

Automated Cloud Onboarding & Workload Mobility

- The Cloud Migration Market
- Why RiverMeadow: Key RiverMeadow Competitive Advantages
- RiverMeadow's Business Model
- Your Path to the Cloud
- Unlock the Benefits of the Cloud and Unburden IT
- Cloud Readiness: Removing Friction & Mitigating Risks
- From the Gartner Files: The Four Key Risks of Developing and Executing a Cloud Sourcing Strategy
- Anatomy of a Cool Technology
- Brokering Workloads Among Clouds
- Disaster Recovery as a Service

Featuring research from



The Cloud Migration Market



The Cloud is still in a formative stage. Some businesses have moved server workloads to the cloud, but many more are still figuring out cloud strategies. All have legacy workloads that would probably benefit from migration to the cloud. Until now, migrating brownfield server workloads to the cloud has required significant planning, software development or redesign, and possibly costly and lengthy help from professional services organizations.

RiverMeadow solves the toughest challenges of migrating workloads to the cloud, providing an alternative approach with a complete migration platform that simplifies and automates many conversions, and allows customization for those workloads that require it. The RiverMeadow Cloud Migration SaaS is an extensible, adaptable migration platform that automates workload mobility into and between clouds, enabling users to migrate workloads to the cloud, from the cloud and between cloud instances and cloud service providers (CSPs) with ease. As a SaaS tool, the RiverMeadow SaaS is always available where and when you need it. Its complete API makes it easy to embed in other systems, to use its intuitive GUI, or to adapt its GUI for customer needs.

Automated conversion solves the most complicated portion of a migration: matching server workload to the target cloud context and transformation of the workload into an image that runs in the target cloud environment. Because RiverMeadow's Cloud Migration SaaS converts workloads at the OS rather than application level, the migration process is further simplified for the user, who only needs to select the original server and the target cloud. Some conversions can be performed with only this information, but for more complicated, "high touch" workloads the RiverMeadow SaaS allows pre- and postmigration scripts to make changes and updates to the server(s) being migrated.

Automation of legacy workload migrations into the cloud dramatically minimizes cost, complexity, and time. Customization and cleanup provided by professional services is easily accommodated with the RiverMeadow SaaS. Any required software changes are at a low level in the stack and performed automatically by RiverMeadow. And only minimal planning is necessary because the migration happens quickly and retains the workload's user interface, functionality, and APIs. RiverMeadow has created a market-leading solution by developing a comprehensive workload migration platform that automates core conversion challenges.

Workload Migration Market Size Forecast



RiverMeadow conservatively estimates the size of the market for migrating workloads into and between clouds over the next five years at \$11.6B for companies that have either not yet moved to the cloud, or will move between clouds. Further, workload migrations enable the broader market for cloud services.

Cloud Service Providers (CSPs) and Cloud Service Brokers (CSBs) both benefit as more businesses move to the cloud. CSPs profit from more customers, and they can use the RiverMeadow SaaS to easily migrate their end user customers from physical data centers into the CSP's cloud. CSBs can embed RiverMeadow within their own products, thereby simplifying their migration efforts. In turn, CSBs can focus on enabling their services teams and providing higher value to their customers.

Generally, a critical challenge for IaaS software and hardware manufacturers has been to move more end users into the cloud. RiverMeadow's SaaS meets this challenge, growing the market of cloud users and hence the demand for cloud hardware and software to support them. This greatly extends RiverMeadow's reach to customers whose primary engagement is with CSPs and CSBs.

There's an important functional distinction between migrations performed by RiverMeadow and those performed by other professional services organizations. As software, the RiverMeadow solution scales, whereas migrations performed by professional services are labor intensive. In addition to the

The Cloud Migration Market



financial benefits for RiverMeadow, experience with migrations becomes part of the RiverMeadow SaaS, consistently improving quality and pushing the boundaries of which kinds of migrations can be automated – growing RiverMeadow's migration market.

While RiverMeadow benefits both CSPs and CSBs, the relationship with CSBs is particularly beneficial to RiverMeadow. This dovetails well with the projected growth of Cloud Service Brokers [Gartner Research, Examining the Magnitude of the Cloud Services Brokerage Opportunity, 15 August 2012, Daryl C. Plummer, Gregor Petri, Ed Anderson, Benoit J. Lheureux, Tiffani Bova]. Some migrations require work that goes beyond simply migrating a workload into the cloud. Integration with other legacy or cloud systems may have to be redesigned or implemented, a new user interface may be required, or other refinements may be needed to provide better operation in the cloud. While these clearly are outside the scope of the RiverMeadow SaaS, it might fit perfectly into a CSB's services. A CSB can use RiverMeadow to quickly migrate a workload into the cloud, and then perform customization services on the already-operational workload. Breaking a complex task into simpler pieces allows the CSB to be more efficient.

The cloud business is so nascent, and there are so many interrelated trends, it's hard to be certain about actual market numbers. Regardless, the building growth of the cloud market cannot be denied, nor can the value RiverMeadow provides by simplifying cloud on boarding via automated workload migrations.



Why RiverMeadow

Key RiverMeadow Competitive Advantages



In a growing market of vendors migrating applications from physical data centers into private, public, and hybrid clouds, RiverMeadow Cloud Migration SaaS stands out with a unique combination of advanced technical capabilities, innovative solution packaging, and effective approach. RiverMeadow customers benefit with high quality migrations delivered in less time at lower cost.

- The RiverMeadow SaaS automates the core migration functionality of transforming workloads into cloud-ready form, which requires labor-intensive work in other migration solutions.
- All RiverMeadow customers (Cloud Service Providers & Brokers, Services Organizations and Systems Integrators) benefit as new migration functionality is developed and added to the RiverMeadow SaaS. In contrast, labor-intensive migration shops tend to embed migration methods into their professional services practices, which do not automatically scale to all of their customers.
- The automated migration of legacy workloads to specific clouds de-emphasizes the technical details of choosing a target cloud, and allows choice to be based on business issues such as SLAs, cost, and reliability of the cloud provider.

- By migrating entire server workloads and not individual applications, RiverMeadow avoids the need to match specific legacy services and capabilities with those in target clouds. Other migration approaches must work around poor matches between legacy and target environments, and develop and debug software shims to improve the match – all of which add costs and delays for the customer.
- Delivering a migration solution as a SaaS with minimal intrusion into the legacy environment (servers need not be quiesced until final cut over and agents are not used) simplifies migration logistics and increases flexibility.
- Offering a RESTful API to all SaaS functionality allows CSPs and CSBs to embed RiverMeadow into their own practices and user experience, and enables creation of custom functionality to seamlessly extend migration capabilities.
- Automated migrations allow programmatic control, consistent with disaster recovery practices and simplified management approaches such as DevOps.

