Intel IT Center

PLANNING GUIDE

Private Cloud Infrastructure as a Service

Steps to Providing Cloud Services Delivery for Greater Agility and Efficiency

WHY YOU SHOULD READ THIS DOCUMENT

This guide summarizes valuable information and practical steps for IT managers who want to plan and implement private cloud infrastructure as a service (IaaS) as the first step toward cloud services delivery, including:

- How building a cloud service delivery model will help your organization take full advantage of the agility and efficiency benefits of cloud computing
- The key technologies and capabilities that you need to move from an IT virtualization practice to a private cloud computing practice
- A framework for approaching your private cloud project that lays the groundwork for moving to a hybrid model when you are ready
- A quick review of the five leading cloud management platforms (CMPs): Apache CloudStack*, Eucalyptus* cloud platform, Microsoft* cloud software, OpenStack* cloud software, and VMware* vCloud Director*

Contents

The Path to Simplified Delivery of Cloud Services

Today the cloud is a proven delivery model, with a growing number of enterprises realizing impressive agility and efficiency benefits. As the technology matures, the trend is for organizations to extend cloud deployments to even more flexible private, hybrid, and public cloud models. The new models promise exciting new ways to expand the scope of value-added business services, address top priorities like big data and Bring Your Own Device and mobility initiatives, and deliver enterprise applications as services.

Many organizations no longer question the value proposition associated with cloud computing. But the conversation has changed—from "Should we do it?" to "How should we do it to get the most value?" Intel wants to help you simplify delivery of your cloud services so that your business can realize the full benefits now, while laying the groundwork to move to a more elastic hybrid model.[1] The purpose of this guide is to help you take the first step—building a private self-service cloud on a highly virtualized foundation.

Why Private Cloud?

Many companies are already virtualizing their IT environment and have been doing so for years. Initially, virtualization was deployed for compute resources, primarily as a cost-saving technology. Organizations soon recognized that virtualization provided efficiency benefits as well as enhanced agility and security.

Most clouds are built on virtualized infrastructure technology. Cloud computing originated as a new way to deliver IT services by providing a customer interface to automated, self-service catalogs of standard services, and by using autoscaling to respond to increasing or decreasing user demand. From an IT perspective, a private self-service cloud offers the key advantages of speed, agility, and efficiency while maintaining control of sensitive intellectual property (IP) and data.

Private clouds also enable IT to be more responsive to the business and to work more effectively with its constituencies—business users, suppliers, partners, employees, and others.

Without private clouds, line-of-business (LOB) requests to IT for provisioning server or storage capacity for key business initiatives can take weeks—or even longer. With a private, self-provisioning cloud, users can be up and running in hours or even minutes, with no or minimal interaction with IT. Projects don't languish, and users can gain access to the capacity they need on demand. IT can provide better service, monitor demand, and maintain control of sensitive workloads and resources. Users benefit with increased speed to market and the ability to go after short-term opportunities.

Best Practices and Insights from Intel IT

Intel IT solves some of today's most demanding and complex technology challenges—right here at home. Our computing environment supports 95,200 employees globally and includes 68 data centers and 147,000 devices. To create as much business value for Intel as possible, we proactively invest in and implement innovative IT strategies and capabilities, including cloud computing, consumerization of IT, and big data analytics.

Intel has realized significant benefits from deploying its own private cloud, from increased agility—server provisioning dropped from 90 days to 45 minutes—and reduced operational costs—$21 million in savings since 2009. Throughout this planning guide, we'll share best practices from Intel's cloud journey to reinforce our recommendations, help you reduce organizational risk, and simplify your path to the cloud.

Find additional insights and best practices from Intel IT leaders about strategic planning, creating business value, improving productivity, managing growth, and more at Intel IT.

Offering a private self-service cloud also provides these benefits, important for the evolution of your cloud services:

- Establishes a foundation for new services, such as platform as a service (PaaS),[2] to accelerate customer application deployment and promote cloud-aware application design principles.
- Enables extension to public service providers that can augment and expand your private cloud via a hybrid cloud model to manage spikes in demand and other one-off circumstances. IT can now "build the base, and rent the spike" for optimal efficiency.
- Positions IT as the broker of cloud services across the enterprise. In this role, IT can offer perspectives and skills to help users find the best internal or external solution for their needs, as well as better utilize existing private cloud resources. Also, IT can reduce the risk of exposing sensitive IP and data to outside vendors and help to meet LOB expectations on price, capacity, and provisioning speed, while ensuring that organizational requirements for security and data governance are in place.

