# ONUG Hybrid Cloud Working Group Framework

# Version 1.0

A white paper from the
ONUG Open Hybrid Cloud
Working Group

May, 2016

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

## Definition of Open Networking

Open networking is a suite of interoperable software and/or hardware that delivers choice and design options to IT business leaders, service and cloud providers. At its core, open networking is the separation or decoupling of specialized network hardware and software - all in an effort to give IT architects options in the way in which they choose to design, provision, and manage their networks. These technologies must be based on industry standards. The standards can be de-facto as adopted by a large consortium of the vendor community, open in the sense that they are community based, or defined as standards by the prevailing standards bodies. Open networking hopes to deliver on two promises:

1) Decoupling of network hardware and software which mitigates vendor lock-in and shifts network architecture structure options to users
2) Significant reduction of the total cost of ownership model, especially operational expense

## Table of Contents

Executive Summary

**Section 1:** Open Hybrid Cloud Technical Architecture

**Section 2:** Open Hybrid Cloud Security

**Section 3:** Open Hybrid Cloud Lock-in Identifiers

**Section 4:** Legal/Compliance/Contract Language

**Section 5:** Skill-set/Operational Model Challenges

**Section 6:** Industry Recommendations and Hybrid Cloud Provider Requirements

Open Hybrid Cloud Working Group Members

Glossary

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

## Open Networking User Group (ONUG)

ONUG is one of the largest industry user groups in the IT infrastructure market. Its board is comprised exclusively of IT business leaders, with representation from Fidelity Investments, FedEx, Bank of America, UBS, Cigna, Pfizer, GE, JPMorgan Chase, Morgan Stanley, Citigroup, Credit Suisse, Gap and Yahoo. The ONUG mission is to enable greater choice and options for IT business leaders by advocating open, interoperable hardware and software-defined infrastructure solutions that span the entire IT stack, all in an effort to create business value.

The ONUG community is led by IT business leaders and aims to drive industry dialogue to set the technology direction and agenda with vendors, standards and open source organizations. To that end, ONUG hosts two major conferences per year where use cases are developed and members vote to establish a prioritized list of early adopter, open interoperable hardware and software-defined infrastructure projects that communicate propensity to buy and budget development. The vendor community stages proof of concepts based upon ONUG Use Cases, while standards and open source organizations prioritize their initiatives and investments based upon them. ONUG organizes working groups to fully develop use cases and set industry initiatives. ONUG also hosts user summits and smaller, regional user-focused Fireside Chat Meet-Ups through the year.

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

## Document Scope

The scope of this document is to provide a framework or a way to think about open hybrid cloud deployments from an aggregated cross-industry point of view. The requirements that are set forth in this document are collective among working group member companies. The Open Hybrid Cloud (OHC) framework calls for a set of common services to be delivered by cloud providers. While the impacts discussed are commensurate with the Information Technology Infrastructure Library (ITIL) service delivery model, enterprises can leverage the information to be included in its Request for Information (RFI) to cloud providers and adapt to scale and suit their current or planned organizational support delivery and maturity capabilities.  While the impacts discussed are commensurate with an ITIL service delivery model, enterprises can leverage the information for an RFI and adapt to scale and suit their current or planned organizational support delivery and maturity capabilities.

## Out of Scope

The working group focused its efforts on ***what*** is needed to deliver on important OHC framework components plus a common set of cloud services for the enterprise market. The working group did not focus and does not offer the ***how***; that is, there is no specific protocol(s) or Application Program Interface(s)(API) specified to deliver on the OHC framework. The working group leaves that work to cloud providers and standards communities. ONUG strongly encourages open interfaces and protocols in the construction of multivendor interoperable OHC services and solutions to deliver the greatest value and choice to enterprise IT executives.

## Executive Summary

The Open Networking User Group or ONUG community voted to establish a new working group to develop a framework to communicate best practices for an Open Hybrid Cloud (OHC) use case. Following ONUG Fall 2015 in NYC, hosted by Morgan Stanley and New York University, an invitation-only working group made up exclusively of IT executives was formed. The ONUG OHC working group met every other week and includes IT executives from GE, Citigroup, FedEx, Bank of America, Intuit, Gap, Kaiser Permanente, Morgan Stanley, JP Morgan Chase, et al.--representatives making up a broad cross-section of the global economy.

The ONUG OHC working group framework includes sections on security, technical architecture, contract language/terms/issues, lock-in identification, IT culture/organization design and skill set requirements and, lastly, a set of requirements plus industry recommendations. The goal of the working group is to create a best practice framework in an effort to level the playing field among the largest public cloud providers. The framework identifies a common set of capabilities to be offered by cloud providers, cloud brokers as well as assets that should/could be owned and controlled by enterprise IT.

The ONUG OHC working group framework seeks to commoditize infrastructure and increase choice among enterprise buyers of public cloud services. The goal is to provide the ONUG community with a framework, which identifies a minimum set of common functions and collective requirements that IT business leaders may leverage when consuming hybrid cloud services. One aspect of achieving that goal and provided in this report is to provide a common language to discuss key aspects of hybrid cloud computing for enterprise buyers, regulators/auditors and cloud providers.

The ONUG OHC working group takes the position of being all in on cloud computing as a fundamental service in the delivery of IT services.  Important topics of re-factoring or cloudification of applications, new ways of doing business via cloud delivery, and competition between hardware vendors and cloud providers are not covered in this topic.

The OHC working group offers the following:

1. A common encryption key management approach be provided by hybrid cloud providers or brokers and that key ownership be with consumers;
2. A set of standard foundational services be provided by hybrid cloud providers or brokers, including compute, storage, backup, database, networking;
3. A set of standard northbound orchestration Application Program Interfaces (APIs) be provided by hybrid cloud providers or brokers to facilitate control of cloud services via a consolidated enterprise owned and controlled orchestration software;
4. A standard policy definition and language by hybrid cloud providers or brokers to express workload policy centrally within enterprise policy engines which is then distributed and enforced locally to workload within cloud providers with a full set of audit capabilities;
5. A three-component open hybrid cloud architecture is recommended for large enterprise deployments;
6. Professional negotiators negotiate hybrid cloud service agreements;
7. A need for large scale cloud providers in Asia and Europe.

## Section 1: Open Hybrid Cloud Technical Architecture

In this section, we discuss technical architecture from a building block and control/ownership demarcation perspective. Topics out of scope are data tiering structure and how it's governed from an InfoSec perspective, business continuity and disaster recovery, detailed orchestration API strategy and network function virtualization.

