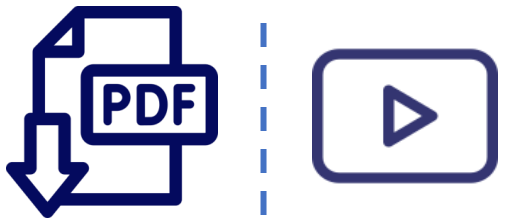
سحابة CDN

- والذي بدوره يعيد توجيه الطلب إلى إحدى الخلفيات الخلفية الخاصة بك. اعتمادًا على المحتوى الذي يتم تقديمه ، سيتم إعادة توجيه الطلب إلى مجموعة مثيل us-central1 أو حاوية تخزين us-east1 إذا كان المحتوى من الواجهة الخلفية قابلاً للتخزين المؤقت ، فيمكن لموقع التخزين المؤقت في سان فرانسيسكو تخزينه للطلبات المستقبلية. بمعنى آخر ، إذا طلب مستخدم آخر نفس المحتوى في سان فرانسيسكو ، فقد يكون موقع ذاكرة التخزين المؤقت الآن قادرًا على تقديم هذا المحتوى. يؤدي هذا إلى تقصير وقت الذهاب والإياب ويحفظ الخادم الأصلي من الاضطرار إلى معالجة الطلب. وهذا ما يسمى بضربة ذاكرة التخزين المؤقت. لمزيد من المعلومات حول المحتوى الذي يمكن تخزينه مؤقتًا.
- يرجى الرجوع إلى الوثائق. الآن ، يتم تسجيل كل طلب Cloud CDN تلقائيًا داخل Google Cloud ، ستشير هذه السجلات إلى حالة "Cache Hit" أو "Cache Miss" لكل طلب HTTP لموازن التحميل.
- سوف تستكشف مثل هذه السجلات في المختبر التالي.



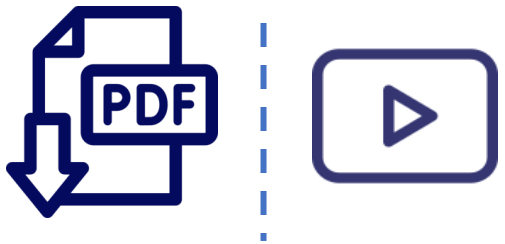
- سحابة CDN

- ولكن كيف تعرف كيف ستقوم Cloud CDN بتخزين المحتوى الخاص بك مؤقتًا؟ كيف تتحكم في هذا؟ هذا هو المكان الذي تكون فيه أوضاع التخزين المؤقت مفيدة. باستخدام أوضاع التخزين المؤقت ، يمكنك التحكم في العوامل التي تحدد ما إذا كان Cloud CDN يقوم بتخزين المحتوى الخاص بك مؤقتًا أم لا باستخدام أوضاع التخزين المؤقت. تقدم شبكة CDN السحابية ثلاثة أوضاع للتخزين المؤقت ، والتي تحدد كيفية تخزين الاستجابات مؤقتًا ، وما إذا كانت Cloud CDN تحترم توجيهات ذاكرة التخزين المؤقت التي يرسلها الأصل أم لا ، وكيف يتم تطبيق TTL لذاكرة التخزين المؤقت.
- أوضاع التخزين المؤقت المتاحة هي USE_ORIGIN_HEADERS و CACHE_ALL_STATIC و FORCE_CACHE_ALL
- يتطلب وضع USE_ORIGIN_HEADERS استجابات الأصل لتعيين توجيهات ذاكرة التخزين المؤقت الصالحة ورؤوس التخزين المؤقت الصالحة.



- سحابة CDN

- يخزن الوضع CACHE_ALL_STATIC تلقائيًا المحتوى الثابت الذي لا يحتوي على التوجيه no-store أو الخاص أو no-cache.
- يتم أيضًا تخزين استجابات المنشأ التي تحدد توجيهات التخزين المؤقت الصالحة مؤقتًا.
- يخزن الوضع FORCE_CACHE_ALL الاستجابات مؤقتًا دون قيد أو شرط ، متجاوزًا أي توجيهات ذاكرة التخزين المؤقت التي تم تعيينها بواسطة الأصل.
- يجب عليك التأكد من عدم تخزين المحتوى الخاص لكل مستخدم مؤقتًا (مثل استجابات HTML الديناميكية أو واجهة برمجة التطبيقات) في حالة استخدام خلفية مشتركة مع هذا الوضع c.



موازنة تحميل وكيل SSL

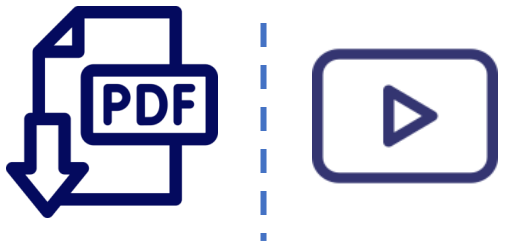
- دعنا نتحدث عن وكيل SSL وموازنة تحميل وكيل TCP وكيل SSL هو خدمة موازنة تحميل عالمية لحركة المرور المشفرة غير HTTP ينهي موازن التحميل اتصالات SSL للمستخدم في طبقة موازنة التحميل ، ثم يوازن الاتصالات عبر مثيلاتك باستخدام بروتوكولات SSL أو TCP.
- يمكن أن تكون هذه الطبعات في مناطق متعددة ، ويقوم موازن التحميل تلقائيًا بتوجيه حركة المرور إلى أقرب منطقة ذات سعة. تدعم موازنة تحميل وكيل SSL كلاً من عناوين Pv4 او Pv6 الحركة مرور العميل وتوفر توجيهًا ذكيًا وإدارة الشهادات وتصحيح الأمان وسياسات SSL.
- يعني التوجيه الذكي أن موازن التحميل هذا يمكنه توجيه الطلبات إلى مواقع الخلفية حيث توجد سعة.
- من منظور إدارة الشهادة ، ما عليك سوى تحديث شهادتك التي تواجه العميل في مكان واحد.
- عندما تحتاج إلى تبديل هذه الشهادات.
- يمكنك أيضًا تقليل عبء الإدارة لمثيلات الجهاز الظاهري باستخدام الشهادات الموقعة ذاتيًا في مثيلاتك.

موازنة تحميل وكيل SSL

- بالإضافة إلى ذلك ، إذا ظهرت ثغرات أمنية في مكدس SSL أو TCP، فسيقوم GCP بتطبيق التصحيحات في موازن التحميل تلقائيًا للحفاظ على مثيلاتك آمنة.
- للحصول على القائمة الكاملة للمنافذ التي يدعمها موازنة تحميل وكيل SSL والمزايا الأخرى ، يرجى الرجوع إلى قسم الارتباط في هذا الفيديو. يوضح مخطط الشبكة هذا موازنة تحميل وكيل SSL.
- في هذا المثال ، يتم إنهاء حركة المرور من المستخدمين في ولايتي أيوا وبوسطن عند طبقة موازنة الحمل العالمية. من هناك ، تم إنشاء اتصال منفصل لأقرب مثيل للخلفية.
- بعبارة أخرى ، سيصل المستخدم في بوسطن إلى منطقة شرق الولايات المتحدة ، وسيصل المستخدم في ولاية أيوا إلى منطقة وسط الولايات المتحدة ، إذا كانت هناك سعة كافية.
- الآن ، يمكن لحركة المرور بين الوكيل والخلفية استخدام SSL أو TCP.
- أوصي باستخدام SSL.

موازنة تحميل وكيل TCP

- بروكسي TCP هو خدمة موازنة تحميل عالمية لحركة المرور غير المشفرة وغير HTTP ينهي موازن التحميل جلسات TCP الخاصة بالعميل في طبقة موازنة التحميل ثم يعيد توجيه حركة المرور إلى مثيلات الجهاز الظاهري باستخدام TCP أو SSL.
- يمكن أن تكون هذه الطبعات في مناطق متعددة ويقوم موازن التحميل تلقائيًا بتوجيه حركة المرور إلى أقرب منطقة لديها سعة. تدعم موازنة تحميل وكيل TCP عناوين IPv4 و IPv6 لحركة مرور العميل. على غرار موازن تحميل وكيل SSL، يوفر موازن تحميل وكيل TCP توجيهًا ذكيًا وتصحيح أمان.
- للحصول على القائمة الكاملة للمنافذ التي يدعمها موازنة تحميل وكيل TCP والمزايا الأخرى ، يرجى الرجوع إلى قسم الروابط في هذا الفيديو. يوضح مخطط الشبكة هذا موازنة تحميل وكيل TCP.



موازنة تحميل وكيل TCP

- في هذا المثال ، يتم إنهاء حركة المرور من المستخدمين في ولايتي أيوا وبوسطن عند طبقة موازنة الحمل العالمية.
- من هناك تم إنشاء اتصال منفصل إلى أقرب مثيل للجهة الخلفية.
- كما هو الحال في مثال موازنة تحميل وكيل SSL، سيصل المستخدمون في بوسطن إلى منطقة شرق الولايات المتحدة وسيصل المستخدم في ولاية أيوا إلى المنطقة الوسطى للولايات المتحدة إذا كانت هناك سعة كافية.
- الآن يمكن لحركة المرور بين الوكيل والخلفية استخدام SSL أو TCP، وأوصي أيضًا باستخدام SSL هنا.

موازنة حمل الشبكة

- الآن ، دعنا نتحدث عن موازنة حمل الشبكة ، وهي خدمة موازنة حمل إقليمية. موازنة تحميل الشبكة هي خدمة موازنة تحميل إقليمية بدون وكيل. بمعنى آخر ، يتم تمرير كل حركة المرور من خلال موازن التحميل بدلاً من إنشاء وكيل لها. لا يمكن موازنة حركة المرور إلا بين مثيلات الأجهزة الظاهرية الموجودة في نفس المنطقة ، على عكس موازن التحميل العام. تستخدم خدمة موازنة التحميل هذه قواعد إعادة التوجيه لموازنة حمل أنظمتك استنادًا إلى بيانات بروتوكول IP الواردة ، مثل العنوان والمنفذ ونوع البروتوكول. يمكنك استخدامه لتحميل موازنة حركة مرور UDP ولتحميل حركة مرور TCP و SSL على المنافذ غير المدعومة مع موازنات تحميل وكيل TCP ووكيل SSL.
- تعتمد بنية موازن تحميل الشبكة على ما إذا كنت تستخدم موازن تحميل الشبكة المستند إلى خدمة الواجهة الخلفية أو موازن تحميل الشبكة المستند إلى التجمع المستهدف.
- دعنا نستكشف هذه بمزيد من التفصيل.

موازنة حمل الشبكة

- يمكن أن تكون موازنات تحميل الشبكة الجديدة مجنونة ، ولكنها خدمة خلفية إقليمية تحدد سلوك موازن التحميل وكيف يوزع حركة المرور عبر مجموعات مثيل للخلفية. تتيح خدمات الواجهة الخلفية ميزات جديدة غير مدعومة مع مجموعات الأهداف القديمة ، مثل دعم الفحوصات الصحية غير القديمة ، و TCP ، و SSL ، و HTTP ، و HTTPS و HTTP / 2 ، والتحجيم التلقائي مع مجموعات المثيلات المُدارة ، واستنزاف الاتصال ، والتكوين. سياسة تجاوز الفشل. يمكنك أيضًا نقل موازن تحميل الشبكة القائم على التجمع المستهدف لاستخدام خدمات الواجهة الخلفية بدلاً من ذلك. ولكن ما هو مورد التجمع المستهدف؟ يحدد مورد التجمع الهدف مجموعة من المثيلات التي تتلقى حركة مرور واردة من قواعد إعادة التوجيه. عندما توجه قاعدة إعادة التوجيه حركة المرور إلى تجمع مستهدف ، يختار موازن التحميل مثيلًا ، من تجمعات الأهداف هذه استنادًا إلى تجزئة عنوان IP المصدر والمنفذ ، وعنوان IP الوجهة والمنفذ.

موازنة حمل الشبكة

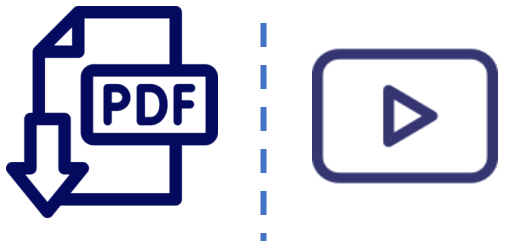
- لا يمكن استخدام تجمعات الأهداف هذه إلا مع قواعد إعادة التوجيه التي يمكنها معالجة حركة مرور TCP و UDP.
- الآن ، يمكن أن يحتوي كل مشروع على ما يصل إلى 50 مجموعة مستهدفة ، ويمكن لكل تجمع مستهدف إجراء فحص صحي واحد فقط. أيضًا ، يجب أن تكون جميع مثيلات التجمع الهدف في نفس المنطقة ، وهو نفس القيد المطبق على موازن تحميل الشبكة.

موازنة الحمل الداخلي

- بعد ذلك ، دعنا نتحدث عن موازنة الحمل الداخلي.
- موازن تحميل TCP / UDP الداخلي هو خدمة موازنة تحميل إقليمية خاصة لحركة المرور المستندة إلى TCPو UDP.
- بعبارة أخرى ، يمكّنك موازن التحميل هذا من تشغيل خدماتك وتوسيع نطاقها خلف عنوان IP خاص لموازنة التحميل. هذا يعني أنه لا يمكن الوصول إليه إلا من خلال عناوين IP الداخلية أو مثيلات الجهاز الظاهري في نفس المنطقة.
- لذلك تقوم بتكوين عنوان IP داخلي لموازنة تحميل TCP / UDP ليعمل كواجهة أمامية لمثيلاتك الخلفية الخاصة.
- نظرًا لأنك لا تحتاج إلى عنوان IPعام لكي تقوم بتحميل خدمة متوازنة ، فإن طلبات العميل الداخلي تظل داخلية لشبكة VPC ومنطقتك ، غالبًا ما يؤدي هذا إلى تقليل وقت الاستجابة نظرًا لأن كل حركة المرور المتوازنة للحمل تظل داخل شبكة Google مما يجعل التهيئة الخاصة بك أبسط بكثير.
- دعنا نتحدث أكثر عن فوائد استخدام خدمة موازنة تحميل TCP / UDP داخلية محددة بالبرمجيات.
- لا تعتمد موازنة التحميل الداخلي لـ Google Cloud على جهاز أو مثيل VM.

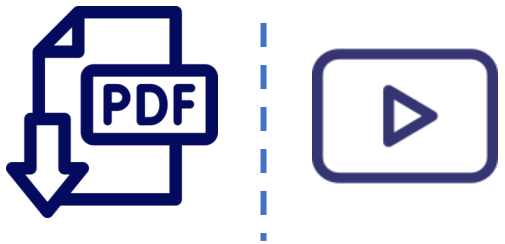
موازنة الحمل الداخلي

- بدلاً من ذلك ، فهو حل موازنة تحميل موزع بالكامل معرّف برمجيًا. في نموذج الوكيل التقليدي لموازنة التحميل الداخلي ، كما هو موضح على اليسار ، تقوم بتكوين عنوان IP داخلي على جهاز أو مثيلات موازنة التحميل ، ويتصل مثيل العميل الخاص بك بعنوان IP هذا. يتم إنهاء حركة المرور الواردة إلى عنوان IP عند موازن التحميل ، ويحدد موازن التحميل نهاية خلفية لإنشاء اتصال جديد بـ.
- بشكل أساسي ، لديك اتصالان ، أحدهما بين العميل وموازن التحميل والآخر بين موازن التحميل والنهاية الخلفية.
- توزع موازنة التحميل الداخلي لـ Google Cloud طلبات مثيل العميل إلى الأطراف الخلفية باستخدام نهج مختلف ، كما هو موضح على اليسار. إنه يستخدم موازنة تحميل خفيفة الوزن مبنية على قمة Andromeda، مكدس المحاكاة الافتراضية لشبكة Google، لتوفير موازنة تحميل معرّفة بالبرمجيات والتي تقدم حركة المرور مباشرة من مثيل العميل إلى مثيل خلفي.