Source: Rivermeadow Software

BUILD & FIX	TIME TO MARKET		LIFT & SHIFT
NANUAL • Install software on source machine. • Image machine locally and transfer image files. • Stage, configure and verify server in target environment.	TEMPLATES Install run-time shim or dependencies in target environment. Start with a "known" image template. Install all app software &configure the source machine. Export and deploy server image into target environment.	 APP VIRTUALIZATION CONTAINERS Uses application virtualization to wrap applications on the source machine in a container and migrate the application to the target machine. May require manual configuration updates at the target machine. Some overhead is incurred in running the application within a container. 	AS-IS MIGRATION • Windows & Linux OS source server support • As-is, live server migration • Automated target cloud & user set-up • Web GUI w/ integrated RESTFul API • Agentless collection & deployment • Hypervisor agnostic • Auto-virtualize physical servers • Correctioneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

RiverMeadow Business Model



RiverMeadow has created a new market category: migration of businesses' legacy workloads to the cloud with minimal human intervention. With a savvy combination of technical capabilities and a focus on widely-used server workloads, RiverMeadow dramatically reduces the barriers businesses face when migrating existing workloads to private, public, or hybrid clouds. By carving out critical migration capabilities and forming relationships with cloud service providers (CSPs) and cloud service brokers (CSBs) who own the relationship with the end customer, and provide the rest of the infrastructure for a comprehensive entry to the cloud, RiverMeadow's Cloud Migration SaaS becomes a ubiquitous workload migration tool.

As a first step, RiverMeadow differentiated itself from other migration solutions. Most solutions focus on moving individual pieces of a server workload, requiring effort to build the surrounding infrastructure or integrate with services present in the cloud. Instead, RiverMeadow migrates an entire server workload, preserving its internal structure and thereby requiring only the substitution of low-level drivers and other services with equivalent cloud drivers and services. The result is a significant reduction in effort required to make the cloud workload operational. Other vendors of migration solutions require selection of a pre-existing template to best match and replace the workload being migrated. However, an exact match is extremely unlikely, causing problems for the migration that must be resolved by additional integration or customization work to make the migrated workload operational.

The RiverMeadow Cloud Migration SaaS is the leading highvalue, low-risk workload migration solution. Risk is minimized by the RiverMeadow migration process, which clones the source server to a test cloud, leaving the source server operational throughout the entire workload migration process. RiverMeadow also enables customers to pre-test common IT processes such as upgrading antivirus software or OS patches by cloning and migrating a server to the cloud, testing upgrades and changes on the clone, and verifying success prior to updates to production systems, ensuring confidence in the quality and success of the ultimate server or workload migration.

With its automated migration solution, RiverMeadow becomes an in-demand vendor for CSPs and CSBs who want to provide easy onboarding for customers moving to the cloud. CSBs and CSPs embed the RiverMeadow SaaS within their migration services, optimizing their cloud on-boarding processes. CSPs,



channel partners and OEMs benefit from the ability to build migration capability into their service offerings, automating and increasing the velocity of workload migrations while preserving an audit trail of all actions. By avoiding potentially messy migrations and focusing on higher-level integration and customization efforts, server workloads are ready for production use in the cloud much more quickly. Customers benefit with quicker ROI for their move to the cloud, CSPs and CSBs benefit with more customers and increased rate of service, and RiverMeadow benefits with more migrations served.

CSPs and CSBs have many choices when integrating the RiverMeadow SaaS into their business. They can expose the RiverMeadow user interface to pass existing migration functionality on to their professional services teams, or to their customers in a self-service mode. For maximum flexibility, all RiverMeadow functionality is available programmatically via its API, greatly increasing the opportunities for leveraging RiverMeadow. A new interface can be created or the existing CSP or CSB user interface can call RiverMeadow directly. Additional workload migration functionality can be integrated, such as custom scripting of pre or post migration configuration, policy-guided cloud brokering, or any other value add the CSP or CSB can find or build.

And the RiverMeadow SaaS features a powerful delegation model that makes it easy for RiverMeadow to grant usage rights to its partners and channels. RiverMeadow grants delegation capability for n workload migrations to a channel partner, e.g. a CSB or OEM enabling that channel partner, in turn, to delegate n workload migrations to its customers or partners, e.g. a VaR, and so on. This simple, direct delegation model allows RiverMeadow's ecosystem of partners to perform workload migrations using the RiverMeadow Cloud Migration SaaS with all access rights, policies and practices of the original delegation grant.



RiverMeadow Business Model



RiverMeadow enables its partners and channels to serve their customers directly, without any involvement from RiverMeadow, bypassing, or delegating, the entitlement to use RiverMeadow downstream for workload migrations. CSPs can set themselves up as target clouds in as little as day via RiverMeadow's automated, email and form-based set-up process. CSPs can rapidly begin creating user accounts and migration allotments, accelerating the growth of their cloud migration businesses while delivering immediate value to end customers.

RiverMeadow maintains a unique record of each migration, making it simple and rapid to document when, by whom and where each server workload was migrated. For CSPs, channel partners and customers, this level of migration visibility provides a total audit trail, complete with migration characteristics, simplifying regulatory and audit compliance.

The level of automation and simplification RiverMeadow provides is a key business value, backed by innovative features. The RiverMeadow SaaS can transform workloads between any of a wide variety of architectures and hypervisors. Moreover, it not only supports many different clouds, but it can broker workloads to clouds based on business requirements, SLAs, and other characteristics. The RiverMeadow SaaS hides the detailed technical mechanisms of the cloud and allows users to instead focus on and control business-oriented policies.

RiverMeadow's class-leading workload migration product is an extremely flexible platform for moving legacy server workloads into the cloud simply and effectively, with an extensible scripting environment available for pre and post migration workload configuration and customization. CSPs and CSBs derive value by embedding the RiverMeadow SaaS into their operational environments, leveraging RiverMeadow to streamline and expand their migration services. The ultimate beneficiaries are their enterprise and SMB customers who receive the benefits of the cloud more quickly.





Your Path to the Clouds



Businesses are considering how they can benefit from moving IT operations into the cloud. For some, the cloud is a blank slate offering a world of new resources. Others would like to move their current IT software solutions into the cloud, thereby receiving the performance, cost, and management benefits of the cloud. Building new systems in the cloud is called a greenfield opportunity, while moving existing software – what we refer to as server workloads – to the cloud is called brownfield. It's important to consider the benefits – and possible pitfalls – of both before committing to your path into the cloud.

Greenfield cloud implementations are a luxury because you can create new applications without worrying about the constraints of the old system. You don't have to revise the existing implementation or maintain compatibility with your legacy environment. As an added benefit, you may be able to take advantage of new computing services provided in your target cloud environment.

But there's a cost in making your business wait for a new cloud deployment to be developed. The longer legacy systems stay active in your physical data center, the longer you'll have to maintain legacy applications and hardware. Only then can you start to recoup development costs. Further, tribal knowledge, the thought and design that enabled creation of the original system, may be unavailable. The team that architected the system, set up the server, or developed the application may no longer be intact or still with the company. In those cases, rebuilding becomes exponentially more difficult if not completely impossible.