The figure below provides a framework that places technical functions into three categories and identifies ownership demarcation or control domains.  Functions within the blue background are owned and controlled by enterprise IT while cloud providers own yellow functions with joint control between cloud provider and enterprise IT.

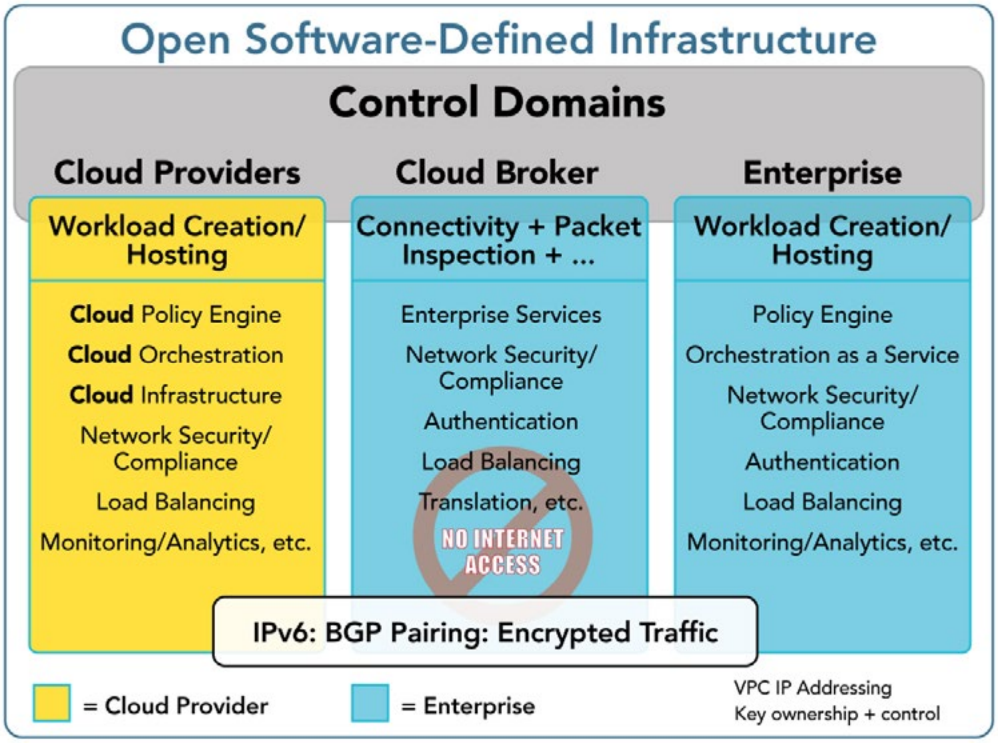
The ONUG OHC working group has created a three-category technical architecture consisting of cloud providers, cloud brokers and enterprise.  One of the goals of this architecture is to build out a data center edge to the cloud broker so as to minimize or mitigate the amount of flows entering deep into private data center infrastructure.

As many network services are becoming virtualized and software based, plus most large enterprise data centers are transitioning toward a software-defined infrastructure architecture, we call this infrastructure that spans cloud providers, cloud brokers and enterprise a ***Cloudified Open Software-Defined Infrastructure***. It's interesting to note that during the late 1990s, service providers and enterprise/government agencies converged on a common internet-based architecture for computer networking. Today, cloud providers and enterprise/government agencies are converging on an Open Software-Defined Infrastructure.

The first set of requirements identified by the ONUG OHC working group focused around connectivity and IP addressing that spans between cloud providers, cloud brokers and enterprise data centers. From a connectivity point of view, the ONUG OHC working group requires:

1) IPv6 is the IP address scheme that spans across all three entities. IPv6 is fundamental to address space support in the era of the industrial internet or machine-to-machine (M-to-M) communications that leverage hybrid cloud resources. Large enterprises expect to see IP address requirements balloon to the hundreds of thousands to millions of IP addresses to support M-to-M and the industrial internet.
2) Virtual Private Cloud or VPC IP addressing is under the control and distribution of enterprise IT.
3) No NATing (Network Address Transitioning).
4) Border Gateway Protocol (BGP) paring or peering for IP routing.
5) Traffic is encrypted end-to-end with encryption key ownership residing with enterprise IT control exclusively.

The IPv6 requirement is clearly one with impact as it spans not only the hybrid cloud architecture, but the enterprise architecture as well. Note that policy in many organizations is IP addressing based. The shift toward IPv6 will break this affinity of IP address-based policy in exchange for managing the device/entity as an infrastructure function.



Open Software-Defined Infrastructure

Control Domains

Cloud Providers

Workload Creation/ Hosting

Cloud Policy Engine
Cloud Orchestration
Cloud Infrastructure
Network Security/ Compliance
Load Balancing
Monitoring/Analytics, etc.

Cloud Broker

Connectivity + Packet Inspection + ...

Enterprise Services
Network Security/ Compliance
Authentication
Load Balancing
Translation, etc.
NO INTERNET ACCESS

Enterprise

Workload Creation/ Hosting

Policy Engine
Orchestration as a Service
Network Security/ Compliance
Authentication
Load Balancing
Monitoring/Analytics, etc.

IPv6: BGP Pairing: Encrypted Traffic

🟨 = Cloud Provider
🟦 = Enterprise

VPC IP Addressing
Key ownership + control

The ONUG OHC technical architecture provides cloud-based services for applications in the low, medium and medium+ categories as identified in section 1.

The following provides descriptions of technologies within each of the three ONUG OHC technical architecture components:

**Cloud Providers:** The cloud provider component may be one or more cloud providers, such as Amazon, Microsoft/Azure, Google, Rackspace, etc. Cloud providers provide workload creation tools and hosting services. Each cloud provider usually provides its own cloud management system that includes policy engine, orchestration tools and virtualized infrastructure, such as security/compliance, load balancing, monitoring and analytics, etc. Access to these cloud management tools is provided to consumers (enterprise IT, DevOps, business unit managers, etc.) via the above architecture. Note that there are "n" cloud providers offering "n" cloud management systems, which are mostly manual, requiring different IT skill sets for each cloud provider's services. Currently cloud provider tools are not integrated into enterprise tool sets.