موازنة الحمل الداخلي

- لمزيد من المعلومات حول أندروميدا ، انظر قسم الارتباط في هذا الفيديو. الآن ، موازنة تحميل HTTPS الداخلية من Google Cloud عبارة عن موازن تحميل إقليمي قائم على الطبقة السابعة قائم على الوكيل والذي يمكّنك أيضًا من تشغيل وتوسيع نطاق خدماتك خلف عنوان IP لموازنة التحميل الداخلي. تدعم الخدمات الخلفية بروتوكولات HTTP و HTTPS و HTTP / 2 موازنة تحميل HTTPS الداخلية هي خدمة مُدارة بناءً على وكيل Envoy مفتوح المصدر. يتيح ذلك إمكانات ثرية للتحكم في حركة المرور استنادًا إلى معلمات HTTPS.
- بعد تكوين موازن التحميل ، يقوم تلقائيًا بتخصيص وكلاء Envoy لتلبية احتياجات حركة المرور الخاصة بك. الآن ، تمكنك موازنة التحميل الداخلي من دعم حالات الاستخدام مثل خدمات الويب التقليدية ثلاثية المستويات.

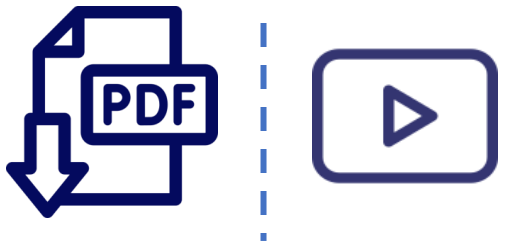


موازنة الحمل الداخلي

- في هذا المثال ، تستخدم طبقة الويب موازن تحميل HTTPS خارجيًا يوفر عنوان IP عالميًا واحدًا للمستخدمين في سان فرانسيسكو وأيوا وسنغافورة وما إلى ذلك. تقع الأطراف الخلفية لميزان التحميل هذا في مناطق الولايات المتحدة الغربية ، والولايات المتحدة الوسطى ، وآسيا الشرقية الأولى لأن هذا هو موازن تحميل عالمي.
- ثم تقوم هذه الأطراف الخلفية بالوصول إلى موازن تحميل داخلي في كل منطقة مثل التطبيق أو الطبقة الداخلية. تقع الأطراف الخلفية لهذا المستوى الداخلي في منطقة West One A و Central One B و Asia East One B أما المستوى الأخير فهو المستوى المستند إلى البيانات في كل منطقة من هذه المناطق.
- وتتمثل فائدة هذا النموذج ثلاثي المستويات في عدم تعرض الطبقة القائمة على البيانات ولا طبقة التطبيق خارجيًا.
- هذا يبسط الأمن وتسعير الشبكة.

مقدمة المعمل: تكوين موازن تحميل داخلي

- دعنا نطبق بعض مفاهيم موازن التحميل الداخلي التي ناقشناها للتو في المعمل.
- في هذا التمرين المعملي ، تقوم بإنشاء مجموعتي مثيل مُدارتين في نفس المنطقة ، ثم تقوم بتكوين واختبار موازن التحميل الداخلي مع مجموعات المثيلات كخلفيات كما هو موضح في مخطط الشبكة هذا.



معمل – LAB: تكوين موازن التحميل الداخلي

- في هذا التمرين المعملي ، تقوم بإنشاء مجموعتي مثيل مُدارتين في نفس المنطقة.
- ثم تقوم بتكوين واختبار موازن تحميل داخلي مع مجموعات المثيلات كخلفية.
- نصائح لمختبرات الدورة التدريبية
- احصل على أقصى استفادة من Coursera و Qwiklabs من خلال تجربة نصائحنا أدناه.
- تجنب الخلط بين الحساب والتصفح الخاص.
- أغلق هذه الصفحة وسجل الدخول مرة أخرى إلى Coursera في وضع التصفح المتخفي قبل الانتقال.
- عند العودة إلى هذه الدورة التدريبية وصفحة الإرشادات المعملية ، انقر فوق "فتح الأداة" للمتابعة.
- تجنب الخلط بين الحساب والتصفح الخاص.

- **معمل** – LAB: **تكوين موازن التحميل الداخلي**

- **باستخدام وضع التصفح المتخفي ، يضمن ذلك عدم استخدامك لحساب** Google **الخاص بك عن طريق الخطأ (بما في ذلك** Gmail**) أثناء الوصول إلى** Google Cloud Console.
- **يمنع هذا أيضًا** Qwiklabs **من تسجيل خروجك من حسابات** Google **الخاصة بك.**
- **الإرشادات التفصيلية لاستخدام وضع التصفح المتخفي في** Google Chrome **متوفرة هنا.**
- **اعتمادًا على المستعرض الخاص بك ، قد يُطلق على وضع التصفح المتخفي أيضًا اسم الاستعراض الخاص أو استعراض** InPrivate.

معمل – LAB: تكوين موازن التحميل الداخلي

- لضمان الانتهاء من المختبر تم وضع علامة عليه في كورسيرا:

1. قم بالوصول إلى كل معمل فردي بالنقر فوق فتح الأداة في كورسيرا

2. أكمل المختبر في Qwiklabs
3. انقر على "إنهاء المعمل" في Qwiklabs

4. أغلق نافذة أو علامة تبويب متصفح Qwiklabs

- معمل – LAB: تكوين موازن التحميل الداخلي

- للتفاعل مع المتعلمين الآخرين:

إذا كنت تواجه أي صعوبة في المعامل ، فنحن نشجعك على النشر عنها في منتديات المناقشة الخاصة بهذه الدورة التدريبية. إذا لم تكن لديك مشاكل مع المعامل ، ففكر في تصفح منتديات المناقشة للحصول على فرص لمساعدة زملائك المتعلمين.

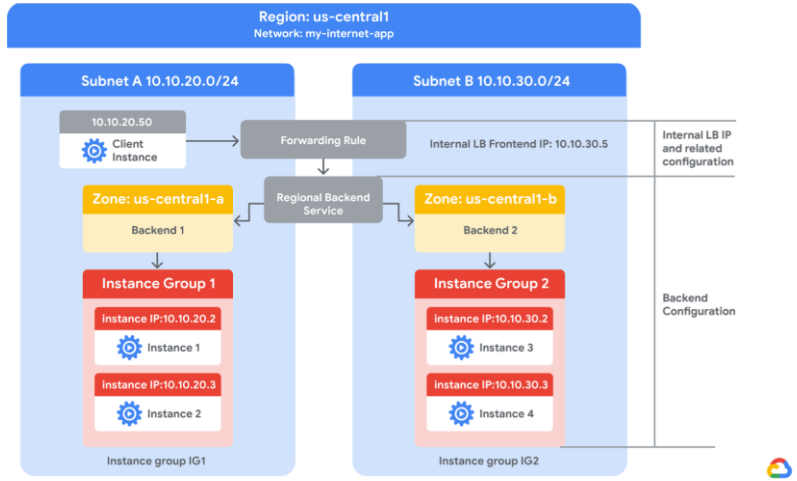
- لتقديم طلب دعم:

إذا كنت تواجه مشكلات فنية مع المختبرات أو التصنيف ، فيرجى إرسال طلب دعم هنا:

https://qwiklab.zendesk.com/hc/en-us/requests/new

معمل – LAB: Configuring an Internal Load Balancer

- تقدم Google Cloud موازنة التحميل الداخلية لحركة المرور المستندة إلى TCP / UDP.
- يمكّنك موازنة التحميل الداخلية من تشغيل خدماتك وتوسيع نطاقها خلف عنوان IP خاص لموازنة التحميل لا يمكن الوصول إليه إلا من خلال مثيلات الجهاز الظاهري الداخلية.
- في هذا التمرين المعملي ، تقوم بإنشاء مجموعتي مثيل مُدارتين في نفس المنطقة.
- ثم تقوم بتكوين واختبار موازن تحميل داخلي مع مجموعات المثيلات كخلفية ، كما هو موضح في مخطط الشبكة هذا:



مراجعة معملية: تكوين موازن تحميل داخلي

- في هذا الدرس ، أنشأت مجموعتين من مجموعات المثيلات المُدارة في منطقة وسط الولايات المتحدة مع قواعد جدار الحماية للسماح بحركة مرور HTTP لتلك المثيلات وزيارات TCP من مدقق صحة GCP ثم قمت بتكوين واختبار موازن التحميل الداخلي لمجموعات المثيلات هذه. يمكنك البقاء في جولة معملية ، ولكن تذكر أن واجهة مستخدم GCPs يمكن أن تتغير. لذلك قد تبدو بيئتك مختلفة قليلاً. حسنًا ، أنا هنا في وحدة تحكم GCP، وفي هذه المعامل المشابهة للمختبرات الأخرى ، قمنا بالفعل بإنشاء بعض الموارد مسبقًا من أجلك. يمكنك استكشافها مرة أخرى إذا انتقلت إلى قائمة التنقل ثم انتقلت إلى Deployment Manager، فسترى نشرًا هنا. أنشأنا شبكة بها شبكتان فرعيتان وبعض قواعد جدار الحماية. يمكننا أيضًا استكشافها من خلال الانتقال إلى شبكة VPC.
- هذا ما ذكرته تعليمات المختبر بالفعل. لذا أنقر هناك ، ولدي بالفعل الشبكة الافتراضية ، وهنا تلك الشبكة الإضافية التي قمت بإنشائها باستخدام شبكتين فرعيتين.
- ولدي أيضًا بعض قواعد جدار الحماية لأولئك هنا للسماح لـICMP و SSH و RDP.

مراجعة معملية: تكوين موازن تحميل داخلي

- حسنًا ، ما سنفعله الآن هو أننا سننشئ المزيد من قواعد جدار الحماية. سنقوم بإنشاء واحد لـ HTTP ومن ثم سنقوم أيضًا بإنشاء البعض للتحقق من الصحة. لذلك اسمحوا لي فقط بالنقر فوق "إنشاء قاعدة جدار الحماية" وسيكون هذا مشابهًا إلى حد ما لما فعلناه بالفعل لمعمل موازن تحميل HTTP، والفرق الكبير هو أن لدينا الآن شبكتنا الخاصة التي سنقوم بتطبيق هذا عليها. سيكون لدينا أيضًا علامات مستهدفة ، وخلفية موازن التحميل ، ونطاقات IP، ونريد HTTP من أي مكان ، وسيكون HTTP هو TCP 80.
- لذلك يمكننا النقر فوق "إنشاء" ثم سنكرر نفس الشيء لـ المدقق الصحي. لذلك اسمحوا لي بنسخ اسم قاعدة جدار الحماية وتطبيقها على الشبكة الصحيحة للواجهة الخلفية لموازنة التحميل كعلامة الهدف. الآن نطاقات IP، سنقوم بنسخها واحدة تلو الأخرى هنا. لذلك اسمحوا لي أن ألصق واحدة ، قاعدتها ودعني أمسك بالآخر ، وألصقها أيضًا. في الوقت الحالي ، سأقوم فقط بجميع المنافذ تحت TCP، ولكن يمكنك أن تكون أكثر تحديدًا قليلاً اعتمادًا على ما تريد أن يبحث عنه المدقق الصحي.
- لننقر على "إنشاء" وسنقوم الآن بتكوين قوالب المثيل ومجموعات المثيل.

مراجعة معملية: تكوين موازن تحميل داخلي

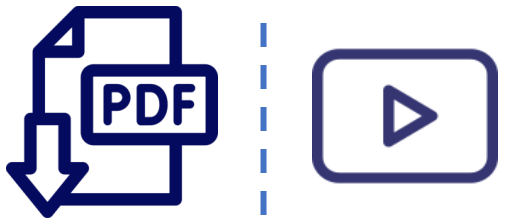
- لذلك اسمحوا لي بالانتقال إلى Compute Engine ثم Instance Templates.
- سنقوم بإنشاء قالب هناك واستدعاء نموذج المثيل واحد فقط.
- اسمحوا لي أن أنقر على "إنشاء". هذا هو الاسم الموجود بالفعل هناك ، ثم يمكنني توسيع أمان الإدارة ، إنه الشبكات. الآن شيئان ، أولاً وقبل كل شيء في موازن تحميل HTTP، كان لدينا صورة مخصصة. في هذه الحالة ، سنقوم بالفعل بإعداد برنامج نصي لبدء التشغيل. لذلك ، ضمن البيانات الوصفية ، سأقدم كمفتاح عنوان URL للنص البرمجي لبدء التشغيل ، وفي حاوية التخزين السحابية التي يمكن الوصول إليها بشكل عام ، قمنا بوضع ملف بدء التشغيل. يمكنك الذهاب إلى هناك ويمكنك بالفعل مراجعة ذلك والرابط الموجود في المختبر. ثم سأذهب إلى الشبكات. لقد قمت بإنشاء كل قواعد جدار الحماية هذه. تنطبق على علامات شبكة محددة وهي أيضًا لشبكة معينة. لذا دعني أتأكد من تحديد الشبكة الصحيحة.
- وحدد علامة الشبكة ، وسيكون هذا للشبكة الفرعية أ. لذا يمكنني الآن النقر فوق "إنشاء".
- ثم سنقوم بإنشاء نموذج مثيل آخر للشبكة الفرعية ب.


مراجعة معملية: تكوين موازن تحميل داخلي

- لذا دعني أنتظر حتى يتم إنشاء هذا ثم سأقوم بإنشاء واحد آخر من هناك عن طريق تحديده والنقر على "نسخ". سيتم تغيير الاسم تلقائيًا والفرق الرئيسي هو أنني الآن بحاجة للتأكد من تحديد الشبكة الفرعية المختلفة. سيكون هذا للشبكة الفرعية bثم انقر فوق "إنشاء" أيضًا. لذلك بمجرد أن نحصل على هذه ، يمكننا الآن إنشاء مجموعات المثيل المُدارة. لذلك اسمحوا لي بالانتقال إلى مجموعات المثيل وبدء التشغيل من خلال إنشاء المجموعة الأولى الخاصة بنا واسميها مجموعة المثيل الأولى. ستكون هذه منطقة واحدة. سيكون مركز الولايات المتحدة 1 أ.
- سنستخدم نموذج المثيل الأول وسنختار هذا على أساس استخدام وحدة المعالجة المركزية. لنقم بتعيين 80 على أنها استخدام ، بحد أدنى واحد بحد أقصى خمسة ، ويمكنني تغيير فترة التهدئة على سبيل المثال إلى 45 ثانية ، والآن يمكنني النقر فوق "إنشاء".
- يمكنني أيضًا إرفاق التحقق من الصحة هنا أو إرفاق ذلك لاحقًا بموازنة التحميل.
- بالتأكيد انقر فوق "إنشاء" وسنكرر نفس الشيء لمجموعة المثيل الثانية.
- وسيكون هذا الآن واحدًا آخر ، على أساس نموذج المثيل الآخر ، أيضًا في US central1.