After all that, yesterday's greenfield becomes today's brownfield. Once you develop an application in the Cloud it's subject to the same migration complexities and costs as, for example, would be incurred when migrating a physical Windows server's workload into a cloud environment.

The reality for most businesses is existing systems are meeting real business challenges today. An ideal scenario is to simply move legacy workloads to a cloud environment as-is, avoiding disruptions to employees or customers and accruing hardware savings right away. Unfortunately, it's been difficult to find a way to easily move existing workloads to the cloud. Most cloud workload migration solutions require careful planning, and are imple mented by tools that must be licensed and installed on physical systems. Only RiverMeadow's Cloud Migration SaaS is a pure cloud-based solution. Other migration solutions require your workload's dependencies on operating system and other services to be manually matched to equivalents provided by the clouds to which you wish to migrate. Even when these dependencies line up with cloud offerings initially, and they almost never do, you're at risk of problems as the cloud environment evolves. When one considers the complexity of the matching - physical servers run Windows or Linux, while target virtual servers run on ESX, KVM, XEN, Hyper-V, and Parallels, and Clouds run on CloudStack, vCloud, AWS, and many variants of OpenStack - possible incompatibilities are everywhere.



Your Path to the Clouds



RiverMeadow delivers a better approach for brownfield cloud migrations. First, RiverMeadow's Cloud Migration SaaS automatically collects an image of your source servers in a non-intrusive way (no agents, no quiescing servers, and no software to buy). Next, RiverMeadow matches your workload's legacy system dependencies with the hypervisor, operating system, and services offered by cloud providers and converts your workload onto the target hypervisor as virtual machines that are fully compatible with the target cloud environment. Finally RiverMeadow deploys the converted workload into the cloud, ready to run. RiverMeadow is hypervisor agnostic; you don't have to choose a template that "sort of fits" your migrated system. We convert your legacy system directly to an exact equivalent that runs in the target cloud. All the complexities other migration solutions require you to confront when matching your legacy workload to the cloud environment are eliminated because the RiverMeadow SaaS handles them automatically.

With RiverMeadow, your business benefits quickly. Your legacy workloads run in the cloud sooner, there are fewer chances for problems created by the migration, and RiverMeadow's ability to move your system to any cloud prevents lock-in to your first cloud destination. You'll achieve ROI while your competition is still on the cloud learning curve, developing new systems for the cloud, or working through the difficulties caused by overcomplicated migrations.

The shortest and easiest path to the cloud is provided by RiverMeadow's Cloud Migration SaaS. Your tried-and-true existing applications will be moved into the cloud without requiring redesign, re-engineering, or reconsideration of business processes which already meet your daily business needs. While your competition is re-building their applications for the cloud, you'll be enjoying the financial and performance benefits of having your IT workloads running in the cloud - and your IT customers will enjoy the continuity of service delivery they depend on.

Source: Rivermeadow Software



river

Unlock the Benefits of the Cloud & Unburden IT



Saving money on data center hardware may be the most visible advantage of moving to the cloud, but it is certainly not the only benefit. The cloud represents a paradigm shift in computing, with the same level of influence client-server computing had 25 years ago. Although the cloud provides cost savings and productivity improvements, the bigger impact is a different way of approaching computing.

Let's start with the pragmatics. Moving workloads to a cloud will reduce the demand on hardware resources, just as virtualization already has. Even a private cloud business will require less hardware because pooled resources are better utilized (assuming, of course, existing hardware can be repurposed as cloud servers). A move to the public cloud will dramatically reduce the need for in-house servers, and client financial structures will move from capital to operational expenditure. Clients also will be able to reclaim some physical floor space and reduce power consumption.

A more significant benefit of migrating workoads to the cloud is reduced management costs. RiverMeadow's Cloud Migration SaaS makes it easier to deploy server workloads to clouds than traditional deployment of software to physical servers. That's partly because cloud IaaS environments that meet the processing capabilities of a workload can easily be created at will. In addition, physical characteristics of workloads, such as the operating system and other software services, are abstracted away, allowing the workload to match many more cloud environments than traditional physical servers. In fact, it is so easy to spin workloads into cloud environments that "cloud sprawl" can result – a proliferation of workloads in the cloud. Using a cloud management tool that provides visibility and control of workloads in the cloud solves this.

As use of the cloud grows, customers will find new techniques to streamline development of cloud workloads, from Agile and iterative development that improves workload usability to a new view of software requirements aligned with core business needs. SaaS solutions such as Salesforce.com already embody these new approaches (their success is based on these advances).

You may find, as others have, that you can eventually benefit by replacing some of your legacy workloads with SaaS solutions already in the cloud. However, significant changes to the services provided by your IT infrastructure can have unintended consequences and other disruptions for IT users. As Gartner has observed [Gartner Research, The Four Key Risks of Developing and Executing a Cloud Sourcing Strategy, 18 January 2013, Jim Longwood, Edward Wilson-Smythe], you should carefully plan the use of new cloud applications and services before replacing your legacy systems. Before you take that leap of faith to new applications in the cloud, RiverMeadow offers a path that retains your legacy systems without disruption while gaining many of the benefits of the cloud.

RiverMeadow Cloud Migration SaaS employs a 'Collect, Convert, Deploy' model to migrate one server workload, or a suite of servers and their workloads, at the same time. In a single operation, direct-attached storage volumes are collected, along with server characteristics and metadata, and placed into a staging zone. These volumes become golden images representing the full operational state of the servers, from applications and their data to the underlying operating system.

During the Collect phase of a workload migration, the RiverMeadow Cloud SaaS collects parameters of the source system, including disk volume size, application configuration, OS, drivers, and memory allocation. These are then converted into target image(s) that match the user's target cloud.

Drivers are then injected at the image level, tested and injected into the target cloud environment and equivalent drivers and information for a target system are injected into the golden images. The RiverMeadow SaaS auto-virtualizes physical servers as it migrates them to the cloud during the conversion process, enabling CSPs to directly on-board non-virtualized



Unlock the Benefits of the Cloud & Unburden IT



servers by automating the conversion and directly deploying the virtualized server into the cloud. The resulting images are then ready to be deployed to one or more clouds of potentially different attributes and orchestrations, and operation of the images' applications continued in the new context(s).

Maximum velocity and value are achieved by automating each of these steps.

An important upshot of the benefits of RiverMeadow SaaS workload migration is the positive impact on IT organizations. Many IT organizations have been on a never-ending treadmill of trying to keep up with user demands for development and maintenance of customized business systems. At the same time, businesses have been trying to control costs and IT increasingly has been seen as too tactical and unable to reduce its burn rate. Companies want to see IT take a strategic role in the business.

