

# What Does Network Connectivity Mean?

Network connectivity describes the extensive process of connecting various parts of a network to one another, for example, through the use of routers, switches and gateways, and how that process works.

Network connectivity is also a kind of metric to discuss how well parts of the network connect to one another. Related terms include network topology, which refers to the structure and makeup of the network as a whole.

There are many different network topologies including hub, linear, tree and star designs, each of which is set up in its own way to facilitate connectivity between computers or devices. Each has its own pros and cons in terms of network connectivity.

IT professionals, particularly network administrators and network analysts, talk about connectivity as one piece of the network puzzle as they look at an ever greater variety of networks and the ways networking pieces go together.

# What is cloud management?

## Everything you need to know

Cloud management refers to the exercise of control over public, private or hybrid cloud infrastructure resources and services. A well-designed cloud management strategy can help IT pros control those dynamic and scalable computing environments.

Cloud management can also help organizations achieve three goals:

- *Self-service* refers to the flexibility achieved when IT pros access cloud resources, create new ones, monitor usage and cost, and adjust resource allocations.
- *Workflow automation* lets operations teams manage cloud instances without human intervention.
- *Cloud analysis* helps track cloud workloads and user experiences.

Without a competent IT staff in place, it's difficult for any cloud management strategy to succeed. These individuals must possess knowledge of the proper tools

and best practices while they keep in mind the cloud management goals of the business.

## **Why is cloud management important?**

Companies are more likely to improve cloud computing performance, reliability, cost containment and environmental sustainability when they adhere to tried-and-true cloud optimization practices.

There are many ways to approach cloud management, and they are ideally implemented in concert. Cost-monitoring tools can help IT shops navigate complex vendor pricing models.

Applications run more efficiently when they use performance optimization tools and with architectures designed with proven methodologies.

Many of these tools and strategies dovetail with environmentally sustainable architectural strategies to lower energy consumption.

Cloud management decisions must ultimately hinge on individual corporate priorities and objectives, as there is no single approach.

## **Cloud management goals and characteristics**

Arguably the biggest challenge to cloud management is *cloud sprawl*, which is exactly what it sounds like: IT staff loses track of cloud resources, which then multiply unchecked throughout the organization. Cloud sprawl can increase costs and create security and management problems, so IT shops need governance policies and role-based access controls in place.

# Cloud management components



## Automation and orchestration

- Application migration
- VM images/instances
- Configuration management



## Security

- IAM
- Encryption
- Mobile/endpoint security



## Governance and compliance

- Risk assessment/threat analysis
- Audits
- Service and resource governance



## Performance Monitoring

- Storage
- Networks
- Applications
- Compute



## Cost Management

- Cloud instance right sizing
- User chargeback and billing

Essential areas of cloud management include the automated and orchestrated instances and configurations, secure access and policy adherence, and monitoring at all levels -- all done as cost-efficiently as possible.

Start with a cloud migration strategy that incorporates proper documentation and ensures only necessary data and workloads are moved off premises. Address multi-cloud management, self-service portals for users and other forms of provisioning and orchestration.

Cloud management platforms provide a common view across all cloud resources to help monitor both internal and external cloud services. Management platform tools can help guide all individuals that touch an application's lifecycle. Regular audits can keep resources in check. Finally, consider third-party tools to help fine-tune enterprise usage, performance, cost and business benefits.

Be sure to set metrics to help identify trends and provide guidance on what you want to measure and track over time. There are plenty of potential data points, but every enterprise should choose the ones that matter most to their business. Consider the following:

- Data about the utilization of a compute instance's volume and performance (processor, memory, disk, etc.) provides insight about the application's overall health.
- Storage consumption refers to storage tied to the compute instances.
- Load-balancing services distribute incoming network traffic.
- Database instances help pool and analyze data.
- Cache instances use memory to hold frequently accessed data and thus avoid the need to use slower media, such as disk storage.

Functions, also called *server less computing services*, are used to provision workloads and avoid the need to supply and pay for compute instances. The cloud provider operates the service that loads, executes and unloads the function when it meets trigger parameters


## **Security management**

The major public cloud vendors continue to invest in their services and improve cloud security, such as their ability to fend off distributed denial-of-service attacks. Some experts say that today's cloud attacks are far less devastating than on-premises ones because cloud attacks are generally limited to a single misconfigured service, whereas a local attack might devastate an entire infrastructure.

