

IBM SmartCloud: Building a Cloud Enabled Data Center



Redguides
for Business Leaders

Pietro Iannucci
Manav Gupta



- Learn how to choose the infrastructure as a service (IaaS) solution that best matches your business needs
- See how to create an open and extensible IaaS solution
- Explore the details of the Cloud Enabled Data Center adoption pattern



Executive overview

Organizations are looking for ways to get more out of their already strained IT infrastructure as they face new technological and economic pressures. They are also trying to satisfy a broad set of users (internal and external to the enterprise) who demand improvements in their quality of service (QoS), regardless of increases in the number of users and applications. Cloud computing offers attractive opportunities to reduce costs, accelerate development, and increase the flexibility of the IT infrastructure, applications, and services.

Infrastructure as a service (IaaS) is the typical starting point for most organizations when moving to a cloud computing environment. IaaS can be used for the delivery of resources such as compute, storage, and network services through a self-service portal. With IaaS, IT services are delivered as a subscription service, eliminating up-front costs and driving down ongoing support costs.

IBM® has defined the Cloud Computing Reference Architecture (CCRA) based on years of experience of working with customers who have implemented cloud-computing solutions. The IBM CCRA is a blueprint or guide for architecting cloud-computing implementations. It is driven by functional and nonfunctional requirements that are collected from many cloud-computing implementations. IBM CCRA provides guidelines and technical work products, such as service and deployment models, and has defined the overarching implementations as *adoption patterns*. An adoption pattern embodies the architecture patterns that represent the ways organizations are implementing cloud-computing solutions. An adoption pattern can help guide the definition of your cloud-computing solution.

The adoption pattern for IaaS as defined by the CCRA is called the *Cloud Enabled Data Center adoption pattern*. The Cloud Enabled Data Center adoption pattern contains prescriptive guidance on how to architect, design, and implement an IaaS solution. It also defines the core requirements and provides guidance on adding new capabilities as they are needed.

The Cloud Enabled Data Center adoption pattern contains four architectural patterns. Each architectural pattern addresses a specific set of business needs for an IaaS solution. This modular architecture allows the extension of an IaaS solution by adding new capabilities and components as needed.

This IBM Redguide™ publication highlights the Cloud Enabled Data Center adoption pattern and describes how you can use it to define an IaaS solution. This guide is intended for chief technology officers, data center architects, IT architects, and application architects who want to understand the cloud-computing infrastructure necessary to support their applications and

services by using an IaaS solution. It explains the technical and business benefits of a Cloud Enabled Data Center solution. It introduces a Cloud Enabled Data Center maturity model where each maturity level corresponds to an increase in the degree of automation and the cloud-computing capabilities that are available. In addition, this guide describes the architectural framework provided by the IBM CCRA and explains details about the Cloud Enabled Data Center adoption pattern.

Business value of a Cloud Enabled Data Center solution

In the cloud-computing arena, the private cloud plays a fundamental role. It combines the major advantages of the public cloud, such as strong standardization, self-service automation, scalability, and metering, with the advantages of on-premise data centers. On-premise data centers provide advantages such as strong security, increased customization capabilities, and increased control over QoS.

In the private cloud context, providing IaaS is the natural starting point to implement a cloud-computing model. By using IaaS, you can deliver the most fundamental IT services, such as computing, storage, and network resources, in a more efficient and cost effective way. IaaS also enables the various lines of business (LOBs) to rapidly deliver new services or adapt existing services. A private IaaS provides an extensible model that you can use to extend the cloud resources to include resources from a public cloud (referred to as a *hybrid cloud model*). For these reasons, IaaS is gaining increased visibility with corporate executives and LOB leaders.

Even though cloud computing is presently a small percentage of the overall IT market, it is one of the fastest growing segments. The private cloud portion is one of the areas that enterprises are currently investing in. If you look at the cloud market from the type of cloud services, you can see that IaaS represents more than the 25 percent of the entire investment in the private cloud space. It is becoming evident that IaaS, in relation to the private cloud, is where most enterprises are planning to invest in the next three years. This effort will align their IT and business models to a cloud-oriented service model.

Business drivers for a Cloud Enabled Data Center model

The following key business drivers influence an organization to implement a Cloud Enabled Data Center:

- ▶ **Manage costs**

Cost is a key consideration in business decisions, and organizations are challenged to find new ways to do more with less. This situation is important for IT organizations that need to ensure that their IT investments are real business enablers and not cost drivers.

- ▶ **Respond to changing business needs**

Businesses are faced with increasing pressure to launch new products and services ahead of the competition and to quickly respond to change. IT infrastructure underpins the business and must be agile to respond to changing business events. For example, as new products or services are launched, the supporting IT infrastructure must be able to scale-out quickly to meet increased transaction volumes.

- ▶ **Increased dependence on technology**

Businesses today rely more on technology to deliver services of value to themselves and their clients. The adoption of technology is increasing at a faster pace than ever before, and in some cases, it is giving rise to new businesses. For example, with an expanding number of new sensors and devices available, there is a growing need for reliable ways to

collect and access information and efficiently process and analyze information. The capabilities to satisfy these needs might be delivered by new technologies and services.

- ▶ Faster time to deployment

Compressing the amount of time required in realizing a business idea into a service or product is often a key strategic business objective. In addition, as entry barriers lower in most industries, organizations need to deliver services faster than ever before to stay ahead of the competition. Accelerating time-to-market in a repeatable and reliable way is crucial for organizations to realize revenues faster, control market share, enhance brand image, and retain customers. IT plays an important role by improving availability dates of IT systems that support business needs.

Risks in implementing a Cloud Enabled Data Center model

As with any new mechanism to deliver services, risks are associated in adopting a cloud-computing delivery model, including the following risks:

- ▶ A Cloud Enabled Data Center requires alignment of IT processes toward a service-oriented architecture (SOA). IT and the LOBs need to identify and agree upon the services and their required service levels. A *service* is defined as a capability delivered to an internal or external user who is completing a task associated with the business or organization. The services are made available through the service catalog.

To coordinate these various activities, a new role might be identified. The person with this role interacts with the LOBs, understands their requirements, and translates those requirements into services to be delivered and supported by the IT organization. A misalignment between the cloud-computing services and the IT organization can risk implementing an ineffective cloud-computing model that does not deliver the expected value.

- ▶ A lack of adequate governance poses the risk of unauthorized or rogue access to services. Organizations must ensure that the items in the service catalog are available only to those people with the appropriate approvals and credentials.
- ▶ The creation of a service catalog requires IT to invest more effort into the design and automation of the services than in traditional or standard service delivery. This change might identify new development skill requirements that are not available in the IT organization. If the requirements are not identified, this change can reduce the effectiveness of the solution.
- ▶ The lure of automation might lead to over engineered solutions. Although such projects might be technically rewarding, the return to the business might not be advantageous. All new deployments must carefully consider the boundaries of automation.
- ▶ Resistance to change can be the biggest risk. To counteract this situation, adequate investment in training is required to ensure that the new delivery model is adopted across the organization.

Benefits of a Cloud Enabled Data Center model

A Cloud Enabled Data Center has the following main benefits:

- ▶ Allow organizations to shift focus quickly

With the quick availability of IT resources (such as servers and storage), the Cloud Enabled Data Center model allows organizations to focus on the core business and providing value to their clients.

- ▶ Lower cost of deployment

By using high levels of automation, IT resources are made available faster, repeatedly, and accurately. For example, IT does not have to incur the cost of configuring a server every time it needs one.
- ▶ Provide faster deployment and retirement of systems

With standardized services offered through the service catalog, IT can provision systems faster. In some cases (such as development and test workloads), users might be allowed to provision the servers and manage them through a web-based portal. The ability to automate the deprovisioning of the resources (after a period of use) is important. This approach ensures that resources that are no longer used are returned in the pool of available resources and can be reused for other purposes.
- ▶ Establish a utility service

A Cloud Enabled Data Center provides a *pay-as-you-use* model, which can be used to measure and charge individual LOBs for their IT usage.
- ▶ Create predictable deployment

A Cloud Enabled Data Center promotes standardization of components, which are made available through the service catalog and the description of the service itself. This approach ensures a predictable outcome every time a service is requested.
- ▶ Support dynamic scaling

A scale-up and scale-down infrastructure is required to support a business service. When a business experiences periods of high demand, a new IT infrastructure can be provisioned to meet temporary increases in workloads. The provisioned IT infrastructure can be deprovisioned when it is no longer required. This approach adds enormous flexibility to the IT environment and ensures optimal utilization of resources.
- ▶ Greater level of control and visibility

Every task performed by the Cloud Enabled Data Center solution is monitored and reported so that organizations have greater visibility to the use of IT resources.

Capability maturity model for a Cloud Enabled Data Center

If you look at the risks and investments that are needed to implement a Cloud Enabled Data Center solution, making a radical change is not the best approach. You should use a more pragmatic and step-by-step approach that allows you to progress in the adoption of a Cloud Enabled Data Center solution. Incremental stages of evolution have been identified and defined as maturity levels within the overall capability maturity model. With each maturity level, the Cloud Enabled Data Center becomes more robust. It evolves from initial inception and deployment to an optimized, enhanced, and monetized environment that delivers additional business value at each level.

The maturity model defines an evolutionary improvement path for organizations that are embarking on cloud computing from virtualization (initial level) to monetization (highest level). The model can also be used as a benchmark for comparison and as an aid to understand the Cloud Enabled Data Center solution. For example, the model can be used to compare the cloud-computing deployments of two different organizations.

Each level in the maturity curve is implemented with capabilities that are required by that specific maturity level. At each level of the maturity curve, functions are stacked on top of the ones from the previous level. The software and hardware components that implement these capabilities are also included. With this approach, you can create an incremental architecture,

where each level of the maturity curve has a corresponding “architectural pattern” that implements it. Each architectural pattern stacks on top of the architectural pattern for the previous level and creates the basis for the architectural pattern that implements the next level in the maturity curve.

“Designing a Cloud Enabled Data Center solution” on page 11 describes the architectural patterns of a Cloud Enabled Data Center solution and how they map to each level of the cloud maturity model.

The Cloud Enabled Data Center capability maturity model consists of five maturity levels as illustrated in Figure 1:

- ▶ Virtualized
- ▶ Deployed
- ▶ Optimized
- ▶ Enhanced
- ▶ Monetized

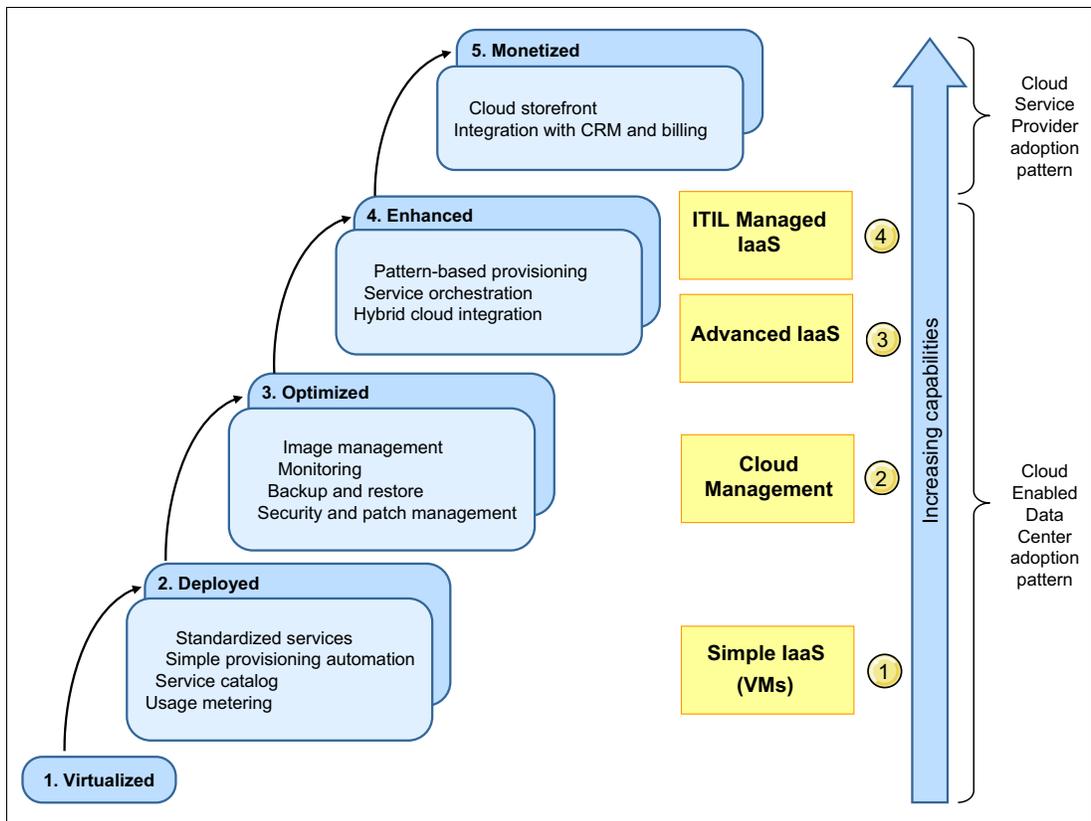


Figure 1 Capability maturity model maturity levels

Each maturity level has the following details:

- ▶ Virtualized (maturity level 1)

Many organizations are at this level today. At this level, virtualization in the data center exists for managing storage, network, or compute virtualization by using hypervisors. Virtualization offers an immediate benefit from optimization and an increase in hardware resources usage. Further benefits are gained by the simplification of some resources that are configured through the higher level of abstraction by the management software of the hypervisors. Virtualization alone does not solve all the problems because at this level, little automation is available to support virtualization. Success depends on the maturity of

individual infrastructure components and the motivation of the system administrator to fulfill a request.