مراجعة معملية: تكوين موازن تحميل داخلي

- دعونا نفعل ذلك في ب. على سبيل المثال ، قم بتغيير استخدام وحدة المعالجة المركزية المستهدفة لمطابقة ما كان لدينا سابقًا وهو 80 ، والحد الأقصى خمسة ، ثم تبريده إلى 45 ، ومن ثم يمكننا المضي قدمًا وإنشاء ذلك أيضًا.
- لذلك إذا قمت بالنقر فوق مثيلات VM الآن ، يجب أن يكون لدي بالفعل مثيل من مجموعة المثيل الأول ، وإذا عدت إلى هنا ، يجب أن أقوم بالتحديث لرؤية ذلك المثال الآخر. يمكننا أن نرى أنه يتم الآن إنشاء المثيل الآخر لمجموعة المثيل الثانية. حتى نتمكن من التحقق مرة أخرى من أنه يتم إنشاؤها هنا. لذلك نرى أن لدينا الآن مجموعة مثيل واحدة لكل منهما.
- والآن ما يمكننا فعله هو إنشاء أداة VM للتنقل إلى هذه الحالات. لذلك يمكننا أن نرى أيضًا بالمناسبة ، إذا نظرنا إلى عناوين IP الداخلية ، فهما جزء من موقع مختلف يرتبان ، وإذا نقرت على nic zero هنا ، يمكننا أن نرى واجهة الشبكة التي يمثل هذا جزءًا منها. يمكنك أن ترى أنه جزء من الشبكة الفرعية أ ، هذا صحيح.
- إذا قمت بالنقر فوق الجزء الآخر ، يمكنك رؤية هذا الجزء من الشبكة الفرعية ب.
- لذلك تحتوي كل شبكة فرعية الآن على مجموعة مثيل بداخلها.

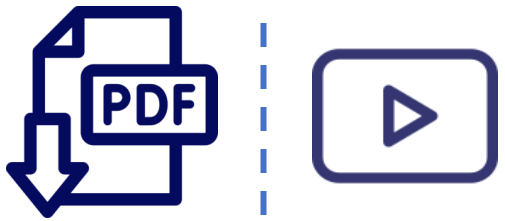


مراجعة معملية: تكوين موازن تحميل داخلي

- لذا اسمحوا لي أن أنشئ حالة أخرى. سيكون هذا هو الأداة المساعدة VM الخاصة بنا.
- الآن موازن التحميل الداخلي إقليمي ، لذلك أريد استخدام نفس المنطقة. يمكننا استخدام منطقة مختلفة ، دعنا نقول الولايات المتحدة المركزية F1.
- أحتاج إلى آلة صغيرة جدًا لهذا الغرض فقط وأريد التأكد من وجودها في الشبكة الصحيحة ، لذا دعني أقوم بتوسيع هذا الخيار لأسفل هنا ، والتواصل والتأكد من أن هذا موجود في شبكتي الصحيحة. لدي خيار بين شبكتين فرعيتين مختلفتين هناك ، دعنا نرى ما إذا كانت الشبكة الفرعية أ. إذا كنت أرغب في مطابقة هذا مع مخطط الشبكة الذي لدينا ، فيمكنني تحديد عنوان IP الداخلي الفعلي. لذا فبدلاً من خاصية Ephemeral Automatic، يمكنني اختيار مخصص سريع الزوال ، ثم اكتب فقط عنوان IP هذا. مرة أخرى ، هذا فقط لمطابقة مخطط الشبكة الذي لدينا.
- يمكنني النقر فوق "تم" على ذلك وبعد ذلك يمكنني المضي قدمًا وإنشاء ذلك.

مراجعة معملية: تكوين موازن تحميل داخلي

- الآن تشير إرشادات المعمل إلى التأكد من أن عناوين IP التي لديك تتطابق مع إرشادات المعمل. هذا لأن هذه هي عناوين IP المتاحة الأولى.
- مرة أخرى ، الأول والثاني محجوزان بالإضافة إلى الأخير والثاني حتى الأخير ، ولهذا نبدأ بالنقطة الثانية هنا وهنا لدينا النقطة 50 لأننا حددنا ذلك. لذا يمكنني الآن الانتقال إلى SSH إلى الأداة المساعدة VM وتستند جميع أوامر curl إلى هذين IPs لذلك يختلف المشاهدون. ربما تريد معرفة ما إذا كان لديك بعض الحالات الأخرى التي تحتاج إلى حذفها أولاً. سأقوم بالتجعيد أولاً إلى عنوان IP الأول هنا. لذا اسمحوا لي فقط بنسخ ذلك مباشرة من تعليمات المختبر. ما يتم عرضه هنا هو فقط الصفحة التي قمنا بإعدادها لهذه الحالات. يأتي هذا مباشرة من البرنامج النصي لبدء التشغيل ، وهو يخبرني فقط بعنوان IP الذي أتيت منه. حسنًا ، لقد جئت من هذا إلى الأداة VM، وهو يحمل الاسم ، وهذا يخبرني أنه قادم إلى هذه الحالة.
- ويخبرني بالمنطقة والمنطقة ويمكنني تكرار الأمر نفسه للمثال الآخر.
- ولا يخبرني أنا مرة أخرى من نفس العنوان ، ولكن حالة مختلفة ومنطقة مختلفة.

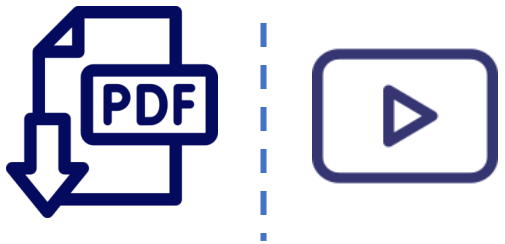


مراجعة معملية: تكوين موازن تحميل داخلي

- سيكون هذا مفيدًا حقًا عندما يكون لدينا إعداد موازن التحميل الداخلي. نحن نطلق على عنوان IP المتوازن نفسه ، يجب أن نكون قادرين على رؤية أنه إذا اتصلنا عدة مرات كان ذلك نوعًا من التنقل بين الخلفيات المختلفة التي أنشأناها. لذلك يمكننا بالفعل الخروج من هنا في الوقت الحالي ، وما سنفعله الآن هو تكوين موازن التحميل الداخلي. للقيام بذلك ، سأذهب إلى قائمة التنقل ، وأذهب إلى خدمات الشبكة ، وموازنة التحميل. سنقوم بإنشاء موازن تحميل. سيكون هذا موازنة تحميل TCP، لذا اسمحوا لي أن أبدأ ذلك. سيكون فقط بين أجهزة افتراضية ، وهذا موازن تحميل داخلي. عندما أفعل ذلك يقيدني أن أكون إقليميًا. لقد غطينا ذلك في الشرائح أن موازن التحميل الداخلي إقليمي ، لذلك سأقوم بالنقر فوق "متابعة" ثم سأعطيه اسمًا. دعنا فقط نسميها موازن التحميل الداخلي الخاص بي.
- سنقوم بتكوين الواجهة الخلفية. على وجه التحديد ، هذا في منطقة معينة مما يمنحك مركزية 1.
- الشبكة هي تطبيقي الداخلي ثم مجموعة المثيل ، سنختار مجموعة المثيل الأول.
- ثم انقر على "تم" ثم نضيف خلفية أخرى والتي ستكون مجموعة المثيل الثانية ثم انقر على "تم" لذلك.

مراجعة معملية: تكوين موازن تحميل داخلي

- الآن لم ننشئ فحصًا صحيًا سابقًا ، يمكننا القيام بذلك هنا الآن. لذلك اسمحوا لي أن أبدأ في إنشاء فحص صحي ، فقط أطلق عليه فحص صحة ib الداخلي الخاص بي TCP 80
- هذا رائع ، وهنا مرة أخرى لدينا معايير الصحة ، وسوف نتحقق من الفاصل الزمني ، والوقت المستقطع ، وكيف سيتم ذلك تحديد ما إذا كانت النهاية الخلفية صحية أم غير صحية. لذلك دعونا نحفظ ونواصل ذلك. يمكننا أن نرى أن لدينا علامة اختيار زرقاء. تم إعداد هذا كله. حتى الآن يمكنني النقر فوق تكوين الواجهة الأمامية ، الشبكة الفرعية. دعنا على سبيل المثال نضع هذا في الشبكة الفرعية ب. بالنسبة إلى IPالداخلي ، يمكننا في الواقع الحفاظ على عنوان IPداخلي ثابت. دعنا نعطي هذا الاسم ، والذي يسمى IP الداخلي المتقدم الخاص بي ، وبدلاً من التعيين تلقائيًا ، يمكننا اختيار اسمنا الخاص لأنه مجرد عنوان IP داخلي ويمكننا مطابقة هذا مرة أخرى مع مخطط الشبكة.



مراجعة معملية: تكوين موازن تحميل داخلي

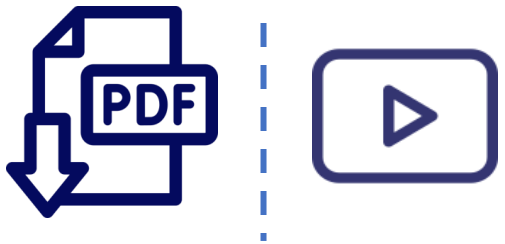
- لذلك سيكون 10.10.30.5 ، دعنا نحتفظ بذلك ، وبعد ذلك سننهي تكوين موازن التحميل عن طريق تعيين المنفذ هنا على 80 ، وسأضغط على "تم" والآن يمكننا مراجعة ونضع اللمسات الأخيرة على هذا ، لدينا خلفيتان. نرى القياس التلقائي على ذلك ، نرى المناطق ولدينا الواجهة الأمامية نفسها. لذلك لدينا عنوان IP الدقيق ، الطريقة التي يمكننا بها الوصول إلى موازن التحميل الداخلي هذا. لذلك اسمحوا لي أن أنقر فوق "إنشاء" ثم دعنا ننتظر حتى يتم إنشاء موازن التحميل قبل أن ننتقل إلى الخطوة التالية. لذلك نحن هنا ، في الواقع ، أنقر فوق "تحديث" ويمكننا أن نرى أن موازن التحميل قد تم إعداده بالكامل. الآن حددنا عنوان IP، لذا لا يتعين علي الحصول عليه من هنا.

مراجعة معملية: تكوين موازن تحميل داخلي

- بدلاً من ذلك ، سأعود إلى مثيلات Compute Engine الخاصة بي وأستخدم الأداة المساعدة VM للتنقل إلى عنوان IP الخاص بموازن التحميل. لذلك سأقوم فقط بتجفيف ذلك ، وبما أن لديّ برنامج بدء التشغيل هذا على الواجهة الخلفية ، فإن هذا يحدد المثال الذي أبحث عنه. سيعطيني هذا الآن المزيد من المعلومات.
- لذلك سأقوم بتجعيد عنوان IP وفي المرة الأولى التي قمت فيها بذلك ، يمكنك أن ترى أنه يستهدف مجموعة المثيل الثانية.
- لنقم بتشغيل ذلك مرة أخرى ، مجموعة المثيل الثانية مرة أخرى ، نصي الثاني مرة أخرى.
- ربما يتم تشغيل الأمر عدة مرات ودعنا نرى ما إذا كان بإمكاننا الحصول على بضع خلفيات مختلفة.
- لذا قم بتشغيله هنا عدة مرات ، يمكنك أن ترى أن 2 ، 2 ، 2 ، 2 ، ثم يحتوي على 1 ، 2 ، 2 ، 2 ، 1.
- لذلك يمكننا بالتأكيد أن نرى أنه موازنة الأحمال بين الخلفيات المختلفة التي لدينا.
- وهذه نهاية المعمل.

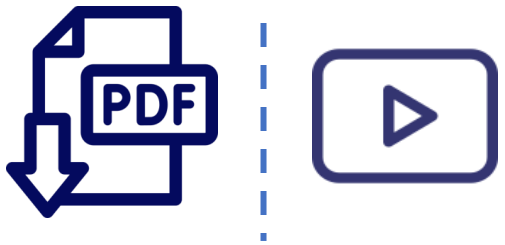
اختيار موازن التحميل

- الآن ، بعد أن ناقشنا جميع خدمات موازنة الأحمال المختلفة داخل GCP، دعني أساعدك في تحديد موازن التحميل الذي يلبي احتياجاتك بشكل أفضل. أحد الفوارق بين موازنات تحميل GCP المختلفة هو دعم عملاء IPv6 تدعم خدمات موازنة التحميل الوكيل HTTPS و SSL و TCP فقط عملاء IPV6 يمكّنك إنهاء IPv6 لموازنات التحميل هذه من معالجة طلبات IPv6 من المستخدمين وتوكيلهم عبر IPv4 إلى الواجهة الخلفية الخاصة بك.
- على سبيل المثال ، في هذا الرسم البياني ، يوجد موقع ويب ، www.example.com، تمت ترجمته بواسطة Cloud DNS إلى كل من عنوان IPv4 و IPv6 يتيح ذلك لمستخدم سطح المكتب في نيويورك ومستخدم الهاتف المحمول في ولاية أيوا الوصول إلى موازن التحميل من خلال عناوين IPv4 و IPv6 على التوالي. ولكن كيف تصل حركة المرور إلى الخلفيات وعناوين IPv4 الخاصة بهم؟ حسنًا ، يعمل موازن التحميل كوكيل عكسي.
- وينهي اتصال عميل IPv6 ويضع الطلب في اتصال IPv4إلى الواجهة الخلفية.



اختيار موازن التحميل

- على المسار العكسي ، يتلقى موازن التحميل استجابة IPv4 من الواجهة الخلفية ويضعها في اتصال IPv6 مرة أخرى إلى العميل الأصلي. بعبارة أخرى ، يتيح تكوين إنهاء Pv6 الموازنات التحميل الخاصة بك أن تظهر مثيلات الواجهة الخلفية كتطبيقات IPv6 لعملاء IPv6 ، الآن ، لتحديد موازن التحميل الذي يناسب تنفيذك لـ GCP، ضع في اعتبارك الجوانب التالية لموازنة تحميل السحابة. موازنة الحمل العالمي مقابل موازنة الحمل الإقليمي ، موازنة الحمل الخارجية مقابل الداخلية ، ونوع حركة المرور.
- إذا كنت بحاجة إلى خدمة موازنة تحميل خارجية ، فابدأ من أعلى يسار مخطط التدفق هذا. أولاً ، اختر نوع حركة المرور التي يجب أن يتعامل معها موازن التحميل. إذا كانت هذه هي حركة مرور HTTP أو HTTPS، فإنني أوصي باستخدام خدمة موازنة تحميل HTTPSكموازن تحميل للطبقة السابعة. بخلاف ذلك ، استخدم مسارات حركة مرور TCP و UDP للمخطط الانسيابي هذا لتحديد ما إذا كان وكيل SSL أو وكيل TCP أو خدمة موازنة تحميل الشبكة تلبي احتياجاتك.
- إذا كنت بحاجة إلى خدمة موازنة تحميل داخلية.



اختيار موازن التحميل

- فلديك خدمة موازنة التحميل الداخلية المتاحة وهي تدعم حركة مرور TCP و UD.
- كما ذكرت في بداية هذه الوحدة ، هناك بالفعل موازن تحميل داخلي آخر لحركة مرور HTTPS ولكنه في مرحلة تجريبية اعتبارًا من هذا التسجيل.
- موازن التحميل السادس مخصص لحركة مرور HTTP أو HTTPS ومعناه الإقليمي لعملاء IPv4.
- إذا كنت تفضل الجدول على مخطط انسيابي ، فإنني أوصي بهذا الجدول الموجز. يساعدك هذا الجدول في تحديد موازن التحميل الصحيح استنادًا إلى نوع حركة المرور ، وتوزيع الواجهة الخلفية الخاصة بك على الصعيد العالمي أو الإقليمي ، ونوع عناوين IP الخاصة بالواجهة الخلفية الخارجية أو الداخلية.
- يسرد هذا الجدول أيضًا المنافذ المتاحة لموازنة التحميل .
- ويسلط الضوء على أن Global Load Balancers فقط يدعم عملاء IPv4 و IPV6.