High-Performance Cloud Capabilities

The U.S. National Institute of Standards and Technology (NIST) identifies several essential characteristics of a high-performing private cloud.[3]

- **On-demand self-service** – Users can automatically provision their own computing resources as needed and without requiring human intervention, typically through an interactive portal that enables them to configure and manage these services themselves.
- **Broad network access** – Resources are available via the network and can be accessed by multiple devices, including smart phones, tablets, laptops, and desktops.
- **Rapid elasticity** – Resources can be quickly and transparently expanded or contracted depending on demand. Scaling is automatic to users, and provisioning what they need is transparent.
- **Measured service** – Usage is measured and can be monitored, controlled, and reported for transparency.
- **Location-transparent resource pooling for multiple tenants** – Compute, storage, and networking resources are pooled to serve multiple user groups (tenants) with different physical and virtual resources that can be dynamically assigned and reassigned according to user demand. Because users generally have no control of the exact location of the resources, there is a sense of location independence, although location may be specified at a higher level of abstraction (country, state, data center).

BMW's Private Cloud Strategy

One example of a company successful in deploying a private cloud is BMW. The BMW Group is pursuing a long-term cloud strategy in two phases with short development cycles and specific short-term objectives. The first phase focuses on delivering private cloud services; phase two extends the private cloud to a hybrid model. The decision to start with a private cloud infrastructure was designed to avoid data and infrastructure security issues, provider dependencies, and integration deficiencies that are often encountered with public cloud infrastructures.

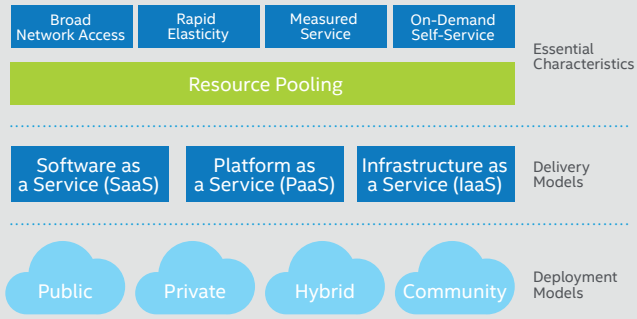
For its private cloud environment, BMW uses modularized open architecture based on industry standards and usage models from the Open Data Center Alliance to create secure platform and infrastructure layers, business orchestration, and technical automation.

Find out more about BMW's cloud strategy in Open Data Center Alliance*: The Private Cloud Strategy at BMW.

In addition to these capabilities, NIST also defines service delivery layers and deployment models. Deployment models include private, public, community, and hybrid clouds. Service layers for each of these delivery models include:

- **Infrastructure as a service (IaaS)** – Cloud infrastructure is the collection of hardware and software that enables the essential characteristics of the cloud. IaaS enables users to self-provision these resources in order to run platforms and applications.
- **Platform as a service (PaaS)** – PaaS enables users to adapt legacy applications to a cloud environment or develop cloud-aware applications using programming languages, services, libraries, and other developer tools.[2]
- **Software as a service (SaaS)** – Users can run applications via multiple devices on cloud infrastructure.

National Institute of Standards and Technology (NIST) Cloud Computing Model



Based on the U.S. National Institute of Standards and Technology (NIST) definition of cloud computing. (Source: *Cloud Computing Synopsis and Recommendations*. NIST Special Publication 800-146 (May 2012). http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

About Cloud Delivery Models

- **Private** – Cloud infrastructure is provisioned for use by a single organization that comprises multiple tenants. Private clouds may be operated on- or off-premises and are behind the company firewall.
- **Public** – A cloud service provider offers services to multiple businesses, academic institutions, government agencies, and other organizations with access via the Internet.
- **Hybrid** – Hybrid clouds combine two cloud delivery models (for example, private and public) that remain unique as entities but are bound together by technology that enables data and application portability. Cloudbursting is an example of one way enterprises use hybrid clouds to balance loads during peak demand periods.
- **Community** – Cloud infrastructure is provisioned for the exclusive use of a specific community of user organizations with shared computing requirements such as security, policy, and compliance.

From Virtualization to Orchestration—the Path to Private Cloud

Results from a Gartner survey of 505 data center managers worldwide indicate that planned or in-process virtualization of infrastructure workloads will increase from approximately 60 percent in 2012 to almost 90 percent in 2014.[4] This continuing growth makes cloud computing an obvious next step for many organizations.

The key steps in the journey to private cloud are virtualization, automation, and orchestration.