At this level, the following types of situations can arise:

- The IT staff cannot meet commitments or requests from the organization in a timely and repeatable manner.
- There is a lack of standardized services that are easily accessed by the users. This situation causes long times (measured in weeks) to obtain new capacity (such as compute or storage) in order to support business needs.
- Most of the time is spent in ensuring that the firewall access rules are correct and port flows are configured on the new servers.
- There are wide variations in cost, schedule, and quality targets. Most of the work performed is manual, even though there might be some automation (typically by using scripts that are written by system administrators to support their activities).

► Deployed (maturity level 2)

At the deployed level, the virtualization technologies are augmented with an automation layer. Basic management processes are established to track cost, support schedules, and manage functions. IT can deliver new capacity to meet business needs without requiring a capital investment to acquire a new infrastructure each time.

Cloud Enabled Data Centers at this level exhibit the following capabilities:

- Standardization of services

Standardization of services reduces significantly the number of different platforms or middleware that is supported. It allows organizations to shift focus back to delivering value to clients rather than on the IT infrastructure. This approach simplifies management of infrastructure and reduces errors.

- Basic provisioning automation

After the services are standardized, delivery can be automated. IT can automate delivery of one or more virtual servers with attached storage by using a self-service portal. Additional manual configuration might be required to deploy application components or to integrate newly provisioned capacity with existing systems.

- Service catalog

Standardized services with automated delivery are now available by using a service catalog. Users might be allowed to take snapshots of provisioned images and add them to the catalog.

- Usage metering

All provisioned infrastructure is monitored, and usage is reported. Organizations use these reports to show the cost of IT to LOB organizations to request funding and capacity planning.

► Optimized (maturity level 3)

At maturity level 3, an organization deploys all the functions of maturity level 2 and incorporates additional capabilities to manage the infrastructure. This activity reduces the operational costs and improves the service-level agreements (SLAs) and QoS.

At this maturity level, a set of mature management processes performs the following activities:

- Monitors the infrastructure health
- Feeds the monitoring data into the capacity planning and forecasting processes to optimize utilization

- Ensures that any virtual machines (VMs) that created comply with the corporate and security standards for such items as security patches, firewalls, antivirus, and antispymware

Maturity level 3 defines and requires the following set of capabilities to deliver an optimized cloud infrastructure:

- Image management, which includes processes for discovering, capturing, installing, replicating, importing, and exporting virtual images
- Monitoring, which helps you optimize the IT infrastructure performance and availability
Monitoring software can be used to manage operating systems, databases, and servers in IT environments.
- Backup and restore, which enables the recovery of data and environments that have been lost or corrupted because of a hardware or software failure or an unexpected incident
- Patch management, which provides unified, real-time visibility, and enforcement to deploy and manage patches
- Security compliance, which addresses the complexities and costs of IT security risk management and compliance

It covers the capabilities that support the entire lifecycle in assessing, planning, implementing, monitoring, and maintaining compliance to the enterprise security policies.

- Optional: Historical reporting and trending, which is useful to see if any issues need attention, such as uncontrolled growth over time
- Optional: Capacity planning to measure known variables and to develop an educated estimate of resource requirements based on those measurements
It considers unknown variables and assessing their impact on the estimates that are derived from the known variables.
- Optional: Event management, which formalizes the event handling process.
It also ensures consistent responses to events, eliminates duplication of effort, and simplifies the configuration and maintenance of the tools used for event management.

► Enhanced (maturity level 4)

At maturity level 4, an organization has deployed all vital and important functionality and processes that are defined by maturity levels 2 and 3. At level 4, the IT organization invests most of its effort building new services that use the capabilities that are covered by maturity levels 2 and 3. With level 4, the focus shifts to high value services such as provisioning of application topologies, disaster recovery of cloud environment, and cloud-based backup services.

Maturity levels 3 and 4 have two functional differences. Level 4 provides organizations with the ability to orchestrate provisioning of services across data centers and provisioning to off-premise public clouds to dynamically scale out and handle peak loads.

The enhanced maturity level focuses on the following capabilities:

- Pattern-based provisioning prepares and supplies cloud-computing patterns within an IT environment and delivers them as a cloud service. Cloud-computing patterns are logical descriptions of the physical and virtual assets that comprise a cloud-computing solution. They can be used to model multitiered application environments (such as an SAP environment) and complex middleware environments (such as a cluster environment for developing Java Platform Enterprise Edition (Java EE) applications).

- Service orchestration is about stitching together hardware and software components to deliver and manage the lifecycle of any type of IT services using a cloud delivery model. Service orchestration uses automation to manage and maintain services efficiently. The activities range from creating virtual servers on demand to creating IT services on demand. Service orchestration can also enable the users who created services to manage them.
 - By using hybrid cloud integration, you can connect your hybrid world of public clouds, private clouds, and on-premise applications. With this capability, you can quickly integrate, manage, and secure these core assets to better support your current business needs.
 - Integration with the enterprise Information Technology Infrastructure Library (ITIL) processes allows better governance for the cloud infrastructure and for the cloud services that are created through it. Because of the complex and critical nature of the cloud services that are provided at this maturity level, each infrastructure change must go through a corresponding change management process. Also, any problem must be managed through an efficient incident management process.
- Monetized (maturity level 5)
- At maturity level 5, an organization has already deployed all the capabilities and processes that are defined by the other maturity levels. At this level, the IT organization has moved from being a cost center to generating revenue by offering a utility service to obtain compute and storage to other organizations or companies or to consumers or users. At this level, vigorous processes are in place for service inception, development, offering, billing, and retirement. This level also has a greater focus on the ease of use and customizability of user interfaces.

The monetized level 5 includes the following capabilities:

- Service storefront provides a richer user experience for customer management and reporting functions. It integrates typical e-commerce capabilities, such as shopping cart and credit card payments, to address consumer and enterprise marketplaces.
- Integration occurs with customer relationship management (CRM) and billing, so that you can provide customers the services that they request with the contracted SLAs or QoS at the agreed to price.
- Federated services are a standards-based means of sharing and managing the identity data of people to support single sign-on across secure domains and organizations. These services allow an organization to offer services externally to trusted business partners and to provide services to personnel in different internal departments and divisions.

In many cases, the monetized level 5 represents the natural evolution of a Cloud Enabled Data Center solution toward a Cloud Service Provider business model. For this reason, this maturity level is included but is not explored in this guide because the solutions at level 5 are outside the scope of Cloud Enabled Data Center. For a detailed description of the Cloud Service Provider adoption pattern and related business models, see *IBM SmartCloud: Becoming a Cloud Service Provider*, REDP-4912.

IBM Cloud Computing Reference Architecture

IBM CCRA provides a set of complementary architecture patterns to build cloud-computing solutions that are organized into four main adoption patterns. The adoption patterns categorize the cloud-computing business models and technical goal. They also represent the way most customers approach cloud-computing solutions. For each of these cloud adoption

patterns, the CCRA identifies common architecture patterns that describe the technologies that underlie each type of cloud-computing implementation.

The IBM CCRA also includes common architecture patterns for items that cut across all the adoption patterns, including security, resiliency, performance, and governance. These common patterns enable a consistent base to support a broad set of business and technical goals that are realized through different cloud deployments.

The following cloud adoption patterns are identified by the IBM CCRA:

- ▶ Cloud Enabled Data Center adoption pattern

The Cloud Enabled Data Center adoption pattern is typically the entry point into the cloud solutions space. It provides guidance on the definition, design, and deployment of cloud-computing solutions that deliver IaaS typically within the enterprise boundaries.

- ▶ Platform-as-a-service (PaaS) adoption pattern

The PaaS adoption pattern describes how to design cloud-computing solutions that deliver preconfigured ready-to-execute runtime environments or middleware stacks onto which applications can be deployed. It also describes how to tie together application development and application deployment processes into a single continuous delivery process based on application development and IT operations (DevOps) principles.

- ▶ Cloud Service Providers adoption pattern

The Cloud Service Provider adoption pattern defines cloud-based solutions that provide cloud services through a service provider model. A service provider is an organization that provides the cloud usually for external customers. A service provider manages and provides cloud services as a general provider, rather than operating a computing facility for its own organization.

- ▶ Software-as-a-service (SaaS) adoption pattern

The SaaS adoption pattern defines the architecture for definition and operation of SaaS applications. The Cloud Service Provider adoption pattern provides the architecture that enables SaaS applications to be managed and offered by the cloud service provider. The cloud service provider also supports systems that provide the environment in which SaaS business models are realized.

Figure 2 shows an overview of the IBM Cloud Computing Reference Architecture that includes the Cloud Enabled Data Center adoption pattern.

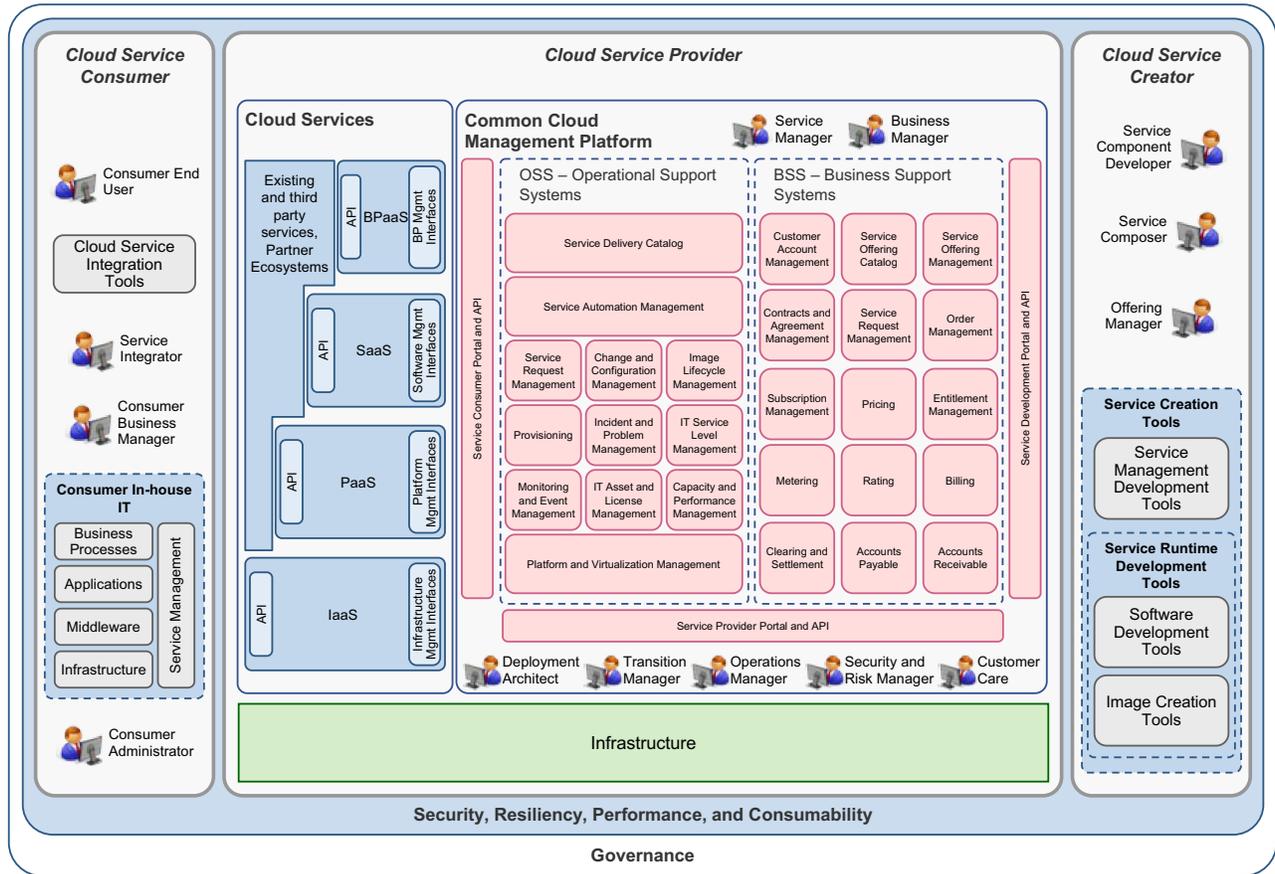


Figure 2 IBM CCRA architecture overview

Figure 2 shows the operationally oriented services and the business-oriented capabilities that are needed to implement a cloud-computing solution. For each of the four cloud adoption patterns, the IBM CCRA defines which services are mandatory and which are recommended or can be included depending on the specific customer needs.

For the Cloud Enabled Data Center adoption pattern, the IBM CCRA identifies the most common use cases for a private IaaS cloud solution. It also determines the mandatory, recommended, or optional services to implement that solution. In addition, it describes the physical components that make up these functions and how these components can be integrated together to realize the required scenarios.

The Cloud Enabled Data Center adoption pattern takes a pattern-based approach to provide modular building blocks that provide incremental functionality. This adoption pattern has been segmented into four architectural patterns, called *macropatterns*. Each macropattern addresses a specific subset of the IaaS use cases and describes the components that are needed to implement them. Each macropattern represents a different level in the cloud maturity model for Cloud Enabled Data Center solutions, with each macropattern at the next level incorporating the capabilities of previous macropatterns.