- **أي مما يلي ليس خدمة موازنة تحميل Google Cloud؟**
  - موازنة تحميل HTTP(S)
  - موازنة تحميل وكيل SSL
  - موازنة تحميل وكيل TCP
  - **موازنة تحميل المعرفة بالأجهزة**
  - موازنة حمل الشبكة
  - موازنة الحمل الداخلي

- **ما هي خدمات موازنة تحميل Google Cloud الثلاثة التي تدعم عملاء IPv6؟**
  - موازنة الحمل الداخلي
  - موازنة تحميل وكيل TCP
  - موازنة حمل الشبكة
  - موازنة تحميل HTTP(S)
  - موازنة تحميل وكيل SSL

- **أي مما يلي يُعد سياسات قياس تلقائي قابلة للتطبيق لمجموعات المثيل المُدارة؟**
  - عبء العمل المستند إلى قائمة الانتظار
  - مقاييس المراقبة
  - استخدام وحدة المعالجة المركزية
  - قدرة موازنة الحمل

مراجعة الوحدة

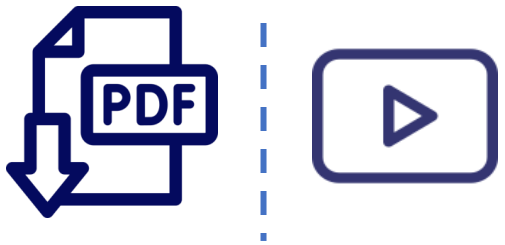
- في هذه الوحدة ، نظرنا في الأنواع المختلفة من موازنات التحميل المتوفرة في GCP جنبًا إلى جنب مع مجموعات المثيلات المُدارة والقياس التلقائي.
- ستتمكن من تطبيق معظم الخدمات والمفاهيم المغطاة من خلال العمل من خلال معملين لهذه الوحدة.
- ناقشنا أيضًا معايير الاختيار بين موازنات التحميل المختلفة وألقينا نظرة على مخطط انسيابي وجدول ملخص لمساعدتك في اختيار موازنات التحميل المناسبة.
- تذكر أنه من المفيد أحيانًا الجمع بين موازن التحميل الداخلي والخارجي لدعم خدمات الويب ذات المستويات الثلاثة.

وحدة نظرة عامة

- الآن بعد أن غطينا العديد من خدمات وميزات Google Cloud، فمن المنطقي التحدث عن كيفية أتمتة نشر البنية التحتية لـ Google Cloud ، يعد استدعاء Cloud API من التعليمات البرمجية طريقة فعالة لإنشاء البنية التحتية. لكن كتابة التعليمات البرمجية لإنشاء البنية التحتية تنطوي أيضًا على بعض التحديات. تتمثل إحدى المشكلات في أن قابلية صيانة البنية التحتية تعتمد بشكل مباشر على جودة البرنامج. على سبيل المثال ، يمكن أن يحتوي البرنامج على عشرات المواقع التي تستدعي Cloud API لإنشاء أجهزة افتراضية. يتطلب إصلاح مشكلة تعريف جهاز افتراضي واحد أولاً تحديد أي من عشرات المكالمات التي تم إنشاؤها بالفعل.
- سيتم تطبيق أفضل الممارسات القياسية لتطوير البرامج ، ومن المهم ملاحظة أن التطبيقات تخضع لتغييرات سريعة تتطلب صيانة التعليمات البرمجية الخاصة بك. من الواضح أن هناك حاجة إلى مستوى آخر من التنظيم وهذا هو الغرض من Terraform يستخدم Terraform نظامًا من القوالب عالية التنظيم وملفات التكوين لتوثيق البنية التحتية بتنسيق.
- يسهل قراءته وفهمه ، يخفي Terraform مكالمات Cloud API الفعلية .

وحدة نظرة عامة

- ذلك لا تحتاج إلى كتابة الكود ويمكن التركيز على تعريف البنية التحتية. في هذه الوحدة ، سنغطي كيفية استخدام Terraform لأتمتة نشر البنية التحتية وكيفية استخدام Google Cloud Marketplace لإطلاق حلول البنية التحتية.
- ستستخدم Terraform لنشر شبكة VPC وقواعد جدار الحماية ومثيلات VM في المختبر لهذه الوحدة.
- لنبدأ بالحديث عن Terraform.



Terraform

- حتى الآن ، كنت تقوم بإنشاء موارد google cloud باستخدام وحدة تحكم google cloud و cloud shell.
- نوصي بوحدة التحكم السحابية من Google، عندما تكون جديدًا في استخدام خدمة ما أو إذا كنت تفضل واجهة المستخدم. تعمل Cloud shell بشكل أفضل عندما تشعر بالراحة عند استخدام خدمة معينة وتريد إنشاء موارد بسرعة باستخدام سطر الأوامر.
- يأخذ Terraform هذه خطوة إلى الأمام
- Terraform، هي إحدى الأدوات المستخدمة للبنية التحتية كرمز أو IaC.
- قبل أن نتعمق في فهم التضاريس ، دعنا نلقي نظرة على البنية التحتية مثل الكود. في جوهرها ، تسمح البنية التحتية كرمز ، بتوفير وإزالة البنى التحتية بسرعة. عند الطلب ، يعد توفير النشر قويًا للغاية. يمكن دمج هذا في خط أنابيب تكامل مستمر ، مما يسهل المسار إلى النشر المستمر.
- التزويد المؤتمت للبنية التحتية ، يعني أنه يمكن توفير البنية التحتية عند الطلب.

الملف تفاعلي قم بالنقر على الأيقونة

Terraform

- كما تتم إدارة تعقيد النشر في التعليمات البرمجية. يوفر هذا المرونة لتغيير البنية التحتية مع تغير المتطلبات. كل التغييرات في مكان واحد. يمكن الآن للبنية التحتية لبيئات مثل التطوير والاختبار تكرار الإنتاج بسهولة ويمكن حذفها على الفور عندما لا تكون قيد الاستخدام ، وكل ذلك بسبب البنية التحتية كرمز. يمكن استخدام عدة أدوات لـ IaC.
- تدعم Google cloud terraform، حيث يتم وصف عمليات النشر في ملف يُعرف باسم التكوين. هذا يفصل جميع الموارد التي يجب أن تكون بارعة. يمكن تعديل التكوينات باستخدام القوالب ، مما يسمح بتجريد الموارد إلى مكونات قابلة لإعادة الاستخدام عبر عمليات النشر ، بالإضافة إلى terraform، يوفر google cloud أيضًا دعمًا لأدوات IaC الأخرى بما في ذلك CHEF و puppet و Ansible و Packer ، ومع ذلك ، في هذه الدورة ، سوف نركز على التضاريس.
- Terraform هي أداة مفتوحة المصدر تتيح لك توفير موارد google cloud .
- يتيح لك Terraform توفير موارد Google السحابية مثل الأجهزة الافتراضية والحاويات والتخزين والشبكات بملفات التكوين التعريفي.

الملف تفاعلي قم بالنقر على الأيقونة

Terraform

- ما عليك سوى تحديد الموارد المطلوبة في التطبيق الخاص بك بتنسيق تعريفي ، ونشر التكوين الخاص بك. تتيح لغة تكوين HashiCorp أو HCL وصفًا موجزًا للموارد باستخدام الكتل والوسيطات والتعبيرات. يمكن تكرار هذا النشر مرارًا وتكرارًا بنتائج متسقة ويمكنك حذف عملية نشر كاملة بأمر واحد أو بنقرة واحدة. تتمثل فائدة النهج التعريفي في أنه يسمح لك بتحديد التكوين الذي يجب أن يكون والسماح للنظام بتحديد الخطوات التي يجب اتخاذها. بدلاً من نشر كل مورد على حدة ، فإنك تحدد مجموعة من الموارد ، التي تؤلف التطبيق أو الخدمة ، مما يسمح لك بالتركيز على التطبيق. على عكس Cloud shell، فإن terraform سينشر الموارد بشكل متوازٍ. يستخدم Terraform واجهات برمجة التطبيقات الأساسية لكل خدمة سحابية من Google لنشر مواردك.
- يمكّنك هذا من نشر كل شيء رأيناه حتى الآن تقريبًا. من الطبعات إلى قوالب المثيل والمجموعات إلى شبكات VPC وقواعد جدار الحماية وأنفاق VPN والموجهات السحابية وموازنات التحميل.
- للحصول على قائمة كاملة بأنواع الموارد المدعومة.

Terraform

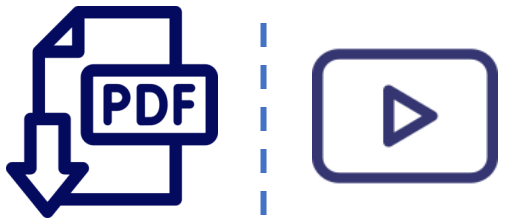
- تم تضمين ارتباط إلى استخدام terraform لصفحة توثيق google cloud في موارد الدورة التدريبية. لغة التضاريس هي واجهة مستخدم للإعلان عن الموارد. الموارد ، هي كائنات البنية التحتية مثل محرك الحوسبة ، وحاويات التخزين ، وما إلى ذلك. تكوين التضاريس ، هو مستند كامل بلغة التضاريس التي تخبر التضاريس بكيفية إدارة مجموعة معينة من البنية التحتية.
- يمكن أن يتكون التكوين من ملفات وأدلة متعددة.
- يتضمن بناء جملة لغة التضاريس ، الكتل التي تمثل الكائنات ويمكن أن تحتوي على صفر أو أكثر من التسميات. الكتلة ، لها جسم يمكّن المرء من إعلان الوسائط والكتل المتداخلة. تُستخدم الوسيطات لتعيين قيمة للاسم والتعبيرات ، والتي تُستخدم لتعيين قيم لمعرفات مختلفة. يمكن استخدام Terraform على العديد من السحب العامة والخاصة. تم تثبيت Terroform بالفعل في Cloud shell.
- يبدأ المثال ، ملف التكوين ، الموضح على اليمين ، بالإشارة إلى أن الموفر هو google cloud.
- ما يلي ، هو تكوين مثيل محرك الحوسبة والقرص الخاص به.

Terraform

- يسمح قسم المخرجات بالحصول على عناوين IP للطبعة المزودة من النشر. دعنا نلقي نظرة على مثال بسيط في terraform.
- قبل الدخول إلى المعمل ، دعني أطلعك على كيفية استخدام terraform لإعداد شبكة الوضع التلقائي باستخدام قاعدة جدار الحماية http.
- في هذا المثال ، سنقوم بتعريف بنيتنا التحتية في ملف واحد ، main.tf .
- نظرًا لأن بنيتنا التحتية تصبح أكثر تعقيدًا ، يمكننا بناء كل عنصر في ملف منفصل لتسهيل الإدارة.
- لنبدأ بملف main.tf ملف main.tf هو المكان الذي نحدد فيه البنية التحتية التي نرغب في إنشائها. إنه بمثابة مخطط لحالتنا التي نرغب فيها. أولاً ، نحدد المزود. بعد ذلك ، نحدد شبكتنا ، ونضبط علامة الإنشاء التلقائي للشبكات الفرعية على true، والتي ستنشئ تلقائيًا شبكة فرعية في كل منطقة.
- قمنا أيضًا بتعيين mtu على 1460.

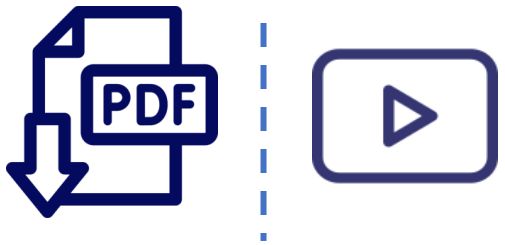
Terraform

- بعد ذلك ، نحدد جدار الحماية الخاص بنا. هنا ، نسمح بوصول tcp عبر المنفذ 80 والمنفذ 8080. يأخذ Terraform ملف main.tf هذا ويستخدمه كمواصفات لما يتم إنشاؤه. بمجرد الانتهاء من ملف main.tf، يمكننا نشر البنية التحتية المحددة في Cloud shell.
- نستخدم الأمر terraform init لتهيئة تكوين جديد للتضاريس. نقوم بتشغيل هذا الأمر في نفس المجلد مثل ملف main.tf. يتأكد الأمر terraform init من تنزيل المكون الإضافي لموفر Google وتثبيته في دليل فرعي من دليل العمل الحالي. إلى جانب العديد من ملفات مسك الدفاتر الأخرى ، سترى رسالة تهيئة المكونات الإضافية للمزود ، يعرف Terraform أنك تعمل من مشروع google وأنك تحصل على موارد Google ينفذ أمر خطة terraform تحديثًا ، ما لم يتم تعطيله بشكل صريح ، ثم يحدد الإجراءات اللازمة لتحقيق الحالة المطلوبة المحددة في ملفات التكوين. يعد هذا الأمر طريقة ملائمة للتحقق مما إذا كانت خطة التنفيذ لمجموعة من التغييرات تتطابق مع توقعاتك ، دون إجراء أي تغييرات على الموارد الحقيقية أو على الحالة.
- يقوم الأمر terraform application بإنشاء البنية التحتية المحددة في ملف main.tf.
- بمجرد اكتمال هذا الأمر ، ستتمكن من الوصول إلى البنية التحتية المحددة.



- **مقدمة المعمل: أتمتة البنية التحتية للشبكات باستخدام** Terraform

- **دعنا نطبق ما تعلمته للتو في معمل عملي حيث ستقوم بأتمتة نشر شبكات** VPC **وقواعد جدار الحماية ومثيلات الأجهزة الافتراضية.**
- **تقوم بنشر شبكة ذات وضع تلقائي تسمى** My Network **مع قاعدة جدار حماية للسماح بحركة مرور** http **أو** ssh **أو** DP **و** ICMP.
- **يمكنك أيضًا نشر مثيلات الجهاز الظاهري الموضحة في مخطط الشبكة هذا.**



- **معمل – LAB: أتمتة البنية التحتية للشبكات باستخدام Terraform**

- في هذا التمرين المعملي ، تقوم بإنشاء تهيئة Terraform مع وحدة لأتمتة نشر البنية الأساسية لـ GCP.
- نصائح لمختبرات الدورة التدريبية
- احصل على أقصى استفادة من Coursera و Qwiklabs من خلال تجربة نصائحنا أدناه.
- تجنب الخلط بين الحساب والتصفح الخاص.
- أغلق هذه الصفحة وسجل الدخول مرة أخرى إلى Coursera في وضع التصفح المتخفي قبل الانتقال.
- عند العودة إلى هذه الدورة التدريبية وصفحة الإرشادات المعملية ، انقر فوق "فتح الأداة" للمتابعة.
- تجنب الخلط بين الحساب والتصفح الخاص.

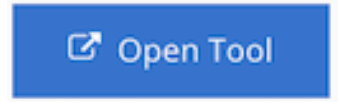
- **معمل** – LAB: **أتمتة البنية التحتية للشبكات باستخدام** Terraform

- **باستخدام وضع التصفح المتخفي ، يضمن ذلك عدم استخدامك لحساب** Google **الخاص بك عن طريق الخطأ (بما في ذلك** Gmail) **أثناء الوصول إلى** Google Cloud Console.
- **يمنع هذا أيضًا** Qwiklabs **من تسجيل خروجك من حسابات** Google **الخاصة بك.**
- **الإرشادات التفصيلية لاستخدام وضع التصفح المتخفي في** Google Chrome **متوفرة هنا.**
- **اعتمادًا على المستعرض الخاص بك ، قد يُطلق على وضع التصفح المتخفي أيضًا اسم الاستعراض الخاص أو استعراض** InPrivate.