Cloud computing and infrastructure as a service (IaaS) promise infinite extensibility, elasticity, seamless shifting of workloads, no vendor cloud service provider lock-in, and reduced service delivery costs. The cloud offers the opportunity for IT to break the vicious cycle demanded by traditional legacy systems in the physical data center. By taking the proactive role of using RiverMeadow SaaS to migrate workloads to the cloud, IT can reduce costs, increase management control, and build a strategy for continuing productivity improvements.





Cloud Readiness

Removing Friction & Mitigating Risks



The ease with which individuals or departments within an enterprise can spin up a Cloud instance – so-called 'shadow IT' - points to one of the strategic risks of Cloud adoption: lack of readiness to engage with a Cloud Services Provider (CSP) or Cloud Services Broker (CSB).

Readiness comes in two main flavors: organizational readiness, which includes an assessment of individual skills, existing architectures, applications, data which may be regulated, and processes and policies; and market readiness, which involves a review of licensing, network maturity, security and IP protection.

As described in Gartner report "The Four Key Risks of Developing and Executing a Cloud Sourcing Strategy", 18 January 2013, 'The readiness of an organization to adopt cloud service offerings, as well as the readiness of different country markets to supply these offerings, varies considerably by enterprise, industry, service category and geography.'

Organizational readiness

While IT organizations may be well aware of issues with readiness to move to the Cloud, individual department heads or Business Process owners may be unaware of the complexity and ramifications of the decision. Although Cloud solutions are well-publicized they are seldom well-understood. Moreover, external factors, including reliable, cost-effective and secure network connectivity, can impact an organization's Cloud readiness. It falls to the CIO and his (or her) team to lead the organization to the Cloud, rather than be led to the Cloud. Key to asserting leadership in Cloud decisions is completion of a readiness assessment.

CIOs must assess their organization's Cloud readiness from an architectural standpoint as well as from an IP and licensing standpoint. Evaluating an organization's readiness to migrate to the Cloud entails a thorough review of applications slated to be moved to the Cloud, especially high-transactionbased workloads, e.g. ERP or CRM systems, which may not be architected for migration. CIOs are well-advised to review application portfolios to assess the Cloud-worthiness of all production applications. This review may lead to changes in the application portfolio to ensure Cloud migration is possible.

Market readiness

Many factors can affect Cloud readiness in non-US and even cross-state-border US markets. Licensing, for example, presents challenges in markets where Cloud offerings are less mature or IP and licensing protections less well understood, promulgated or protected. Within the US, regulations that affect the movement of data over state or county lines can hamstring Cloud readiness efforts for the unprepared.

When preparing to migrate to the Cloud early assessment of readiness is vital, as is creation of a migration plan which specifies application dependencies, availability, reliability and security requirements, network access, and solution maturity and viability.

As a partner to CSBs and CSPs worldwide, RiverMeadow is well positioned to work with service providers to plan and conduct Cloud Readiness Assessments, create mitigation scenarios, and prepare a migration RiverMeadow adds value by eliminating one of the unspoken but real obstacles to cloud readiness: friction. This friction exists at two points in the cloud journey: technical readiness to adopt, and operational readiness to adopt.

As Gartner analyst Gregor Petri notes in Gartner report, "Three Factors Will Significantly Impact Enterprise Cloud Use in the Near to Midterm Future", August, 2013, "Gartner sees many organizations struggling to agree or even discuss a comprehensive or companywide cloud strategy." This operational roadblock to cloud occurs in part because, he notes, "In the past, a central governing body (such as IT) rationalized the different perspectives by virtue of the fact that all solutions at some point had to be deployed on the company's internal infrastructure. With the advent of cloud, this rationalization doesn't happen because each constituency can procure externally-delivered cloud services based on their perceived value." This operational friction can be mitigated, however; as Petri notes, "This is the moment where enterprises need to have the discipline to reassess the technology, their implementation and the provider to bring it back in line with corporate policy and architecture while observing the need to continue to meet the original business goals."



Cloud Readiness

Removing Friction & Mitigating Risks



Solving technical friction is a different matter. Automation of the cloud migration process can reduce friction by avoiding the complexity of manual, highly customized migrations. With features like the ability to perform local migrations via virtual POPs, to near-term advances such as the ability to use a RiverMeadow's local custom migration worker (built on the fly to perform against characteristics of the specific source/ target). This new capability, to be released in Q2 2014, will enable migration worker to be deployed into the target cloud and deleted when the job is over, on a migration-by-migration basis.. RiverMeadow also enables customers to pre-test common IT processes today, such as upgrading antivirus software or OS patches by cloning and migrating a server to the cloud, testing upgrades and changes on the clone, and verifying success prior to updates to production systems, ensuring confidence in the quality and success of the ultimate server or workload migration.

Unlike cloud onboarding or workload migration tools which require manual rebuilding, templating or wrappering within a virtualization container, the RiverMeadow SaaS automates the migration of complete Windows™ or Linux servers "as-is" from physical on-premise or virtual to the Cloud, or between Clouds. A RESTful API enables configuration and pre-runtime setup and customization without requiring hands-on intervention. For maximum flexibility, all RiverMeadow functionality is available programmatically via the Cloud Migration SaaS API, which provides an extensible scripting environment for pre and post migration workload configuration and customization.

Migrating workloads to the cloud can be filled with technical challenges and operational uncertainties. This leads to slowed progress and stalled-out migration initiatives that impede business growth for providers and cost savings for their customers. RiverMeadow's Cloud Migration SaaS removes this friction and delivers true workload mobility to providers and end-users alike by automating what would normally be complex manual steps in the onboarding process while empowering IT leaders to verify interoperability of their applications in the target cloud before final cut over. The RiverMeadow Cloud Migration SaaS is always available where and when you need it.





Migration to cloud-based services provides many benefits but is inherently risky. CIOs can use this checklist of key challenges and best practices to reduce risks when executing a cloud sourcing strategy.

Key Challenges

- The readiness of organizations to adopt cloud service offerings, as well as the readiness of different country markets to supply these offerings, varies considerably by enterprise, industry, service category and geography.
- Cloud service offerings are at different stages of evolution and maturity from a technological, architectural, performance, services and contractual perspective and some are not "enterprise ready" yet.
- There are a range of hidden costs, contractual "gotchas" and risks involved in taking on any new cloud technology and service offerings, and many early adopters are not making the savings they anticipated.

Recommendations

CIOs should:

- Conduct a readiness assessment to confirm the readiness of their company and the market to embark on a cloud services journey.
- Ensure the cloud services offering can meet your reliability, availability, scalability and security (RASS) requirements.
- Confirm the commercial viability of the solution required, considering both life cycle costs and business and technology risks.

 Ensure that the technical and commercial solution avoids hidden "gotchas" that pose significant operational and financial risks.

Introduction

CIOs must align cloud services sourcing strategies and actions directly to business objectives to assure effective outcomes, and must understand the IT services marketplace to effectively evaluate and utilize IT service providers and their offerings for cloud services.