Designing a Cloud Enabled Data Center solution

The IBM CCRA Cloud Enabled Data Center adoption pattern provides a tested and proven approach to defining and implementing IaaS solutions. IaaS is usually the entry point for most organizations that are approaching cloud computing. Because IaaS is the starting point, IaaS must be supported by a modular and flexible architecture that easily allows the integration of more capabilities and more robust capabilities. The Cloud Enabled Data Center adoption pattern provides the necessary modular architecture to accomplish this goal by establishing the architectural framework for designing IaaS solutions.

The Cloud Enabled Data Center adoption pattern includes several key concepts. It also includes typical user roles, use cases, and requirements for a private IaaS.

Cloud Enabled Data Center key concepts

Several key concepts form the basis for the architectural approach used in CCRA. The following key terms and concepts are related to the Cloud Enabled Data Center adoption pattern:

- ▶ Use-case packages

A use-case package is a collection of related use cases that define interactions between an actor who performs a specific activity or task that uses specific Cloud Enabled Data Center functions or capabilities. For example, the set of use cases for interaction with virtualized storage or use cases support identity and access management.

- ▶ Micropattern

A micropattern is a collection of related use-case packages. For example, the micropattern for virtualization is a collection of use-case packages for server virtualization, storage virtualization, network virtualization, and hypervisor management.

- ▶ Macropattern

A macropattern is a collection of micropatterns that, when implemented together, the combined functionality is assessed as compliant with all aspects of a maturity level. For example, the capabilities of pattern-based provisioning, service orchestration, and hybrid cloud integration are implemented by the “Advanced IaaS” macropattern. Also, a macropattern defines the architectural view of the components that implement it. Another typical characteristic of a macropattern is that it typically stacks (in terms of capabilities and components) on top of the previous macropatterns and provides the base for building the next macropattern.

Cloud Enabled Data Center user roles

The Cloud Enabled Data Center establishes new user roles that interact with cloud services. A cloud service can enable the user role to create, offer, use, maintain, and run the cloud-computing services. A user role is delineated by a distinctive set of typical tasks that can be performed by a single person.

Cloud user roles support the design and development of services, and they support the servicing process for the cloud service. Each role can be accomplished by one or more persons. For example, an organization can have a logical construct or a single human being perform the user role. Conversely, a person can fill a role, part of a role, or multiple roles.

Figure 3 shows the user roles that are defined by CCRA that support a Cloud Enabled Data Center solution.

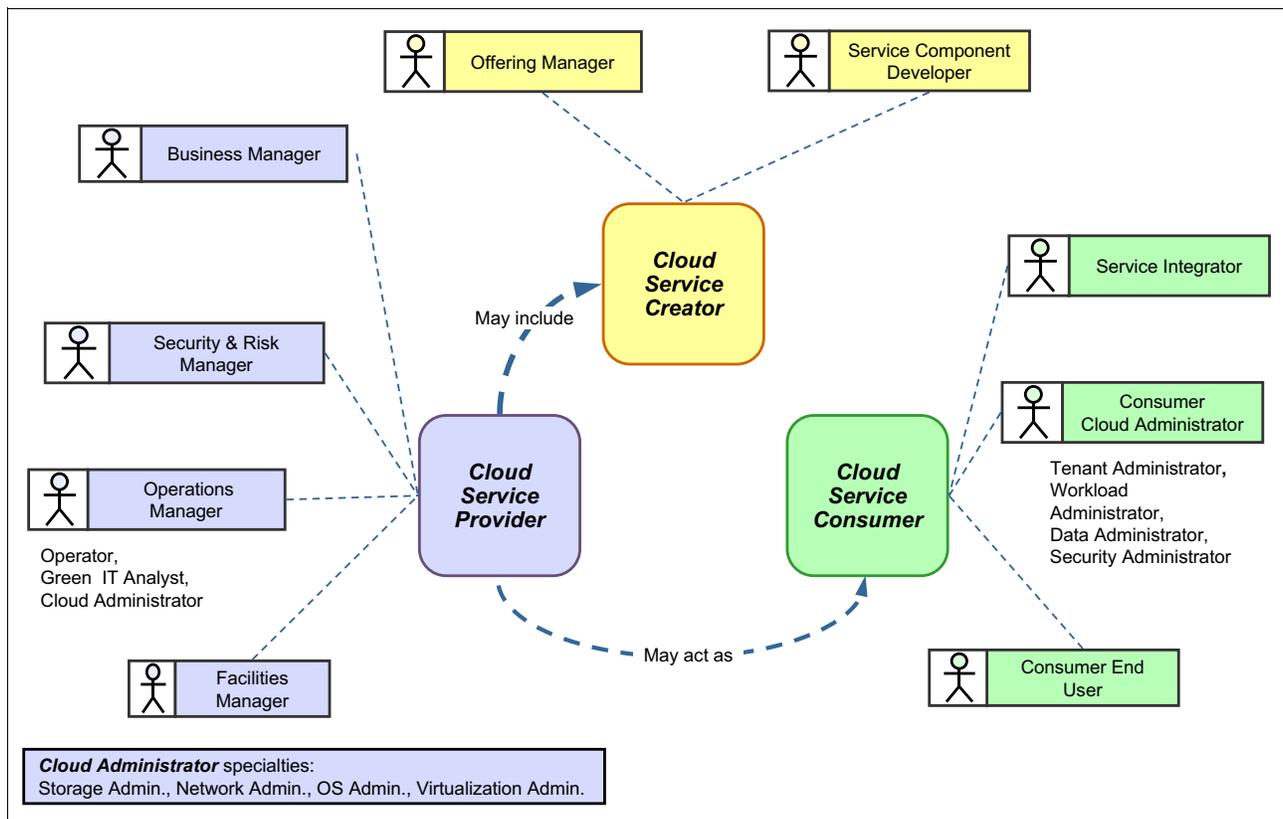


Figure 3 Cloud user roles

Use cases and micropatterns

The CCRA defines the major use cases for the Cloud Enabled Data Center adoption pattern. It also defines a set of micropatterns that encapsulate related use cases with functions that are expected by a user role. Figure 4 shows the micropatterns with their associated use-case groups.

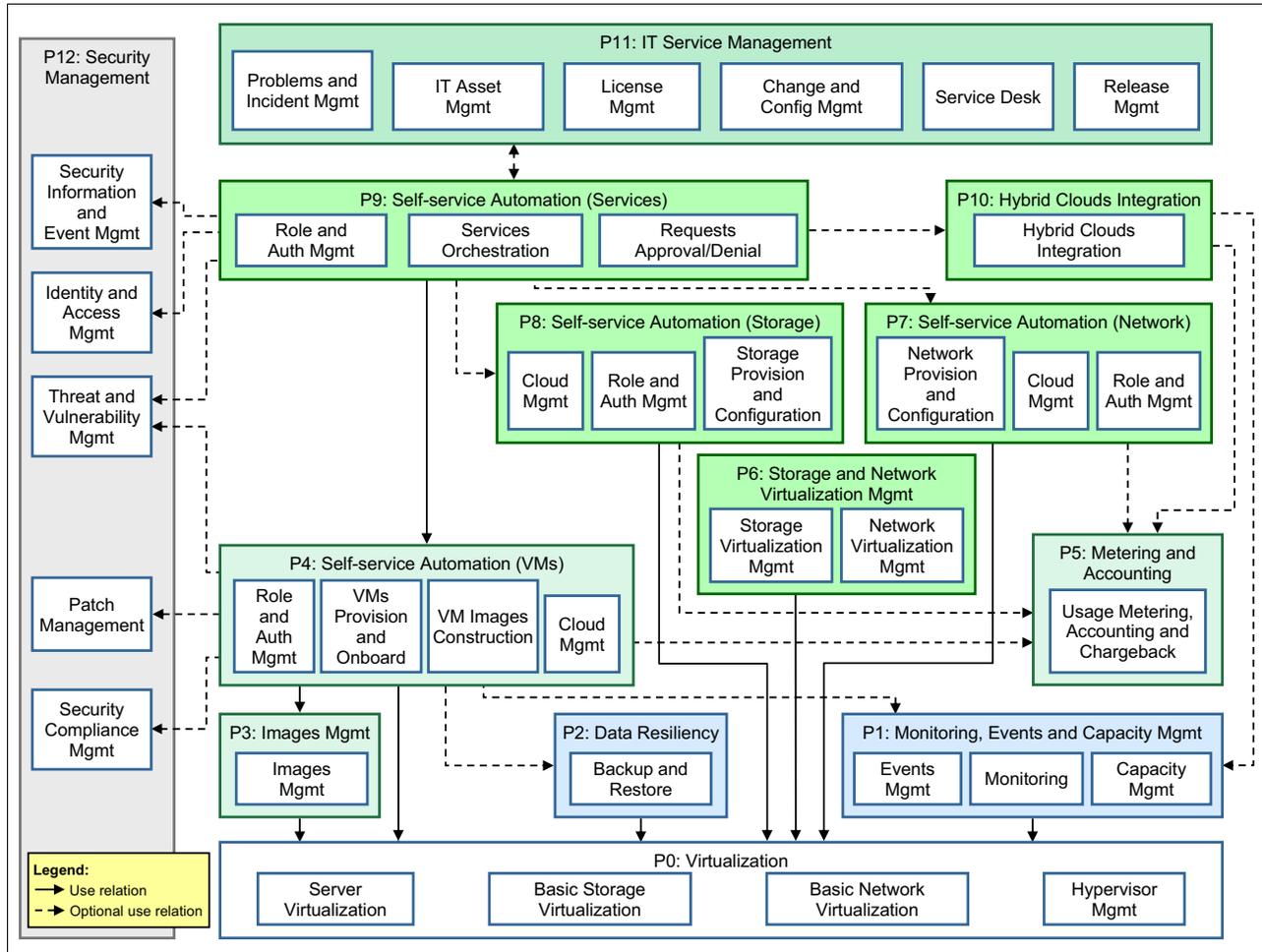


Figure 4 Cloud Enabled Data Center micropatterns and their associated use cases

The micropatterns (shown in Figure 4) provides a comprehensive view of the Cloud Enabled Data Center capabilities. The micropatterns are defined as follows from P0 to P12:

Virtualization (P0) Includes compute, storage, and network virtualization use cases, in addition to hypervisor-management use cases.

Monitoring and event and capacity management (P1) Pertains to monitoring the health of the cloud infrastructure, collection and management of exception events, and capacity planning.

Data resiliency (P2) Includes use cases for backup of storage volumes, virtual machines, and recovery from a backup if a failure or disruption occurs.

Image management (P3) Includes use cases for image registration and backup, image capturing, deep image search, drift analysis, version control, and management of image sprawl.

Self-service automation (P4)

Contains use cases for onboarding, provisioning, and management of virtual machines (VMs) that are made available from the service catalog.

Metering and accounting (P5)

Includes use cases for the measurement, reporting, and chargeback of the resources of a Cloud Enabled Data Center.

Storage and network virtualization management (P6)

Includes use cases about advanced management capabilities for virtualized storage and network environments, such as storage and network discovery, provisioning, and monitoring.

Self-service automation (storage) (P7)

Includes discovery, configuration, provisioning, commissioning, and decommissioning of storage use cases.

Self-service automation (network) (P8)

Includes use cases for discovery, configuration, and provisioning virtual networks and network devices. Such devices include virtual local area networks (VLANs), virtual routing and forwarding (VRF), load balancers, and firewalls.

Self-service automation (services) (P9)

Includes use cases for provisioning and configuration of complex services that consist of more than one VM, storage, and network element or use cases for production workloads.

Hybrid cloud integration (P10)

Includes use cases for deployment of workloads to public clouds, integration of service management, and governance across on-premise Cloud Enabled Data Center and public clouds.

IT service management (P11)

Includes use cases for implementing the ITIL processes. Example processes include incident and problem management, change and configuration management, IT asset management, license management, service desk, and release management in a private cloud environment.

Security (P12)

Includes use cases for securing different levels of the Cloud Enabled Data Center solution and infrastructure, such as identity and access management, and for securing the virtual infrastructure, security event management, and automation of security checks for complex services.

Nonfunctional requirements

In addition to the required use cases, Cloud Enabled Data Center solutions are heavily influenced by nonfunctional requirements. For example, the implementation of an IaaS solution that provisions many VMs quickly to support thousands of users would be different from an IaaS solution for a handful of users who require only a few VMs.

For this reason, nonfunctional requirements are key to determining the maturity level of an IaaS solution. They also heavily influence the design of the solution, for example, by determining where components are deployed and how they are integrated into the solution.

Table 1 summarizes key non-functional requirements for IaaS solutions.