- **Virtualization.** The underpinning for the majority of high-performing clouds is a virtualized infrastructure. Virtualization has been in data centers for several years as a successful IT strategy for consolidating servers. Used more broadly to pool infrastructure resources, virtualization can also provide the basic building blocks for your cloud environment to enhance agility and flexibility.
- **Automation.** With the virtualization of first simple and then more complex applications, the next step is to reduce manual processes via automation. An automated resource pool with capabilities to provision, monitor, and report on underlying infrastructure provides faster access to users and increases IT productivity for routine tasks such as regular patching for thousands of virtual machines (VMs).
- **Orchestration.** To further enhance data center efficiency and agility, IT needs to enable policy-driven workload management and movements, as well as deliver capabilities for self-service and metering. Orchestration is also a critical capability required for deploying software-defined networking (SDN), software-defined storage (SDS), and network function virtualization (NFV) as your data center evolves to software-defined infrastructure (SDI). SDI is the technology foundation for a fully virtualized, automated, and orchestrated data center for service-assured IT and promises benefits of even greater efficiency, agility, and security.

Virtualization Is Not Cloud Computing

Here's the difference: Virtualization abstracts compute resources—typically as virtual machines (VMs)—with associated storage and networking connectivity. The cloud determines how those virtualized resources are allocated, delivered, and presented. Virtualization is not necessary to create a cloud environment, but it enables rapid scaling of resources in a way that nonvirtualized environments find hard to achieve.

From Virtualization to Private Cloud Services: Five Steps

The path from virtualization to a self-service private cloud poses technical as well as organizational challenges related to management and operational processes, culture, and politics. The following five high-level actions serve as a framework to help you understand and successfully address the organizational and technology issues you will face. Many of the specific activities involved will take place simultaneously. Neglecting any one of these can trip you up and cause your project to fail.

The framework:

- **Step 1: Develop a cloud strategy** – Establish where you want to go.
- **Step 2: Manage organizational and business process change** – Get the business on board.
- **Step 3: Organize IT around services delivery** – IT shifts its role to a broker of cloud services.
- **Step 4: Put the right technology in place** – Set short-, medium-, and long-term goals.
- **Step 5: Manage a data-driven cloud** – Use analytics to improve operations.

About Intel's Cloud Strategy

In 2009, Intel IT began work on a core business strategy to build an enterprise private cloud. The complex, multiyear approach was designed to increase agility, boost infrastructure efficiency, and provide high availability, as well as host highly demanding, mission-critical business applications.

Intel IT made the decision to build the cloud from the inside out in three phases:

- Phase 1: We created hosting platforms, implementing infrastructure as a service (IaaS) to enable broader enterprise usage models.
- Phase 2: Then we built on our success by offering platform as a service (PaaS) to encourage cloud-aware application development for specific use cases.
- Phase 3: Currently, we are laying the foundation for hybrid clouds to maximize agility and provide bursting capability.

Source: *Intel IT Open Cloud—What's Under the Hood, and How Do We Drive It?* Intel Developer Forum 2013 CLDS004 (September 11, 2013).

Step 1: Develop a Cloud Strategy

A cloud strategy clearly articulates the benefits, approach, and expected outcomes for your technology investment across your organization. Tied to LOB goals, it helps you get senior management buy-in and manage expectations—both keys to your success. Your cloud strategy should include:

- **The high-level business case** – Describe the benefits to both IT and the business and the expected return on investment.
- **Implementation phases** – Define short-term, mid-term, and long-term goals for delivering services with related benefits. For example: Intel IT implemented IaaS first to enable broader enterprise use cases.
- **Workloads** – Identify the workloads you plan to move to the cloud and the associated user groups.

- **Cloud architecture** – Define cloud architecture, including the components of IaaS, PaaS, and SaaS, as well as security and related systems such as backup and disaster recovery.
- **Client devices** – Define how users will access the cloud and integrate with your enterprisewide mobile strategy.
- **Monitoring and management** – Determine how you will manage your cloud, monitor health and performance, and define success.
- **IT-business relationships** – Define how IT will partner effectively with the business to specify business process requirements and request services.

With a cloud strategy, you now have an overarching approach to cloud computing across the organization. Use it as a tool to deepen relationships with LOB managers, generate some excitement for your project, and manage expectations for each phase of implementation. Plus, it's a roadmap for where you want to go, helping to direct virtualization efforts so you can fully achieve the value on your private cloud investment and lay the groundwork for a more elastic hybrid model. A cloud strategy will also help you avoid the potential for shadow IT created by business units who may go to a public cloud provider in the absence of private cloud services in the enterprise.

Step 2: Manage Business Process Change

Business process changes are pervasive in a cloud implementation. For your cloud project to succeed, you must collaborate with process owners to accurately document the processes and tasks affected and determine how to minimize the number of required human control points. Plus, you need management cooperation to implement any changes to existing processes that might benefit from the automation; and you will be developing new processes, such as how users access and specify the cloud resources they need. By drawing on cross-domain expertise, you ensure that your technical considerations benefit from business knowledge of the activities and tasks to be automated and avoid the potential of user and management apathy—or worse, hostility.