Cloud-based services (see Note 1) can offer cost-effective, flexible and scalable IT solutions to meet a company's evolving business needs, but migrating to the cloud is a major shift for organizations and can be risky. Although some risks are similar to traditional service delivery models, cloud-based services have a much higher potential to reduce control over strategic and operational decisions — and to amplify any adverse impact on clients.

ClOs can address these risks with a well-defined sourcing strategy and execution plan. Risk management must extend across all stages, from defining services to executing sourcing activities and through ongoing service-delivery management. This research describes the risks that impact the viability of cloud solutions and offers a structured approach to identifying and addressing them; it is categorized into four best practice areas:

Figure 1. Stepwise Approach to Meeting Your Cloud Services Requirements



RASS = reliability, availability, scalability and security Source: Gartner (January 2013)

- The readiness of your organization and the market
- The ability of solutions to be reliable, available, scalable and secure
- Commercially viability
- Avoiding hidden "gotchas"

Figure 1 illustrates how these risk elements can be integrated into a straightforward sequencing of your sourcing action plan for your cloud services sourcing strategy. Use a cloud readiness assessment process and then use a deal sweet-spot analysis as part of the market scan to speed up the shortlisting of prospective cloud service provider offerings.

Analysis

These four groups of best practice recommendations stem from Gartner's interactions with organizations considering a cloud services-based sourcing strategy.¹ For each best practice we provide an outline of risks and possible mitigation actions.

Make Sure Both Your Company and the Market Are Ready Ensure Local Market Readiness and Maturity

Risks:

Many cloud offerings are early in the Hype Cycle, which introduces market maturity risks.² Access to readily available, reliable, secure and lowcost network connectivity can also be an issue in remote geographies.³ Without such access you can't take full advantage of new offerings without unnecessary execution risk, nor leverage lessons learned by early adopters in more mature markets.

In emerging markets some providers rebadge existing offerings as cloud, a process sometimes called "cloud washing." For help in deciding whether a service qualifies as a cloud offering see "Data Center Outsourcing, Hosting or Cloud? Use Gartner's Market Map and Compass to Decide," "Five Things That Private Cloud Is Not" and "Don't Be Fooled By Offerings Falsely Masquerading as Cloud Infrastructure as a Service." In these markets many independent software vendors aren't fully able to meet the licensing challenges of running their software in cloud environments.

Mitigation:

Review the maturity of cloud services offerings in your market, other organizations' cloud service adoption, and the quality of network availability/access — then tailor your sourcing strategy accordingly. Ensure that the local offerings provide the desired level of maturity, costeffectiveness and scalability or consider collaborating with providers to invest in cloud service offerings that align with your requirements.

Address Technology and Architecture Readiness and Maturity

Risks:

Many enterprises are unaware of significant architectural barriers to migrating existing applications, and particularly high business-transactionbased ERP workloads, to the cloud.⁴ Most high-volume business transaction application platforms are between three and five years away from being mature enough for early mainstream consumers to consider moving some traditional workloads to cloud-enabled application platforms. This often leads to "cloud Frankenstein" scenarios, with multiple architectures at various levels of migration to the cloud, increasing complexity, operational risk and life cycle costs.⁵

Mitigation:

- Consider common infrastructure architecture and platforms and consolidate architectures if needed prior to cloud migration.
- Use a phased approach to implementing cloud-based applications.
- Prioritize your application portfolio for migration to the cloud.

Not all applications will be viable candidates for migration and those that are may require significant remediation and replatforming to work in a virtualized environment.

Define a longer-term road map for remediating/migrating applications to cloud-based services. For each phase you should define the subset of applications and underlying technologies to migrate, while also defining the application interfaces and handoffs required to ensure seamless delivery of business functionality to users and easy supportability of the hybrid architecture. Also assess which applications should be run on a private or hybrid cloud and which might be candidates for public cloud, such as email or development and testing environments.

Address Organization Readiness and Governance Impacts

Risks:

Enterprises are at different states of organizational readiness for cloud migration and many lack the decisionmaking processes needed for such major changes in IT direction. A common governance model is essential to guide cloud decisions.⁶ Moving to cloud services also means dealing with smaller and less mature vendors that may be technologically innovative but lack maturity and discipline when it comes to standards and governance.

Because providers are responsible for most of the services involved in cloud delivery, client companies retain only strategic direction-setting related to business and technology priorities. Those companies must, therefore, rely more heavily on alignment and governance processes — as well as outcomebased performance measures — to manage and oversee the outsourcing relationship. This represents a significant shift in responsibilities and some companies will struggle to staff, manage and maintain the appropriate level of control over the cloud provider.

Mitigation:

Assess your organization's readiness to adopt cloud service offerings at the early stages of strategy planning. Consider both the maturity of governance structures and processes and the skill sets offered by the target retained organization.

Incorporate change management in cloud strategy execution. Clearly identify roles currently performed in-house or through other providers that will need to be performed by the cloud services provider, and assess the impact of this change on control over technology and architecture decisions. Define areas of decision making and control that will be retained, as well as dependencies and handoffs with the provider that enable end-to-end coordination between decision making and execution.

Develop a model for the future-state retained IT organization and identify skill sets needed to support an interaction model with the cloud service providers for ongoing service delivery. Define and establish outcome-based performance metrics that focus less on operational control and more on delivering the business and technology outcomes required. Consider the use of multisourcing service integrator and cloud service broker roles in your strategy.

Finding Cloud Services That Meet Your RASS Requirements Protect Data Sovereignty and Security Risks:

Privacy, sovereignty and security of data are concerns in most mature IT economies (see "Five Cloud Data Residency Issues That Must Not Be Ignored"). Processing data in the public cloud means you have little control over where that data is stored/processed, and limited ability to audit/assure that it meets regulatory compliance.7 Thus, it is more difficult for companies to define their data's geographic footprint at any given time or to address data security and privacy issues in order to contain risk.⁸ Some cloud providers still refuse to tell clients where their data is physically located or to guarantee that data is held locally (in the same country).

Increasing government incursion on data use, added to location issues, poses an operational risk that is a particular barrier to entry for clients in the public, health and financial sectors that require critical data to reside in the same jurisdiction.⁹ While global and local providers offer services based on locally situated, shared infrastructure in major markets, these may not provide the cost-effectiveness, scalability or service maturity you need.

Mitigation:

Develop a comprehensive policy for data location, privacy, security of access and processing, and ensure that providers are contractually obligated to comply with these provisions. Contracts should unequivocally state that cloud providers will not share personal data with anybody other than those approved third parties that are required to provide the services, and that clients are notified (and must provide approval) before data is moved. Contracts must also allow for specific reporting and auditing capabilities, to ensure ongoing compliance. As part of your pilot you should validate data transmission security and verify the physical location in which data is processed/stored.

Retain Control Over Your Destiny Risks:

Cloud providers can change their technology and architecture without your knowledge or approval.¹⁰ Most major organizations will not rely on a single provider for all their IT solutions, meaning that ongoing interoperability with other technologies and integration with their existing systems, as well as lack of performance guarantees, can present availability and performance risks.