- **معمل** – LAB: **أتمتة البنية التحتية للشبكات باستخدام** Terraform

- **لضمان الانتهاء من المختبر تم وضع علامة عليه في كورسيرا:**

1. **قم بالوصول إلى كل معمل فردي بالنقر فوق فتح الأداة في كورسيرا**



2. **أكمل المختبر في** Qwiklabs
3. **انقر على "إنهاء المعمل" في** Qwiklabs

4. **أغلق نافذة أو علامة تبويب متصفح** Qwiklabs

- **معمل** – LAB: **أتمتة البنية التحتية للشبكات باستخدام** Terraform

- **للتفاعل مع المتعلمين الآخرين:**

إذا كنت تواجه أي صعوبة في المعامل ، فنحن نشجعك على النشر عنها في منتديات المناقشة الخاصة بهذه الدورة التدريبية. إذا لم تكن لديك مشاكل مع المعامل ، ففكر في تصفح منتديات المناقشة للحصول على فرص لمساعدة زملائك المتعلمين.

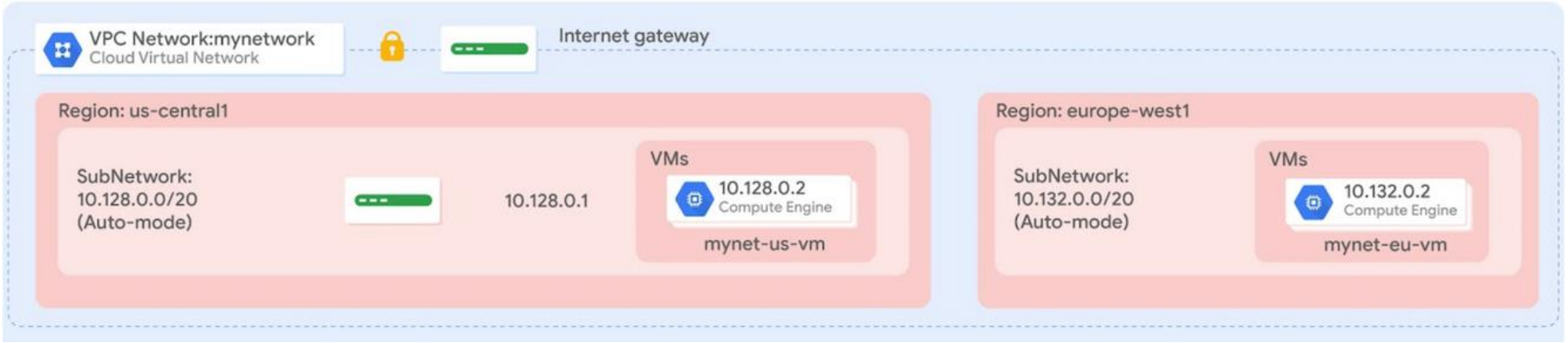
- **لتقديم طلب دعم:**

إذا كنت تواجه مشكلات فنية مع المختبرات أو التصنيف ، فيرجى إرسال طلب دعم هنا:

https://qwiklab.zendesk.com/hc/en-us/requests/new

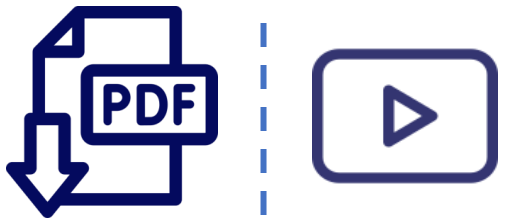
- **معمل** – LAB: Automating the Deployment of Infrastructure Using Terraform

- يتيح لك Terraform إنشاء البنية التحتية وتغييرها وتحسينها بأمان وبشكل متوقع.
- إنها أداة مفتوحة المصدر تقوم بترميز واجهات برمجة التطبيقات إلى ملفات تكوين تعريفية يمكن مشاركتها بين أعضاء الفريق ، ومعاملتها كرمز ، وتحريرها ، ومراجعتها ، وإصدارها.
- في هذا التمرين المعملي ، تقوم بإنشاء تهيئة Terraform مع وحدة لأتمتة نشر بنية Google Cloud الأساسية.
- على وجه التحديد ، تقوم بنشر شبكة واحدة ذات وضع تلقائي بقاعدة جدار حماية ومثيلين VM، كما هو موضح في هذا الرسم التخطيطي:



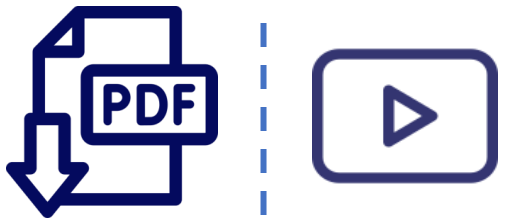
مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- في هذا التمرين المعملي ، أنشأت تهيئة Terraform بوحدة نمطية لأتمتة نشر البنية الأساسية لـ GCP.
- مع تغير التكوين الخاص بك ، يمكن لـ Terraform إنشاء خطط تنفيذ متزايدة ، مما يسمح لك ببناء التكوين العام الخاص بك خطوة بخطوة. سمحت لك وحدة المثيل بإعادة استخدام نفس تكوين الموارد لموارد متعددة مع توفير الخصائص كمتغيرات إدخال. يمكنك الاستفادة من التكوين والوحدة التي قمت بإنشائها كنقطة بداية لعمليات النشر المستقبلية.
- يمكنك البقاء في جولة ولكن تذكر أن واجهة مستخدم GCP يمكن أن تتغير ، لذلك قد تبدو بيئتك مختلفة قليلاً.
- لذلك أنا هنا في وحدة تحكم GCP وأول شيء نريد القيام به هو تهيئة بيئة Cloud Shell ، لاستخدام Terraform تم دمج Terraform الآن في Cloud Shell ، لذلك لنبدأ بالتحقق من الإصدار المثبت. لذلك سأضغط على تنشيط Cloud Shell ثم ابدأ Cloud Shell ، وبعد ذلك سنقوم بتشغيل أمر إصدار Terraform للتحقق من الإصدار.



- **مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام** Terraform

- اسمح لي بتشغيل ذلك هنا ثم سنرى أن هذا هو الإصدار الحالي الذي تم تكوينه. ترى أن هناك إصدارًا أحدث هنا. لا بأس ، يمكنك تنزيل ذلك وتوجد إرشادات في المعمل حول كيفية القيام بذلك. لكن تعليمات المعمل ستعمل مع 12.2 أو أي شيء لاحق. لذلك نحن على استعداد للذهاب. سأقوم بإعداد مجلد لنا ومن ثم سنقوم بتشغيل محرر الكود ، وهو رمز القلم الرصاص الصغير هنا. وسنستخدم محرر الكود الآن للعمل في هذا المجلد الذي أنشأناه للتو ووضع جميع ملفاتنا فيه. وستكون هذه تجربة تفاعلية أكثر بكثير من استخدام محرر سطر أوامر مثل Nano.
- لذا دعنا ننتظر حتى يأتي ذلك ، دعني أحاول توضيح هذا الأمر. وأول شيء سنفعله بمجرد دخولنا هنا هو أننا سننشئ ملفًا يسمى المزود TF وهذا سيساعدنا في تهيئة Terraform لأن Terraform يستخدم بنية قائمة على المكونات الإضافية لدعم العديد من مزودي الخدمات والبنية التحتية المختلفين. لذلك سيحدد ملف الموفر أننا نستخدم Google كمزود.



- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- لذلك اسمحوا لي أن أنقر بزر الماوس الأيمن على TF infra، وأنشئ ملفًا جديدًا كما هو الحال في المزود TF، ثم سنقوم فقط بنسخ ذلك المزود هو Google ويمكنني حفظ ذلك.
- تم تمكين الحفظ التلقائي بالفعل لذلك لن أضطر إلى النقر فوق حفظ طوال الوقت.
- ثم داخل القابض al، سأنتقل إلى هذا المجلد وبعد ذلك سأقوم بتشغيل الأمر Terraform init وسيؤدي ذلك الآن إلى تهيئة الموفر. لذلك يمكننا أن نرى هنا ، هذا هو إصدار الموفر تمت تهيئته. لذلك نحن الآن جاهزون للعمل مع Terraformو Cloud Shell.
- لذلك لنبدأ بتكوين شبكتي. سأقوم الآن بإنشاء ملف جديد في هذا المجلد. أطلق عليها اسم شبكتي TF.
- وسأقوم بنسخ الغلاف الأساسي الذي لدينا في تعليمات المختبر.
- إذن لدينا هنا تعليق ، لدينا البحث.
- والنوع جنبًا إلى جنب مع الاسم ، وبعد ذلك سيكون لدينا أيضًا خصائص الموارد.
- وهذا نموذج أساسي رائع لبدء أي موارد في GCP.

- **مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام** Terraform

- **وستستخدم الاسم ومجال حقل الاسم ، بالإضافة إلى حقل النوع والخصائص لتحديد ما يفعله كل من هذه الموارد حقًا. لذلك أول الأشياء أولا. أريد استبدال النوع بـ** Google_compute_Network.
- **والمهم هنا هو تضمين هذه الاقتباسات لجميع الموارد التي سنقوم بتعريفها. وهذه مجرد شبكة** VPC**، يمكنك العثور على المزيد حول هذا الموضوع في رابطي التوثيق الموجودين في المعمل. يرتبط أحدهما بوثائق** Google Cloud platform **والروابط الأخرى لوثائق** Terraform.
- **الآن ، أريد أيضًا استبدال الاسم. لذلك سنضع اسم البحث مع شبكتي مرة أخرى ، ثم سنقوم بإنشاء بعض الخصائص.**
- **ستكون هذه شبكة خريفية خاصة ، مما يعني أن كل هذه الشبكات الفرعية يتم إنشاؤها تلقائيًا.**

الملف تفاعلي قم بالنقر على الأيقونة

- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

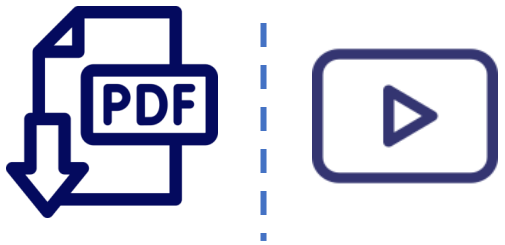
- أحتاج إلى تحديد ذلك ، الخصائص اختيارية لبعض الموارد. ولكن في هذه الحالة ، يجب أن نقول إن إنشاء الشبكات الفرعية تلقائيًا صحيح ، أليس كذلك؟ الآن ، يمكنني التحقق من أن ملفي يبدو تمامًا مثل ما تم توفيره في المختبر. ويبدو أن هذا صحيح. لقد تحركت وتباعدت بعض هذه الخصائص ، فهناك أمر سنقوم بتشغيله لاحقًا والذي سيفعل ذلك بالفعل لنا أيضًا. لذلك هذا ليس حرجًا حقًا في الوقت الحالي. يمكنني المضي قدما وحفظ هذا. الآن بعد ذلك ، أريد تكوين قاعدة جدار الحماية. لدي مرة أخرى بعض التعليمات البرمجية الأساسية لذلك. لذا دعني ألصق ذلك أسفل مورد الشبكة الخاص بي.
- سنقوم بإنشاء ملف سيحكم سيسمح HTTP sh RTP و icmp.
- لذلك من الواضح أنني أريد أن أجد النوع الصحيح. الآن ، يمكنك البحث عن ذلك في وثائق Terraform أو استخدام ما هو موجود في إرشادات المعمل وهو جدار حماية Google.
- ومرة أخرى ، نحتاج إلى وضع علامتي الاقتباس حول ذلك مع ترك مسافة بينهما.
- سيكون لدي أيضًا اسم سيكون اسم قاعدة جدار الحماية.

- **مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform**

- الذي سنراه في الواقع داخل GCP عندما ننشئ هذا والآن هما نوعان من خصائص الموارد المختلفة التي أحتاج إلى توفيرها. إذا كنت تفكر في قاعدة جدار الحماية ، فهناك أمران أساسيان. هناك الشبكة التي تنطبق عليها قاعدة جدار الحماية. هناك نطاقات IP المصدر والبروتوكولات والمنافذ. إذا لم تحدد نطاقات IP المصدر ، فسيتطلب الأمر 0.0.0.0 / 0 فقط ، لذلك في حالتنا ، سنقوم بتعريف الشبكة.
- لذا دعني ألصق ذلك هنا ولأن قاعدة جدار الحماية تعتمد على شبكتها ، فإننا نستخدم مرجع الارتباط الذاتي هذا هنا. وهذا يوجه Terraform لحل هذه الموارد بترتيب تابع. لذلك في هذه الحالة ، يجب إنشاء الشبكة قبل إنشاء قاعدة جدار الحماية. سنفعل الشيء نفسه عندما ننشئ مثيلات VM ، لذا اسمحوا لي الآن أيضًا أن أضيف الخصائص للسماح بمجموعة معينة من البروتوكولات والمنافذ والسماح بها. على وجه التحديد.
- سأقوم بتسجيل TCP 22 لـ RTP 338294 HTTP 84 SSH ثم بروتوكول icmp بأكمله.
- وأنه يمكنني التحقق من أن هذا يبدو تمامًا مثل التعليمات المعطاة لي.

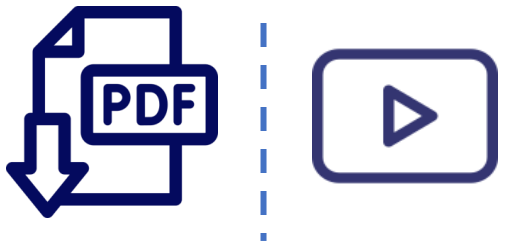

- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- وهذا هو الحال ، لذا يمكنني المضي قدمًا وحفظ ذلك ولكن يتم حفظه تلقائيًا. لذلك لا داعي للتوفير طوال الوقت هنا.
- لذلك سنقوم الآن بتكوين مثيلات DVM وما سنفعله هو أننا سننشئ وحدة مثيل والوحدة هي لشيء يمكن إعادة استخدامه داخل مجلد. لذلك سننشئ وحدة واحدة وسنستخدمها لكل من مثيلات VM التي ستنشئها. للقيام بذلك ، نحتاج إلى إنشاء مجلد للوحدة. لذا دعني أنشئ مجلدًا جديدًا هنا ، وأطلق عليه مثيلًا داخل TF لمجلد وترى أنه أنشأه بالخارج. لذا سأقوم بسحبه في هذا المجلد. بدلاً من ذلك ، كان بإمكاني النقر بزر الماوس الأيمن وإنشاءه وسيظهر المعمل التسلسل الهرمي لهذه المجلدات. والآن داخل هذا المجلد ، سأقوم بإنشاء ملف وأطلق عليه اسم TF الرئيسي. حسنًا ، والآن داخل هذا الملف ، سنقوم مرة أخرى بنسخ بعض التعليمات البرمجية الأساسية لنبدأ. لدينا نوع البحث واسم البحث والنوع الذي سيكون مثيلًا لحساب Google لذا اسمحوا لي أن أستبدل ذلك بالاقتباسات.
- الآن ، بدلاً من إعطائها اسمًا ونوعًا من الترميز الصعب ، سأستخدم الآن متغيرًا.
- لأنني أريد أن أكون قادرًا على إنشاء مثيلات متعددة بأسماء مختلفة متعددة.



- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- لذلك سأقوم باستبدال اسم TF بهذا البناء ومن ثم حيث يتعين لاحقًا تحديد كيفية التأثير على هذه الوحدة من التكوين الأصلي.
- سنقوم أيضًا بإضافة بعض الخصائص وهي المنطقة ونوع الجهاز.
- وهنا مرة أخرى ، نستخدم المتغيرات التي يتعين علينا تحديدها.
- سنقوم أيضًا بإضافة قرص تمهيد. قرص تمهيد آخر ، سنقوم فقط بنوع من الكود الثابت ، وسنمنحه صورة وسيتم استخدامها لجميع الحالات التي نقوم بإنشائها. وبعد ذلك سنضيف أيضًا واجهة شبكة. وهناك ، علينا تحديد شبكة فرعية.
- فأين يعيش هذا المثال؟ وإذا قمت فقط بتقديم هذا البناء هنا ، فسنقوم بتخصيص عنوان IP خارجي أو عنوان IP عام لمثيلتي. الآن ، أنا بحاجة إلى تحديد بعض متغيرات الإدخال ، أليس كذلك؟ لذلك أنا أستخدم متغير إدخال للاسم والمنطقة والنوع والشبكة الفرعية. لذا اسمحوا لي أن أضيف بعض الأشياء فوق موردي.
- وعلى وجه التحديد ، سأضيف متغيرًا للاسم والمنطقة.

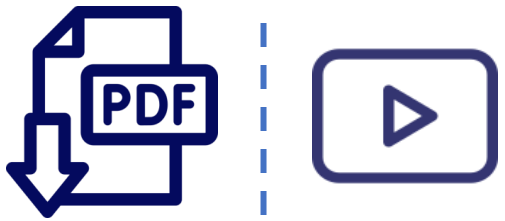


- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- سأقوم أيضًا بتحديد نوع المثيل وإذا قدمت قيمة بين هذه الأقواس ، فستكون هذه هي القيمة الافتراضية. لذلك إذا لم أقدم قيمة أخرى من تهيئتي ، فسيستخدم هذا النوع فقط وهذا نوع من الإعداد الافتراضي على أي حال ، لذلك ربما يكون هذا أمرًا جيدًا. كان بإمكاننا فعل شيء مشابه للصورة وبهذه الطريقة يمكننا التحكم في الصورة من خلال متغير إدخال. الآن ، سأقوم فقط بالتحقق من أن تهيئتي أو يجب أن أقول أن هذه الوحدة تبدو تمامًا مثل إرشادات المختبر وهذا صحيح. الآن ، يمكنني الاستمرار وحفظ هذا والشيء التالي الذي يتعين علينا القيام به هو أننا حددنا الوحدة ولكننا الآن بحاجة إلى استخدام الوحدة ضمن تهيئتي. هنا ، لديّ شبكة وإذا كنت سأحكم ، لكنني الآن أريد أيضًا أن أقول إنني أريد إنشاء مثيلات VM. سأقدم متغيرات الإدخال هذه وهذه هي الوحدة التي أريدك أن تستخدمها.

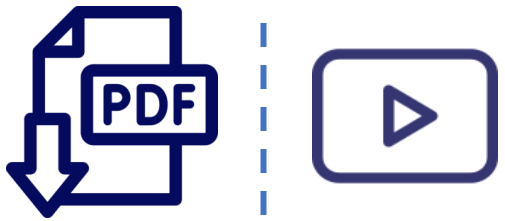
- **مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform**

- سأقوم فقط بنسخ تعليمات المختبر هنا. أنا أحدد الوحدة. أعطيها الاسم ثم أقوم بتعريف المصدر ، وهذا موجود في مجلد المثيل. ثم أقوم بتقديم ثلاثة من متغيرات الإدخال الأربعة لأن لدي بالفعل قيمة افتراضية لأحدها. المهم الآن مرة أخرى هو أنني سأستخدم مرجع الارتباط الذاتي هنا لأنني لا أستطيع إنشاء هذه الحالات أو قاعدة جدار الحماية حتى يتم إنشاء الشبكة. بعد ذلك ، يمكن إنشاء كل هذه الموارد وسيتم إنشاؤها بشكل متوازٍ في وقت لاحق.
- لذلك دعونا نمضي قدمًا ونقوم بإعداد كل هذا. سأقوم الآن فقط بالعمل من Cloud Shell، اسمحوا لي أن أوضح هذا هنا. سنقوم بتشغيل الأمر Terraform fmt وهذا فقط يعيد كتابة ملفات D إلى تنسيق وأسلوب أساسيين. وإذا فعلت ذلك ، فربما تكون قد رأيت للتو أن كل شيء قد تم وضعه قليلاً هنا وهناك ، فهذا ليس حرجًا حقًا. إنه يخبرنا فقط أنه فعل ذلك وبالتحديد ، لقد لامس ملفك شبكتي.



- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- وإذا تلقيت خطأ هنا ، فأنت تريد التأكد من أن التكوين الخاص بك يبدو مشابهًا لتلك الموجودة لدينا حتى الآن. نقوم أيضًا بربط التكوين الذي قام بجميع ملفات TS الثلاثة التي قد لا يبقى الموفر في إرشادات المختبر. لذلك يمكنك دائمًا الرجوع إليهم والتأكد من توافقهم مع ما لديك وإذا لم يكن كذلك ، فأنت تعلم إصلاح ما هو مختلف. الآن سأحتاج إلى تشغيل Terraform، أمر دقيقة مرة أخرى ، وأحتاج إلى القيام بذلك بشكل أساسي لأن لدي الآن وحدة نمطية. سيقول أن هناك بعض الوحدات التي يجب استخدامها ، دعني أبدأها. لقد فعلنا ذلك والآن يمكننا المضي قدمًا والتخطيط لتكويننا. لذا يمكننا أن نقول حسنًا ، نحن على استعداد للذهاب. أخبرني ما الذي ستنشئه عندما أقوم بتشغيل هذا الأمر. لذا ستعمل خطة Terraform خلال هذا وستخبرني أنها ستنشئ هذه الموارد هنا. يخبرني أنه يتم توفير الكثير من القيم ، لكن بعض القيم لن تكون معروفة إلا بعد إنشائها. وبالتحديد ، ستضيف أربعة أشياء مختلفة ، شبكة VPC، وقاعدة جدار الحماية ، والمثالين. لذلك إذا كنا جميعًا جيدًا في ذلك.
- فيمكننا تشغيل أمر تطبيق Terraform.



- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

- سوف يرشدنا في الواقع عبر هذه الموارد مرة أخرى ، ولكن الآن سيسألنا عما إذا كنا مستعدين. لذلك نحن فقط نكتب "نعم" هنا وسوف نبدأ في إنشاء الموارد ويمكنك أن ترى أن الشبكة هي المورد الأول الذي يتم إنشاؤه هنا. وبمجرد إنشاء الشبكة ، ستبدأ في إنشاء جميع الموارد الأخرى بالتوازي. كما أنه يعطينا تحديثًا كل 10 ثوانٍ قائلاً إنه لا يزال يعمل على هذا وهذا أمر مثير للاهتمام. وبهذه الطريقة يمكنك أن ترى أنه على الأقل لا يزال يعمل على هذا ولم أتعثر في شيء ما. لذا دعنا ننتظر حتى يكتمل هذا ثم سنعود مرة أخرى ، هنا ، يمكننا أن نرى أنه تم إنشاء جميع الموارد. كما ذكرت ، يتم إنشاء الشبكة أولاً. وبمجرد اكتمال ذلك ، يمكنك رؤية إحدى حالات قاعدة جدار الحماية ، ويتم البدء في إنشاء المثيلات الأخرى. تم إنشاء الحالات بسرعة كبيرة. وبعد ذلك ننتظر فقط إنشاء قاعدة جدار الحماية. الآن ، دعنا نتحقق بالفعل من إنشاء جميع هذه الموارد من خلال الانتقال مرة أخرى إلى وحدة تحكم gcp لذلك سأقوم بتبديل علامات التبويب هنا وانتقل إلى قائمة التنقل
- وانتقل أولاً إلى شبكة VPC وكل شبكة تأتي افتراضيًا بشبكة افتراضية موجودة هنا
- وهنا يمكننا أن نرى شبكتي التي أنشأناها وهي شبكة عثمانية.

- مراجعة معملية: أتمتة البنية التحتية للشبكات باستخدام Terraform

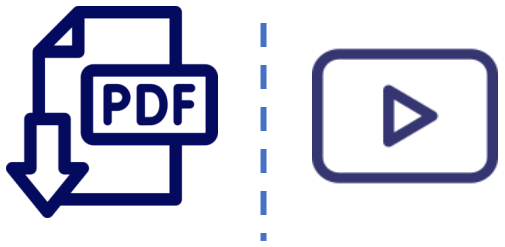
- يمكنه أيضًا الانتقال إلى قواعد جدار الحماية وسأرى أنه قد تم إنشاء قاعدتي النهائية المخصصة مع قاعدة الملف غير الافتراضية. وهذا من شأنه أن يسمح لي بإجراء اختبار ping بين الحالتين اللتين لديهما في الشبكة. لدي حركة مرور icmp مسموح بها. لذلك يجب أن أكون قادرًا على إجراء الأمر ping على عنوان IP الخارجي ، ولكن حتى عنوان IP الداخلي لأن هاتين الحالتين على نفس الشبكة. لذلك دعونا نجرب ذلك. سأعود إلى قائمة التنقل ، انتقل إلى محرك الحساب.
- وسأحصل على عنوان IP الخاص بهذا الجهاز الظاهري الأول ثم SSH إلى الجهاز الظاهري الآخر ثم سنحاول تنفيذ الأمر ping.
- ها انا ذا. اسمح لي بتشغيل الأمر ping ثلاث مرات على عنوان IP هذا.
- ويمكننا أن نرى أن جميع الحزم قد تم إرسالها. لذلك يجب أن يعمل هذا مرة أخرى لأن كلا مثيلي VM موجودان على نفس الشبكة وقاعدة جدار الحماية التي أنشأناها تسمح بحركة مرور icmp.
- وهذه نهاية المختبر.

Google Cloud Marketplace

- دعنا نتعلم المزيد عن Google Cloud Marketplace.
- يتيح لك Google Cloud Marketplace نشر حزم البرامج الوظيفية التي تعمل على Google Cloud بسرعة.
- بشكل أساسي ، يقدم Cloud Marketplace حلولًا على مستوى الإنتاج من موردي الجهات الخارجية ، الذين قاموا بالفعل بإنشاء تكوينات النشر الخاصة بهم بناءً على Terraform.
- تم إنشاء هذه الحلول جنبًا إلى جنب مع جميع مشاريع Google Cloud Services.
- إذا كان لديك بالفعل ترخيص لخدمة جهة خارجية ، فقد تتمكن من استخدام حل الترخيص الخاص بك أو إحضاره.
- يمكنك نشر حزمة برامج الآن وتوسيع نطاق هذا النشر عندما يتطلب التطبيق الخاص بك سعة إضافية.
- تقوم Google Cloud أيضًا بتحديث صور حزم البرامج هذه لإصلاح المشكلات.
- ونقاط الضعف الحرجة ولكنها لا تقوم بتحديث البرامج التي قمت بنشرها بالفعل.
- يمكنك حتى الوصول المباشر إلى دعم الشركاء.

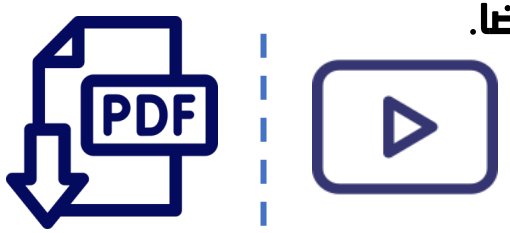
- عرض توضيحي: ابدأ في Google Cloud Marketplace

- اسمح لي أن أوضح لك كيفية إطلاق حلول البنية التحتية في GCP Marketplace.
- هدفي هو نشر مجموعة مصابيح على مثيل Compute Engine واحد.
- تتكون حزمة LAMP من Linux و Apache HTTP Server و MySQL و PHP.
- لذلك أنا هنا في وحدة تحكم GCP ودعنا نمضي قدمًا وننتقل إلى GCP Marketplace.
- سأذهب إلى قائمة التنقل وأذهب إلى السوق.
- الآن ، لدي الكثير من الخيارات المختلفة المتاحة.
- توجد بعض المرشحات على اليسار يمكنها البحث عن طريق البحث مباشرة.
- هناك بعض الحلول المميزة الموجودة هنا.
- لذلك هناك بالفعل الكثير من الأشياء للاختيار من بينها.
- في حالتي ، سأبحث عن مكدس LAMP لأن هذا ما أريد إنشاؤه.



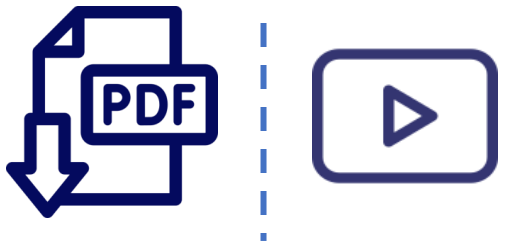
- عرض توضيحي: ابدأ في Google Cloud Marketplace

- هنا ، لدي بالفعل خيارات مختلفة ، هناك مزودين مختلفين ، وهذا ما يعنيه ذلك حقًا. سيقدم مختلف مقدمي هذه الخدمات. سأقوم بالنقر فوق أول واحد موجود هنا. الآن ، لدي صفحة التكوين. أرى محتويات العبوة. يخبرني أن ما هو LAMP مرة أخرى. أستطيع أن أرى أنهم هنا أيضًا ، نظام التشغيل هو Linux لقد تم تثبيت Apache ولديها PHP ولدي MySQL يجب أيضًا تمكين HTTP بشكل أساسي وسنرى ذلك في ثانية.
- لا توجد رسوم استخدام لهذه الخدمة ، إذا كانت كلها مبنية معًا. لدينا مثيل الفواتير. هذا مجرد مثيل n1-standard-1 مع قرصه الدائم ، وهناك خصم للاستخدام المستمر. لذلك إذا قمت بالنقر فوق تشغيل على Compute Engine، فسأحصل على صفحة تكوين VM الفعلية. يمكنني الآن تغيير نوع المثيل إذا أردت. يمكنني إنشاء حالات أكبر ، مثال صغير ، يمكنني تخصيص مثيل ، والآن ، نظرًا لأن هذا هو Apache HTTP، يمكننا أن نرى أنه تم إعداد قاعدة جدار حماية HTTP أيضًا.



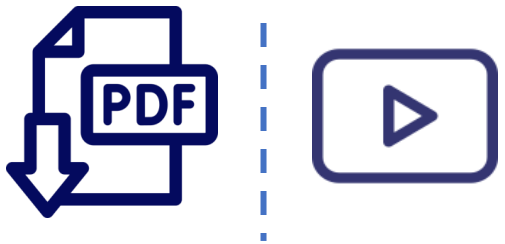
- عرض توضيحي: ابدأ في Google Cloud Marketplace

- لدي أيضًا بعض خيارات الشبكات إذا أردنا وضع هذا في مكان آخر ، فلدي أيضًا بعض الخيارات الإضافية إذا كنت أرغب في تثبيت PHP Myadmin، كل ما هو متاح لي هنا. قد يكون لدي خيارات تسجيل لـ Stackdriver لتمكين تسجيل Stackdriver ومراقبته ، ويمكنني القيام بذلك مباشرة هنا. لذا فهي تشبه صفحة مثيل VM عادية. لذلك سأذهب وأنقر على "نشر" ، وعندما أفعل ذلك ، سأنتقل بنا إلى Deployment Manager يمكنك رؤية كل التهيئة وكذلك جميع الملفات المستوردة معروضة هناك فقط والتي يتم استخدامها خلال هذا النشر. لذلك يمكننا أن نرى مرة أخرى أن الحلول الموجودة في السوق هي مجرد تكوينات Deployment Manager التي تم إعدادها بالفعل لتستخدمها حتى لا تضطر إلى إعادة إنشائها.
- أرى أيضًا أنه يتم إنشاء كلمات مرور ، يتم إنشاء جهاز افتراضي. يمكنني النقر فوق ذلك والحصول على مزيد من المعلومات حوله. يمكننا أن نرى أننا نستخدم في البرامج ولدينا قواعد جدار حماية HTTP.
- لذلك فقط TCPAD الذي يتم تمكينه هنا. لذلك يمكننا فقط انتظار ذلك.