Cloud obviously affects IT-specific processes as well. Capacity management, for instance, becomes radically different in a cloud environment. In the cloud, rather than IT assigning physical resources with unused overhead to handle peak conditions, capacity is governed by predefined limits based on demand for individual applications and provisioned by users.

You also need to implement other processes to better manage your cloud, such as system-related business intelligence and costing information. For example, with manageability and business intelligence tools, you can keep operational costs at a minimum by maintaining a thin overhead of unused capacity and making investments in new infrastructure on a just-in-time basis. Business intelligence capabilities also provide insights into consumption, performance, utilization trends, and security-related events.

Step 3: Organize IT around Service Delivery

Many users in large companies are already familiar with the concept of consuming IT services. Organizing your IT workforce around cloud service delivery enables you to serve the business more effectively as a cloud services broker.

Your role as a cloud services broker is to weigh user needs against the available delivery options for your organization. From the IT perspective, this reduces organization risk, improves resource utilization, and monitors demand. From the perspective of users, they get the right solution to meet their needs—made easy with self-provisioning and automation. Ultimately, you gain experience delivering cloud services that can be extended later to brokering public services in a hybrid cloud model. You also eliminate the need for business users to stand up their own individual cloud silos.

New IT Skills for Cloud Computing

Delivering cloud services requires a shift in IT skills to include abilities in planning, modeling, financial management, building architecture for evolving needs, and performance measurement for efficiency, service analysis, and continuous improvement. While legacy and cloud resources may be managed separately now, the trend is toward a single management structure for both. IT groups are using a combination of tactics to make sure they have the right mix of skills, including hiring new talent and training existing staff.

Step 4: Put the Right Technology in Place

Your cloud won't succeed without the right technology. Set your technology priorities based on the implementation phases and milestones described in your cloud strategy. For example, short-term priorities would typically include implementing pervasive virtualization to integrate compute, storage, network, and physical resources. Next, you might offer IaaS by implementing end-to-end, on-demand, self-service capabilities through service automation and orchestration, while maintaining a high level of security. Longer term, integrating public services into a hybrid model can enable even greater flexibilities such as elastic scaling and cloud bursting.

Reference architectures and out-of-the box workflow templates or building blocks can significantly simplify implementation as well as reduce project time. You'll need your business process documentation to use these tools efficiently, especially for provisioning, scheduling, and automation. Proofs of concept will help increase confidence and point to areas of improvement.

Step 5: Manage a Data-Driven Cloud

End-to-end health and performance monitoring of the environment is essential for cloud management. Without data collection and analytics, you won't have the information you need to benefit from system efficiencies or measure success. A dashboard with integrated operational analytics that encompass facilities, network, storage, compute, and applications can help you assess whether you are meeting availability and performance goals, inform decisions to add capacity, troubleshoot problems, and comply with security and privacy regulations. Plus, at the point where you want to offer externally hosted cloud services, you must have a way to measure overall service availability in place to monitor third-party service level agreements.

About Intel® Cloud Builder Reference Architecture Solutions

Intel can help simplify your path to the cloud with reference architectures and more from Intel® Cloud Builders, a cross-industry initiative aimed at making it easier to build, enhance, and operate cloud infrastructure. Resources include:

- Reference architectures, or recipes, on how to deploy ecosystem solutions built on commercially available offerings from leading systems and solutions providers based on Intel technologies
- Reference implementations describing real-world customer deployments of a reference architecture
- Webcasts providing in-depth presentations on solutions and architectures
- Weekly podcasts on cloud computing topics
- An ecosystem of more than 60 leading cloud computing companies that can provide cloud solutions based on Intel Xeon® processor-based servers

Find more at intelcloudbuilders.com/library.

Building High-Performance IaaS: Three Key Technology Steps

IaaS is the virtualized, multitenant infrastructure that underpins your private cloud and enables multiple applications for business groups across the enterprise to share. IaaS is built and delivered using a set of technologies that start with virtualization as the basic building block. A cloud management platform enables you to run a multitenant environment using the resources from the virtual infrastructure and security technologies at every level. Although clouds are built with IaaS, PaaS, and SaaS service layers, infrastructure services are the most typical private cloud services offered today.

Step 1: Implement Pervasive Virtualization

Virtualization is the foundation for an agile, scalable cloud—and the first practical step for building cloud infrastructure. Virtualization abstracts and isolates the underlying hardware as VMs in their own runtime environment and locates multiple VMs for computing, storage, and networking resources in a single hosting environment. These virtualized resources are critical for managing data, moving it into and out of the cloud, and running applications with high utilization and high availability.

Virtualization is managed by a host server running a hypervisor—software, firmware, or hardware that creates and runs VMs. The VMs are referred to as guest machines. The hypervisor serves as a virtual operating platform that executes the guest operating system for an application. Host servers are designed to run multiple VMs sharing multiple instances of guest operating systems.