Table 1 Key nonfunctional requirements

Category	Requirements (examples)	Explanation
Reliability, availability, and serviceability	High availability and resiliency of cloud management and managed infrastructure	Typically measured by key performance indicators (KPIs) such as the following examples: <ul style="list-style-type: none"> ▶ 99.99 percent availability of management environment ▶ 99.99 percent availability of workload
	Disaster recovery of cloud management and managed infrastructure	Measured by KPIs such as restoring service within 4 business hours
Performance	<ul style="list-style-type: none"> ▶ User interface response times ▶ VM provisioning time ▶ Service provisioning time 	Typically measured by KPIs such as the following examples: <ul style="list-style-type: none"> ▶ Complete image provisioning within 8 minutes of request ▶ Access gained to a file within 100 milliseconds, excluding full transfer time or rate ▶ Capability to provision 100 VMs concurrently
Scalability	<ul style="list-style-type: none"> ▶ Number of concurrent users ▶ Number of VMs/services provisioned per minute/hour ▶ Support multiple data centers 	Typically measured by KPIs such as the following examples: <ul style="list-style-type: none"> ▶ Number of concurrent users ▶ Number of VMs or services provisioned per minute or hour ▶ Number of customers per point of delivery; terabyte capacity
Consumability	<ul style="list-style-type: none"> ▶ User interface usability ▶ Time to value (TTV) ▶ Return on investment (ROI) ▶ Total cost of ownership (TCO) 	Consider the following examples: <ul style="list-style-type: none"> ▶ Ease of use for non-subject matter experts ▶ Starting simple and extend by integration of external systems and functional growth ▶ Low build and administrative costs
Extensibility	<ul style="list-style-type: none"> ▶ Plug new hypervisors support ▶ Extend a service with new actions ▶ Customize user interfaces ▶ Multitenancy 	Support for design and development of new services, extensibility model for existing service to adapt to customer needs
Security	Support of security standards and best-practices such as British Standard 7799, Information Technology Security policy ITCS 104, data privacy, Lightweight Directory Access Protocol (LDAP), Virtual Partition Manager (VPM), Multi-VLAN support, audit, vulnerability, and antivirus	Determination of industry relevant compliance standard and application of them to cloud management system

Some nonfunctional requirements are also influenced by the workloads that you want to deploy through your IaaS solution. Although development and test environments usually have limited (if any at all) requirements for monitoring and backup, the same is not true for production environments. For example, in a production environment, you might be asked to provide disaster recovery capabilities or advanced security protection features.

As you deploy workloads that are increasingly mission critical, the nonfunctional requirements of your solution increase. In the same way, these workloads and nonfunctional requirements increase the sophistication level of a Cloud Enabled Data Center solution.

Macropatterns

To further abstract and simplify the design of a Cloud Enabled Data Center solution, use case sets were aggregated together into micropatterns. To drive this abstraction to a higher level, multiple micropatterns are grouped into a macropattern. Macropatterns provide incremental increases in capabilities and functionality and describe, from an architectural perspective, the solution to implement.

Figure 5 shows the macropatterns that are identified for Cloud Enabled Data Center and illustrates how they are mapped over the micropatterns.

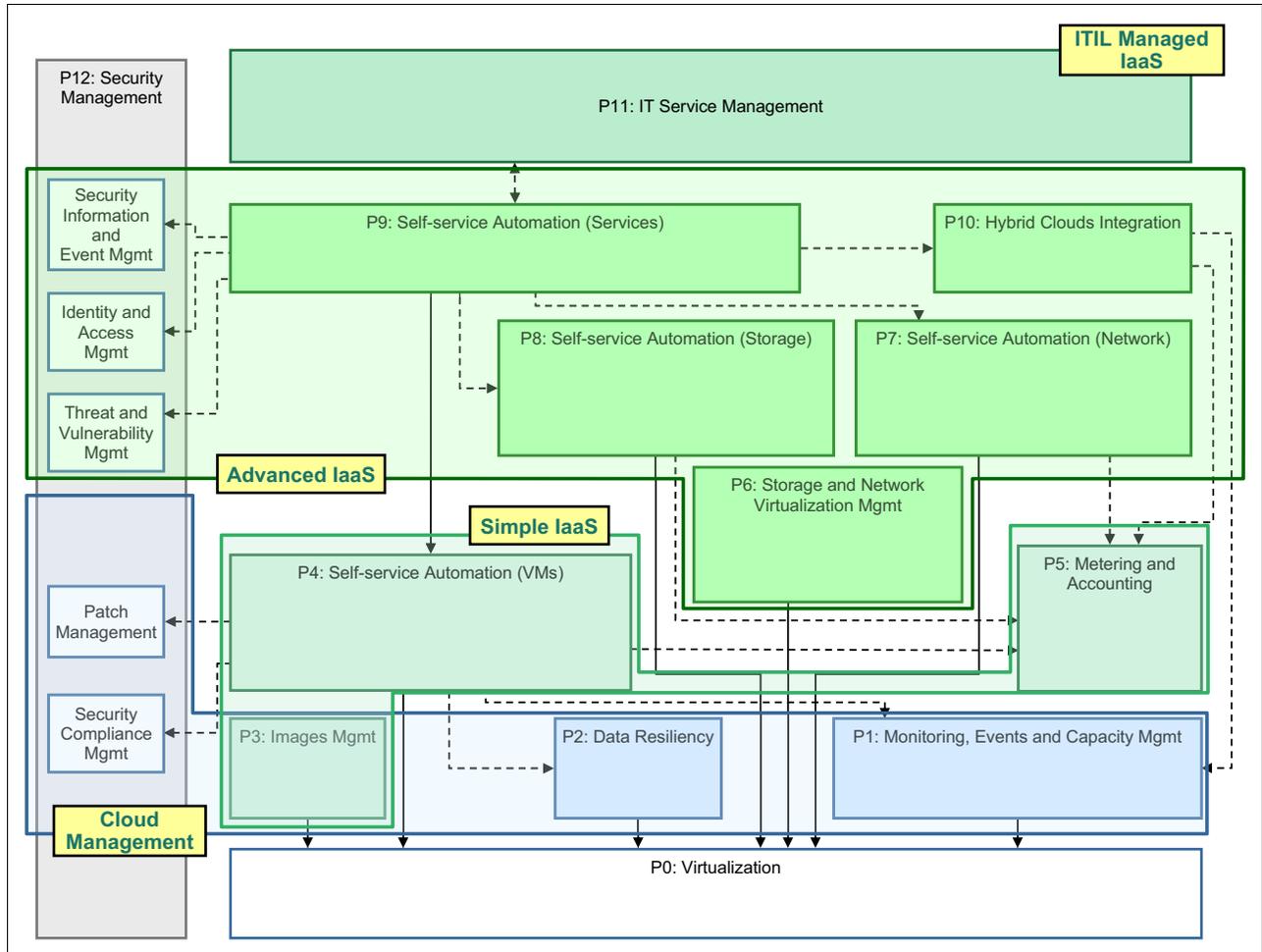


Figure 5 Macropatterns for micropatterns and use cases groups

Each macropattern represents a subset of the entire Cloud Enabled Data Center adoption pattern and addresses a business problem through a specific set of capabilities. However, macropatterns are just recommendations that you can use to consider or not to consider a specific capability based on your operational and business needs and costs considerations.

Figure 6 shows how the four macropatterns map to the different levels of the Cloud Enabled Data Center maturity model that is described in “Capability maturity model for a Cloud Enabled Data Center” on page 4.

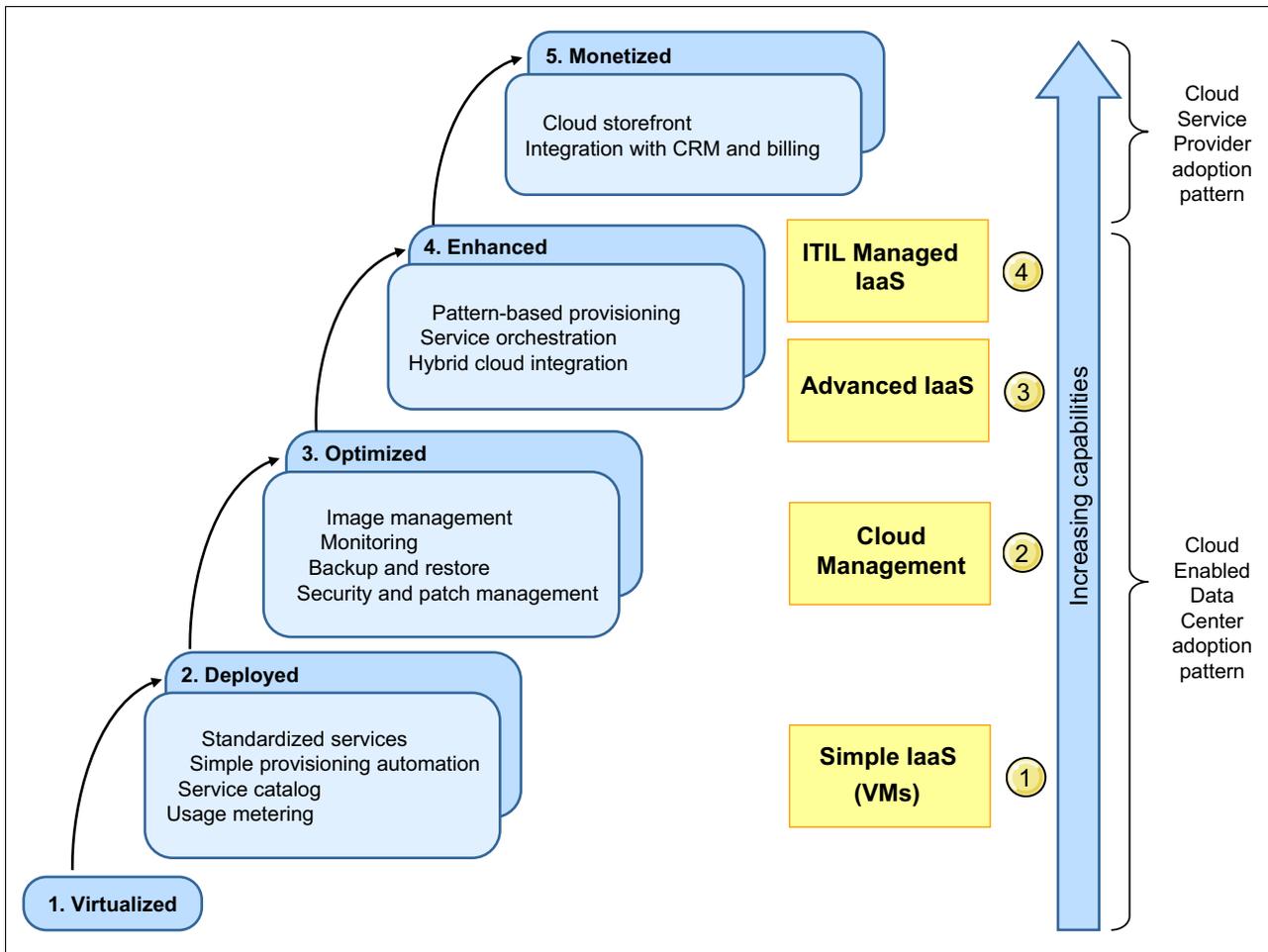


Figure 6 Macropatterns mapped to Cloud Enabled Data Center maturity model

By using these four Cloud Enabled Data Center macropatterns, you can implement solutions that address the business needs and the capabilities described in levels 1 - 4 of the maturity model. These four Cloud Enabled Data Center macropatterns are also prerequisites for building more sophisticated solutions that are oriented to the Cloud Service Provider business models as required by Monetized level 5 of the maturity model.

The following macropatterns that are defined for the Cloud Enabled Data Center adoption pattern build on top of each other, starting with the simplest micropattern:

► Simple IaaS (VM)

This micropattern is the entry point in the IaaS cloud space. You can use it to start building a multitenant cloud infrastructure and model that delivers simple VMs (configured with the appropriate network and storage) that cover the most common business needs for cloud computing.

► Cloud management

This macropattern complements the Simple IaaS macropattern by adding management capabilities that you can use to manage such requirements as SLAs, security, resiliency, and capacity planning. This macropattern helps you further optimize the IT processes,

manage complexity of virtualization and automation, and increase efficiency for both the infrastructure that provides the cloud and the cloud service itself. This macropattern addresses nonfunctional requirements in the area of reliability, availability, and basic security.

► **Advanced IaaS**

This macropattern is used to create a more sophisticated cloud infrastructure for delivery and management of complex and critical IaaS in highly demanding environments. It also can deploy services in more than one data center or to scale out to off-premise public clouds.

Dealing with the complex, production-like environments, this macropattern also addresses nonfunctional requirements in the area of performance, scalability, extensibility, and advanced security.

► **ITIL managed IaaS**

For this macropattern, the Advanced IaaS macropattern are integrated with ITIL process. This macropattern defines a cloud-computing environment that integrates with the existing enterprise applications, systems, and processes. This integration is accomplished by including the cloud infrastructure and services in the enterprise ITIL processes. This macropattern is typically the last step in the transformation of a Cloud Enabled Data Center. It is generally the prerequisite step for implementing more sophisticated Cloud Service Provider Solutions that move the maturity level of your cloud solution to the Monetized level 5 in the capability maturity curve.

Figure 7 shows a more schematic view of the four macropatterns and their key capabilities. It also shows how these macropatterns stack one on top of the other to build more sophisticated Cloud Enabled Data Center solutions.