Nevertheless, IT shops must remain vigilant to guard against security threats. Google, AWS and Microsoft, among others, do not take full responsibility to keep cloud data safe. Cloud users must understand their shared responsibility in the cloud to protect their data. Cloud security best practices include configuration management, automated security updates on SaaS, and improved logging and access management. Cloud configurations today are more standard, and standard configurations are easier to secure.

# Guide to the shared responsibility model

■ USER'S RESPONSIBILITY ■ SERVICE PROVIDER'S RESPONSIBILITY



	EXAMPLES	APPLICATIONS	MIDDLEWARE	VIRTUALIZATION	DATA	Q/S	NETWORKING	RUNTIME	SERVERS	STORAGE
<b>SaaS</b>	Dropbox, Salesforce CRM, Zoom, Microsoft 365, Google Workspace	■	■	■	■	■	■	■	■	■
<b>PaaS</b>	Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	■	■	■	■	■	■	■	■	■
<b>IaaS</b>	Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)	■	■	■	■	■	■	■	■	■

SOURCE: <https://www.ibm.com/cloud/learn/saas-vs-iaaS-what-s-the-difference-and-how-to-choose>  
ILLUSTRATION: ILLUSTRATIONS

© 2020 TECHTARGET. ALL RIGHTS RESERVED. 

The cloud security model delineates which areas of cloud security are up to cloud providers to ensure and which are the responsibilities of users.

Security dashboards and trend analysis tools let enterprises look into their environment to help it stay secure. Cloud versions are far more flexible than the tools that live on premises. For example, an enterprise can activate a service provider's online dashboard and quickly receive visibility into an online attack.

## Cloud security challenges

Cloud security breaches and incidents still occur even as security technologies improve and service providers gird their networks. People can attack network hosts and web apps as fast as they can be fortified. Cloud administrators should test their environments and have the latest security audits and reports. Take care when adopting new technologies, such as AI and machine learning, which use many data sources and therefore broaden the range for potential attacks.

## Cost management

Cloud computing costs can spiral if they are not managed from the start. Numerous short-term and long-term cost optimization strategies for cloud configurations can help keep budgets in line.

Start with choosing the right provider. There are different ways to run an application: hosted on VMs on a service, containerized, or hosted in a serverless computing environment. Each has varying cost and management complexity. The trick is to find the right balance between cost and enterprise needs. Apply the following considerations:

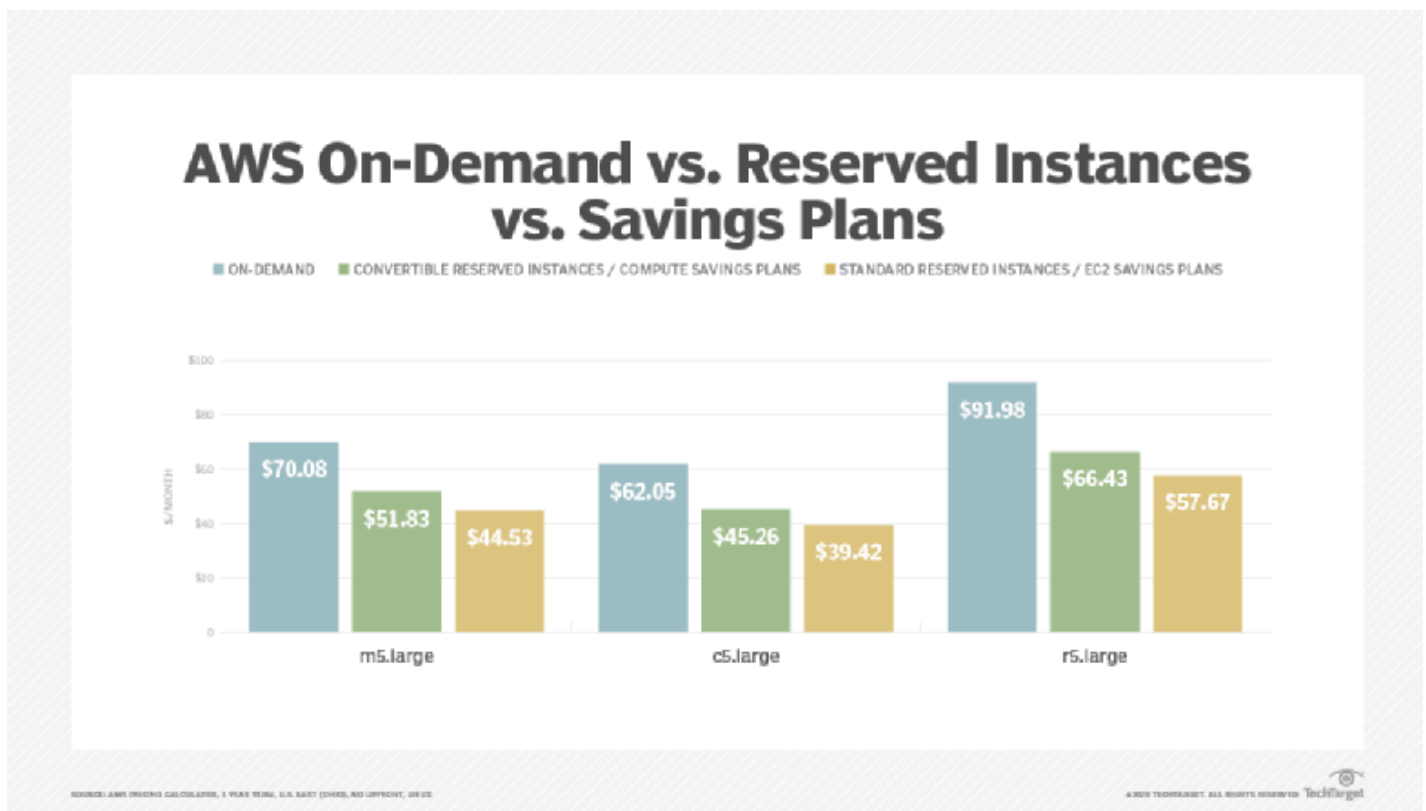
- **Determine how much redundancy your application needs.** One way to achieve cloud redundancy is to pick a hosting option that distributes workloads across multiple data centers within a region. This is a low-cost strategy but has the least amount of redundancy. Another way is for users to mirror workloads across more than one region, which offers more redundancy but at a higher cost.
- **Determine the appropriate size and scale for your installation.** Tools can help identify a more efficient --- meaning less expensive -- VM instance for the workload you want to run. Reserved instances cost less than on-demand VMs, though they must be booked in advance. Preemptible instances are cheapest but risk interruption by the cloud service provider, so they aren't a fit for consistent workloads that require uptime. Autoscaling, typically part of a cloud vendor's overall framework, can increase or decrease resources as demand shifts.
- **Minimize data movement.** Cloud providers charge for data egress. If you move data frequently, choose the appropriate cloud services setup for that. Also, recognize that moving data can increase security risks.
- **Consider third-party tools.** Third-party cost-management tools may offer better capabilities for management, monitoring and security than a cloud platform's native services. They also tend to work in multi-cloud environments.
- **Look to advanced technologies for assistance.** Cloud management can be tricky, even if you do everything right. Some users and experts believe artificial intelligence and machine learning can efficiently and significantly reduce cloud costs. Vendors already offer tools that incorporate capabilities to scan cloud workloads, quickly detect anomalies and alert administrators about an issue that might affect the cloud bill.

## Cost management challenges

Detailed information about cloud costs may not be easily accessible. A customer might search across regions, accounts and numerous attached cloud services to calculate the total cost for just one individual service, such as backup snapshots.

The COVID-19 pandemic and related economic factors spurred enterprises to move more workloads to the cloud, which underscores the need for cost optimization practices.

AI tools and machine learning supplement the actions of humans but don't replace them. Software can identify additional information that staff may miss, but people must collaborate when analyzing cloud cost strategies and make judgment calls based on resources and experience. In-house staff should know how cloud usage affects the bottom line, both in IT and business lines.



Comparison of AWS pricing models: On-Demand, Reserved Instances, and Savings Plans.

## Governance and compliance

In recent years, cloud vendors have grappled with regulations that govern how they can use personal data. Specifically, the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) took effect. Cloud providers offered different responses to these regulations, but in general their services comply with regulations that involve data transparency.

A bigger challenge is how cloud providers help customers ensure compliance while they use these platforms. Amazon, Google, Microsoft and others offer resource portals to guide customers through the compliance process.

