**TIP - 01 Control Your Costs**

Cloud platforms such as Amazon RDS, Microsoft Azure, and Google Cloud’s Anthos can automate many basic operational database deployment tasks. However, they don’t remove all of the challenges that you should have the power to lower their costs. Reducing costs isn’t just about buying additional capacity.

- **Slowly**, the instinct is often to purchase more capacity to meet your end-user expectations. But, in the long run, this can quickly become expensive and doesn’t fix underlying issues. Cloud providers create and maintain cloud database infrastructure, whether hosted on-premise, or at a co-location facility, or if you purchase services from a cloud provider or database-as-a-service provider. All major cloud providers have experienced outages, but two things can make the effects of outages worse:
  - First, cloud vendors market their platforms as “Fully Managed”, leading people to assume they are absolved of responsibility for their database. However, applications’ responsibility for their database. However, applications’ responsibility for before entering into a contract. You need to ensure you understand what you and your provider are responsible for before entering into a contract.

Keep It Private

Cloud computing brings various new regulatory, privacy, and security challenges. The cloud provider is responsible for implementing appropriate security and confidentiality to protect your sensitive data in the cloud.

- **Fifth**, end-to-end encryption is a shared responsibility, and poor set-up and configuration can be the cause of failed security. Your internal IT team must have specific expertise in this area, or if you have a knowledge gap, you need to work with a trusted dedicated cloud partner who can help you take full advantage of a multi-cloud approach.

Finally, utilize reviews, risk assessments, and audits to confirm that your cloud provider meets the data protection standards set out in your contract. Establish a dedicated security team to ensure your cloud resources and questions are well-protected immediately.

**TIP - 02 Choose a Reliable Provider and Educate Your Team**

Embrace Hybrid and Multi-Cloud Options

- **Choose a Reliable Provider**
  - You need to ensure you understand what you and your provider are responsible for before entering into a contract. You need to ensure you understand what you and your provider are responsible for before entering into a contract.

Keep It Private

Cloud computing brings various new regulatory, privacy, and security challenges. The cloud provider is responsible for implementing appropriate security and confidentiality to protect your sensitive data in the cloud.

- **Fifth**, end-to-end encryption is a shared responsibility, and poor set-up and configuration can be the cause of failed security. Your internal IT team must have specific expertise in this area, or if you have a knowledge gap, you need to work with a trusted dedicated cloud partner who can help you take full advantage of a multi-cloud approach.

Finally, utilize reviews, risk assessments, and audits to confirm that your cloud provider meets the data protection standards set out in your contract. Establish a dedicated security team to ensure your cloud resources and questions are well-protected immediately.

**TIP - 03 Take Security Seriously**

In the wild, Cloud Services are as easy to use as they are

- **Fifth**, end-to-end encryption is a shared responsibility, and poor set-up and configuration can be the cause of failed security. Your internal IT team must have specific expertise in this area, or if you have a knowledge gap, you need to work with a trusted dedicated cloud partner who can help you take full advantage of a multi-cloud approach.

Finally, utilize reviews, risk assessments, and audits to confirm that your cloud provider meets the data protection standards set out in your contract. Establish a dedicated security team to ensure your cloud resources and questions are well-protected immediately.

**TIP - 04 Keep It Private**

Cloud computing brings various new regulatory, privacy, and security challenges. The cloud provider is responsible for implementing appropriate security and confidentiality to protect your sensitive data in the cloud.

- **Fifth**, end-to-end encryption is a shared responsibility, and poor set-up and configuration can be the cause of failed security. Your internal IT team must have specific expertise in this area, or if you have a knowledge gap, you need to work with a trusted dedicated cloud partner who can help you take full advantage of a multi-cloud approach.

Finally, utilize reviews, risk assessments, and audits to confirm that your cloud provider meets the data protection standards set out in your contract. Establish a dedicated security team to ensure your cloud resources and questions are well-protected immediately.

**TIP - 05 Embrace Hybrid and Multi-Cloud Options**

This year, the number of companies using more than one cloud service or platform continues to grow. According to recent Gartner research, **50%** of companies are now using two or more cloud platforms.

- **Second**, many cloud vendors market their platforms as “Fully Managed”, leading people to assume they are absolved of responsibility for their database. However, applications’ responsibility for their database. However, applications’ responsibility for before entering into a contract. You need to ensure you understand what you and your provider are responsible for before entering into a contract.

Keep It Private

Cloud computing brings various new regulatory, privacy, and security challenges. The cloud provider is responsible for implementing appropriate security and confidentiality to protect your sensitive data in the cloud.

- **Fifth**, end-to-end encryption is a shared responsibility, and poor set-up and configuration can be the cause of failed security. Your internal IT team must have specific expertise in this area, or if you have a knowledge gap, you need to work with a trusted dedicated cloud partner who can help you take full advantage of a multi-cloud approach.

Finally, utilize reviews, risk assessments, and audits to confirm that your cloud provider meets the data protection standards set out in your contract. Establish a dedicated security team to ensure your cloud resources and questions are well-protected immediately.

**For further information you can also visit our dedicated cloud partner, but please note that you can also check out the Percona Database Performance Blog for practical and technical insights into using open source software in the cloud.**

**Contact Us**

We can provide onsite or remote Percona Consulting for current or planned projects, migrations, or issues and help you keep your databases running optimally.

- **316-9775 (USA), +44 203 608 6727 (Europe), or email us at sales@percona.com.**