An Oracle White Paper
April 2010

How Cloud Service Consumers Manage and Govern Cloud-Based Applications

ORACLE

Introduction

If your organization is like most others, you are evaluating the cloud architecture to understand how to gain the benefits of consuming cloud services. Whether you plan to consume cloud services in the context of a private cloud or across the open internet, many management and governance challenges can stand in your way. Oracle's composite application management solutions provide capabilities that address the requirements of consuming cloud services and can significantly reduce the many risks associated with the cloud architecture. This paper briefly discusses the challenges of consuming cloud services and the ways Oracle improves your chances of success.

If you are a consumer of cloud services, whether internal or external, your governance and management needs are different from those of cloud service providers. Many organizations will find themselves in both roles, because composite applications may provide and consume cloud services as part of a single business transaction. For an overview of the management issues for cloud services providers, see the companion white paper, "How Cloud Service Providers Manage and Govern Cloud APIs."

Cloud services deliver on-demand capabilities, such as storage, computing, and payment services, following a utility model. Providers host these services remotely (in the public cloud) or on their own premises (in a private cloud), and you are charged only for what you use. The management needs of cloud services consumers are somewhat different from those of service providers. You must locally monitor service performance and reliability, you need to ensure that your consumer applications secure sensitive data before sending it beyond the corporate firewall, and you need to ensure the appropriate application of security tokens.

Although they simplify some aspects of IT, cloud services can actually make your application environment more complex. This complexity introduces more-stringent requirements for managing services in the context of the larger enterprise.

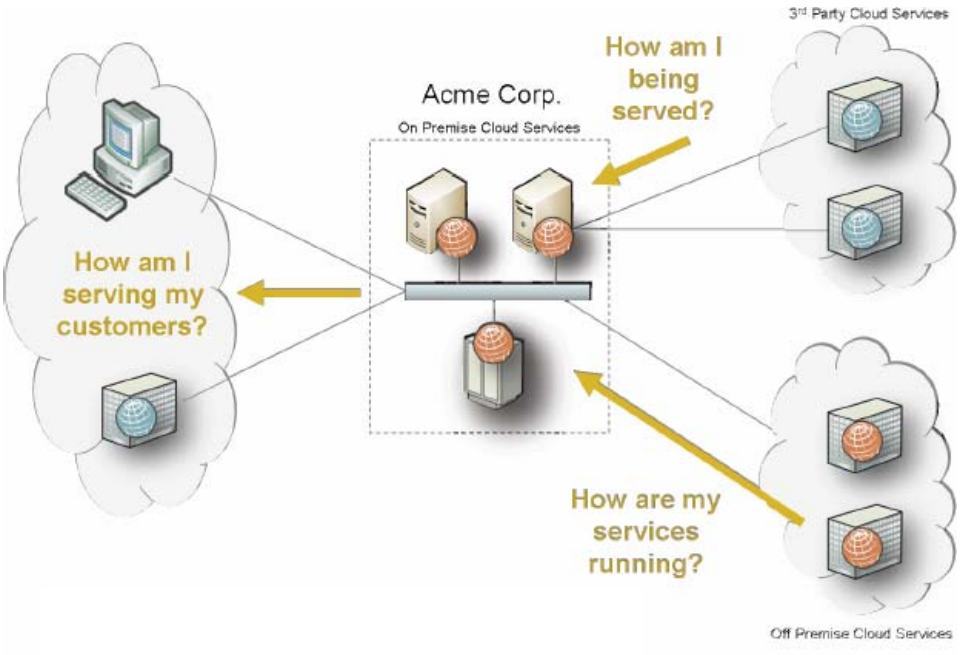

Figure 1. Service-level concerns for managing cloud APIs include defining and then monitoring compliance with SLAs in real time.

What cloud services have in common is that they are not under the direct control of the teams responsible for the applications that consume them or the business transactions that flow across them. This disconnect can create issues for business continuity while upping the ante for user and data privacy, security and compliance, and reliability and availability.

Performance and Health Monitoring

Even the most respected and trustworthy cloud services providers experience hiccups in service delivery. Yet few providers of cloud services offer much visibility into how their services are performing or alerts when a service degrades or, even worse, goes down.