## **Cloud governance and compliance challenges**

IT pros have their hands full keeping up in the current regulatory environment. Around the world, data protection teams are overwhelmed by the sheer number of requests that increase their workload, particularly with regard to the GDPR. There is also a need to fight the false notion that just because one is compliant, one is secure -- adherence to standards does nothing to stop phishing attacks or other cloud breaches. Hone your organization's alignment with regulations and rules with a cloud governance framework.

## **Cloud automation**

Cloud automation, sometimes referred to as *orchestration*, reduces the repetitive, manual work involved to manage cloud workloads. The main idea is to boost operational efficiencies, accelerate application deployment and reduce any human error that can bring down applications. To achieve this, IT pros need orchestration or automation tools.



# Common cloud automation tasks

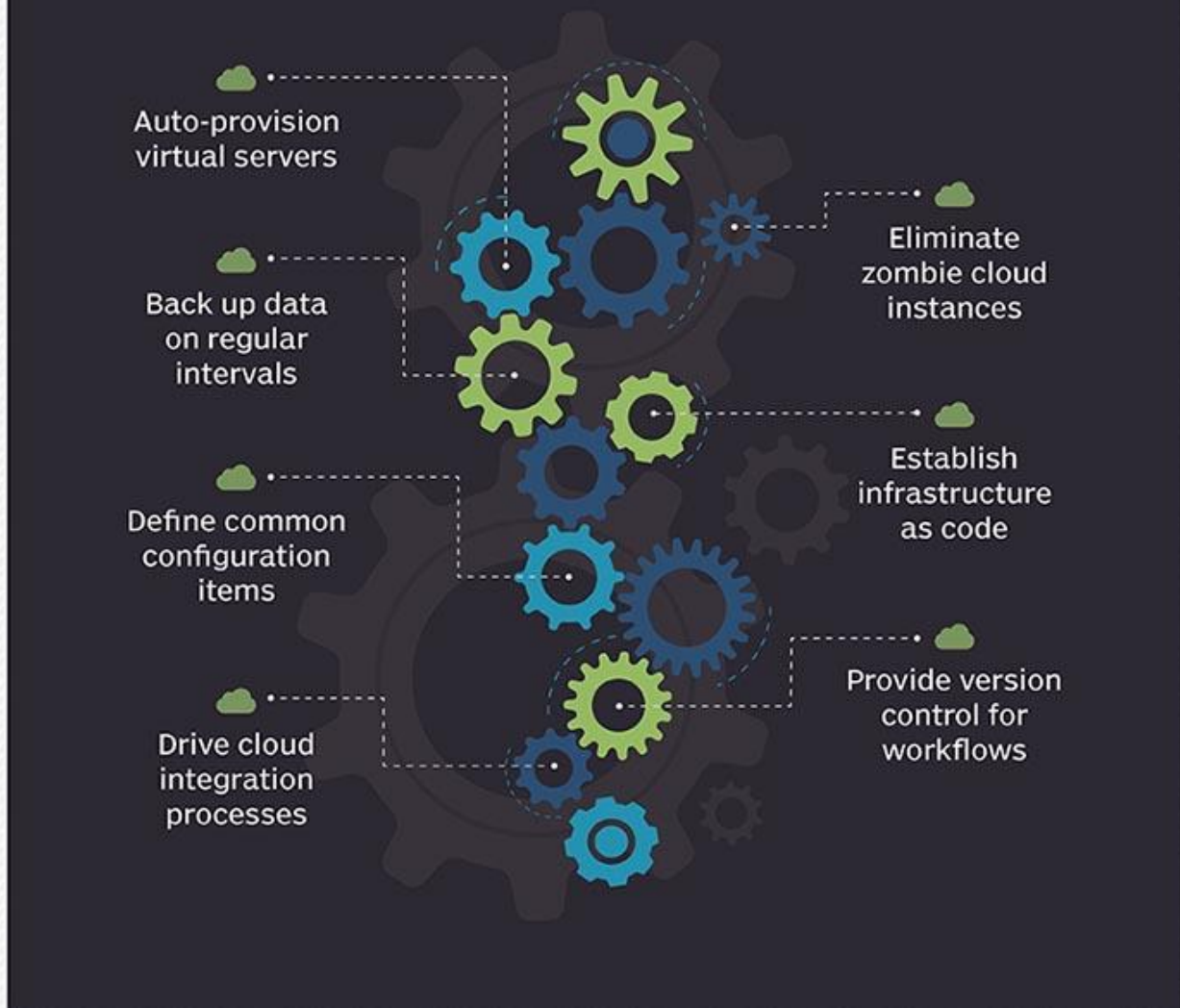


ILLUSTRATION: LIGHTCOM/GETTY IMAGES

© 2018 TECHTARGET, ALL RIGHTS RESERVED 

Common cloud automation tasks include automatically provisioning infrastructure, version control for workflows and performing backups.

Software targets different areas of cloud automation, from on-premises tools for private clouds to hosted services from the big cloud service providers, such as Microsoft Azure Automation and the automation feature in AWS Systems Manager.

## Cloud automation challenges

Automation typically saves time and money, but a big challenge for enterprises is that users may feel automation will put them out of a job. In most cases, automation supplements a job and frees up the cloud pro to do other work.

## Cloud provisioning

Cloud provisioning refers to how a customer procures and orchestrates the use of a cloud provider's resources and services, from compute and VM instances storage volumes to additional capabilities, such as data analytics and machine learning.

Proper resource allocation starts with right-sizing instances and VMs for appropriate scalability, which ideally occurs during the development phase. Optimized cloud capacity parameters not only ensure workloads run efficiently, but also can prevent a lot of wasted money. Identify what an application requires to run properly, and cut anything unnecessary. Cloud providers offer tools and templates to further optimize resource deployments.

There are three types of cloud provisioning models, with differences in the resources offered and how they are delivered and paid for:

- **Advanced provisioning.** The customer signs a formal contract of service with the cloud provider, which delivers agreed-upon resources and services. The customer is charged a flat fee or is billed on a monthly basis.
- **Dynamic provisioning.** Cloud resources are deployed to match a customer's fluctuating demands, typically scaled up to handle spikes in usage and scaled down when demands decrease. The customer is billed on a pay-per-use basis.
- **Self-service provisioning.** The customer buys resources from the cloud provider through a web interface or cloud brokerage portal. Resources are quickly made available for use, sometimes within hours or minutes.

A self-service brokerage will not completely eliminate administrative tasks, but it will shift some of the workload away from the IT service desk. IT Ops teams still must maintain the portal.