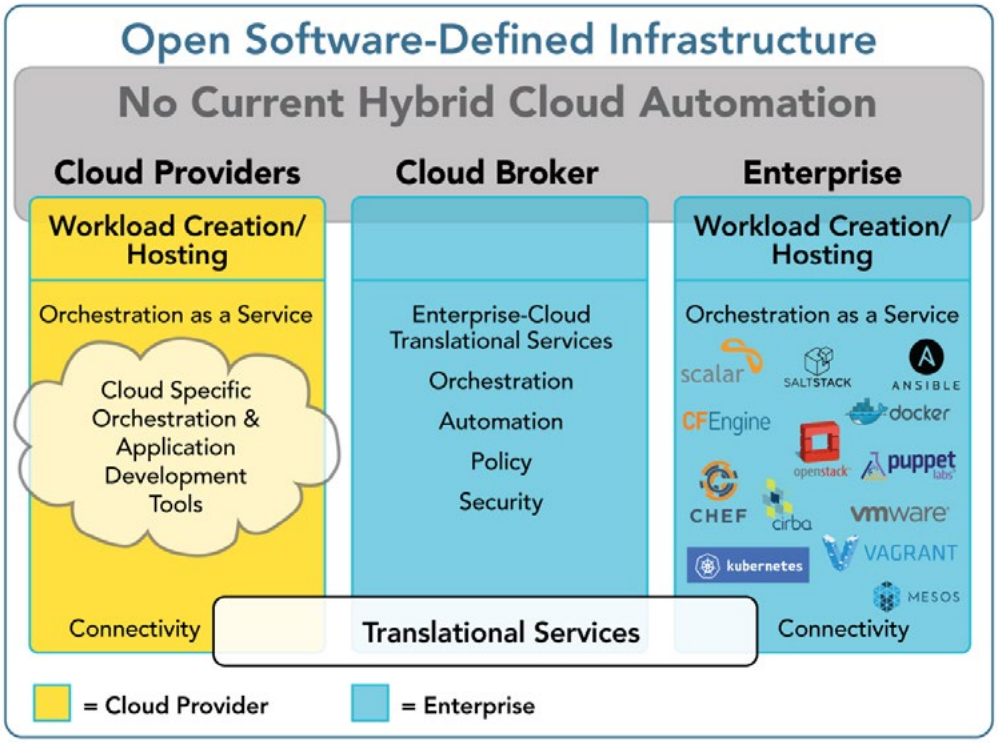
**Cloud Broker:** The cloud broker component is a colocation facility providing exchange point access to multiple cloud providers, bandwidth, cabinets/rack space, operating space, storage etc. There are many companies providing the cloud broker function, including Equinix, AT&T, Verizon, Sprint, et al. The cloud broker is the new "far edge" of a corporate data center reaching into a range of cloud providers. The cloud broker provides colocation real estate and, for most, fiber exchange point access to various clouds providers. The cloud broker importantly provides deep packet/traffic inspection to identify and mitigate exploits and anomalistic behavior before they enter a corporate data center. Packet inspection/scanning or censoring of traffic occurs in the cloud broker to mitigate exploits before entering corporate data centers from cloud providers or exploits trying to do damage to cloud hosted services from private clouds.

In addition, the cloud broker provides common infrastructure services, such as authentication, load balancing, Domain Name System/Dynamic Host Configuration Protocol (DNS/DHCP), Time, Active Directory, Single Sign-On, Intrustion Prevention System (IPS)/Firewall security, monitoring and analytics, etc. This list of infrastructure services is growing, and the more IT is delivered via a cloud solution, the more infrastructure services will be exposed in a very secure way at the edge of the network in the cloud broker.

Being purposefully is important, as extracting enterprise infrastructure services from deep within the corporate data center to the cloud broker stops traffic from traversing all the way down into the enterprise data center, or what most consider is the most protected IT space, is fundamental. Why risk access to this secure space just to provide authentication services, network services, time services, load balance, etc.? These extracted enterprise infrastructure services are architecturally federated back down into the data center core, but these infrastructure services are being moved to the cloud broker because enterprise architects are effectively moving their data centers into a public cloud.

Two objectives drive the decision to move common network services to the cloud broker, and those are: exploit mitigation and cloud performance improvement. In addition to transport plus infrastructure services, translational services that map cloud specific automated orchestration and application development tools to enterprise automated orchestration and application development tools are important cloud broker services. These enterprise services are under the control of enterprise IT and if provisioned correctly, could be common with enterprise IT services. Additional translational services should include enterprise overlay and network service virtualization interoperability and extension into cloud-based overlay plus network service virtualization.

**Enterprise:** The enterprise component is a corporate data center or private cloud infrastructure. Of significant importance to the ONUG OHC technical architecture is policy and Orchestration as a Service (OaaS) so as to facilitate business unit on-demand IT service delivery. The enterprise component consists of all the resources expected within a corporate private cloud including network, compute, storage plus infrastructure services, including security/compliance, authentication services, load balancing, monitoring/analytics, etc.


Open Software-Defined Infrastructure
No Current Hybrid Cloud Automation
Cloud Providers
Cloud Broker
Enterprise
Workload Creation/ Hosting
Orchestration as a Service
Cloud Specific Orchestration & Application Development Tools
Connectivity
Enterprise-Cloud Translational Services
Orchestration
Automation
Policy
Security
Workload Creation/ Hosting
Orchestration as a Service
scalar
SALTSTACK
ANSIBLE
CFEngine
docker
openstack
puppet labs
CHEF
cirba
vmware
kubernetes
VAGRANT
MESOS
Connectivity
Translational Services
= Cloud Provider
= Enterprise

The state of hybrid cloud automation orchestration is that, on the enterprise side, there is very little automation especially around networking. For example, DNS is just starting to get APIs, which is critical for faster provisioning on the cloud side, and load balancing is just starting to be equipped with automation mechanisms. In short, provisioning is mostly a manual process today.

One of the key hybrid cloud computing goals is to provide on-demand IT service delivery to enable business unit managers' creation of workload in either the public or private cloud. One of the largest gaps in hybrid cloud computing is the limited-to-no integration/modules/APIs between enterprise and cloud orchestration systems. Cloud providers Amazon, Microsoft/Azure/Google, et al., have invested heavily in their own orchestration systems. All ONUG OHC working group member companies offer OaaS to their stakeholders. Most leverage automated orchestration software from firms such as Chef, Ansible/RedHat, SaltStack, Scalar, Puppet, Mesos, Kuberbnetes, CFEngine, Cirba, Vagrant and others. Most orchestration is manual today and segmented between public and private clouds. Cloud providers that support OpenStack APIs, Ansible APIs, Puppet APIs, Chef recipe and Vmware's vSphere/vCloud offer hybrid cloud orchestration, but these offerings are limited and proprietary in most cases.