Virtualization also provides several key capabilities for cloud computing, including resource sharing, VM isolation, and load balancing. In a cloud environment, these capabilities enable scalability, high utilization of pooled resources, rapid provisioning, workload isolation, and increased uptime.

About Virtualization Best Practices

Intel IT implemented pervasive virtualization as part of the plan for the company's private cloud, achieving more than 75 percent virtualization of servers by 2014. Virtualization best practices that lay the groundwork for building Intel's cloud services include:

- Establishing a standardized, repeatable process for identifying, virtualizing, and managing the life cycle for virtualized servers
- Creating demand from business groups by explaining plans, promoting private cloud benefits, and proving that virtualization would not impact their production environments
- Resolution of technical limiters, such as security, storage replication, backup and recovery, very large virtual machines (VMs), and Sarbanes-Oxley compliance, in order to virtualize mission-critical applications

Learn more about pervasive virtualization from *Best Practices for Building an Enterprise Private Cloud*.

Today, the trend in virtualization has moved from reducing costs by consolidating data centers to increasing flexibility and agility through the pervasive use of virtualization for faster service deployment and dynamic placement of workloads. Pervasive virtualization is a strategic approach that provides a method for judiciously bringing legacy applications into your cloud to meet your strategic goals or as time and budget allow. Its benefits include better quality of service, improved availability and business continuity, faster resource deployment, and lower energy consumption.

Step 2: Select Your Cloud Management Platform

With increased virtualization infrastructure, you also need greater management, automation, and orchestration capabilities. At this juncture, you can decide to:

- Use a virtualization management platform that can also be used or extended easily for the cloud.
- Augment existing tools with an expanded set of cloud management capabilities on top of your existing virtualization management platform.
- Add a new cloud management platform (CMP) that can run the cloud and your existing virtualization environment.

Cloud Management Platforms

A cloud management platform can help greatly in adding automation and orchestration capabilities and delivers service quality, security, and availability for workloads running in cloud environments. CMP offerings vary widely in terms of platform maturity, architecture complexity, and capabilities. At minimum, a CMP should provide:

- Direct user access to the system
- Self-service capabilities and interfaces
- Workflow engine
- Automated provisioning
- Metering and chargeback functionality

More advanced capabilities might include performance and capacity management, interoperability between private and public IaaS offerings, connectivity to and management of external clouds, application life-cycle support, back-end service catalogs, and integration with external enterprise management systems.

The cloud management platform you choose should be based on organization size and complexity, the degree of heterogeneity in your virtualized infrastructure, and the cloud functionality you require. With heterogeneous infrastructure, you are more likely to benefit from using IT operations management architectures to manage both legacy and cloud environments. For data centers with homogeneous infrastructure, evaluating the vendor as your supplier is a good place to start.

About Open Data Center Alliance* Cloud Usage Models

The Open Data Center Alliance (ODCA) is an independent IT consortium composed of global IT leaders who work on a unified customer vision for long-term data center requirements, including critical cloud infrastructure needs. ODCA membership includes more than 300 companies representing more than USD 100 billion in annual IT spend. ODCA began releasing a roadmap of IT requirements in 2011, including master usage models for compute infrastructure as a service and service orchestration, as well as security, management, governance, and monitoring. Intel is the nonvoting technical advisor to ODCA. Learn more at opendatacenteralliance.org.

Automation and Orchestration

Automation is a key capability of elastic, high-performing cloud environments. By eliminating or minimizing manual processes and requiring minimal human control points, you can optimize and manage resources faster, deliver more streamlined services, manage service life cycle, and respond to changing conditions.

About Intel IT's Automated Workflow

Intel IT created a workflow automation layer for the company's private cloud infrastructure through a modular, extensible framework that simplifies system integration and provides the prerequisites for fully functional, self-provisioned virtual machines (VMs) with compute, storage, and network resources. The modular design enables Intel IT to introduce additional automation capabilities as business and technical needs change.

Get more detail in *Best Practices for Building an Enterprise Private Cloud*.

Orchestration software provides the automated intelligence that dynamically arranges, coordinates, and manages the elements of your cloud environment. Orchestration of end-to-end services enables flexibility, economy of scale, and on-demand delivery for virtualized resources and provides the ease and convenience users expect when they access the cloud.

Orchestration has two main jobs: aligning service requests with available resources and monitoring the health of the physical and virtualized environment. These functions enable your cloud to scale up or down based on demand at specified performance levels. To accomplish this, orchestration manages across different systems to:

- Connect and automate workflows to deliver a specified service.
- Manage configuration, capacity, metering, and chargeback.
- Track and report on cloud performance and availability.
- Monitor and manage power, including energy consumption and cooling requirements.
- Monitor security threats and adherence to security policies, including access, authorization, and identity management.
- Take effective actions and make adjustments based on feedback from monitoring tools.
- Predict potential issues so they can be addressed before they become major problems.