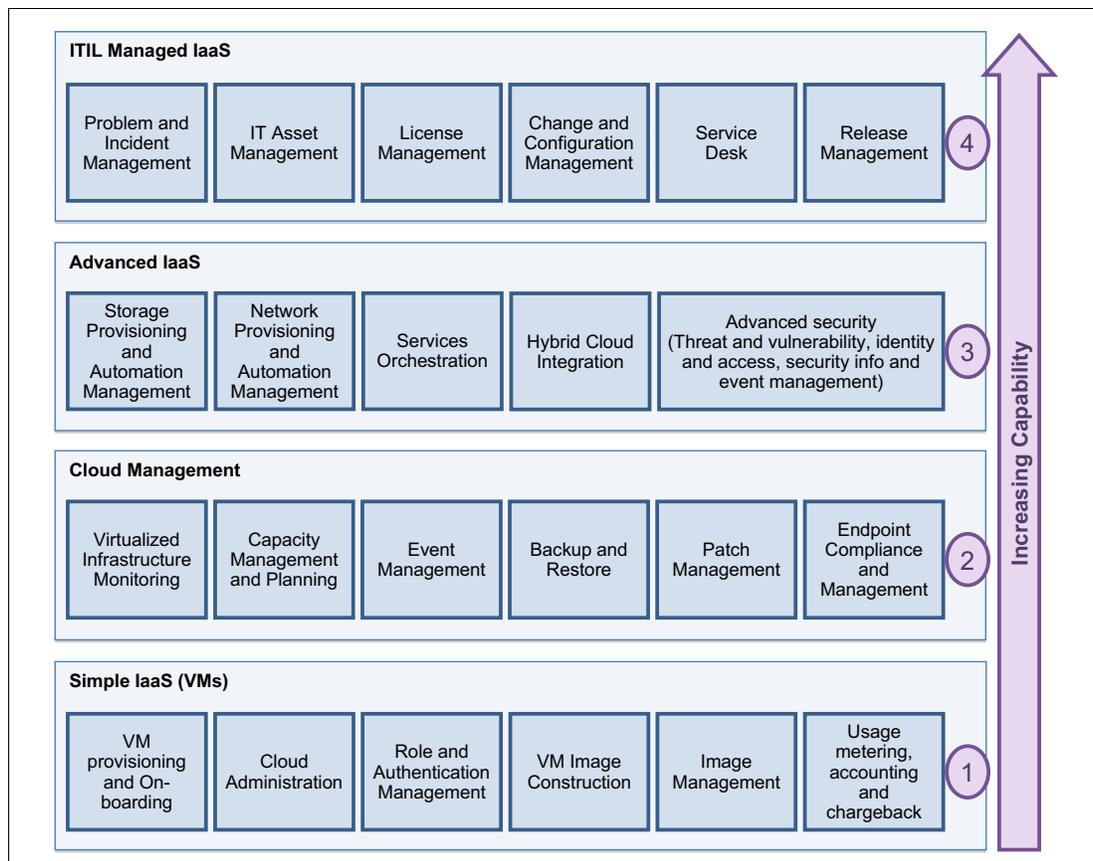


Figure 7 Cloud Enabled Data Center macropattern view

Simple IaaS

The Simple IaaS macropattern (also called the *VM provisioning macropattern*) focuses on automating the delivery of VMs using a cloud-computing model. It is the starting point to a Cloud Enabled Data Center solution.

This macropattern has the following two main aspects:

- ▶ VM provisioning, which focuses on the following capabilities:
 - VM self-service provisioning in a multitenant environment
 - The possibility to attach VMs to preconfigured networks and storage
 - Enablement of onboarding existing VMs under control of the cloud management infrastructure
- ▶ Metering and accounting (optional services)

Even if the customer is not a cloud service provider, metering and accounting can be used to measure the usage of cloud services and quantify potential savings.

The Simple IaaS macropattern (row 1 at bottom of Figure 7 on page 18) contains the following functional blocks of key capabilities:

- ▶ VM provisioning and onboarding

The existing virtualization capabilities are used to provide a simple interface to consumers of IT to provision VMs to satisfy the customers' needs. The underlying resources that are required by a VM (such as processor, memory, storage, and network resources) are preconfigured and made available as resources that are attached to a VM as requested. There might be a simple workflow to approve creation of VMs. VMs that exist in the data center might be discovered by this macropattern and onboarded under the control of the cloud management infrastructure. Alternatively, they can be migrated from one cloud environment to another.
- ▶ Cloud administration

Cloud administration provides capabilities to administer a cloud environment, such as adding new storage or computational resources in the cloud pool or defining new segregated networks.
- ▶ Role and authentication management

The Cloud Enabled Data Center ecosystem has many users, who each performs different roles. This capability can assign users to roles and can ensure that authorized access to cloud resources exists to perform a task, such as approving the creation of VMs.
- ▶ VM image construction

This capability provides tools to build virtual images for deployment into the Cloud Enabled Data Center.
- ▶ Image management

VMs tend to drift from the original copy (provided by the service catalog) as new security and operating system (OS) patches are installed. This capability provides tools to create new VMs, establish version control, search for and compare images, and delete images from your virtual images templates repositories.
- ▶ Usage metering, accounting, and chargeback

As workloads are abstracted from the physical infrastructure that supports them, it is not possible to build a chargeback model based on the allocation of physical resources. Instead, you must meter the resources that are used by each workload running on the shared infrastructure. This capability provides tools to track the usage for each characteristic of a workload (such as processor, memory, storage, and network), rating each characteristic and generating consumption-based chargeback reports.

Cloud Management

As the Cloud Enabled Data Center solution matures and you begin to deal with business and mission-critical workloads, you need to ensure that your underlying infrastructure performs well. Also, you might need to reduce (as much as possible) the unexpected failures or overloads that can cause you to miss your SLAs. Such workloads can require better orchestration and support to recover quickly if a disaster occurs. Capacity planning becomes more important, because the business expects IT to be more agile and accommodate new workloads quickly.

These additional requirements are fulfilled by the set of management tools that are provided by the Cloud Management macropattern. The Cloud Management macropattern has various optional services and components that provide the following services:

- ▶ Health management of the cloud management environment and cloud-managed services
- ▶ Capacity planning of cloud infrastructure
- ▶ Backup and restore of cloud services
- ▶ Event management
- ▶ Patch management and security compliance

The functional blocks in the Cloud Management macropattern deliver the following key capabilities (shown in row 2 of Figure 7 on page 18):

- ▶ Virtual infrastructure monitoring

A highly virtualized infrastructure requires a virtualization monitoring tool that provides end-to-end visibility. Although the virtualization helps to reduce costs, improve availability, and increase flexibility, it makes it difficult to determine the root cause of service performance degradation. This capability provides the tools to monitor virtual infrastructure use by the Cloud Enabled Data Center, ensures availability of business critical applications, and quickly identifies, isolates, and remedies performance issues.

- ▶ Capacity planning

One promise of cloud computing is that virtualization reduces the number of servers that are needed. Therefore, you must identify the balanced amount of cloud infrastructure that is required to meet the anticipated needs of users. This capability provides the tooling and governance to help capacity planners define the right business context and requirements. The analysis is necessary so the Cloud Enabled Data Center can continue to meet the performance goals of a business application while contributing to the organization's financial goals.

- ▶ Event management

As the super charged data center delivers services to support business-critical applications, you must identify exception situations quickly and determine the root cause of the problem. This capability provides the tools and best practices to collect events that come from the different elements of the infrastructure, correlate them, and eventually trigger notifications or remediation actions.

- ▶ Backup and restore

This capability provides tools and governance for backup processes to enable service to be restored within agreed service levels to ensure that the business is protected.

- ▶ Patch management

This capability provides tools and governance to ensure that the VMs that are provisioned are patched to the right security and version levels.

- ▶ Endpoint compliance and management

This capability provides tools to ensure that all the deployed VMs are compliant with the organization's security and enterprise policies.

Advanced IaaS

The complexity of the virtualized infrastructure increases as the Cloud Enabled Data Center solution is used to deliver business-critical applications. These applications have typically strict security requirements. Therefore, they need to be configured with security elements such as firewalls. They usually support high volumes of data or users. As a result, they are required to attach high-quality storage to the VMs or to configure load balancers to optimize their utilization. There is increased pressure to eliminate application downtime from planned server maintenance. High availability might be required across entire virtualized infrastructure to withstand physical server failures. The compute clusters might require spare nodes to withstand single node failures.

The main functional blocks that implement this macropattern (shown in row 3 of Figure 7 on page 18) deliver the following key capabilities:

- ▶ Storage provisioning and automation management

This capability provides functions for discovery of storage resources, dynamic provisioning, allocation of storage resources, monitoring, provisioning, and configuration capabilities across different heterogeneous devices. With this capability, you can automatically provision different types of storage resources (defined as cloud-computing services), making them available to the computing resources. Also, these (provisioned) storage resources can be used to generate a new revenue stream by offering a new service such as storage-as-a-service.

- ▶ Network provisioning and automation management

This capability provides functions for management and discovery of network resources, dynamic provisioning and allocation, and monitoring across heterogeneous devices. With this capability, you can automatically configure a load balancer or allocate a new network that can be deployed as part of a cloud service and used by the VMs. Also, these network resources can be used to generate a new revenue stream by offering them as a network as a service.

- ▶ Cloud services orchestration

One of the most powerful capabilities provided by this macropattern is the automated arrangement, coordination, and management of complex computer systems, middleware, and services. You can use this capability to deliver a complex business application that consists of two or more VMs with attached storage and interconnectivity. Another example is to provision across data centers by using a single self-service interface. The self-service interface includes the following capabilities:

- Self-service provisioning of infrastructure elements such as VMs, storage, or network elements with multitenancy
- Self-service provisioning of complex integrated infrastructure services

- ▶ Hybrid cloud integration

Hybrid cloud integration provides the capability to provision to external cloud-computing environments (such as public clouds) to meet peak workloads. This optional capability makes it possible to provision VMs into a public cloud and to securely connect and manage from a private infrastructure. It can also implement cloud bursting scenarios in case of workload peaks or for cost reasons.

- ▶ Advanced security

The advanced security capabilities support more complex environments, which require more sophisticated security to protect against threats and vulnerability. This support is accomplished by providing identity and access controls, security information, event management, and log information management.

ITIL managed IaaS

Because the Cloud Enabled Data Center solution delivers complex cloud services, its management processes must be integrated with the organization's IT management processes such as change management and incident management.

This capability is typically required when delivering complex and composite services in environments similar to production environments. This macropattern allows for registration of cloud services in a Configuration Management Database (CMDB) and for the services to be placed under control of the major enterprise ITIL processes. The ITIL managed IaaS (shown in row 4 of Figure 7 on page 18) includes the following capabilities:

- ▶ Problem and incident management
- ▶ IT assets management
- ▶ Licenses management
- ▶ Change and configuration management
- ▶ Service desk
- ▶ Release management

This capability is also a prerequisite to moving your Cloud Enabled Data Center solution to a Cloud Service Provider business model. In the Cloud Service Provider business model, governance and control capabilities are important to ensure the QoS and SLAs that are typical of the Cloud Service Provider business.

Cloud Enabled Data Center architecture overview

Figure 8 shows the high-level architecture for the Cloud Enabled Data Center and its services. The services are segmented into the four macropatterns so that you can incrementally create your Cloud Enabled Data Center solution.

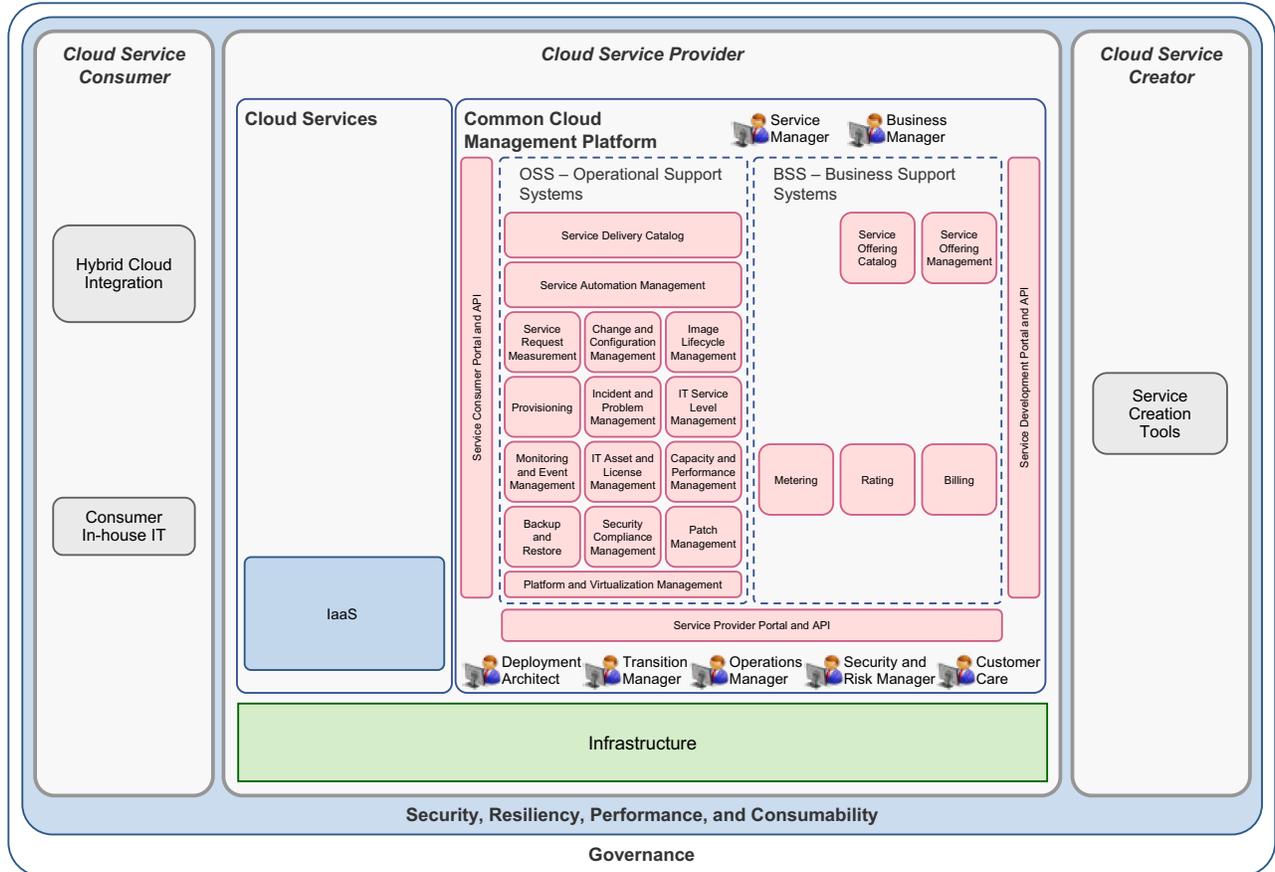


Figure 8 Cloud Enabled Data Center high-level architecture

Figure 9 introduces the components that are needed to implement the services. It also provides the architectural overview of the Cloud Enabled Data Center, using the IBM CCRA patterns-based approach.