There are standards initiatives to link enterprise and cloud automation orchestration and workload creation tools, such as orchestration APIs, Oasis Cloud Application Management for Platforms (CAMP) programmatic interfaces, yaml/json application definition interface, etc. In addition, cloud providers will increasingly offer APIs from their orchestration systems, such as Amazon's Redshift, that allow enterprise orchestration tools to provision certain aspects of cloud providers' services. These are important developments but are currently limited.

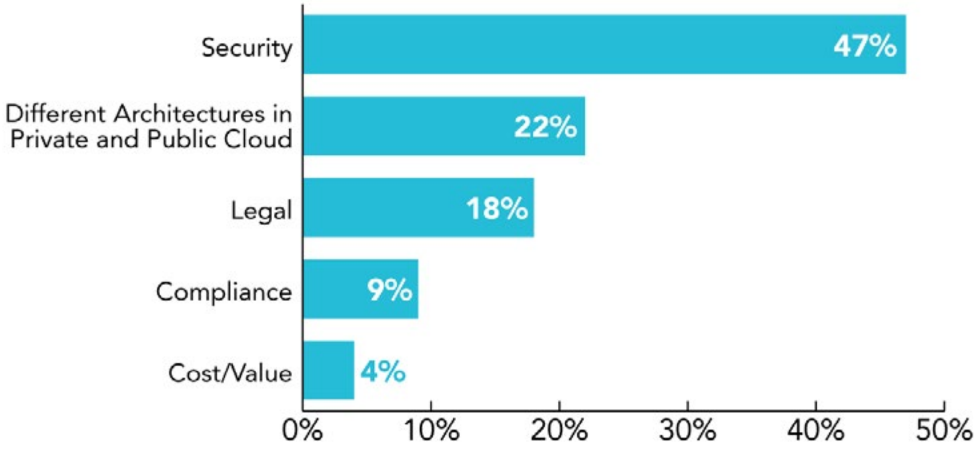
The ONUG OHC working group offers the following best practices for implementing an open hybrid cloud technical architecture:

- Control cloud broker services as a private cloud
  – Cloud broker is part of a corporate network
- Move as many infrastructure services to the cloud broker entity to mitigate the number of flows entering into the core of private clouds
- Enterprise control of IP address administration of public cloud VPC space
- Encrypt traffic end-to-end with key ownership residing within enterprise
- Secure private connectivity between cloud providers and cloud broker via deep packet inspection (DPI), firewall and IPS at cloud broker
- Seek role-based access control of cloud infrastructure services
- Seek OaaS via recipes that are delivered to orchestrate on cloud providers, VMWare and Docker

## Section 2: Open Hybrid Cloud Security

Security is a fundamental service to be integrated into hybrid cloud solutions. During a poll at ONUG Fall 2015, the ONUG community expressed that security is by far the biggest obstacle to hybrid cloud deployment. In response to that poll, the ONUG OHC working group addresses this topic first in this framework.

What are the Biggest Obstacles to Hybrid Cloud Deployment?



Various organizations are developing cloud security constructs. The ONUG OHC working group supports efforts, such as ISO 20071, which details requirements for an information security management system (ISMS) and the Cloud Security Alliance that provides best practices for providing security assurance within cloud computing.

But there are fundamental security gaps, such as inspection tools that span public and private clouds in compute, network and storage resources, security policy engines and their enforcement that spans public and private cloud infrastructure. The ONUG OHC working group expects that cloud security to remain an area of concern for some time with its ongoing review and recommendations conducted within the ONUG Software-Defined Security Services working group. For the ONUG OHC working group, we focus on security tiers mapped into applications.

### Hybrid Cloud Security Tiers

A key attribute of security architecture in OHC is the ability for IT to control and manage inspection of all traffic flows. Inspection points in cloud brokers are a best practice, as detailed in section 2 of this framework. Further, encrypted traffic on an end-to-end basis is a best practice with IT to maintain control and ownership of encryption keys.

In addition to deep packet inspection, encryption and key ownership, the ONUG OHC working group supports the process of classifying applications and/or data into risk categories or tiers. Once data is segmented into risk tiers, appropriate security protection zones are assigned.

Four risk tiers are identified: Low, Medium, Medium+, and High. A posture of untrusted zones is inherent in this taxonomy and is addressed through control and management of traffic inspection technology. Preferred access to public cloud providers is facilitated via a cloud broker with either private lines or Virtual Private Network (VPN) connectivity for the categories below, with the possible exception of externalized web hosting.

| Security Tier | Data | Control Set |
|---|---|---|
| Low | Public | Minimum Set |
| | non-sensitive internal | Traffic DPI inspection and scanning: Especially internet egress flows |
| | | Session broker |
| | | Internet bound traffic routed back to proxy |
| | | Multifactor authentication |
| Medium | Confidential | All of low + |
| | SOX, Critical Apps | Critical Control Set |
| | | ISO 27001 |
| | | Traffic DPI inspection and scanning: Mandatory internet egress flows |
| Medium+ | US Only | All of Medium + |
| | Gov't CUI (Controlled Unclassified Information) | US Person Support |
| | Export Control | |
| High | Restricted | Internal standards |
| | IP | |

The following provides a description of the categories identified within the matrix.

**Low:** The low-risk tier catalogs applications and/or data as public, non-sensitive information. External customer-facing information or website applications/data falls into the low-risk category. This tier is appropriate for native public cloud hosting. The low-risk tier contains a security protection zone that is the most lenient. However, traffic on route to a public cloud is by way of a specific inspection zone within a cloud broker, where the inspection of this traffic is to be managed by IT in the inspection zone, a sort of DMZ. In addition, VPC access to the cloud provider is configured to mitigate against flow/reach back of internet traffic entering the enterprise from cloud provider. In addition to DPI and packet scanning within cloud brokers, IT executives choose to deploy host inspection tools that allow IT operations to inspect host in both public and private cloud.