Orchestrating Your Data Center: Software-Defined Infrastructure

Intel has a vision for an exciting next-generation data center with software-defined infrastructure (SDI) where applications define the system, and where IT services are fully automated and orchestrated. SDI promises to deliver even greater efficiencies and flexibility, with the latest hardware and software providing service assurance; provisioning management; and pooled compute, network, and storage resources.

Intel is investing in SDI in three areas:

- **Broadest-enabled ecosystem** – Integrated and optimized products for all leading commercial and open-source operating environments for more seamless data center operations
- **Exposed and integrated telemetry** – Exposed hardware and infrastructure attributes integrated with orchestration software for deeper insight and optimal provisioning management
- **Platform and architectural leadership** – Standards-based compute, network, and storage building blocks to drive maximum infrastructure efficiency and flexibility

The CMP Landscape

The CMP market is still evolving, and vendors offer solutions with varied feature sets. The open-source solutions typically provide a low-cost point of entry for the software and the prospect of application portability, but may require a significant amount of in-house development. Commercial vendors provide off-the-shelf capabilities, and are typically higher cost than open-source offerings.

Choosing the appropriate CMP for your cloud environment depends on your current virtualization environment, the scope of your cloud strategy, your business requirements, the availability of skilled resources, and your budget. The following table provides a basic description and additional features and capabilities for five leading CMPs.

Cloud Management Platform	Description	Additional Features and Capabilities
Apache CloudStack*	A top-level project of Apache Software Foundation that offers an open, flexible cloud orchestration platform for private and public clouds, the Apache CloudStack platform is based on the Java* language and provides self-service infrastructure-as-a-service (IaaS) capabilities.	• Compute orchestration • Network as a service; user and account management • Native API and Amazon* Web Services (AWS) API translator so that apps written for the CloudStack platform can run in AWS • Resource accounting of network, compute, and storage resources • Multitenancy and account separation • "First-class" user interface • Support for hypervisors from Xen, KVM, and VMware
Eucalyptus Systems	This open-source provider with strong technical ties to Amazon Web Services enables a company to move seamlessly from a private cloud to a hybrid model by bursting into the Amazon public cloud as needed.	• Self-service user console • Dashboard for cloud management tasks • Mixed hypervisor environments • Storage area network (SAN) integration to take advantage of storage arrays • Identity management with fine-grained role-based access control • Accounting, chargeback, and quota management • Usage reporting and pattern analysis • Automated installation with guided configuration of cloud components • Support for industry-standard AWS APIs and hypervisors from Xen, KVM, and VMware

Cloud Management Platform	Description	Additional Features and Capabilities
Microsoft* Hyper-V* software and Microsoft System Center	Microsoft Cloud OS is a set of technologies, tools, and processes built on the Windows Server* operating system with Hyper-V software, Microsoft System Center, and the Windows Azure* platform. Combined, these technologies provide a consistent platform for infrastructure, applications, and data.	• Virtualization of servers, network, storage, and applications • Automated self-service web portals and a provisioning engine • Extensibility with third-party partner solutions • Unified management view across private, hosted, and public clouds • Single identity for secure user and device management • Can handle petabytes of data with Microsoft SQL Server* software
OpenStack* cloud software	An open-source platform currently available under the Apache* 2.0 license, OpenStack can be deployed for private cloud as a free software download with in-house deployment or from a vendor. The modular design enables integration with legacy and third-party technologies.	• Massively scalable redundant storage for high availability • Strong, token-based security and compute security groups • Shared services for identity management, image management, and a web interface • Native API and Amazon Elastic Compute Cloud* (EC2)-compatible API • Administrative dashboard to monitor the cloud environment • Self-provisioning for users • Compatibility with software-defined networking (SDN) such as OpenFlow* technology • Supports hypervisors from Xen and KVM
VMware* vCloud Director*	The VMware vCloud* Suite is a comprehensive, integrated cloud platform that includes the elements to build cloud environments and operationalize VMware vSphere* virtualized environments. VMware vCloud Director ties all the pieces of the cloud together.	• Rapid policy-controlled, self-service provisioning of virtual machines (VMs) and applications • Trust-zone policies to protect and control traffic to IT-governed groups of VMs • Comprehensive data center monitoring and management • Compatibility with SDN • Disaster protection; operational and regulatory compliance • Self-service portal access • High-performance service levels for disaster recovery, security, and compliance

Step 3: Implement Cloud Security

As you move beyond virtualizing your data centers to building your private cloud, security must evolve to support both traditional and new vulnerabilities. Cloud environments require a new take on security, with challenges around resource isolation, security event management, and data protection, including VM isolation, secure VM migration, virtual network isolation, and security event and access monitoring. Plus, with multiple business groups accessing cloud resources, visibility into secure data flow and compliance with business-specific security policies is critical.