- عرض توضيحي: ابدأ في Google Cloud Marketplace

- المثيل هو أعلى. إنه مجرد تكوين بعض البرامج الأخرى. ثم بمجرد تشغيله ، يمكننا الحصول على مزيد من المعلومات حول حزمة LAMP التي أنشأناها للتو. ثانيًا ، انقر مرة أخرى على LAMP، الذي لا يزال معلقًا. ولكن بمجرد تشغيله ، سيكون لدينا المزيد من المعلومات هنا.
- دعونا نرى. ليس لديه العنوان بعد. لا يزال معلقًا ، وها نحن ذاهبون. إذن لدينا عنوان ، لدينا مستخدم بكلمة مرور ، والمثال ، والمنطقة ، وجميع معلومات النوع. يمكننا زيارة الموقع ، يمكننا SSH لذلك. لدينا بعض الخطوات القادمة. يمكننا أيضًا فتح حركة مرور HTTPS، وتغيير كلمة المرور ، وتعيين عنوان IP خارجي ثابت بدلاً من الافتراضي الحالي إذا كان عنوان IP سريع الزوال.
- يمكننا معرفة المزيد عن البرنامج الجاري تثبيته. ولكن يمكننا أيضًا النظر إلى هذا من منظور Compute Engine.
- لذلك إذا انتقلت إلى Compute Engine، فسأرى أيضًا المثيل هنا.
- هذا هو مدى سهولة إطلاق حلول البنية التحتية في سوق GCP.

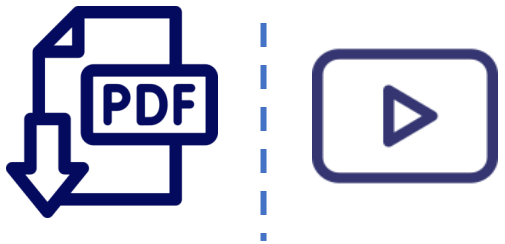


- **ما فائدة كتابة النماذج لتهيئة** Terraform؟
  - يسمح لك بتشغيل برنامج إدارة التكوين.
  - يسمح لك بتجريد جزء من التكوين الخاص بك في كتل بناء فردية يمكنك إعادة استخدامها
  - يسمح لك بترميز خصائص مواردك

- **ماذا يقدم** Google Cloud Marketplace؟
  - نظام فوترة مركزي لجميع خدمات وتطبيقات Google Cloud
  - حلول على مستوى الإنتاج من موردي الجهات الخارجية الذين قاموا بالفعل بإنشاء تكوينات النشر الخاصة بهم بناءً على Terraform
  - منصة لتداول مثيلات VM

مراجعة الوحدة

- في هذه الوحدة ، قمنا بأتمتة نشر البنية التحتية باستخدام Terraform، وألقينا نظرة على حلول البنية التحتية في Cloud Marketplace الآن ، قد تقول إن بذل كل الجهود لنشر شبكة ، وقاعدة جدار الحماية ومثيلين VM لا يقنعك باستخدام Terraform.
- هذا صحيح إذا كنت تحتاج فقط إلى إنشاء هذه الموارد مرة واحدة ولا تتوقع أبدًا الحاجة إلى إنشائها مرة أخرى.
- ومع ذلك ، بالنسبة لأولئك منا الذين يديرون العديد من الموارد ويحتاجون إلى نشرها وتحديثها وتدميرها بطريقة قابلة للتكرار ، تصبح أداة أتمتة البنية التحتية مثل Terraform ضرورية.



نظرة عامة عن الوحدة

- ناقشنا في الوحدة الأخيرة كيفية أتمتة إنشاء البنية التحتية. كبديل لأتمتة البنية التحتية ، يمكنك التخلص من الحاجة إلى إنشاء بنية أساسية من خلال الاستفادة من خدمة مُدارة. الخدمات المدارة هي حلول جزئية أو كاملة تقدم كخدمة. إنها موجودة في سلسلة متصلة بين النظام الأساسي كخدمة والبرنامج كخدمة اعتمادًا على مدى تعرض الأساليب والضوابط الداخلية. يتيح لك استخدام خدمة مُدارة الاستعانة بمصادر خارجية للكثير من النفقات الإدارية والصيانة إلى Google إذا كانت متطلبات التطبيق الخاص بك تتناسب مع عرض الخدمة. في هذه الوحدة ، نقدم لك نظرة عامة على BigQuery و Cloud Dataflow و Cloud Dataprep بواسطة Trifecta و Cloud Dataproc.
- الآن ، كل هذه الخدمات مخصصة لأغراض تحليل البيانات. ونظرًا لأن هذا ليس محور تركيز سلسلة الدورات التدريبية هذه ، فلن يكون هناك أي مختبرات في هذه الوحدة.
- بدلاً من ذلك ، سيكون لدينا عرض توضيحي سريع لتوضيح مدى سهولة استخدام الخدمات المدارة.
- لنبدأ بالحديث عن BigQuery.

BigQuery

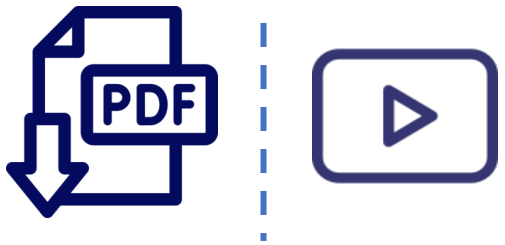
- BigQuery هو مستودع بيانات سحابي غير خوادم في Google Cloud وقابل للتطوير بدرجة عالية وفعال من حيث التكلفة.
- إنه مستودع بيانات بحجم بيتابايت يسمح باستعلامات فائقة السرعة باستخدام قوة معالجة البنية التحتية لـ Google.
- نظرًا لعدم وجود بنية أساسية يمكنك إدارتها ، يمكنك التركيز على الكشف عن رؤى ذات مغزى باستخدام SQL المألوف دون الحاجة إلى مسؤول قاعدة البيانات.
- يتم استخدام BigQuery بواسطة جميع أنواع المؤسسات. يمكنك الوصول إلى BigQuery باستخدام Cloud Console، باستخدام أداة سطر الأوامر ، أو عن طريق إجراء مكالمات إلى BigQuery rest API باستخدام مجموعة متنوعة من مكتبات العملاء مثل Java أو nash أو Python هناك أيضًا العديد من أدوات الجهات الخارجية التي يمكنك استخدامها للتفاعل مع BigQuery مثل تصور البيانات أو تحميل البيانات. فيما يلي مثال على استعلام SQL قياسي في جدول يسمى بقالة.
- ينتج عن هذا الاستعلام عمود إخراج واحد لكل عمود في الجدول باسم مستعار لمحلات البقالة G.

تدفق البيانات

- دعنا نتعلم قليلاً عن Cloud Dataflow.
- Cloud Dataflow هي خدمة مُدارة لتنفيذ مجموعة متنوعة من أنماط معالجة البيانات.
- إنها في الأساس خدمة مُدارة بالكامل لتحويل وإثراء البيانات في أوضاع الدفق والدُفعات بموثوقية وتعبير متساويين.

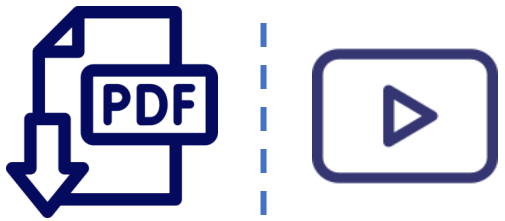
باستخدام Cloud Dataflow، يتم التعامل مع الكثير من تعقيدات إعداد البنية التحتية وصيانتها نيابة عنك.

- إنه مبني على البنية الأساسية لـ Google Cloud وتم تعديله تلقائيًا لتلبية متطلبات خط أنابيب البيانات لديك ، مما يسمح له بالتوسع بذكاء ليشمل ملايين الاستعلامات في الثانية ، يدعم Cloud Dataflow التطوير السريع والمبسط لخطوط الأنابيب عبر واجهات برمجة تطبيقات SQL و Java و Python في حزمة Apache Beam SDK، والتي توفر مجموعة غنية من العناصر الأولية لتحليل النوافذ والجلسات ، بالإضافة إلى نظام بيئي لموصلات المصدر والمزامنة.



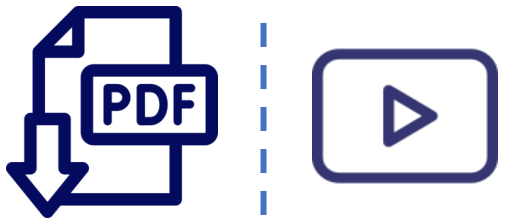
تدفق البيانات

- يرتبط Cloud Dataflow بإحكام بخدمات GCP الأخرى ، مثل Stackdriver، حتى تتمكن من إعداد التنبيهات والإشعارات ذات الأولوية لمراقبة خط الأنابيب الخاص بك وجودة البيانات الواردة والصادرة.
- يوضح هذا الرسم البياني بعض الأمثلة على استخدام حالات تدفق البيانات السحابية.
- كما ذكرت للتو ، تقوم Cloud Dataflow بمعالجة تدفق البيانات والدُفعات. يمكن أن تأتي هذه البيانات من خدمات GCP الأخرى مثل Cloud Datastore أو Cloud Pub / Sub، وهي خدمة المراسلة والنشر من Google.
- يمكن أيضًا استيعاب البيانات من خدمات جهات خارجية مثل Apache Avro و Apache Kafka.
- بعد تحويل البيانات باستخدام Cloud Dataflow، يمكنك تحليلها في BigQuery أو AI Platform أو حتى Cloud Bigtable.
- باستخدام Data Studio، يمكنك حتى إنشاء لوحات معلومات في الوقت الفعلي لأجهزة IoT.



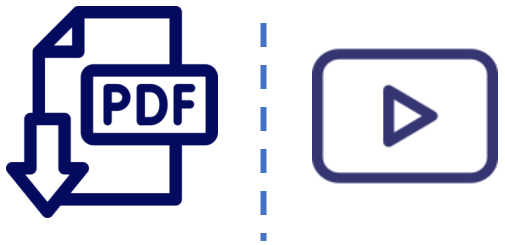
إعداد البيانات

- دعنا نتعلم قليلاً عن Cloud Dataprep.
- Cloud Dataprep هي خدمة بيانات ذكية للاستكشاف المرئي وتنظيفها وإعدادها للبيانات المهيكلة وغير المهيكلة لتقارير التحليل والتعلم الآلي. نظرًا لأن Cloud Dataprep بدون خادم ويعمل في أي مهارة ، فلا توجد بنية أساسية لنشرها تتم إدارتها.
- يتم اقتراح تحويل البيانات المثالي التالي والتنبؤ به مع كل إدخال لواجهة المستخدم حتى لا تضطر إلى كتابة التعليمات البرمجية.
- باستخدام المخطط التلقائي وأنواع البيانات والصلات المحتملة واكتشاف الانحرافات ، يمكنك تخطي تشكيل البيانات الذي يستغرق وقتًا طويلاً والتركيز على تحليل البيانات.
- Cloud Dataprep هي خدمة شريكة متكاملة تديرها Trifacta وتعتمد على حل تحضير البيانات الرائد في الصناعة Trifacta Wrangler ، تعمل Google عن كثب مع Trifacta.



إعداد البيانات

- لتوفير تجربة مستخدم سلسة تلغي الحاجة إلى تثبيت البرامج مقدمًا أو تكاليف الترخيص المنفصلة أو النفقات التشغيلية المستمرة.
- تتم إدارة Cloud Dataprep بالكامل ويتم توسيع نطاقها حسب الطلب لتلبية احتياجات إعداد البيانات المتزايدة لديك حتى تتمكن من الاستمرار في التركيز على التحليل.
- فيما يلي مثال على بنية Cloud Dataprep.
- كما ترى ، يمكن الاستفادة من Cloud Dataprep لإعداد البيانات الأولية من BigQuery أو Cloud Storage أو تحميل ملف قبل إدخالها في مسار تحويل مثل تدفق البيانات السحابية.
- يمكن بعد ذلك تصدير البيانات المحسنة إلى BigQuery أو Cloud Storage للتحليل والتعلم الآلي.

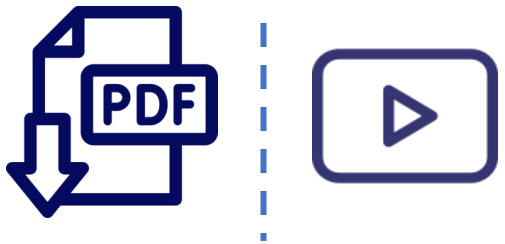


معالجة البيانات

- دعنا نتعلم قليلاً عن Cloud Dataproc.
- Cloud Dataproc هي خدمة سحابية سريعة وسهلة الاستخدام ومدارة بالكامل لتشغيل مجموعات Apache Spark و Apache Hadoop بطريقة أبسط. أنت تدفع فقط مقابل الموارد التي تستخدمها مع الفوترة بالثانية.
- إذا كنت تستفيد من المثيلات الاستباقية في مجموعتك ، فيمكنك تقليل تكاليفك بشكل أكبر. بدون استخدام Cloud Dataproc، قد يستغرق الأمر من خمس إلى 30 دقيقة لإنشاء مجموعات Spark و Hadoop في مكان العمل أو من خلال البنية التحتية الأخرى كمقدمي خدمة.
- مجموعات Cloud Dataproc سريعة في البدء والتوسع والإغلاق حيث تستغرق كل من هذه العمليات 90 ثانية أو أقل في المتوسط.
- هذا يعني أنه يمكنك قضاء وقت أقل في انتظار المجموعات والمزيد من الوقت في العمل مع بياناتك.

معالجة البيانات

- تم دمج Cloud Dataproc مع خدمات GCP الأخرى مثل BigQuery والتخزين السحابي و Cloud Bigtable و Stackdriver Logging و Stackdriver Monitoring.
- يوفر لك هذا نظامًا أساسيًا للبيانات كاملة بدلاً من مجرد مجموعة Spark أو Hadoop.
- كخدمة مُدارة ، يمكنك إنشاء مجموعات بسرعة وإدارتها بسهولة وتوفير المال عن طريق إيقاف تشغيل المجموعات عندما لا تحتاج إليها. مع تقليل الوقت والمال الذي تنفقه على الإدارة ، يمكنك التركيز على وظائفك وبياناتك.
- إذا كنت تستخدم بالفعل شرارة أو Hadoop أو Big أو Hive، فلن تحتاج حتى إلى تعلم أدوات أو واجهات برمجة تطبيقات جديدة لاستخدام Cloud Dataproc.
- هذا يجعل من السهل نقل المشاريع الحالية إلى Cloud Dataproc دون إعادة تطوير.
- الآن ، يمكن استخدام كلا من Cloud Dataproc وتدفق البيانات السحابية لمعالجة البيانات.