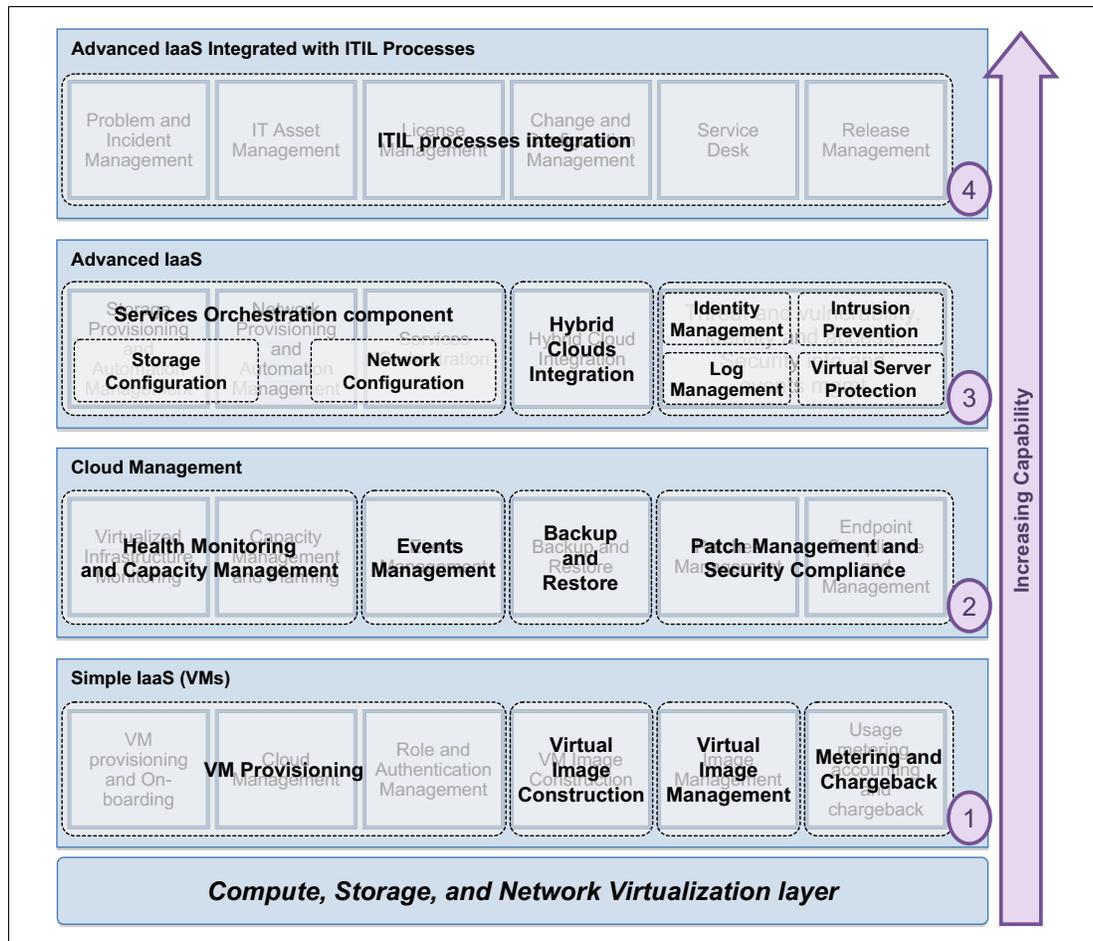


Figure 9 Cloud Enabled Data Center architecture overview diagram

Starting from the bottom of Figure 9, the Cloud Enabled Data Center architecture has the following the layers:

- ▶ The compute, storage, and network virtualization layer provides the base. Most organizations today have adopted virtualization technologies, such as compute and storage hypervisors. In many cases, it common to have a mix of hardware and virtualization technologies from different vendors to avoid vendor lock-in.
- ▶ The Simple IaaS (layer 1) encompasses the self-service provisioning and configuration of VMs from a self-service catalog and the possibility to meter the resources usage for simple reporting or for accounting and chargeback purposes.
- ▶ The Cloud Management (layer 2) provides monitoring, event management, backup and restore, and security and patch management capabilities.
- ▶ The Advanced IaaS (layer 3) support the delivery of value-add services (such as network-as-a-service and storage-as-a-service), provisioning of complex services, advanced security and integration with public clouds.
- ▶ The ITIL Managed Services (layer 4) provides governance and discipline to integrate the service management functions of a Cloud Enabled Data Center with the organization’s enterprise service management systems.

The architecture overview (Figure 9 on page 24) provides mapping between the macropattern and the logical components that implement each pattern. A Cloud Enabled Data Center solution has the following major components:

- ▶ Virtualization capabilities are provided through hypervisors. Hypervisors are a prerequisite function for the IBM cloud management solutions.
- ▶ Services provisioning encompasses the automatic provisioning and configuration of VMs, properly configured with their storage and network requirements from a self-service catalog. This subsystem also includes components that allow creating standard virtual image templates and managing their lifecycle.
- ▶ Metering and chargeback measures services usage to help you understand who is using the services and how they are using the services. The service usage is the basis for eventually billing the user.
- ▶ By using monitoring, you can effectively manage the health status of a cloud infrastructure by providing the services that are necessary to deliver the expected QoS and SLAs.
- ▶ Capacity management is used to project future cloud infrastructure needs to support planning for capacity growth, changes, or both.
- ▶ Event management intercepts events that are related to the cloud infrastructure and correlates them to start remediation actions or to determine the status of the provided business services.
- ▶ The backup and restore services are provided for the cloud management infrastructure and for the VMs and storage that are created by the IaaS solution. This feature allows improving the reliability, availability and serviceability (RAS) aspects of an IaaS solution.
- ▶ Patch management and security compliance helps to maintain and secure all the VMs that are created in your cloud environment. It ensures that the VMs are aligned to the latest upgrade and fix levels and are compliant with the required enterprise security policies.
- ▶ Cloud services orchestration enables the creation and automation of the delivery of more sophisticated services, which require the orchestration of VMs, storage, and network infrastructure services. Eventually various human tasks (for example, an approval process or a manual configuration activity) can be handled by using orchestration and orchestration into workflows that automate activities and human tasks.
- ▶ The “Storage Provisioning and Configuration” and the “Network Provisioning and Configuration” components provide a set of high-level services and an abstraction layer to the network and storage infrastructure. By using these components, you can easily provision and configure storage and network elements by shielding you from the different storage and network technologies.
- ▶ Hybrid connectivity allocates infrastructure elements (specifically VMs and storage) into a public cloud and connects them to the private cloud environment.
- ▶ Security consists of various security capabilities (such as patch management, security compliance, and threat and vulnerability management) that are required at the different maturity levels of a cloud implementation.
- ▶ IT Service Management integrates the cloud services with ITIL processes such as change and configuration management, service desk, and licenses management. The capabilities are usually implemented in large enterprise environments to maintain the desired governance level.

Implementing a Cloud Enabled Data Center solution

The capabilities provided by each macropattern are mapped to the appropriate IBM Software components used to implement them. Figure 10 highlights the required software components (in blue), the recommended components (in green), and the optional components for each macropattern (in gray). Optional components can be added, if needed, to solve a specific customer need.

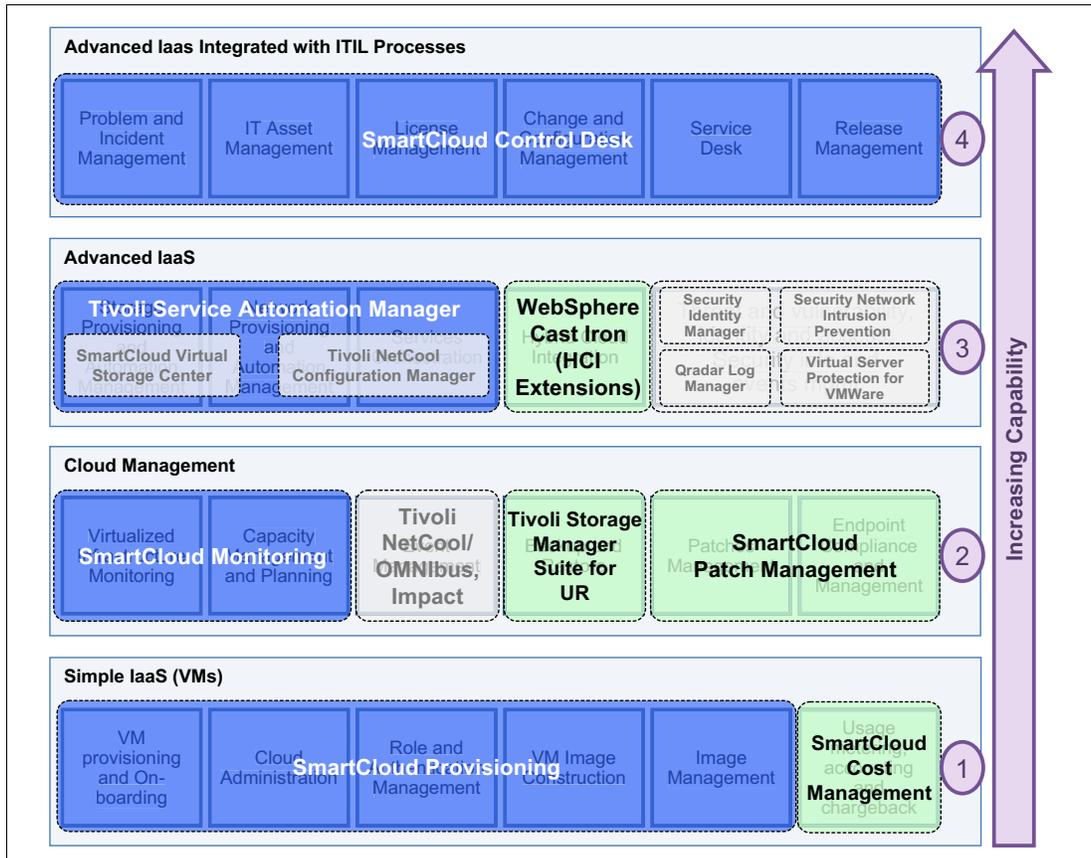


Figure 10 Cloud Enabled Data Center software stack

Simple IaaS (VMs)

The following IBM software components can be used to implement the Simple IaaS macropattern (Figure 10):

- Required: IBM SmartCloud™ Provisioning

IBM SmartCloud Provisioning is the cornerstone of the Cloud Enabled Data Center solutions. It combines infrastructure and platform capabilities to deliver elastic workload management, image lifecycle management, and resilient, high scale provisioning on heterogeneous hypervisor and hardware platforms. With this solution, you gain workload optimized virtualization and cloud infrastructure management. IBM SmartCloud Provisioning provides the following features:

- Rapid application deployment with a repeatable composite application throughout private and public clouds
- Rich image and analytics to manage virtual environments for great efficiency and control over VM sprawl

- Choice of hardware and hypervisor (such as kernel-based VM (KVM), IBM PowerVM®, Microsoft Hyper-V, and Xen Hypervisor) so that you can reduce the cost of licenses, hardware, and labor
 - High scalability to meet business growth with nearly instant deployment of hundreds of VMs.
 - Low touch infrastructure that reduces manual errors, enhances security and compliance, and increases administrator productivity
 - The possibility to create more sophisticated cloud solutions that include two or more VMs configured to work together to implement a specific application or middleware pattern delivered as a cloud service
- **Recommended: IBM SmartCloud Cost Management**
- SmartCloud Cost Management helps deliver cost transparency to track, manage, and allocate IT resource usage accurately by providing visibility into the usage and cost of your infrastructure and other resources that are not IT-related. IBM SmartCloud Cost Management provides the following key capabilities:
- Can meter the usage of cloud resources such as processor, random-access memory (RAM), storage, and network bandwidth
The usage can be tracked per user and for groups of users.
 - Provides users visibility into the cost implications of the services that they are requesting; supports IT departments to bring down the cost while delivering IT services more efficiently
 - Provides a reliable mechanism for cloud service providers to support cloud showback and chargeback processes with an accurate metering and cost rating tool for tracking business offering processes against budgets

Cloud management

The following IBM software products are used to implement the Cloud Management macropattern (Figure 10 on page 26):

- **Required: IBM SmartCloud Monitoring**
- IBM SmartCloud Monitoring monitors the health and performance of a private cloud infrastructure, including environments that contain physical and virtualized components. This software provides the tools that are needed to assess current health and capacity and model expansion, as needed. IBM SmartCloud Monitoring provides the following capabilities:
- Visibility into the cloud infrastructure, including environments that contain physical and virtualized components
 - Monitoring of heterogeneous environments for visibility and control into all areas of the infrastructure, such as physical, virtual, and cloud
 - Policy-driven analytics for intelligent workload placement
 - What-if capacity planning to accommodate capacity growth while optimizing the usage of the existing environment
- **Recommended: IBM Tivoli® Storage Manager Suite for Unified Recovery**
- IBM Tivoli Storage Manager Suite for Unified Recovery is a bundle of Tivoli Storage Manager products and provides backup and restore capabilities for the entire cloud environment. It can efficiently back up VMs and storage infrastructures and restores them if a failure occurs.