**Medium:** The medium-risk tier catalogs applications and/or data as confidential, and as such, its risk profile is higher as is its security controls. For medium-risk tier applications/data, VPC's are tightly managed with limited control domains. Internet reach back is highly mitigated in this tier. Traffic heading to the corporate data centers pass through an inspection zone for DPI plus scanning via IPS within a cloud broker. Further, internet-bound traffic is routed back to a proxy. Authentication is facilitated via multi-factor authentication.

Examples of applications that could be placed in the medium-risk tier are aspects of Enterprise Resource Planning (ERP) business management software. That is, some applications that are used to run the business, but not intellectual property or patent data for example, as this would be classified into the high-risk category.

Security technologies in the medium-risk category include all low category security controls plus mandatory DPI plus scanning of flows from internet bound to internal data centers, multi-factor authentication, firewalls and IPS.

**Medium+:** This medium+-risk tier is assigned to applications and/or data that contain higher sensitivity, such as government-controlled unclassified information, export control, DoD data, regulatory compliance attributes, etc. This tier includes data that cannot be moved outside of national boundaries. GovCloud services is a landing zone for this category of traffic.

**High:** The high-risk tier contains applications and/or data that are restricted to internal corporate use exclusively and are to be hosted on internal/private data centers. For example, patents, critical business process, sensitive financial information and applications, plus unstructured data fall into this category.

IT orchestration and provisioning related management applications and data may be categorized in the medium- or high-risk tiers.

IT organizations may consider cataloging their application risk tiers by considering application criticality and application-less data criticality/sensitivity perspectives. In addition, level of business impact if breached, lost, unavailable, etc., scenarios is another useful lens in which to review applications during the cataloging process. If the application and/or data is not tied to intellectual property, and it can be hosted in a DMZ, then it probably falls into the low category. While cataloging is subjective for every company, it's advisable to engage business units to participate based on guidelines. Based upon the ONUG OHC working group, most applications fall under medium-risk tier.

### Key Management and Distribution in the Era of Hybrid Cloud

There are multiple key management approaches available--some standard and some proprietary. Independent upon which approach or key management technology employed is who owns and controls encryption keys. This is a contractual and technical architecture issue. Some allow their public cloud provider to hold the key, but the key belongs to the enterprise. The key is encrypted, thus the cloud provider cannot use the key, but this is a particular concern as there could be a blind audit of the cloud provider, which increases the possible risk of corporate data in the cloud being exposed. Many corporations will keep more applications in the high-risk tier, thanks to issues around holding of encryption keys, unless IT has total responsibility and control of key management.

The following is a list of common security requirements that fall under the control of IT executives and are provided by cloud providers or cloud brokers. Some of the following may be provided by cloud providers or cloud brokers, but are exclusively controlled by IT executives.

- Access controls and auditability
- Event management and alarming
- Confidentiality, policy management
- Isolation/separation of workload within cloud provider and cloud broker
- Support from a network security perspective:
- Alerts, logging, based on security rules, such as change of infrastructure (authorized, or non-authorized) that span across public and private cloud
- From cloud providers or translational services from cloud brokers support for:
- Network Function Virtualization functions for Intrusion Detection System (IDS)/IPS and firewall
- Distributed Denial of Service (DDoS) Function and Noisy Neighbor control
- Virtual machine security control (capability like hyTrust)

- Identity federation (SAML, oAuth, etc.)
- Multi-factor authentication
- From cloud providers:
- Ability to monitor privileged access and activities for admins with access to cloud management
- Ability to provide environmental segregation (dev/test/prod)

## Section 3: Open Hybrid Cloud Lock-in Identifiers

In this section, the ONUG OHC working group members identify key hybrid cloud lock-ins. The ONUG OHC working group also provides general guidance to mitigate against such cloud lock-ins. In future versions of this document, the working group may offer technical approaches or strategies for lock-in mitigation. We offer this list of cloud provider lock-ins to bring awareness to the ONUG community. Note that these lock-ins are not nefarious. It's important to note that hybrid cloud computing is a relatively new approach to IT service delivery and as such, many cloud providers and cloud brokers have developed solutions ahead of standards or open source code availability, which is to be expected and, at times, beneficial. Be it as it may, these are paths to being locked-in.

- Workload creation tools
- Non-standard orchestration tools between Enterprise-Cloud
- Non-standard Provisioning/Scheduling/Automation tooling between enterprise-cloud
- Data mobility: High cost and complexity to move data between cloud providers and Cloud-Enterprise
- The higher level of cloud services used, the more proprietary--on average
  - Cloud bursting is a good example.
- There is a high barrier of market entry; that is, large enterprise Capex spend plus complex managed service contractual negotiation
- Cloud broker lock-in: lack of open source solutions
  - Cloud broker translational services tend to be proprietary

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

### Hybrid Cloud Lock-in Mitigation and Buyer Beware

In addition to the above lock-in identifiers, there is a set of buyer beware topics identified by the working group--compliance being one of these buyer beware topics. The concept of compliance is fundamental in regulated industries, and cloud service providers are behind the curve in offering auditable compliance reporting. For example, workload that is provisioned within a cloud provider needs to demonstrate and communicate to auditors who may have access to this workload and workload data. That is, once a virtual machine, for example, is purchased and provisioned in the cloud, what assurances are there that a cloud provider employee or cybercriminal can't destroy it, recreate or copy it, modify it, add something into it, take something out of it, create a backdoor to it, etc.? What assurances can the cloud provider offer, in an auditable way, to assure that someone or something does not have access to enterprise-owned cloud-hosted asset? That is, what is the integrity, auditability of the cloud-provisioned asset? It's not good enough to have control over the asset's integrity but that control must be demonstrated to an auditor.

In addition to compliance as a buyer beware, the following are also buyer beware:

- Know what you are buying
  - Cloud brokers offer access to multiple cloud providers but each cloud provider requires different connectivity and security postures requiring unique micro-segmentation per cloud provider
  - All cloud providers are not the same, each have unique attributes, strengths and weaknesses
- Understand geographic differences between cloud providers
  - Awareness of suboptimal routing
- Expect delays since most auditors are in a steep cloud computing learning curve

Hybrid cloud is a new IT delivery mechanism, and the industry will continue to journey toward a cloud path. However, cloud provider lock-in can be mitigated, and the best current approach is to hold onto to those essential infrastructure services that are core to your business, core to the security of your network and core to your enterprise data center. In short, maintain absolute control of technologies that secure networks while infrastructure services move to cloud broker placement in the new data center edge where enterprise control is assured. Do not move essential and all security infrastructure services all the way into a cloud provider, as this will assure being locked-in to that cloud provider. Lock-in mitigation is currently about maintaining total control of infrastructure services and keeping them within the private cloud umbrella. The more those move into the public cloud, the more lock-in is created.