## Cloud provisioning challenges

The classic challenge here is to optimize the allocation of resources and services, balanced against various factors, such as performance, cost and security -- and the priorities for those may change. Many cloud services benefit from, or even depend upon, other services; users must understand these dependencies to not be caught off guard by unexpected usage and costs. Other challenges with provisioning involve the need to anticipate and avoid problems with security and policy enforcement.

## **Cloud monitoring**

Cloud monitoring measures the conditions of a workload and the various quantifiable parameters that relate to overall cloud operations. Results are monitored in specific, granular data, but that data often lacks context.

Cloud observability is a process similar to cloud monitoring in that it helps assess cloud health. Observability is less about metrics than what can be gleaned from a workload based on its externally visible properties. There are two aspects of cloud observability: methodology and operating state. Methodology focuses on specifics, such as metrics, tracing and log analysis. Operating state relies on tracking and addresses state identification and event relationships, the latter of which is a part of DevOps.

## **Cloud monitoring challenges**

One of the biggest challenges for IT teams is to keep up with modern and distributed application designs. As applications evolve, IT teams must adjust their monitoring strategies. Effective cloud monitoring is a complex task. The tools that an organization currently uses may no longer be the ones they need, as different types of applications will need to be monitored in different ways.

## **Performance management**

The goal of application management is to achieve peak application performance. While there is no single architecture that can guarantee peak performance for every application, there are ways to help boost cloud performance across the board:

- **Right-sizing instances.** As mentioned, start by selecting the right resources to run a workload.
- **Autoscaling.** Public cloud computing is dynamic by nature, and you want to be able to add and subtract instances on demand. These services provide ways to apply rules to track when a workload exceeds or recedes from a certain threshold, and trigger resources to readjust.
- **Caching.** Accessing storage can slow application responsiveness. With cached data, an application can execute tasks much faster than if it had to access data that resides in regular storage.
- **Microservices.** In a microservices architecture, an application's major features and functions are built in modular services. An application that is broken into a series of programs that are individually deployed, operated and scaled will be more responsive than one that's monolithic.
- **Event-driven architectures.** Also called *serverless computing*, event-driven architectures can run on cloud services, such as AWS Lambda, Azure Functions and Google Cloud Functions. Here, developers place code for certain software behaviors and functions into the cloud platform. It only operates when it's triggered by an actual event. When the function is complete, it no longer consumes cloud resources.