Cloud security must be adaptive to an environment in which workloads are decoupled from the physical hardware and delivered from a fabric of pooled resources. At the same time, security must protect the physical boundaries of the network edge.

As you plan your security approach to your private cloud, you can also lay the groundwork for eventually moving certain workloads into a public cloud. One way to do this is to provide security as a set of on-demand, scalable services. In this approach, policies are tied to logical attributes that create adaptive trust zones to separate multiple tenants. Workloads and the appropriate security policies can then be associated throughout the workload's life cycle. This approach involves virtualizing security controls throughout the environment, isolating applications, and building context awareness into applications that informs security decisions and delivers compound security policies independent of network topology.

Intel recommends prioritizing five areas for combining physical and virtual controls.

1. Protect data by implementing pervasive encryption, using secure connections, and applying data-loss-prevention policies.
2. Establish and verify identities to control access from client devices and systems that you can trust, and manage API control points at the edge of the network.
3. Secure your data center platform, infrastructure, and client devices by establishing trusted compute pools.
4. Build higher assurance into compliance to streamline auditing and increase visibility into your cloud environment.
5. Enable secure migration from a private cloud environment to public cloud providers.

About Security in Public Clouds

Security is one of the biggest barriers in cloud adoption. If you build a private cloud with strong security controls in place, you probably expect a public cloud provider to offer those same capabilities—especially if you have a hybrid cloud agenda in mind.

To better equip IT managers worldwide with the knowledge and answers they need to take full advantage of public cloud capabilities, Intel developed a tool: Intel® Cloud Finder. Users define required and desired features of their public cloud infrastructure as a service (IaaS) by answering a series of questions across several categories, including security, usability, quality, availability, technology, and business.

The tool matches user responses to the services available from a broad range of leading IaaS providers worldwide. Using Intel Cloud Finder can significantly shorten the time it takes to identify an appropriate public cloud provider.

Learn more at intelcloudfinder.com.

Intel IT and Secure Virtualization Host Architecture

Intel IT implemented secure virtualization by designing a virtualization host and networking architecture that provided private virtual LANs (PVLANs) and separated role-based administration for each host. This provides workload security by using network isolation to control traffic via PVLANs and deploying hosts into secure landing zones that protect applications from attacks originating from the Internet and the intranet.

Learn more in *Best Practices for Building an Enterprise Private Cloud*.

About Intel® Cloud Security Technologies

Together, Intel and McAfee offer several data and infrastructure security technologies for cloud environments.

- Intel® Platform Protection Technology with Trusted Execution Technology[5] (Intel TXT), together with McAfee* Data Center Security Suites, helps detect server systems booting with unknown BIOSes, firmware, and hypervisors and provides hardware-based verification for use in meeting compliance requirements.
- Intel Data Protection Technology with Advanced Encryption Standard New Instructions (Intel AES-NI)[6] and Secure Key enables faster and stronger encryption and decryption of the McAfee endpoint encryption product.
- With Intel Expressway API Manager (Intel EAM), Intel packages a leading software-as-a-service (SaaS) API sharing portal from Mashery with Intel's on-premises service gateway for API management. Intel EAM integrates and surfaces legacy data as APIs and then shares them with developers via the API sharing portal for enterprise and mobile development. At runtime, developers can apply mobile-friendly security, create real-time app mash-ups, and broker how apps are exposed across hybrid on-premises environments to cloud environments. The Intel Expressway product family is a core part of the Intel and McAfee cloud data center and comes integrated with several McAfee technologies, including McAfee ePolicy Orchestrator* (McAfee ePO*) for monitoring security events.

Next Steps: A Checklist

By moving from virtualization to a private cloud with self-service and other attributes in place, you have taken the first major step toward brokering cloud services throughout your organization. As you become more familiar with the technology, new challenges will arise—opportunities, really. For example, you may cloud-enable an application with unpredictable demand or notice spikes or sudden drops in demand. These are opportunities that can prompt you to expand your service offerings, cloud-enable more legacy applications, or take the next step to a hybrid cloud model.

Here's a quick checklist summarizing how you can move from virtualization to a private cloud services model. When you're ready to go further, read Intel's *Hybrid Cloud Checklist: Operationalizing Your Hybrid Cloud*.

Develop a Cloud Strategy

- ☐ Describe the anticipated business benefits and return on your investment.
- ☐ Set short-, mid-, and long-term goals.
- ☐ Identify the workloads and user groups you want to move with each project phase.
- ☐ Describe your cloud solution architecture and its components.
- ☐ Identify the client devices you will support.
- ☐ Describe how you will monitor and manage your cloud and define success.

