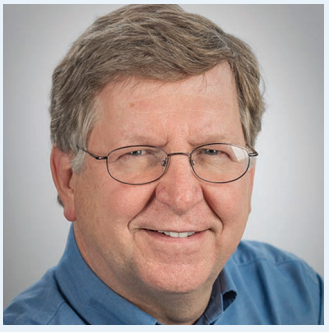
Cloud Standards as Roadmaps for Migration

IN PREVIOUS ISSUES, I'VE EXPLORED TOPICS RELATED TO THE GENERAL LANDSCAPE OF STANDARDS AND HOW THEY DEVELOP. I've talked about some specific cloud-native standards, such as the Open Cloud Computing Interface (OCCI, http://occi-wg.org); the Topology and Orchestration Specification for Cloud Applications (TOSCA, www.oasis-open.org/committees/tosca), the Cloud Data Management Interface (CDMI, www.snia.org/cloud/cdmi); the Open Container Initiative runtime specification, image format, and associated runc command line tools (OCI, www.opencontainers.org); and several other active standardization efforts that are in various stages of implementation and usage in cloud computing.

ALAN SILL

Texas Tech University,
alan.sill@standards-now.org



There are many challenges related to the sheer breadth and scope of the landscape of cloud computing that make it impossible to develop a single standard that covers all varieties of activity. Despite these challenges, as I predicted in previous articles, cloud standards are in fact emerging. Beyond those just mentioned, another successful example of the strong emergence of cloud standards is provided by Amazon Web Services' recent announcement that its API Gateway products would increase the level of support provided for direct use of the API standards Swagger and the Restful API Markup Language (RAML).[1]

In late 2015, the Swagger specification was donated to the OpenAPIs Initiative (https://openapis.org), being run by the Linux Foundation with the backing of many active cloud companies and projects. These developments confirm the potential for adoption of cloud API standards as a precursor to and positive indicator for other cloud standards successes.

In this issue, I'll tackle further issues directly related to migration to the use of cloud methods, and survey these topics from a standards perspective. Because cloud services form the basis for an increasing fraction of conventional business services, many aspects of their use are not only increasingly based on standards, but are also now becoming targets for regulation, especially with respect to the use, storage, and protection of data. I'll summarize some recent activities in this area and their resulting implications for compliance.

Patterns of Migration

In human and animal societies, population migration takes place through several distinct patterns. The term "migration" generally implies a transition from one location to another. In cloud terms, such transition implies movement of workloads from one hosting environment to another.

Types of migration in the human or natural world that could have analogies in this context include nomadic, sporadic, periodic, or permanent displacements. These can be distinguished from each other by the frequency—for example, one-time versus occasional migrations—and in the case of multiple migrations, the regularity or predictability of the interval between the occurrences.

2325-6095/16/$33.00 © 2016 IEEE

Migration in the animal kingdom is usually periodic, based on regular patterns of weather or conditions related to the population life cycle. In the cloud context, however, migration is usually considered in terms of a one-time shift of working styles and modalities from an older type of information technology delivery to cloud-based methods. The starting state for this migration could be an on-premises physical infrastructure or an externally contracted service, but is more likely to be the former. The ending state after cloud migration is more likely to be externally contracted, but could involve user-owned or hybrid cloud resources. (See the January/February 2016 issue of *IEEE Cloud Computing* for articles on hybrid cloud deployments.)

Migration can further be subdivided into preplanned, opportunistic, or emergency categories. An example of the latter category that's relevant to clouds is disaster recovery or emergency response that results in the need for failover. An example of the opportunistic category is migration from one provider to another driven by cost or by reasons related to technology fit.

A preplanned, permanent, one-time move from traditional information technology to the cloud currently dominates discussions and user patterns. As time goes on, we might see more examples of nomadic, opportunistic, or even emergency migration behavior. Some combinations of these types and categories of migration are more likely than others; periodic preplanned migration seems unlikely, for example.

Before deciding on a physical journey, it's usual and even advisable to consult maps and the experiences of others who have made the trip before. These days, review sites and advertising are available for nearly any destination on the globe, and guidebooks (both physical and electronic) exist.

The single most important factor governing the decision to shift important business functions to the cloud appears to be trust. This factor includes considerations of trust related to the reliability, security, and predictability of the behavior of cloud vendors, and other considerations related to how governments and users will respond to changes in the nature of service delivery that result from shifts to cloud-based services.

As standards emerge to establish predictability in the patterns for use and for interconnection of cloud services, they can form the basis for the type of regulation that both encourages innovation and also helps to establish trust. Some standards are already in place to govern protection and use of data in cloud services. These and others that are still being written are necessary components to provide a roadmap for future migration and for the trustworthy use of the cloud.