## Section 4: Legal/Compliance/Contract Language

In this section, the working group focused on best practices when negotiating public cloud multiyear service contracts. The approach of being descriptive was eliminated as different industry sectors have unique regulatory, compliance and audit requirements. Some industries require Payment Card Industry (PCI) compliance, Health Insurance Portability and Accountability (HIPAA) compliance, Protected Health Information (PHI), Presidential Policy Directive on Critical Infrastructure (PPD-21), Sarbanes-Oxley (SOX) compliance, etc. The following section provides the top best practices as discussed by the ONUG OHC working group.

**Look Beyond Website Pricing:** All members of the OHC working group negotiate directly with various public cloud providers for service and seldom rely upon cloud provider website pricing. Cloud provider service contract negotiation is a long-term process as they are encompassing and detailed.

**Engage Professional Negotiators:** Depending upon industry sector, negotiating public cloud service provider multiyear contracts can take as long as 18 months and cost hundreds of thousands of dollars in legal fees.  A common best practice is to engage professional negotiators to negotiate public cloud service contracts. These professionals could be in-house legal staff or external.

**Cloud Service Contracts ARE NOT Outsourcing Contracts:** Public cloud-managed service contracts are different than existing boilerplate contracts used for classic outsourcing arrangements as liability, auditability, attestation, etc., are different in the cloud world. That is, the amount of auditability and attestation is completely different in the cloud world than in either insourcing or outsourcing contracts. In other words, public cloud service agreements are not classic outsourcing arrangements--meaning that even if your company has experience with outsourcing, this is different.

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

**Licensing:** Software licensing needs careful consideration once public cloud providers are engaged; for example, placing a database in the public cloud could impact existing corporate licensing agreements. Licensing may be based upon the number of CPUs that the software is accessed by which may increase significantly once the application is placed in the cloud where more employees, et al., can now access. International access to licensed applications will also be impacted. Licensing will also impact indemnity.

**Auditability and Attestation:** Most large public cloud providers are just starting to discuss the topic of auditability and attestation. From an accounting point of view in an audit, an accountant expresses an opinion as to whether or not a set of financial statements is presented fairly with respect to the generally accepted accounting principles. In an attestation engagement, an accountant expresses an opinion on the reasonableness of a particular assertion or set of assertions. Examples of assertions covered by attestation engagements include financial forecasts and compliance with laws or procedures. From a cloud computing point of view, auditability is focused upon how much are consumers/auditors/IT executives going to be able to see under the public cloud provider covers to facilitate auditability of compliance. Further, public cloud providers may also provide attestation or a type of certification of its operations in the way they operate in compliance to various regulations.

**Compliance Officer Training:** Auditors are just starting to understand cloud computing, and this training gap can create frustration. The language of cloud computing and location of assets is foreign to many auditors.  Many have not been trained to understand the difference between physical and virtual servers and the agility that accompanies software-defined infrastructure. This translates into difficulty in demonstrating compliance. Cloud providers would be well served if they provided training programs and tools, such as CyberArk, for auditors and IT executives. This issue creates a daily battle for many large enterprises wishing to do business with cloud providers.

**Engage a Qualified Security Assessor or QSA:** A large part of the cloud service provider contract is to understand risk and mitigate this risk as much as possible. Scenarios, such as protections for data at rest, and who owns that data if the cloud provider becomes defunct or is comprised, need to be thought through carefully. A QSA is helpful to identify vulnerabilities.

**International SLA or Service Level Agreement:** SLA language is difficult to create with cloud service providers when workload is to be distributed throughout the world. For example, if an outage occurs in one geography and the cloud provider wishes to push that workload to another data center around the world; however, there may be government restrictions that prevent the transmit of such data through various countries/governments, then meeting SLAs could be compromised. Clearly if workload stays within the U.S., then SLA definition is much easier; however, when workload and data transit the U.S., SLA definition and even taxation issues arise, increasing the level of difficulty in contract language.

**Liability:** Liability of cloud providers is a point of discussion in current managed service contracts. For example, in outsourcing arrangements, liability can cover losses and damages or liability up to the value of the outsourced asset. Cloud providers, however, seek liability to cover the dollar amount spent. That is, if a company spends $50,000 per year with a cloud provider to host an application and experiences damages of $10,000,000, the cloud provider seeks its liability to cover $50,000. This level of liability will limit the type of applications that will migrate to cloud providers to the low- to medium-risk levels.

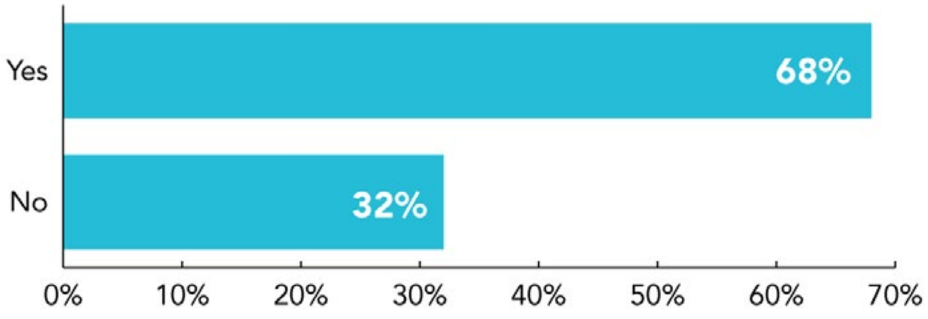
## Section 5: Skill-set/Operational Model Challenges

One of the biggest issues in deploying hybrid cloud solutions is that of skill sets and IT organizational culture. Most IT organizations are organized around silos of IT, such as compute, network, storage, applications, DevOps, virtualization, etc., while IT organizations are exploring different organizing models such as full-stack organizations where IT skills are not siloed but mixed including a silo skill set along with programming skills such as Python. That is, a network engineer would have some level of proficiency in storage or compute, or DevOps, or a programming language in addition to his/her deep network engineering skills.