Mitigation:

Define and implement clear governance models for vendor decisions that could have an impact on technology and architecture changes. If possible, build in provider obligations for the performance of third-party interfaces. Look at the cloud service brokerage role for simplifying the integration of the various components in your cloud ecosystem.

Put business-aligned service levels in your contract to ensure the cloud services can deliver the end-toend performance required by your business.

Pilot the Candidate Cloud Services Risks:

Early adoption of new technologies and service offerings, major migration decisions, and betting the future of your IT and business functions on new developments carries major risks. Worst-case scenarios include costly project overruns, business processes not working properly and the business coming to a standstill because core functions don't work efficiently or properly. Comparing differing cloud service offerings is difficult as they often have different technical and service roots and DNA, as we can see in the evolution of offerings from Amazon Web Services and Google compared to traditional providers like IBM, HP or CSC.

Mitigation:

Assess the suitability for cloud services in non-critical business areas and build up a working knowledge of what those cloud service offerings can offer. This might include common office systems such as email as well as using infrastructure as a service (laaS), which is easier to use in test and development environments (see Note 2).

Do a market scan and use a deal sweetspot analysis to shortlist candidate offerings — to pilot a small number of services to validate vendor claims across a select range of services (see "IT Procurement Best Practice: Use a SaaS Pilot Phase" and "Seven Stages to a Successful Hosted Virtual Desktop Rollout: Stage 6a, Pilot Preparation"). Areas to assess include whether solutions provide ease of access, scalability and use; good security; performance under load and consistency with your architectural policies (see "Toolkit: Mitigating Risks in Cloud Infrastructure as a Service"). Develop test criteria and success factors to evaluate the pilot and to act as stage gates for decisions to expand.

Confirm the Commercial Viability of Cloud Solutions Insist on Balanced Contractual Terms Risks:

Factors related to contract, pricing and transition can expose you to significant operational and financial risks (see "Manage Risk and Unexpected Costs During the Cloud Sourcing Revolution" and "Ten Ways to Avoid SaaS Delivery Problems and Protect Your Organization"). Cloud services contracts are less mature, and typically have standardized but simplified sets of master services agreement clauses and limited schedules relative to traditional IT services contracts.¹¹ Many cloud services providers reserve the right to change all or part of the agreement once it is signed, or to cancel services with minimal notice. These practices expose users to risks related to the technology solution meeting business needs, limited control over their longerterm risk profile, and limited recourse in the event of issues with service delivery — thus transferring the incidence of risk disproportionately onto the client company.¹²

Mitigation:

Approach contracts for enterprise-focused, cloud-based services expecting providers to provide similar protections — related to performance and liability — to traditional services contracts. Changes in service terms must be based on mutual agreement rather than a unilateral right for the provider. This will lead to some providers being excluded from consideration. Build compliance with your desired contract terms and key service levels into your evaluation of any cloud service, as well as the usual solution functionality and cost savings. If you cannot accept the risks, exit the negotiations.

Control Transition and Transformation Risks

Risks:

Because most cloud offerings are not mature enough to support moving traditional enterprise workloads to cloudenabled application platforms — and migrating and transforming application portfolios to support cloud services can be costly — failures in either area can pose critical risks.

Mitigation:

Understand that application transformation and replatforming are necessary prerequisites for the transition to cloud-based services. You should

incorporate transition costs into the cloud business case and manage any transformation activities as higherrisk projects.

Define clear provider obligations for your migration to the cloud and link one-time transition payments, and the start of ongoing costs, to the acceptance of specific deliverables related to the transition. During the pilot stage assess cloud implementation providers on their track record in similar exercises and on their ability to use repeatable conversion/migration processes to reduce transformation risks. Leverage established operational frameworks to reduce transition risks.

Beware Unintended Price Impacts Risks:

Cloud contracts rarely guarantee reduced costs over time (see Note 3) and present a range of hidden costs that can lead to adverse pricing variations, as we see in many mobile phone pricing regimes.

Mitigation:

For enterprise-based services, negotiate a commitment to annual unit price reductions and build in volume-based pricing bands to avoid escalating costs.

For commoditized cloud services use the market's natural competitive forces to drive down pricing, but ensure you can renegotiate pricing on a regular basis.

Avoid Hidden "Gotchas" That Pose Significant Operational and Financial Risks Mitigate Provider Lock-In

Risks:

Risks related to provider or technology dependence do not vanish with cloud services. Once contracted, a cloud service provider may deliver its contracted services in perpetuity. In reality, and with providers having control over most parts of the standardized delivery model, client companies are more critically dependent on providers than in traditional models.

Getting your data back after a contract termination (see Note 4), as well as the time it takes to switch to a new provider, can pose significant risks (see Note 5).

Mitigation:

- Review the architectural compatibility of your service options to minimize the risk of technology lock-in.
- Ensure that any termination clauses have clear provisions for protection of intellectual property (IP) and transfer of data to you smoothly and without cost.
- Prepare for a provider switch to be executed quickly to ensure continuity of service.
- Ensure that contracts provide for all data to be returned in a predefined format within 30 days of termination and for the provider to maintain, back up and secure the data until it is returned.

 Negotiate terms that allow no termination for the provider's convenience and, failing that, negotiate for at least six months' notice for the provider to terminate (see the previous discussion on balanced contract terms).

Retain Control Over Offshoring Decisions

Risks:

Global service delivery models are a key tenet of many cloud service offerings. Without appropriate visibility, clients may find a significant part of their service delivery being carried out in offshore locations, often without their knowledge.¹³ This can expose clients to privacy and security risks as well as significantly higher cultural, reputational, customer retention or political risks, even if providers ensure appropriate controls over operations.

Mitigation:

Identify which roles must remain onshore (or even on-site) and which roles can be delivered from offshore locations. Retain control over approvals for any offshore delivery resources. Specify data access standards and policies, including technical standards for encryption and transmission; access controls at the offshore delivery location; and background and/or security check protocols for offshore resources that access client data.

Avoid Shelfware as a Service Risks:

Shelfware as a service is the concept of paying for a software subscription that is not being accessed by an end user. Underutilizing the contracted number of licensed seats or processing units leads to hidden costs and suboptimal ROI.

Mitigation:

Ensure you have good demand management practices in place for your cloud services and develop integrated and proactive capacity planning practices to address changes across the technology stack.

Evidence

¹ Gartner analysts take regular calls on cloud service options. We have also taken an average of 11 sourcing strategy calls per month in the past two years, which invariably include discussion on cloud service options. In addition, a range of client examples and material cited in the notes emanate from Gartner's consulting assignments.

² Gartner's Hype Cycle analysis shows that, while globally many cloud service offerings are in early phases of adoption, the level of adoption of key services like laaS and SaaS varies considerably in different countries around the world.