Oracle's composite application management solutions enable you to monitor traffic as it flows across your organizational boundary out to the cloud. You can also configure alerts for when traffic slows down or the service goes down entirely. Importantly, you can be the first customer to know that a cloud infrastructure has gone down.

Transaction Tracking

Your composite applications may make use of a cloud service as part of an end-to-end business transaction. For example, you may have automated a process for selling goods over the internet. If so, your internal systems handle receiving and processing the order from a customer. As part of the purchase transaction, however, your system calls out to a remote service that provides inventory information from a third-party supplier. Let's say this cloud service goes down, which means that your purchase transactions start freezing. Your service is dropping transactions, and your customers are calling support. How do you locate the failure in time to save the business?

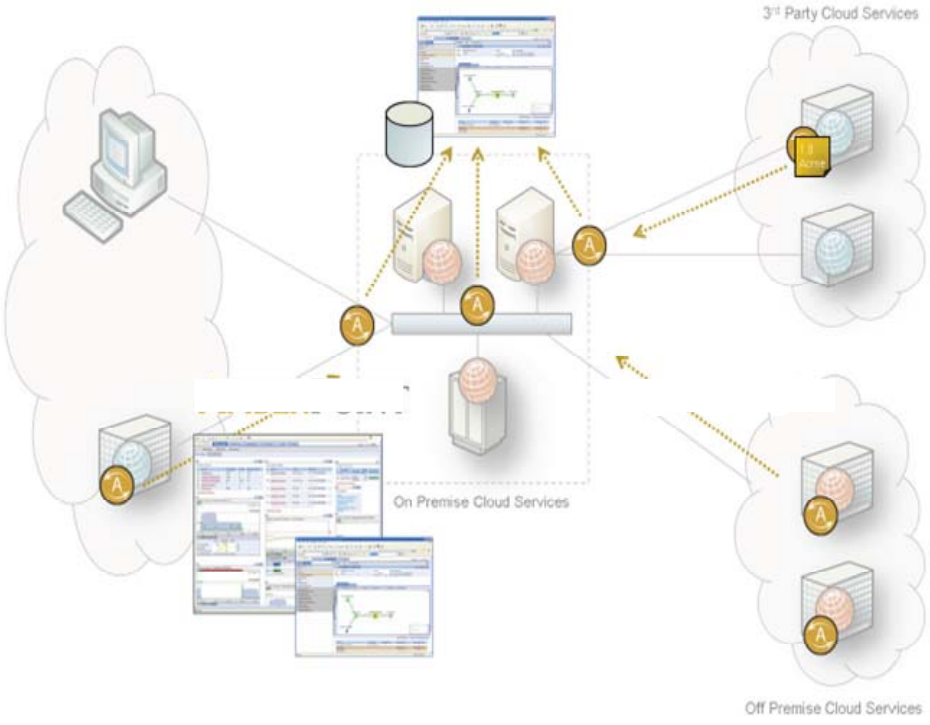

Figure 2. Oracle's composite application management gives you transaction visibility in an enterprise cloud environment.

Complying with Service Provider Security Policies

The service provider secures every type of valuable cloud API one way or another. It might use API keys, username/password combinations, X.509 certificates, or some form of single-sign-on token. This means that your applications need to implement one (or more) of these security mechanisms. If you find yourself consuming more than one service, your developers will need to implement these mechanisms within service consumer applications. When it comes time to switch services, you will need to go through a whole code cycle to begin consuming the new services. Because many cloud APIs rely on proprietary security mechanisms such as API keys, vendor lock-in and higher switching costs often result from secure integrations.

Composite application management enables service consumer applications to meet the security requirements of cloud service providers dynamically. It can examine the security policy applied to a provider service and dynamically add required security tokens such as Web Services Security (WS-Security) passwords. If there is a need for digitally signed or encrypted requests, Oracle can automatically perform those operations on behalf of consumer applications. The main benefit is that developers do not need to code security into client applications. Moreover, when providers update security policies, your applications will not break or require an additional code cycle to remain in compliance.