► **Recommended: IBM SmartCloud Patch Management**

IBM SmartCloud Patch Management manages patches automatically for multiple operating systems and applications across physical and virtual servers regardless of location, connection type, or status. IBM SmartCloud Patch Management provides the following benefits:

- Reduces security risks by reducing remediation cycles, especially in development and test environments, where virtual machines that are not patched increase the risk of hacking and virus exposure
- Improves performance with reliable, nonstop cloud computing that can automatically tolerate and recover from software and hardware failures
- Saves IT costs by automating provisioning operations and providing a service interface
- Reduces complexity through ease of implementation, use, and simplified cloud administration

► **Optional: IBM Tivoli Netcool/OMNIBus**

IBM Tivoli Netcool/OMNIBus is operations management software that consolidates complex IT and network operation management tasks. It provides event collection, correlation, and automation capabilities. This component is critical for Cloud Enabled Data Centers to deliver business-critical services and where it is important to identify and resolve the most critical problems quickly.

Advanced IaaS

The following software implements the Advanced IaaS macropattern (Figure 10 on page 26):

► **Required: IBM Tivoli Service Automation Manager (IBM Service Delivery Manager)**

This product is the cornerstone to implement sophisticated Cloud Enabled Data Center solutions. By using IBM Tivoli Service Automation Manager, users can request, deploy, monitor, and manage cloud-computing services with these capabilities:

- Provides traceable approvals and processes
- Provides management of storage and network resources
- Provides a workflow engine to model and deliver complex services that combine two or more virtual machines with attached storage and the desired network interconnectivity

This product can be combined with SmartCloud Provisioning to use its functions in the area of virtual images library management and application or middleware patterns to provide more sophisticated solutions.

► **Required: IBM Service Delivery Manager (or Tivoli Service Automation Manager)**

By implementing IBM Service Delivery Manager, the data center can accelerate the creation of service platforms for various workload types. It provides a high degree of integration, flexibility, and resource optimization with the following core service management capabilities:

- A self-service portal interface for previously placed computing reservations of virtualized environments, including storage and networking resources
- Automated provisioning and deprovisioning of resources
- Real-time monitoring of physical and virtual cloud resources
- Integrated usage and accounting chargeback capabilities that can help system administrators track and optimize system usage
- Built-in high availability of the cloud management platform
- Prepackaged automation templates and workflows for the most common resource types

IBM Service Delivery Manager is a bundled solution that includes Tivoli Service Automation Manager, SmartCloud Monitoring, and SmartCloud Cost Management delivered as preintegrated virtual images.

► Recommended: IBM WebSphere® Cast Iron® Cloud Integration

By using WebSphere Cast Iron Cloud Integration, you can rapidly connect a hybrid of public clouds, private clouds, and on-premise applications. WebSphere Cast Iron Cloud Integration is required to implement scenarios where peak demand on IT infrastructure can be served by provisioning additional infrastructure in a public cloud infrastructure (such as IBM SmartCloud Enterprise or Amazon EC2). You can provision VMs into a public cloud and securely connect them to the on-premise environment. You can integrate WebSphere Cast Iron Cloud Integration with IBM SmartCloud Monitoring to monitor the VMs that are provisioned in the public cloud environment. You can also manage them from the same SmartCloud Monitoring dashboard that is used to monitor the private cloud infrastructure.

► Optional: IBM SmartCloud Virtual Storage Center

SmartCloud Virtual Storage Center provides storage virtualization management including discovery, monitoring, provisioning, and configuration of virtualized storage capabilities. In the cloud context, this component provides an abstraction layer to perform storage provisioning and configuration actions on several heterogeneous storage infrastructures. These high-level services can be used directly by the storage administrator to simplify the storage management tasks. Alternatively, they can be used by a cloud service that is defined in TSAM to automate storage provisioning and configuration tasks. This component is recommended when you need to deliver Storage-as-a-Service capabilities or when you need to include particular storage configuration tasks in your cloud services across heterogeneous storage infrastructures.

► Optional: IBM Tivoli Netcool® Configuration Manager

Tivoli Netcool Configuration Manager provides provisioning and configuration capabilities for virtualized networks. In the cloud context, this component provides an abstraction layer to perform network provisioning and configuration tasks on a number of heterogeneous network devices and infrastructures. These high-level services can be directly used from the network administrator to simplify the network management tasks. The services can also be used from a cloud service defined in Tivoli Service Automation Manager to automate the configuration of network devices as part of the delivery of a cloud service. This component is recommended when you need to include particular network configuration tasks in your cloud services across heterogeneous network devices and infrastructures.

► Optional: IBM Security Identity Manager

Security Identity Manager is a solution that delivers security rich, policy-based user and role management across the IT infrastructure. This solution is used to map the Cloud Enabled Data Center roles to the appropriate users in the organization and to automate the creation, modification, recertification, and termination of user privileges throughout the user lifecycle.

► Optional: IBM Qradar Log Manager

IBM QRadar Log Manager is a comprehensive solution for organizations that are looking to implement a distributed event log manager to collect, archive, and analyze network and security event logs. Qradar Log Manager is used to perform an integrated analysis of network and security information of the cloud infrastructure and provide awareness of network security threats that need to be resolved quickly.

► Optional: IBM Security Network Intrusion Prevention

IBM Security Network Intrusion Prevention solutions provide comprehensive protection and reduce the cost and complexity that are associated with deploying and managing

point solutions. Security Network Intrusion Prevention is used to discover threats to the Cloud Enabled Data Center infrastructure. It is also used to take preventive measures against threats to these high value assets and to protect the workloads from threats such as SQL injection and cross-site scripting attacks.

- ▶ **Optional: IBM Virtual Server Protection for VMware**

IBM Virtual Server Protection for VMware is used in Cloud Enabled Data Center solutions to meet regulatory compliance by limiting critical data access, tracking user access, and providing virtual infrastructure reports. It provides defense-in-depth, dynamic security with VM rootkit detection, virtual infrastructure auditing, and monitoring of network traffic through hypervisor integration.

Advanced IaaS integrated with ITIL processes

The IBM SmartCloud Control Desk software components is required and used to implement the Advanced IaaS that are integrated with the ITIL processes macropattern (Figure 10 on page 26). IBM SmartCloud Control Desk is a solution that is ITIL compliant and includes the following capabilities:

- ▶ An efficient service desk to handle service requests and manage incidents
- ▶ A self-service catalog that helps users solve their own problems and provides an intuitive self-help portal and a complete catalog of services
- ▶ Change, configuration, and release management provides advanced impact analysis and automated change procedures to reduce risk and support integrity of services
- ▶ IT asset lifecycle management, which provides inventory management and software license compliance capabilities

This capability helps to manage assets throughout their lifecycle, optimizing usage of digital and physical assets and minimizing compliance risks.

Integrating with existing systems in your environment

Organizations that embark on implementing a Cloud Enabled Data Center solution might have existing systems that require integration to use existing capabilities. The following examples of existing systems and capabilities might need to be integrated:

- ▶ **Authentication**

Customers usually have authentication, authorization, and accounting (AAA) systems in place and require services to use the systems. Integration using LDAP or similar protocols is common and supported in this approach.

- ▶ **Authorization**

Similar to authentication, authorization for access is provided through the AAA integration. Often more authorization steps are necessary, including some that occur in the service itself, such as various privacy checks. Authorization can have more integration points with a policy management function or privacy function.

- ▶ **Billing**

Organizations that deploy cloud-computing solutions might already have their billing systems enabled so that charges are allocated to customers and invoiced. In this case, the cloud metering and chargeback processes need to be integrated with the existing billing process. This capability can be achieved by using technologies, such as file transfer or message queuing, to transfer the data into the billing system.

- ▶ Hardware and virtualization infrastructures

In many environments, it is common to find a mix of different hardware and virtualization technologies due to a mix of specific application needs, company strategic choices to avoid vendor lock-in, or heritage of the past. In these cases, the Cloud Enabled Data Center solution should be able to support the greatest number of hardware and virtualization platforms working concurrently. From this point of view, the IBM technology for Cloud Enabled Data Center supports a mix of virtualization environments, including VMWare virtualization products, IBM PowerVM, IBM z/VM® operating system, Microsoft Hyper-V server, KVM, Xen Hypervisor, and various hardware architectures.

- ▶ Network and security infrastructure

Cloud Enabled Data Center solutions are typically deployed into environments that have existing network infrastructure for the edge of the network (such as routers and edge security appliances). The Cloud Enabled Data Center resources must be provisioned in accordance with the security policies and standards of these existing systems.

- ▶ ITIL processes

Organizations that deploy cloud-computing solutions might have ITIL-based processes implemented through third-party tools that can be easily integrated with the cloud-computing processes. This integration can be realized by modifying the cloud-computing services to start the ITIL processes during the service deployment phase. Alternatively, from an ITIL process, it is possible to start a cloud-computing service.

- ▶ Monitoring, backup and restore, event management, and security

Organizations that deploy cloud-computing solutions might have one or more of these service management capabilities implemented in their IT environment. In this case, they can keep using these service management capabilities. They can also use the extensibility capabilities of the IBM cloud-computing solution to integrate them with the cloud-computing processes and infrastructure.

- ▶ Integration with firewalls and load balancers

Firewalls and load balancers are essential elements of an IT environment. Organizations that deploy cloud have firewalls in place to protect their applications and infrastructure. They also have load balancers to enable applications to easily scale up the number of users or transactions that are supported at any time. These two key infrastructure elements are typically managed by two different teams: the security team and the network teams. The deployment process of a business application can be affected greatly by the interactions between these two teams because of how they configure the firewall and the load balancer. With a Cloud Enabled Data Center solution, this risk can be eliminated by using built-in automation to configure firewalls and load balancers as part of a service creation process.

- ▶ Integration with existing service catalogs or web storefronts

Many IT organizations already use a mechanism to expose the list of the services that they provide and a way for their users to request those services. In the simplest cases, this mechanism is based on a trouble-ticketing system that is extended to manage all the IT requests. In the more sophisticated scenarios, this mechanism can be implemented by using a service catalog or a web front end. In all cases, the component that implements the Cloud Enabled Data Center solution provides a set of standard Representational State Transfer (REST) APIs. These APIs expose, start, and manage all the cloud services from an existing ticketing system, service catalog, or a web storefront.

Architectural decisions

The following key architectural decisions can influence a Cloud Enabled Data Center solution are summarized:

- ▶ Metering scope

Metering is a mechanism for gathering compute resource usage. Organizations can get a better handle on resource use and cost when they work in the cloud-computing environment. However, it is easy to attempt to measure everything such as hypervisors, virtual disk size, network I/O, occupied IP addresses, virtual processors and random-access memory (RAM). The complexity of the cloud-computing solution increases with the metrics that are being collected. When you deploy a Cloud Enabled Data Center solution, consider the scope of metering. Detailed usage and chargeback reports increase the complexity of the solution and might require more monitoring components.

- ▶ Service catalog

The Cloud Enabled Data Center solution provides a set of services (typically virtual machines) that users can provision through a self-service portal. You need to consider whether to embed the applications (such as middleware and database) within the base operating system image or to create more deployment workflows to provision the applications. Placing the applications with the operating system images reduces the time to deploy the solution, but makes currency management difficult.

- ▶ High availability

Cloud computing introduces the concept of *management* (tooling for automation) and *managed* (data center infrastructure that is automated) components. It might be desirable to have the management systems highly available. However, this approach comes at the cost of additional effort and resource requirements. Similarly, it might be desirable to have highly available managed environment. However, it would require more resources (such as spare nodes in the compute cluster) and new tools (such as tools to restart a VM in case of hardware failures).

- ▶ Managed infrastructure

An organization that adopts a Cloud Enabled Data Center solution might want to automate the provisioning of its entire existing data center infrastructure, such as a storage area network (SAN) or network-attached storage (NAS), compute servers, and network switches. In this case, careful consideration is required to select the infrastructure that would provide the best value.

Roadmap to developing the solution

The roadmap to develop a private cloud solution to deliver IaaS can easily be provided by the macropattern approaches shown in Figure 11. At each stage, the roadmap addresses a subset of IaaS scenarios that provide a well-defined and tangible business value. Additional scenarios can be implemented by adding new components into the roadmap.