³ At a major global company with operations across the Middle East, Asia and Africa, the majority of employees were unable to access cloud-based services due to issues with network availability and/or access, leading to cloud services being limited to mature locations in North America, Europe and parts of Asia/Pacific, and use of alternative local solutions for other markets, leading to significantly higher complexity and cost.

⁴ High-transaction application platforms (ERP or banking, for example) often need a distributed architecture across multiple high-availability data centers.

⁵ A major North American company evolved to four different versions of IaaS architecture, each tailored to specific virtualization technologies and service models, leading to the inability to execute enterprisewide architecture or sourcing strategies.

⁶ For a major global company, the federated IT decision-making model and high level of business unit (BU) autonomy led to multiple initiatives and standards. The company needed to evolve a strong, centralized decisionmaking and governance process to coordinate standards, service delivery, and delineations between local and central IT, and include other functions such as procurement, legal, and architecture in the governance model.

⁷ For example, while the Patriot Act provisions related to data located in the U.S. is a common concern for companies located in other countries, similar risks exist in several other jurisdictions. Several major countries, such as China, India and the U.K. seek similar or higher levels of visibility into data by law enforcement agencies. There are also specific considerations in banking and health in Europe to name a few regulatory, privacy and security constraints. ⁸ Canadian public sector organizations and other entities with significant sovereign oversight find migration to cloud-based services a challenge due to the location of most mature cloud providers in the U.S., which limits the range of services that can be migrated to the cloud.

⁹ In some North American and Canadian states or provinces, the need for personal data to be resident within the boundaries of the state/province poses an additional barrier to cloud execution.

¹⁰ One large U.S. healthcare player's cloud vendor moved unilaterally to a new architecture and took data outside of its protected environment — leading to significant issues with regulatory noncompliance.

¹¹ Several popular cloud providers are well known for contracts that offer a lower level of commitment to warranty, fit for purpose, regulatory compliance, or limitation of liability, which are all critical considerations. "Four Risky Issues When Contracting for Cloud Services" cites details of various standard cloud contracts that Gartner analysts have reviewed.

¹² A major North American company had to learn the hard way that cloud service providers like Amazon and Google would not bend from a contractual standpoint. For example, Amazon would not even agree to a nonassert clause, which essentially meant that the client would have no protection of their IP.

river

¹³ For a large Canadian client with a significant strategic role in economic management and public policy, the outsourcing vendor gradually moved critical technical skills offshore without informing the client. This led to significant issues in the support of complex high-volume transactional applications and inability of the client to access specialized resources when required.

Note 1

Cloud-based services include infrastructure as a service (laaS), platform as a service (PaaS), software as a service (SaaS) and integrated platformbased business process services business process as a service (BPaaS).

Note 2

Two major Gartner clients have adopted private laaS as a pilot of cloud use, focusing initially on nonproduction application development environments and eventual expansion to other environments upon successful execution of the pilot against predefined success criteria.

Note 3

In traditional IT service contracts, clients expect a reducing cost profile for services, based on three factors: declining cost for technology inputs over time; increased productivity of service delivery; and reduced costs based on higher volumes. The first two factors can lead to a 5% to 8% per year reduction in annual costs over three to five years (as described in the presentation "Driving Outsourcing Cost Reductions Through Innovation and Productivity Improvements" presented at the 2009 Gartner Outsourcing and Vendor Management Summit. The third factor can lead to as high as a 50% to 70% reduction in unit costs for incremental volumes 25% higher than baselines, based on Gartner's review of recent unitized pricing in traditional managed infrastructure delivery models.

Note 4

When a contract does not specify that data needs to be returned in a specified file structure at termination, and providers use proprietary encryption for data storage, clients have significant issues with access to data and providers have scant motivation to assist. Some contracts also state that, if a client has not transferred the data within 30 days, the cloud services provider has no obligation to provide security or backup of the data and can destroy it after this period unless prohibited by law. Providers also charge transfer fees (per GB of data, for example) to return data, which can be a significant cost when you include backup files and archives.

Note 5

A number of cloud contracts allow the provider to terminate the agreement with 30 days written notice, or within 30 days of renewal. For some cloud capabilities, it would be almost impossible to find an alternative solution and migrate to it within 30 days. For example, a major Canadian company was presented with a "take it or leave it" contract from a cloud service provider that contained no provisions for data access and transfer upon termination, giving the provider the unilateral right to destroy data after termination. Despite a favorable business case for the migration to cloud-based storage, this provision made the transaction unviable for the client.

> Gartner RAS Core Research Note G00249819, D. Scott, M. Govekar, A. Lakhani, G. Petri, 10 April 2013

Anatomy of a Cool Technology

RiverMeadow is proud Gartner chose us as one of its Cool Vendors in Cloud Management, 2013[Gartner Research, Cool Vendors in Cloud Management, 2013, 10 April 2013, Donna Scott, Milind Govekar, Gregor Petri, Aneel Lakhani]. A key piece of the decision was recognition that our RiverMeadow Cloud Migration SaaS is cool technology. We've made it easy to use, but that's just the surface over serious software that does the hard work so you don't have to.

RiverMeadow's SaaS is a flexible platform for performing server workload migrations and supporting tasks. It includes a user friendly GUI for directing migration action and an API for programmatic control of all RiverMeadow functionality. Access via API allows RiverMeadow to be supplemented with additional functionality, and easily embedded within other systems. Regardless of how RiverMeadow is accessed, it streamlines migration tasks and reduces complexity by solving the hardest migration challenges internally – all without cost headaches.

It lets the user focus primarily on which server workloads are being migrated and the performance requirements that must be met when workloads are moved to a cloud.

When a migration is started, RiverMeadow collects server characteristics and metadata, creating a golden image that's deposited in a staging zone. This process has minimal impact on the workload's environment: servers don't need to be quiesced and agents don't need to be installed. Once within the staging zone, the workload is converted into an image that can be deployed as a fully compatible VM in the target cloud, with technical details of the source platform (e.g., low-level drivers and local IP addresses) replaced by equivalents in the target environment. RiverMeadow allows the use of preconversion or post-conversion scripts to manage any additional processing required, such as workflow configuration.

CSPs and CSBs who embed RiverMeadow in their systems can layer intelligence onto RiverMeadow to meet new challenges. For example, to enable automated brokering of workloads to clouds, operational policies can be added to workloads the extended RiverMeadow system would use to select clouds to which the workflow may be deployed. If RiverMeadow were being used interactively, the user would simply have to pick one of the clouds offered from the RiverMeadow GUI to deploy and start the workflow. Otherwise, RiverMeadow would select the best matching cloud for the workload by itself and deploy to it automatically. As the name implies, RiverMeadow's SaaS doesn't require any installation or licensing. It runs and is accessed from the Cloud as a service. It may be used interactively via a simple user-friendly GUI, or accessed programmatically via a RESTful API. The GUI is a good choice for managing migrations that require choices or need monitoring. The API opens interesting possibilities for large volumes of migrations, migrations that occur on a schedule, or other scenarios.