Protecting Data

Interacting with remote services means that your data is going beyond the corporate firewall. This can create regulatory problems—for even seemingly innocuous information. A cloud provider may have datacenters scattered across the country or around the planet. When your data crosses the enterprise boundary, you have no idea where it will be stored. You may also have no idea exactly how the data is stored and how or whether backups happen. These are all good reasons to encrypt or filter any potentially sensitive data before it hits the cloud.

The Secure Sockets Layer (SSL) protocol, now known as Transport Layer Security (TLS), is a common technology for performing on-the-wire encryption. However, you cannot rely on SSL to protect your information once it reaches the target service. Although SSL is useful for protecting login credentials used to create a secure session, it is not a good idea to rely on SSL for all your data protection. If you do, your data will probably be stored in the clear once it is at rest at the other end of the pipe.

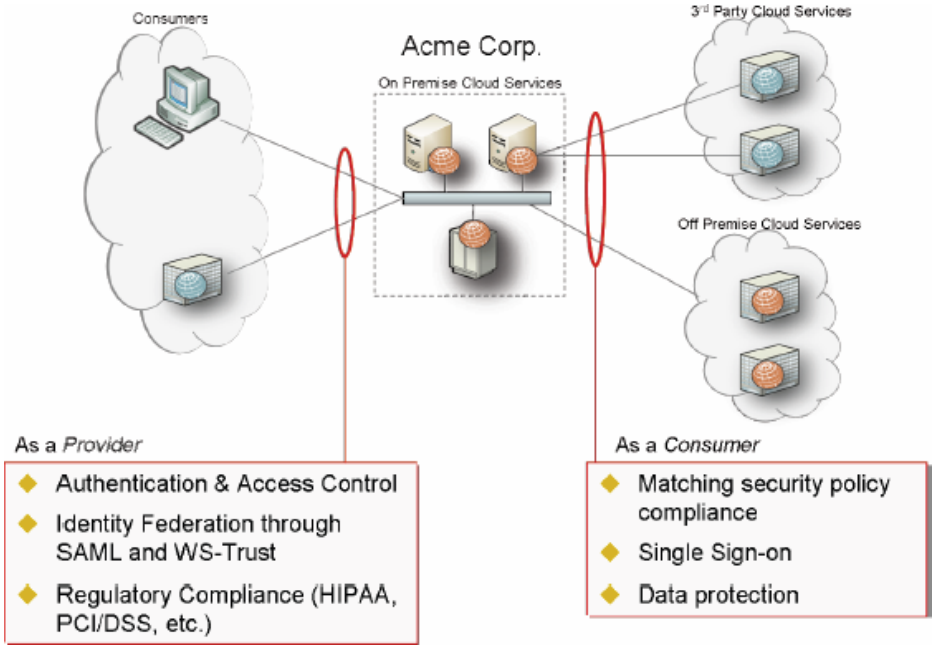

Figure 3. Cloud API security for providers and consumers protects services and data.

Oracle provides the necessary support for data encryption to ensure that your data is safe as it flows across intermediaries and cloud services. Oracle's composite application management employs unique role-based data filtering policies that provide for fail-safe mechanisms, ensuring that sensitive and regulated data—Social Security numbers, credit cards, and the like—is stripped out of messages as necessary. This helps you comply with Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and other regulations as you take advantage of the cloud.

Conclusion

Oracle's composite application management enables organizations to embrace the cloud with confidence by addressing the unique challenges confronted by cloud services consumers. Its contributions to cloud service consumers include

- Monitoring of the performance and operational health of the system
- Comprehensive transaction tracking capabilities
- Compliance with the security policies of cloud service providers
- Encryption of data to ensure that it is safe as it flows across intermediaries and cloud services, enabling organizations seeking to leverage the benefits of cloud services to do so while significantly reducing the inherent risks of the cloud architecture

Oracle's composite application management provides the means to address the requirements of consuming cloud services and can drastically diminish the many threats associated with the cloud architecture.

Oracle is committed to developing practices and products that help protect the environment

How Cloud Service Consumers Manage and Govern Cloud-Based Applications
April 2010

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

SOFTWARE. HARDWARE. COMPLETE.