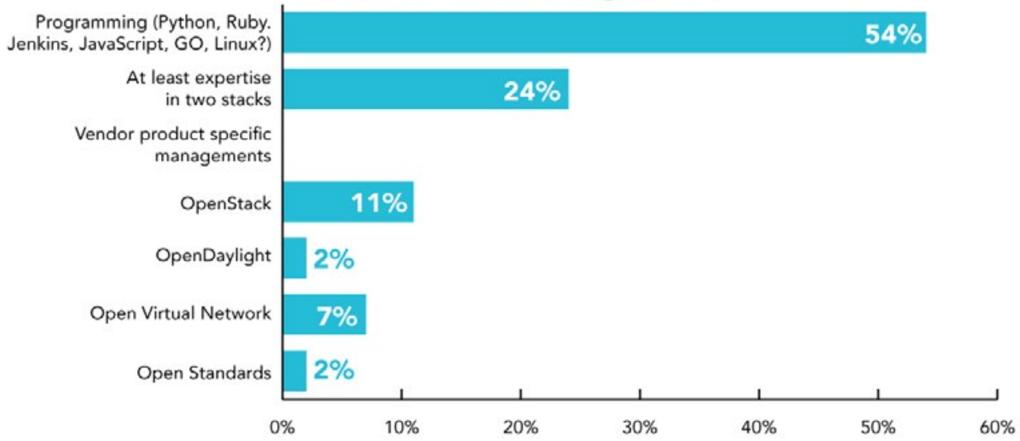
At previous ONUG meetings, the community has voted that 68% of hiring managers are still hiring Cisco Certified Internetwork Expert (CCIE) skill sets into their IT organizations. In addition, 78% of hiring managers voted that programming skill sets, such as Python, Ruby, Jenkins, JavaScript, GO, etc., and at least expertise in two stacks are required for new hires into full-stack engineering roles.

From the above data and the OHC working group members, it became clear that skill sets and new tools are needed to design, build, deploy and manage open hybrid cloud infrastructure. IT engineers are becoming multi-disciplined with storage engineers knowing some network, network engineers knowing some compute and compute engineers knowing some storage, although each expertise possesses a deep skill set in one area.  However, what

Are You Still Hiring CCIE Skill Sets?



they don’t have are common methods to operate and provision hybrid cloud or software-defined infrastructure. That is, what is lacking in today's IT organization is programming skills in which to perform data gathering for troubleshooting, optimization, etc. In short, skills to operate in various cloud models are lacking.


What is the Most Important Skill Set Needed for a Full-Stack Engineer?

The age of specialization within a silo is changing. As more and more large corporations adopt open hybrid cloud and private cloud infrastructure, a new IT specialization will emerge. The way in which IT service is delivered and managed is fundamentally changing, and IT organizations need this new specialization. That is, IT organizations will not need engineers with Command Line Interface (CLI) skills but those with programming skills.

Yet the cloud cycle is early on, and the industry hasn’t standardized and simplified cloud infrastructure to the point of commoditization where IT organizations don’t need IT technical staff who specialize in network, or security, or load balancing, or storage anymore. These skills are still needed. That is, cloud infrastructure has not simplified anywhere near to the point that all skill sets converge to one person who can do everything.

Cloud infrastructure promises to simplify/abstract IT so that IT organizations gain operational efficiency with fewer skills needed to manage more IT service delivery; however, while the industry is on this path, it is not there yet.

For example, there are people who know how to program, or know how to deliver infrastructure for trading systems, and they are not the same people who deliver a web’s front end of the internet. There are different specializations. They might all use the same C++ tools, open source tools on github, etc. This is the change that’s coming to network infrastructure in particular; that is, we still need people who know how routers, switches, load balancers, firewalls, etc. work, but knowing their way around a particular router or switch is not important.

IT will still need network engineers who know what routing means, and why one would use BGP instead of RIP (Routing Information Protocol), etc. Understanding network architecture choices is a highly needed specialization within the large enterprise. The ONUG community loathes to forgo the learning of the last ten years. This history and evolution of network architecture is fundamental to stable IT service delivery. Even to this day, many IT organizations discuss architecture choices, such as the use of Standing Tree to deliver IT mobility across a large layer two domain, but forget how this approach does not scale.

### The Full-Stack Organization

The OHC working group’s view on organizational design is based upon a need of multiple skill sets or specialties with a collaborative culture to deliver cloud-based IT. It’s unrealistic that a full-stack engineer exists; that is, there are too many specialties required for one person. This full-stack perspective is best manifested in an organizational culture made up of mixed skill sets. In the near term, many are creating cloud organizations populated with those of different IT skills in the hope that over time a full-stack organization will emerge with the right incentives and culture guiding it.

These cloud groups may include those with specialization in DevOps, routing, load balancing, programming, firewalls, etc. Some working group members find that this approach leads to increased specialization crossover. As staff are removed from silos where a common skill set is the norm to a mixed specialization organization, it's much easier for an executive to transition from a network specialization to a compute specialization, or virtualization, etc. By pooling mixed skill sets into a collaborative cross specialization culture where taking on new skills is encouraged, a new full-stack organization emerges.

Some have started full-stack organizations by each siloed organization donating one of its personnel to the new group, which starts to build upon different knowledge bases. This knowledge base expansion becomes the root of the culture. The knowledge base becomes important and fundamental to the full-stack organization. The first phase is obtaining agreement upon donating the specialization with the overall goal being that the knowledge base will expand significantly and permanently over the next five years. The full-stack organization is focused on collective skill-sets and the creation of a deep knowledge base that’s equipped to design, build, manage and troubleshoot cloud-based applications that span the full-stack.

While it’s not the expressed goal of a full-stack organization, but an expectation that as cloud-based tools become available and the knowledge base becomes operationalized, IT organizations may not have as many people who need to specialize. Therefore, the overall headcount to support the infrastructure would reduce. In other words, the number of specialized IT operational engineers needed to support some amount of infrastructure devices will decrease. That is, an IT engineer should be able to manage many more devices than today--safely. For example, at ONUG today, one network engineer usually manages less than 200 devices, but in the future that engineer should be able to manage 1,000s to tens of thousands of physical and virtual devices, and those devices could be network, storage or compute.

### Framework Requirement Term Definitions

The following conventions are used in the following section. The requirements that apply to the functionality of this document are specified using the following conventions. Items that are REQUIRED (contain the words MUST or MUST NOT) will be labeled as [Rx]. Items that are RECOMMENDED (contain the words SHOULD or SHOULD NOT) will be labeled as [Dy]. Items that are OPTIONAL (contain the words MAY or OPTIONAL) will be labeled as [Oz]. In addition, a priority value of High (H), Medium (M) or Low (L) may be assigned to each item.