معالجة البيانات

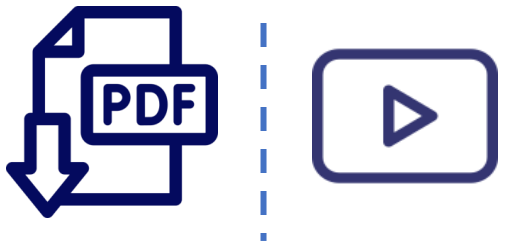
- وهناك تداخل في إمكانيات الدُفعات والبث. إذن ، كيف يمكنك تحديد المنتج الأنسب لبيئتك؟ حسنًا ، اسأل نفسك أولاً عما إذا كان لديك تبعيات ، أو أدوات معينة ، أو حزم في نظام Apache Hadoop أو Spark.
- إذا كان الأمر كذلك ، فمن الواضح أنك تريد استخدام Cloud Dataproc.
- إذا لم يكن الأمر كذلك ، فاسأل نفسك ما إذا كنت تفضل نهجًا عمليًا أو نهج DevOps للعمليات أو نهج عدم التدخل أو عدم وجود خادم.
- إذا اخترت نهج DevOps، فأنت تريد استخدام Cloud Dataproc، وإلا استخدم تدفق البيانات السحابية.

العرض التوضيحي: معالجة البيانات

- دعني أوضح لك كيفية إنشاء مجموعة Cloud Dataproc، وتعديل عدد العاملين في المجموعة ، وإرسال مهمة Apache Spark بسيطة. لذلك أنا هنا في وحدة تحكم GCP ، أول شيء أريد القيام به هو الانتقال إلى Cloud Dataproc.
- هذا بعيد جدًا ، لذا دعنا ننتقل إلى البيانات الضخمة ، لدينا Dataproc.
- سيتحقق مما إذا كان هناك بالفعل مجموعة ليست لدينا حتى نتمكن من المضي قدمًا وإنشاء مجموعة الآن.
- يمكننا البدء بتحديد الاسم. دعنا فقط نسميها مثال المجموعة. ثم لن أقوم بتغيير أي من الإعدادات الأخرى ولكن فقط قم بتمييزها. يمكننا تحديد مكان تخزينه ، ما هي المناطق والمناطق. أي نوع من الوضع الذي يحدد العلاقة بين العقد والعاملين. نريد أن يكون لدينا سيد واحد وعمال.
- يمكنك أيضًا الحصول على إعداد إتاحة عالي ، حيث لديك ثلاثة شرائح رئيسية ثم تحديد اسم العمال.
- لديك أنواع الأجهزة المتاحة للعقد الرئيسية ، لذلك أربع وحدات معالجة مركزية افتراضية.

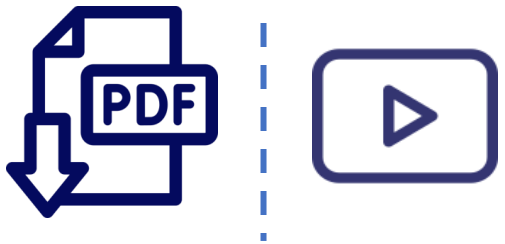
- العرض التوضيحي: معالجة البيانات

- ثم لدينا العمال أيضا. يمكن أن يكون هناك أيضًا أربع وحدات معالجة مركزية افتراضية ، وسيكون هناك اثنان منهم. لذلك في إجمالي القرص نفسه ، سيتم إنشاء 12 وحدة معالجة مركزية افتراضية. إذا انتقلنا إلى الخيارات المتقدمة ، فيمكننا جعل بعض هذه العقد وقائية. يمكننا تحديد الشبكة ، والشبكات الفرعية ، وعلامات الشبكة من حيث قواعد جدار الحماية. اجعل عنوان IP الداخلي هذا فقط ، حاوية التخزين السحابي للصورة المرحلية. يمكنك أن ترى أن هناك الكثير من الخيارات الأخرى وصولاً إلى التشفير المحدد. لذا اسمحوا لي أن أمضي قدمًا وأنشئ هذا التكوين الافتراضي. انقر فوق إنشاء ، ومرة أخرى سيؤدي هذا إلى إنشاء مجموعة من الأجهزة المختلفة لنا الآن. إذا فتحت علامة تبويب أخرى وانتقلت بالفعل إلى Compute Engine ، فسنرى كل تلك الحالات التي يتم إنشاؤها لنا. لذا يمكنني الذهاب إلى Compute Engine ، لذلك على الرغم من أن هذه خدمة مُدارة ، يمكننا رؤية جميع الحالات الموجودة هناك بالفعل. إذن لدينا العقد الرئيسي ولدينا عقدتان عاملة.



العرض التوضيحي: معالجة البيانات

- يأخذون فقط الاسم الذي حددته ثم يلمسون M للسيد ، W للعامل ويبدأ بمؤشر صفري.
- لذا إذا عدت إلى هنا ، يمكنني الانتعاش.
- لا يزال يتم تهيئة الذات المجمعة.
- البرنامج الذي يتم تثبيته وجميع عمليات الإعداد التي تحدث في النهاية الخلفية.
- بمجرد أن تصبح المجموعة جاهزة ، يمكننا المضي قدمًا وربما يمكننا تغيير حجمها.
- نرى أن لدينا حاليًا عقدتان عاملة ويمكننا تغييرها إلى شيء آخر ربما مثل ثلاث عقد عاملة. ثم بعد ذلك سنمضي قدمًا بالفعل ونقدم وظيفة لهذا الغرض. لذا فقد أخذنا دقيقة أو دقيقتين أخريين ، لدينا الكتلة وتشغيلها. يمكنني النقر فوق الكتلة نفسها ويمكنني الحصول على مزيد من المعلومات حول هذا الموضوع. لذلك لدينا هنا كل أنواع إعدادات المراقبة.
- إذا ذهبت إلى حالات VM، فسأرى هؤلاء. يمكنني SSH سيد.

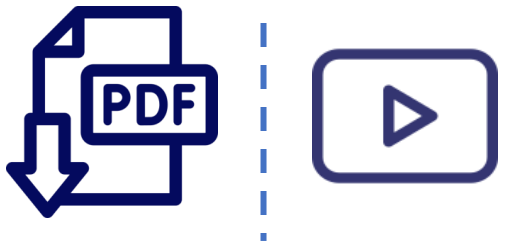


العرض التوضيحي: معالجة البيانات

- أي وظائف لدي والتي ليس لدينا أي وظائف حتى الآن. إذا نقرت على التكوين ، فسنرى أن لدينا حاليًا عقدتان عاملة. إذا قمت بالنقر فوق "تعديل" ، يمكنني تغيير ذلك. لنفترض أننا نريد ثلاث عقد عاملة ، ويمكننا تغييرها إلى ثلاث والضغط على حفظ. سيتم الآن المضي قدمًا وطلب هذا التحديث لنا. لذلك ستقوم بإنشاء عامل آخر وستقوم أيضًا بتحديث السيد ، دع السيد يعرف أن هناك عاملًا آخر هناك. لذلك عندما نقدم الوظائف ، يتم الاستعانة بجميع العمال. لذلك إذا عدت إلى Compute Engine، فسنرى هنا العمال الجدد وهم يعملون بالفعل.
- إذا عدت إلى هنا وقمت بالتحديث ، يمكنك أن ترى أن الكتلة نفسها لا تزال قيد التحديث. يجب أن يستغرق هذا مرة أخرى دقيقة أو دقيقتين فقط ، وبسرعة كبيرة. مرة أخرى ، هذه خدمة مُدارة ولكن يمكننا رؤية مثيلات النهاية الخلفية الفعلية التي يتم الاستفادة منها. لذلك يمكننا أن نرى هنا اكتمال تحديث المجموعة.
- يمكنني النقر فوقه مرة أخرى والانتقال إلى التكوين ويمكننا أن نرى أن لدينا الآن ثلاث عقد عاملة.

العرض التوضيحي: معالجة البيانات

- لذا حان الوقت لتقديم وظيفة. دعنا نذهب إلى قسم الوظائف ونضغط على تقديم وظيفة. يمكنني ترك معرف الوظيفة ، مغادرة المنطقة. من الواضح أنك تريد تحديد الكتلة ، خاصة إذا كان لدي مجموعات متعددة. سيكون نوع الوظيفة في هذه الحالة هو Spark.سأقوم بتحديد فئة رئيسية. هذا فقط من فئة المثال. ما سنفعله في الواقع هو أننا سنقدم مثالًا لحساب قيمة Pi.
- الحجج ، سأعطيها ألف ملف و JAR، سأقدم ذلك أيضًا. ثم يمكنني مراجعة ذلك ، هناك الكثير من الأشياء الأخرى التي أمتلكها ، والتسميات. لذلك أنا مستعد تمامًا. لذلك سأقوم بالنقر فوق تقديم في هذه الوظيفة. ستمضي قدمًا وتقدم ذلك. هذه الوظيفة قيد التشغيل الآن وهذا هو رمز الحالة الموجود هنا الآن. يمكنني أن أضغط على هذه الوظيفة نفسها. هنا يمكنني رؤية الوظيفة قيد التشغيل بالفعل. يمكنني أيضًا مراجعة التكوين مرة أخرى. حتى ترى هنا جميع الإعدادات المختلفة التي حددتها للتو. يمكننا العودة إلى الإخراج. مرة أخرى ، سيقوم هذا الآن بحساب تقريبي لتقدير قيمة Pi ، لذلك سننتظر ذلك فقط.



العرض التوضيحي: معالجة البيانات

- ها نحن ذا. تقول أن Pi هي تقريبًا هذا. لذا فإن المهمة قد اكتملت الآن.
- إذا كان هذا هو كل ما أردنا القيام به ، فيمكننا المضي قدمًا وحذف المجموعة.
- خلاف ذلك ، يمكننا تقديم المزيد من الوظائف.
- في حالتنا ، لقد انتهينا. لذا دعنا نعود إلى المجموعة ، وحددها ، ثم انقر فوق حذف. سيقود أيضًا جميع البيانات ، لا يمكن التراجع عن هذا. تمام. انقر فوق ذلك ، ويمكنك الانتقال إلى Compute Engine، والتحديث هنا ، يمكننا أن نرى بالفعل أنه تم الآن إيقاف كل هذه الأشياء وسيتم حذفها بعد ذلك. بهذه الطريقة يمكنك بسهولة تدوير المجموعات وحذفها بحيث يتم تحصيل رسوم منك فقط مقابل استخدامات الكتلة أثناء الحاجة إليها. لذلك يمكننا الانتظار حتى يتم حذف هذا. لذلك استغرق ذلك دقيقة أو دقيقتين فقط ، يمكننا أن نرى أنه تم حذف الكتلة نفسها وإذا ذهبت إلى الحالات.
- يمكننا أيضًا أن نرى أن جميع الحالات قد ولت.
- هذا هو مدى سهولة إنشاء مجموعة Cloud Dataproc وتقديم وظيفة إلى تلك المجموعة.

- **كيف تكون الخدمات المدارة مفيدة؟**
  - قد تكون الخدمات المدارة بديلاً لإنشاء حلول البنية التحتية وإدارتها.
  - الخدمات المدارة هي خدمات مدفوعة يقدمها بائعون خارجيون.
  - إذا كانت لديك خدمة بنية أساسية حالية ، فستديرها Google نيابةً عنك إذا اشتريت عقد الخدمات المُدارة.
  - الخدمات المدارة أكثر قابلية للتخصيص من حلول البنية التحتية.

- **أي مما يلي يُعد سمة من سمات Dataproc؟**
  - تحدث فوترة Dataproc في فترات زمنية مدتها 10 ساعات.
  - يستغرق عادةً أقل من 90 ثانية لبدء مجموعة.
  - لا يتكامل مع المراقبة السحابية ، لكن لديه نظام مراقبة خاص به.
  - يسمح Dataproc بالتحكم الكامل في إعدادات HDFS المتقدمة.

مراجعة الوحدة

- في هذه الوحدة ، قدمنا لك نظرة عامة على الخدمات المُدارة لمعالجة البيانات في GCP، وهي BigQuery Cloud Dataflow و Cloud Dataprep و Cloud Dataproc.
- تتيح لك الخدمات المدارة الاستعانة بمصادر خارجية في الكثير من النفقات الإدارية والصيانة لشركة Google، بحيث يمكنك التركيز على أعباء العمل بدلاً من البنية التحتية.
- بالحديث عن البنية التحتية ، فإن معظم الخدمات التي غطيناها بدون خادم.
- الآن ، هذا لا يعني أنه لا توجد أي خوادم فعلية تعالج بياناتك.
- تعني عدم وجود خادم يعني أن الخوادم أو مثيلات محرك الحوسبة مشوشة بحيث لا داعي للقلق بشأن البنية التحتية.
- Cloud Dataproc ليست خدمة بدون خادم لأنك كنت قادرًا على عرض.
- وإدارة المثيلات الأساسية والعاملة.

مراجعة سلسلة الدورات

- شكرًا لك على أخذ سلسلة الهندسة المعمارية باستخدام Google Compute Engine Core.
- آمل أن يكون لديك فهم أفضل للبنية التحتية الشاملة والمرنة وخدمات النظام الأساسي التي تقدمها GCP.
- آمل أيضًا أن تجعلك العروض التوضيحية والمختبرات تشعر براحة أكبر عند استخدام خدمات GCP المختلفة التي غطيناها.
- الان حان دورك. انطلق وقم بتطبيق ما تعلمته من خلال تصميم البنية التحتية الخاصة بك في GCP.
- أراك المرة القادمة.

الملف تفاعلي قم بالنقر على الأيقونة

ماذا بعد؟ الحصول على شهادة

- تحقق من مهاراتك العملية في Google Cloud وحقق تقدمًا في حياتك المهنية من خلال شهادة Associate Cloud Engineer
- يمكن أن تساعدك الشهادة على اكتساب المصداقية وتمنحك ميزة في سوق اليوم شديدة التنافسية.
- تُمنح شهادة Associate Cloud Engineer للأفراد الذين يرغبون في إثبات قدرتهم على نشر التطبيقات ومراقبة العمليات والحفاظ على المشاريع السحابية على Google Cloud ، من المستحسن أن يكون لديك 6 أشهر على الأقل من الخبرة العملية في العمل مع Google Cloud ، سيقيم الاختبار قدرتك على:
  - ❑ إعداد بيئة الحلول السحابية
  - ❑ تخطيط حل السحابة وتكوينه
  - ❑ نشر وتنفيذ حل السحابة
  - ❑ ضمان التشغيل الناجح لحل السحابة
  - ❑ تكوين الوصول والأمن

ماذا بعد؟ الحصول على شهادة

- **أوصي بتوسيع نطاق معرفتك من خلال استكمال مختبرات** Qwiklabs **ذاتية السرعة التالية ، وهي أنشطة عملية ذات موضوع واحد ؛ و** Qwiklabs Quests، **وهي مجموعات من المعامل ذاتية السرعة حول موضوع مُركّز:**
  - Quest: Kubernetes in Google Cloud
  - Quest: Google Kubernetes Engine Best Practices: Security
  - Self-Paced Lab: Cloud Functions - Qwik Start
  - Quest: Application Development - Java
  - OR Quest: Application Development – Python

ماذا بعد؟ الحصول على شهادة

- لمساعدتك في تنظيم إعدادك لامتحان Associate Cloud Engineer، نوصي بالتحضير لدورة اختبار Associate Cloud Engineer.
- يمكنك أيضًا التحضير باستخدام دليل الدراسة الرسمي لمهندس السحاب المعتمد من Google Cloud، الذي نشرته Wiley قم بزيارة موقع Google Cloud Certification للحصول على مزيد من المعلومات وللتسجيل.
- حظا طيبا !

النهاية

SHUJAA ALMUTAIRI

2022 - 1444