Get the Business on Board and Create Strong Partnerships

- ☐ Communicate benefits and milestones to users.
- ☐ Develop a plan to manage expectations for each project phase.
- ☐ Engage business users to define and document new and existing business processes.

Organize IT around Service Delivery

- ☐ Determine how teams will work together.
- ☐ Hire or train for cloud-related skills.

Put the Right Technology in Place to Align with Your Strategy and Roadmap

- ☐ Implement pervasive virtualization.
- ☐ Select your cloud management platform.
- ☐ Implement cloud security.

Manage a Data-Driven Cloud

- ☐ Determine how you will monitor health and status.
- ☐ Determine how you will manage compliance.
- ☐ Determine what actions should be automated, and the associated triggers.

Resources to Learn More

To learn more about cloud computing, visit these web sites:

- Cloud computing: intel.com/cloud
- Cloud security: intel.com/cloudsecurity
- Intel Cloud Builders: intelcloudbuilders.com/library
- Intel Cloud Finder: intelcloudfinder.com
- Intel IT Center: intel.com/ITCenter
- Open Data Center Alliance (ODCA): opendatacenteralliance.org/

About Intel IT Virtualization and Cloud

Accelerating Deployment of Cloud Services Using Open Source Software

Intel IT shares how it used OpenStack open-source software in combination with Intel's own internal code and existing enterprise software to deploy a cloud infrastructure that serves as the foundation to transform data center solutions into quickly obtainable, consumable services and paves the way for hybrid cloud delivery.

intel.com/content/www/us/en/it-management/intel-it-best-practices/accelerating-deployment-of-open-source-cloud.html

Applying Factory Principles to Accelerate Enterprise Virtualization

Intel IT set a goal of virtualizing up to 75 percent of the company's Office and Enterprise computing environment to create the infrastructure for a broadly adopted enterprise private cloud.

intel.com/content/www/us/en/virtualization/virtualization-intel-it-applying-factory-principles-paper.html

Intel IT Open Cloud—What's Under the Hood, and How Do We Drive It?

This presentation from the Intel Developer Forum 2013 outlines Intel's cloud strategy and progress to date on a multiyear project to develop a private cloud with on-demand, self-service provisioning (idea to production) in less than one day, zero downtime, and growth with a flat budget.

slideshare.net/LarryCover/intel-it-open-cloud-whats-under-the-hood-and-how-do-we-drive-it

Under the Hood of Intel IT's Private Cloud

Das Kamhout, Intel IT principle engineer, and Raejeanne Skillern, director of cloud computing marketing, discuss Intel's multiyear project to build the company's private cloud. The webcast includes an in-depth look at Intel's private cloud infrastructure and Intel's roadmap for open cloud computing. It also includes how you can build a cloud that expands on demand with self-service provisioning, drive 80 percent utilization of data center resources, achieve server consolidation ratios of 20:1, and accelerate deployment with open cloud computing best practices validated by Intel (60 minutes).

brighttalk.com/webcast/499/43555

Endnotes

1. For more information about Intel's roadmap to hybrid cloud, view the video "Create Advanced Cloud Computing Platforms," Intel (2013). intel.com/content/www/us/en/cloud-computing/cloud-computing-hybrid-platform-solutions-animation.html
2. For more information about PaaS, read the white paper *What Is PaaS*? Intel (July 2014). intel.com/content/www/us/en/cloud-computing/cloud-computing-what-is-paas-cloud-demand-paper.html
3. Badger, Lee, Tim Grance, Robert Patt-Corner, Jeff Voas. *Cloud Computing Synopsis and Recommendations*. U.S. Department of Commerce, National Institute of Standards and Technology Special Publication 800-146 (May 2012). csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf
4. *Will Private Cloud Adoption Increase by 2015*? Gartner Research Note G00250893 (May 12, 2013).
5. No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, and software, and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your system or service provider for availability and functionality.
6. Intel AES-NI requires a computer system with an AES-NI–enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

More from the Intel® IT Center

Planning Guide: Private Cloud Infrastructure as a Service is brought to you by the Intel® IT Center, Intel's program for IT professionals. The Intel IT Center is designed to provide straightforward, fluff-free information to help IT pros implement strategic projects on their agenda, including virtualization, data center design, cloud, and client and infrastructure security. Visit the Intel IT Center for:

- Planning guides, peer research, and solution spotlights to help you implement key projects
- Real-world case studies that show how your peers have tackled the same challenges you face
- Information on how Intel's own IT organization is implementing cloud, virtualization, security, and other strategic initiatives
- Information on events where you can hear from Intel product experts as well as from Intel's own IT professionals

Learn more at intel.com/ITCenter.

Share with Colleagues

0714/RF/ME/PDF-USA 330884-001