Another way IT shops can manage application performance in the cloud is through load balancing, which distributes network traffic so that each instance operates at peak efficiency. In prior days, load balancers operated locally as a data center appliance. Today, it is typically an application that lives on a server and is offered as a network service.

## Cloud management strategies

The success of any cloud management strategy depends not just on the proper use of tools and automation but also on having a competent IT staff in place. IT and business teams must collaborate naturally in order to assimilate to a cloud culture and understand the business's goals.

IT teams must also test cloud application performance, monitor cloud computing metrics, make critical infrastructure decisions, address patch and security vulnerabilities, and update the business rules that drive cloud management.

Organizations also must rethink their change management policies for the cloud, where consumption of resources can be more much more rapid and spread out versus an on-premises IT environment.

Companies that lack a skilled IT staff can seek help from third parties. Third-party apps support budget threshold alerts that can notify finance and line-of-business stakeholders so they can monitor their cloud spending. Cloud brokerages often have a service catalog and some financial management tools. The time to scrutinize cloud spending is early on when apps go into production.

Cloud management training should extend beyond IT and into other departments, from the supply chain to accounting staff. Staff can benefit from cloud training, such as certifications available through the CompTIA Cloud Essentials and AWS Cloud Practitioner programs. If traditional certification programs cost too much, consider online programs including LinkedIn Learning, A Cloud Guru, Linux Academy and others.

## **Cloud management platforms, tools and vendors**

As cloud computing expands across the enterprise, a general cloud management platform can help deploy, manage and monitor all cloud resources. Enterprise IT must form a clear idea on what it wants to monitor before evaluating cloud management platforms to fit those needs -- whether it's individual tools that solve a single problem, such as network performance or traffic analysis, or a comprehensive suite that looks at everything. Some of these decisions will weigh tools from cloud providers, such as security tools from cloud platform vendors or from third-party providers.

The most comprehensive cloud management products offer features that cover these five categories: automation and orchestration for applications and individual VMs; security, including identity management and data protection and encryption; policy governance and compliance, including audits and service-level agreements; performance monitoring; and cost management.

Many multi-cloud management vendors offer a range of tools, each with strengths and weaknesses. Some of the more prominent ones are VMware, CloudBolt Software, Snow Software (which acquired Embotics), Morpheus Data, Scalr and Flexera. Also in this mix are traditional IT service management vendors, such as BMC

Software, CA Technologies, Micro Focus and ServiceNow, which typically serve big companies with ITSM governance processes.

IT shops that use a single public cloud might want to stick with tools offered by that service provider because such tools are designed to enhance those native management platforms. For cloud monitoring, Google Cloud Operations (formerly Stackdriver) monitors Google Cloud as well as applications and VMs that run on AWS Elastic Compute Cloud. Microsoft Azure Monitor collects and analyzes data and resources from the Azure cloud. AWS users have Amazon CloudWatch. Other options include Oracle Cloud Infrastructure's Application Performance Monitoring service and Cisco CloudCenter, as well as tools such as Datadog for cloud analytics and monitoring, and New Relic to track web apps. There are also many open source cloud monitoring options for enterprises comfortable working with open source tools.

## **Private cloud management tools**

For private cloud management, enterprises typically use in-house tools. Applications that run in a private cloud don't get the advantage of unlimited elasticity gained from public cloud services built on an enormous scale of infrastructure. The IT team must be certain that it has adequate, available resources to run the app, and must carefully manage environments to ensure that no one app consumes too many corporate computing resources.

Some in-house tools can include platform-specific management software, such as Turbonomic Operations Manager (now owned by IBM) or Snow Commander. There are also private cloud management tools with sophisticated software frameworks that manage complex hybrid cloud deployments, such as Microsoft System Center Virtual Machine Manager for Hyper-V, VMware vCloud Suite and Citrix Cloud.