The priority will be labeled as [RHx], [DHy] or [OHz] for High priority, [RMx], [DMy] or [OMz] for Medium priority or [RLx], [DLy] or [OLz] for Low priority. The integer values {x, y, z} shall be unique across the document but are not required to be unique across the 3-tuple set {x, y, z}. For example, RM10 and DM10 are allowed whereas RM10 and RL10 are prohibited. Requirements in this document are numbered using increments of 10.

Where needed, related sub-requirements are numbered using increments of 1. The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY” and “OPTIONAL” in this document are to be interpreted as described in Request for Comments (RFC) 2119. All key words use upper case, bold text to distinguish them from other uses of the words. Any use of these key words (e.g., may and optional) without [Rx], [Dy] or [Oz] is not normative. The priority assignments are defined as follows:

**High (H):** Functionality that must be supported at day one and is critical for baseline deployment.

**Medium (M):** Functionality that must be supported, but is not mandatory for initial baseline deployment.

**Low (L):** Desired functionality, which should be supported, but can be phased in as part of longer-term solution evolution.

## Section 6: Industry Recommendations and Hybrid Cloud Provider Requirements

In addition to the requirements and recommendations detailed below, it's recommended the ONUG Software-Defined Security Services working group white paper and associated recommendations be reviewed as it contains pertinent security recommendations for hybrid cloud and private cloud workloads. This white paper can be found on the ONUG website opennetworkingusergroup.com

The following provides industry recommendations for a set of common services to be delivered by all cloud providers for buyers of open hybrid cloud services in the enterprise marketplace. It is encouraged that ONUG community members use these requirements and recommendations within their Request for Quote for hybrid cloud services adapted to scale and suit their current or planned hybrid cloud service needs.

**R-10-Encryption Key Management and Ownership:**
A common key management approach to protect data and encryption key control/ownership options must be provided by all cloud providers. Key management that enables secure communication between policy enforcement mechanism and security policy control plane should follow key management guidelines, such as those offered by SANS Top 20 Critical Controls, NIST in the U.S. and the various European country-specific specifications embedded in ISO 27002:2013, officially entitled "Information technology — Security techniques — Information security management systems — Requirements."

**R-20-Standard Foundational Services:**
A common standard approach to a set of foundational services, including hosting, compute, backup, storage, database and networking including DNS, DHCP, NAT, must be provided by all cloud providers offering open hybrid cloud service to the enterprise market.

**R-30-Standard Northbound Orchestration APIs:**
A common set of northbound APIs that abstract cloud provider operating/management systems to enterprise IT orchestration systems must be delivered by cloud providers offering open hybrid cloud service to the enterprise market. The goal of R-30 is to control all cloud services via a consolidated enterprise owned and controlled orchestration platform.

OPEN HYBRID CLOUD
WORKING GROUP
2016
Open Networking
USER GROUP

**R-40-Standard Policy Definition and Language:**
A common/standard approach to policy definition and language must be provided by cloud providers of open hybrid cloud services to the enterprise market. The goal of R-40 is to express workload policy centrally within enterprise policy engines which are then distributed and enforced local to workload within cloud providers with a full set of audit capabilities.

**D-10-A Three-Component Open Hybrid Cloud Architecture:**
It is recommended that large enterprise customers implement a three-component architecture, including cloud provider, cloud broker and enterprise data center. It's further recommended that IT business leaders consider that IT assets be owned and operated by enterprise IT within cloud broker and enterprise data center.

**D-20-Professional Negotiators:**
It is recommended that IT business leaders seek professional negotiators to assist in the negotiating of hybrid cloud service agreements.

**D-30-Cloud Provider in Asia and Europe:**
The ONUG OHC working group observes the need for a large cloud provider on the order of scale and stature of AWS, Azure or Google Cloud Platform in Asia and Europe geographic theaters that possesses and offers the above requirements. This recommendation addresses a requirement for commonality of hybrid cloud service delivery and consumption on a global scale. Currently, there is no uniformity of cloud provider services within various world geographies.

**D-40-Place Applications into Low-, Medium-, Medium+- and High-Risk Tiers:**
It is recommended that IT organizations catalog their applications into risk tiers as a means to determine which applications may be hosted by cloud providers in an open hybrid cloud infrastructure.

## Glossary

**Public Cloud:** The public cloud is defined as a multi-tenant environment, where an organization buys a "server slice" in a cloud computing environment that is shared with a number of other clients or tenants.

**Private Cloud:** Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to a single organization.

**Internal Cloud:** An internal cloud is a cloud computing service model that is implemented within an organization's dedicated resources and infrastructure. Internal clouds apply virtualization mechanisms, shared storage and network resources to facilitate full control of an organization's cloud computing environment.

**External Cloud:** An external cloud is a cloud solution that exists outside of an organization's physical boundaries. It can be private, public or community-based, as long as it is not located on an organization's property. An external cloud is similar to a public cloud, but they differ in implementation.

**Virtual Private Cloud:** A Virtual Private Cloud (VPC) is an on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as "users" hereafter) using the resources.

**Platform as a Service:** Platform as a Service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.

**Software as a Service:** Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software." SaaS is typically accessed by users using a thin client via a web browser.

**Infrastructure as a Service:** Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS).

## ONUG Open Hybrid Cloud Working Group Members

| | | | | | |
|---|---|---|---|---|---|
| Nick Lippis, Chairman | Open Networking USER GROUP | Gene Sun | FedEx. | Stephen Gannon | JPMORGAN CHASE & CO. |
| Mike Elmore | Cigna. | Carlos Matos | Fidelity INVESTMENTS | Andy Lee | KAISER PERMANENTE. |
| Ali Iloglu | citi | Snehal Patel | Gap Inc. | Mayur Mistry | KAISER PERMANENTE. |
| Harmen Van der Linde | citi | Chris Drumgoole | GE | John Storm | Morgan Stanley |
| Vesko Pehlivanov | CREDIT SUISSE | Joe Ferrell | GE | Nelson Tai | Pfizer |
| Aryo Kresnadi | FedEx. | Pablo Espinosa | intuit | Jim Younan | UBS |

OPEN HYBRID CLOUD WORKING GROUP 2016

Open Networking USER GROUP