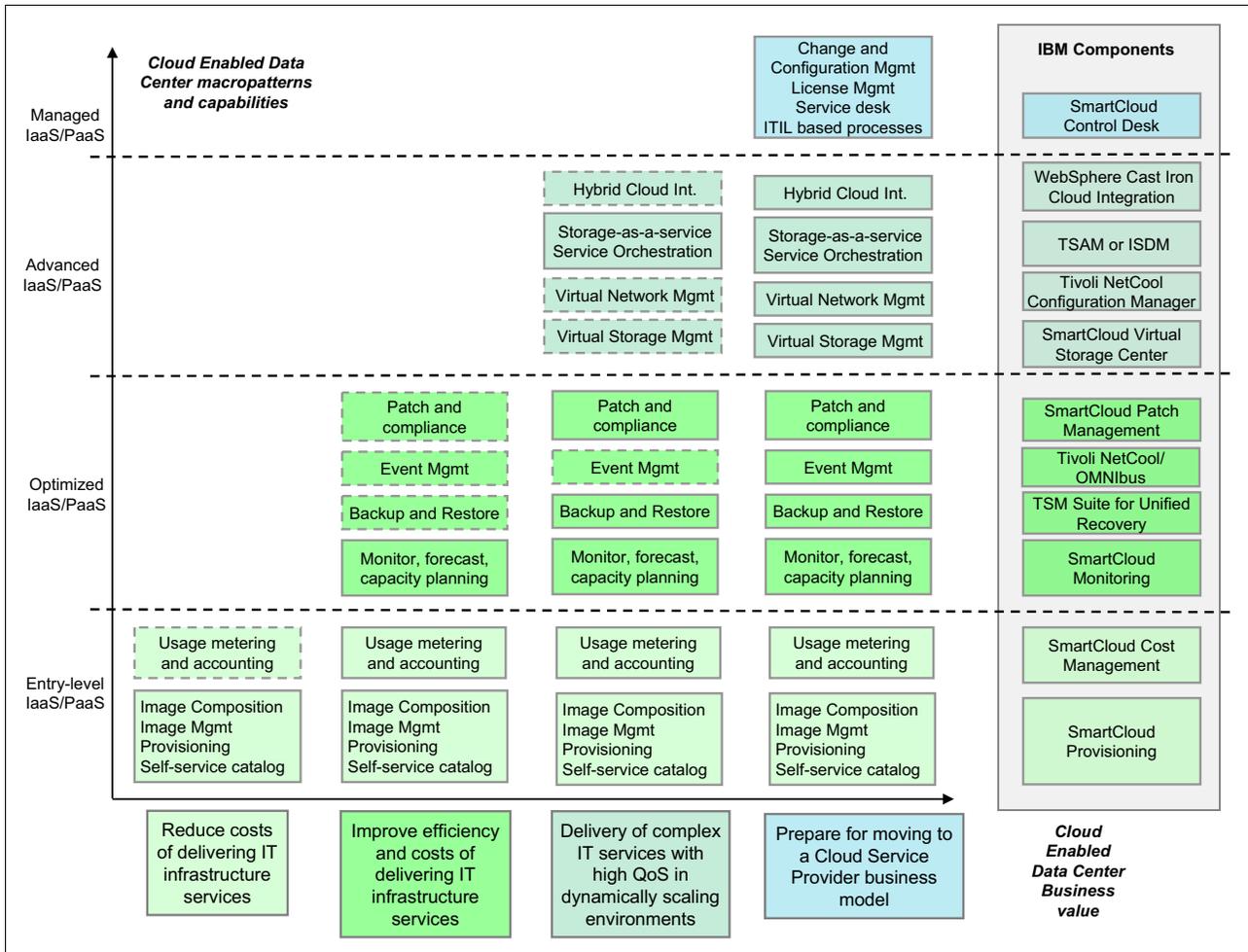


Figure 11 Incremental approach to build Cloud Enabled Data Center solutions based on macropatterns

You must consider that each new component easily stacks on top of and integrates with the existing components. The roadmap provides a step-by-step approach that minimizes risks and enables you to get immediate business value from the deployed components and functions. This approach also fits well with the transformational nature of a cloud adoption journey.

By using an incremental model, the IBM solution makes a complex effort manageable and ensures predictable results. This result is accomplished by using robust assets that are based on a standardized deployment architecture and management processes.

Example deployment scenarios

This section provides two fictitious customer examples that show how you can establish an IaaS based on the Cloud Enabled Data Center solution.

Rapid delivery of simple IaaS

A leading Internet service provider (ISP) wants to expand into the cloud service provider market. The company wants to accomplish this market expansion by starting with IaaS and

disaster-recovery services. By using this approach, the company can test market reaction. If it is successful, the company's long-term plan is to provide PaaS and SaaS solutions. The company wants the solution in production in a few weeks to quickly test this solution with selected customers.

The company needs a lightweight highly functional solution that delivers basic IaaS, such as VMs and storage. The solution must support the delivery of IaaS and provide a good ROI in terms of cost, speed, agility, and minimized operations.

The intended key differentiator is to provide rapid deployment of new services in seconds rather than hours. This capability is fundamental. The company must consider disaster-recovery scenarios where customers need to create hundreds of new VM instances in a few minutes to support their recovered workloads.

The company must rapidly create a solution to test the market reaction. They do not need a strong QoS, SLAs, or strong management and governance capabilities. This requirement leads them to select a solution that is based on the *Simple IaaS* macropattern. By using this macropattern, the company can quickly build a scalable cloud solution, that is ready to test the business value and ROI of the cloud-computing model.

The company implemented IBM SmartCloud Provisioning as the core delivery platform across multiple compute and storage nodes. The solution uses the KVM hypervisor to deliver VMs with minimal license cost, customer management, and VLAN separation. VLAN separation allowed for multitenant isolation at the network and presentation layer. By integrating the solution with IBM Storwize® V7000 Unified Disk Systems, the company can offer variable SLAs for storage. Also, the solution included the capabilities that are necessary for implementing disaster recovery scenarios for storage.

The simple and low maintenance solution based on SmartCloud Provisioning provides the following benefits:

- ▶ The ability for the company to start with a small initial investment
- ▶ The ability to deliver its own IaaS to several customers in a few weeks
- ▶ Direct testing of the solution on the market without incurring signification expenses

Delivery of advanced IaaS

A large worldwide financial institution offered different financial services to its customers. The IT organization was challenged to reduce its capital expenditure and operational expenditure. These challenges were necessary to remain competitive in the post-credit crisis market to drive down IT costs dramatically and to significantly improve delivery time of new IT environments to the business.

The Chief Information Officer (CIO) decided to address these challenges by reorganizing the IT organization and processes toward a cloud computing service-oriented model. This model is based on the automated delivery and management of standardized infrastructures and software stacks that are delivered through a services catalog. The service catalog will become the official and standard way for LOBs to access and ask for IT services. All the services that are delivered through this new cloud-computing model must meet the QoS and SLAs that are required by the IT team. Also, the services must comply with all the corporate policies, including security, change management, and license management.

The company needed the set of capabilities that are typically delivered by level 4 of the cloud maturity model that maps to the *Advanced IaaS Integrated with ITIL Processes* macropattern. To achieve this level of maturity, the company was able to select the architectural components that it needed to deliver the right solution. This approach was important to address the

functional and nonfunctional requirements, without having to deploy the whole solution as described by the macropattern. When using this macropattern some components are mandatory, some are recommended, and some are optional. This approach to the design of the macropatterns gives you the flexibility to choose the components that are needed to meet your needs.

In the solution, the company used IBM Tivoli Service Automation Manager to implement a cloud service catalog that allows the LOBs to request infrastructure services. The infrastructure services include, creation of simple VMs (on different hypervisors technology) starting from a set of standard images, logical partitions (LPARs), storage of different classes, configuration of firewalls, and load balancers.

All the VMs and LPARs created through this service catalog are automatically equipped with the standard monitoring and backup agents based on a third-party solution and with the Tivoli Workload Scheduler scheduling agent. This way, all the new VMs and LPARs are ready to be monitored, backed up, and scheduled through the standard IT tools.

The company also implemented a set of additional services so that users can automatically install and configure the standard banking middleware and databases, such as IBM DB2® and Oracle Database, on top of the requested VMs.

They integrated the Tivoli Service Automation Manager solution with their existing CMDB and license management process. These solutions ensured that, each time a new service is allocated (or deleted) from the service catalog, the CMDB and the software license inventory database are automatically updated to register or unregister the cloud asset or the corresponding software license.

This drastic change brought the following advantages to the IT organization and the entire company:

- ▶ Cut the deployment time of software stacks from two weeks to minutes with good delivery predictability and a near-zero error rate
- ▶ Better utilization of a reduced number of systems, managing resource pools instead of individual systems (producing economies of scale) and using the automatic deprovisioning of resources after expiration
- ▶ Little or no human intervention to deploy new system stacks and improve the server-to-administrator ratio
- ▶ Avoidance of handoff of activities from one person to another

By using this approach, IT can implement a centralized management of progress, perform historical tracking, and obtain insight into where process bottlenecks occurred.

Summary

IBM provides the essential solutions, products, and architecture materials to assist organizations in adopting an IaaS solution in an efficient and cost-effective way. The Cloud Enabled Data Center adoption pattern of the IBM Cloud Computing Reference Architecture provides a comprehensive business and architecture approach to companies that want to establish or extend an IaaS solution. By applying the CCRA, its adoption patterns, and the related detailed guidance, your IT organization can take advantage of the IBM cloud-computing expertise garnered by working with companies around the world.

This guide showed how the Cloud Enabled Data Center adoption pattern covers the business and technical needs and long-term plans for your company. It also showed how to apply the

essential requirements to support an initial deployment. Plus, it explained how to grow the solution as business needs change and expand to support new business opportunities and business models.

The Cloud Enabled Data Center adoption pattern within the IBM CCRA has been implemented and deployed with a wide variety of customers. It provides a sound foundation for building an IaaS solution. IBM customers have created a wide range of IaaS solutions from simple single purpose solutions to sophisticated ITIL aligned deployments. As cloud computing becomes a more integral part of the computing fabric, the flexible architectural model of the CCRA and the Cloud Enabled Data Center adoption pattern will provide a robust platform for your business to thrive on and grow.

Other resources for more information

The following IBM Redbooks® publications are associated with this Redguide:

- ▶ *IBM SmartCloud: Becoming a Cloud Service Provider*, REDP-4912
- ▶ *Cloud Security Guidance IBM Recommendations for the Implementation of Cloud Security*, REDP-4614
- ▶ *Performance Implications of Cloud Computing*, REDP-4875
- ▶ *Performance and Capacity Themes for Cloud Computing*, REDP-4876
- ▶ *Cloud Computing: Save Time, Money, and Resources with a Private Test Cloud*, REDP-4553
- ▶ *Cloud Computing and the Value of zEnterprise*, REDP-4763
- ▶ *Connect Cloud and On-premise Applications Using IBM WebSphere Cast Iron Integration*, REDP-4674

For more information about the products that are introduced in this guide, see the following web pages:

- ▶ IBM SmartCloud Provisioning
<http://www.ibm.com/software/products/us/en/smartcloud-provisioning>
- ▶ IBM SmartCloud Cost Management
<http://www.ibm.com/software/tivoli/products/smartcloud-cost-mgmt>
- ▶ IBM SmartCloud Monitoring
<http://www.ibm.com/software/products/us/en/ibmsmarmoni>
- ▶ IBM Tivoli Netcool/OMNibus
<http://www.ibm.com/software/tivoli/products/netcool-omnibus>
- ▶ IBM Tivoli Storage Manager Suite for Unified Recovery
<http://www.ibm.com/software/tivoli/products/storage-mgr-unified>
- ▶ IBM SmartCloud Patch Management
<http://www.ibm.com/software/products/us/en/ibmsmarpatcmana>
- ▶ IBM Tivoli Business Service Manager
<http://www.ibm.com/software/tivoli/products/bus-srv-mgr>
- ▶ IBM Service Delivery Manager
<http://www.ibm.com/software/tivoli/products/service-delivery-manager>
- ▶ IBM SmartCloud Virtual Storage Center

- <http://www.ibm.com/software/products/us/en/vsc>
- ▶ IBM Tivoli Netcool Configuration Manager
<http://www.ibm.com/software/tivoli/products/netcool-configuration-manager>
- ▶ IBM WebSphere Cast Iron Cloud Integration
<http://www.ibm.com/software/integration/cast-iron-cloud-integration>
- ▶ IBM Security Identity Manager
<http://www.ibm.com/software/security/products/identity-mgr>
- ▶ IBM Security Network Intrusion Prevention System
<http://www.ibm.com/software/tivoli/products/security-network-intrusion-prevention>
- ▶ Qradar Log Manager
<http://q1labs.com/products/qradar-log-manager.aspx>
- ▶ IBM Security Virtual Server Protection for VMware
<http://www.ibm.com/software/tivoli/products/virtual-server-protection>
- ▶ IBM SmartCloud Control Desk
<http://www.ibm.com/software/tivoli/products/smartcloud-controldesk>

The team who wrote this guide

This guide was produced by a team of specialists from around the world working with the International Technical Support Organization (ITSO).

Pietro Iannucci is a Senior Technical Staff Member (STSM) in the Tivoli Services division of IBM Software Group. He is part of a worldwide team that specializes in cloud solutions and helps IBM customers in the design and delivery of cloud implementations. Pietro is also responsible for the architecture specifications for the Cloud Enabled Data Center adoption pattern in the IBM Cloud Computing Reference Architecture. He has over 20 years of experience in software development. For many years, he has been the chief architect of the Tivoli Workload Automation portfolio and guided the technological and architectural evolution of associated products. He has written extensively and created several patents related to scheduling, automation, and cloud computing. Pietro holds a degree in mathematics.

Manav Gupta is a Software Client Architect in Canada bringing thought leadership across IBM Software Group brands to clients in the telecommunications industry. He has 15 years of experience in the telecommunications industry. His areas of expertise include systems management, cloud computing, and big data. He has written extensively on fault and performance management using products and technologies such as IBM Tivoli Netcool, Cloud Computing, and Big Data. Manav holds a degree in mathematics from Maharshi Dayanand Saraswati University in India and has a postgraduate diploma in software development from The Open University, in the United Kingdom.

Thanks to the following people for their contributions to this project:

LindaMay Patterson
ITSO, Rochester, MN

Brian Naylor
IBM Software Group -Tivoli, UK

Jochen Breh
IBM Global Technology Services®, Germany

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4893-00, was created or updated on May 21, 2013.



Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>



The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Cast Iron®	Netcool®	Storwize®
DB2®	PowerVM®	Tivoli®
Global Technology Services®	Redbooks®	WebSphere®
IBM SmartCloud™	Redguide™	z/VM®
IBM®	Redbooks (logo)  ®	

The following terms are trademarks of other companies:

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other company, product, or service names may be trademarks or service marks of others.