RiverMeadow's API allows CSPs and CSBs to build their own user interfaces to the core migration functionality – everything available in the standard GUI is available with API calls as well. This allows the SaaS to take programmatic steps that would have required user action in the GUI, allowing migrations to be streamlined. In some cases, migrations can be managed simply by providing the source server IP addresses and admin access credentials for those workloads. In other cases, there may be reasons to migrate workloads not just once, but on a regular basis to different cloud VMs. For example, QA processes might benefit from having workload instances showing state on a daily basis.

Finally, because RiverMeadow is adept at gathering data from servers, other solutions can be built on top of the RiverMeadow SaaS. For example, a disaster recovery system could use RiverMeadow as the means of collecting workload information on a regular basis, without disrupting the system on which the workload is running.

By designing the RiverMeadow SaaS to perform the task of cloud migration very efficiently, it has become useful in many ways. That is definitely cool.

Source: Rivermeadow Software

river

Brokering Workloads Among Clouds

To which cloud, or clouds, should a business migrate its server workloads? This question has many facets and gets to the core of why one should move to the cloud in the first place. Should you be using a private, hybrid, or public cloud? Which technology and hypervisor should the cloud support? Which clouds offer the performance a workload requires to meet a user's needs?

As cloud technologies and experiences have matured, questions which once would have been answered by IT are now the province of professional services and a growing discipline known as Cloud Service Brokers (CSBs) [Gartner Research, Service Provider Primer: Cloud Services Brokerage, 18 December 2012, Benoit J. Lheureux, Michele Cantara, Tiffani Bova, Donna Scott]. CSBs are companies that add value to cloud services for the benefit of cloud service consumers. Some companies, such as consultancies, have played this role from the early days of cloud commercialization, while others are now joining this growth industry. Some companies are particularly suited to becoming CSBs, particularly Cloud Service Providers (CSPs) who offer IaaS services that support multiple hypervisors and frameworks.

While CSBs can navigate though the many cloud choices, ultimately each business will have to make decisions that suit its context and goals.

Choosing between private, hybrid, and public clouds is a typical starting point. Issues such as compliance, control, and scale are critical and will lead to decisions. However, when it comes time to move a specific workload to one cloud among those choices, RiverMeadow's Cloud Migration SaaS automates the migration.

Which technology and hypervisor should the cloud you select support? RiverMeadow's SaaS can automatically convert server workloads to run on whichever hypervisor and in any cloud necessary, allowing you to choose cloud providers based not on technology, but on business values such as reliability, support, and cost.

Which clouds can meet your workload's performance needs? Given the cloud's elastic scalability, ultimate speed and size may not be an issue, but avoiding over-provisioning is – you should not pay for performance you don't need. RiverMeadow's SaaS platform can be extended by CSBs and OEMs to allow customers to characterize the operational of their workloads. For example, customers could prioritize needs using low cost, SLA agreements, or other parameters, thereby guiding policies to select an appropriate cloud for the workload's needs. To make all of this work, the only other necessary step is to take action: someone will have to decide which clouds you are willing to do business with, create accounts with them, and load access information into the RiverMeadow SaaS. Cloud service providers document the capabilities, prices, and services of their cloud offerings, and RiverMeadow matches this information with the policies associated with each workload. Matches indicate a workload will operate most efficiently on that cloud, and RiverMeadow then uses any policies you've defined to make the final determination of which cloud best meets your needs.

Although RiverMeadow SaaS can solve most tactical challenges in migrating your workloads to the best cloud, there is a role for CSBs and other professional services organizations. They help determine which clouds to build relationships with, and they are often the same organizations that can help integrate workloads into complementary services in the cloud, or provide additional customization necessary after migrating workloads to the cloud.

The RiverMeadow SaaS features a powerful delegation model that makes it easy for RiverMeadow to grant usage rights to its partners and channels. RiverMeadow grants delegation capability for n workload migrations to a channel partner, e.g. a CSB or OEM, enabling that partner, in turn, to delegate n workload migrations to its customers or partners, e.g. a VaR, and so on.

RiverMeadow maintains a unique record of each migration, making it simple and rapid to document when, by whom and where each server workload was migrated. For CSPs, channel partners and customers, this level of migration visibility provides a total audit trail, complete with migration characteristics, simplifying regulatory and audit compliance.

The RiverMeadow Cloud Migration SaaS provides value for the entire Cloud and IT ecosystems: CSPs, channel partners, customer enterprise and government business process owners, and IT teams, ensuring workload availability and reinforcing the importance of IT's role as a business partner and service broker. For these reasons and more, RiverMeadow sees value in working with organizations that help clients understand and navigate the complex cloud ecosystem.

Disaster Recovery as a Service (DRaaS)

After you've migrated your server workloads into the cloud and started production operation, your users will depend on 24x7 availability. Your Cloud Service Provider (CSP) should offer SLAs that govern delivered performance, but your IT organization will be responsible for workload health, just as it was responsible when the workload was in your physical data center. But in the worst case, your CSP may have a failure that prevents your workload from operating at all.

RiverMeadow Cloud Migration SaaS's ability to migrate server workloads can provide the failsafe backup that will protect you in most of the worst outages. The fundamental ability to capture a server's workload and state – whether within a physical, virtual, or cloud environment – and move it to another environment forms the basis of a Disaster Recovery (DR) service.

Enterprises can perform a backup of server workloads with the RiverMeadow SaaS on a regular schedule, at least once a day. Just as when RiverMeadow is migrating a workload, the backup will contain the entire workload and its state. Best practices dictate that the workload be placed into a different cloud environment, perhaps geographically distributed, so the backup is stored safely.

In the event of a catastrophic failure of your cloud-based workload, a collection of workload snapshots will be available for RiverMeadow to migrate to a different CSP or to refresh the failed workload in its already deployed location. RiverMeadow maintains a unique record of each migration, making it simple and rapid to document when, by whom and where each server workload was migrated. For CSPs, channel partners and customers, this level of migration visibility provides a total audit trail, complete with migration characteristics, simplifying regulatory and audit compliance.

Just as with regular workload migrations, RiverMeadow handles all the mechanics of accessing the backed-up workload, automatically transforming it as needed for a different cloud architecture, deploying it to the new cloud environment, and running whatever custom scripts might be required, pre or post migration, to make the workload operational in its new environment. That's a particularly useful feature when conducting DR as post migration scripts can help handle the cutover to the new cloud instance of the recovered workload. Once you've used RiverMeadow SaaS to migrate your physical server workload into the cloud, it's simple to extend your use of RiverMeadow to implement a disaster recovery solution. And because it is based on the RiverMeadow migration platform, you'll have maximum flexibility and convenience for redeploying your workloads to the new cloud of your choice.

Source: Rivermeadow Software

river

rivermeadow

Your Path to the Cloud is published by Rivermeadow Software. Editorial content supplied by Rivermeadow Software is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2014 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Rivermeadow Software's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.