Standards Advisory Groups, and Advisory Activities of SDOs

Several domain-specific advisory groups are active in cloud computing. These include some organizations that exist specifically to prepare guidebooks and white papers that aim to provide advice, rather than to set standards on their own. Examples include the Cloud Standards Customer Council (CSCC, www.cloud-council.org), the Cloud Security Alliance (CSA, https://cloudsecurityalliance.org), and the Open Data Center Alliance (ODCA, https://opendatacenteralliance.org).

> Trust appears to be the most important factor governing the decision to shift important business functions to the cloud.

Each of these organizations publishes guidance, usually prepared by members or representatives of member companies and organizations, that's available either free or for a fee to nonmembers. Table 1 lists some examples of guidance documents. In each case, many more documents of this nature are available at the websites of the respective organizations, as well as from other similar organizations. The table includes examples that are particularly relevant to the topic of cloud migration. A larger list of cloud-relevant standards organizations and efforts

Table 1. Guidance documents for cloud usage from several advisory organizations.

Organization	Document	URL
Open Data Center Alliance	ODCA Master Usage Model: Compute Infrastructure as a Service (ClaaS) Rev. 2.0	https://opendatacenteralliance.org/docs/compute_infrastructure_as_a_service_rev_2.pdf
	ODCA Master Usage Model: Scale-Out Storage Rev. 1.0	https://opendatacenteralliance.org/docs/Scale_Out_Storage_Master_Usage_Model_Rev1.0.pdf
Cloud Standards Customer Council	Migrating Applications to Public Cloud Services: Roadmap for Success	http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf
	Migrating Applications to the Cloud: Assessing Performance and Response Time Requirements	http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-the-Cloud-Assessing-Performance-and-Response-Time-Requirements.pdf
Cloud Security Alliance	Best Practices for Mitigating Risks in Virtualized Environments	https://cloudsecurityalliance.org/download/best-practices-for-mitigating-risks-in-virtualized-environments
	Security Considerations for Private vs. Public Clouds	https://cloudsecurityalliance.org/download/security-considerations-for-private-vs-public-clouds

is available at the Cloud Standards Wiki at http://cloud-standards.org.

Beyond guidance documents of the type listed in the table, the Cloud Security Alliance has also begun to write protocols and specifications of its own, and has formed an internal international standardization council "to coordinate all aspects of standardization efforts within CSA." Many of the organizations listed in the Cloud Standards Wiki also develop specifications, at various levels of formality, that are intended to be useful in cloud settings.

Another pattern of activity that can be pursued either by organizations or individuals is the development of a profile that documents a selection of one or more standards that resolve ambiguities, or that makes definite recommendations or specifications for choices among multiple options for their use. Profiles can be and often are developed and published by organizations other than those that developed the original material they reference.

Government advisory organizations also exist. Within the United States, the National Institute of Standards and Technology (NIST) tracks, encourages, and contributes information to the activities of formal standards developing organizations (SDOs) and advises government agencies on the current state of SDO activity. Other special-purpose organizations exist in different agencies for similar purposes, such as the Defense Information Systems Agency (DISA), with missions that are directly related to their branch of government.

NIST endeavors to conduct a large portion of its work through public working groups and direct involvement in activities of relevant SDOs. Its reports, while generally not presented as standards in and of themselves, are free, usually comprehensive, and widely consulted by other organizations throughout the world. There are equivalent bodies in most other countries. NIST has published several foundational documents in the cloud computing arena, including its widely quoted initial Definition of Cloud Computing,[2] as well as a Reference Architecture[3] and Standards Roadmap.[4]

DISA is an example of a government agency with a slightly different mission. Its charter includes the responsibility to advise the various branches of the US military on required and permitted standards to be used in purchasing and contracting for information technology services. As part of this mission, DISA maintains an Information Technology Standards and Profile Registry (www.acqnotes.com/acqnote/careerfields/dod-information-technology-standards-and-profile-registry), which must be consulted in planning for any related project or purchase.

Another example of this type of government agency activity is the Office of the National Coordinator for Health Information Technology (ONC), which operates an Office of Standards and Technology that publishes an interoperability roadmap and a formal annual Interoperability Standards Advisory (www.healthit.gov/policy-researchers-implementers/interoperability) summarizing best available standards and implementation specifications in the area of healthcare information technology.

Similar government and government-related advisory and survey activities have taken place throughout the globe. In Europe, efforts to create a "digital single market" with a level playing field for multiple cloud providers have led the European Commission to sponsor studies and reports on cloud standards for several years. Among the most notable of these have been the cloud standards coordination and survey reports issued by the European Telecommunications Standards Institute (ETSI),[5] the Standards and Interoperability for eInfrastructure Implementation Initiative (SIENA),[6] as well as a set of position papers from European cloud-related projects and organizations gathered through a related series of CloudScape conferences (www.cloudscapeseries.eu/position-papers).

In the Asia-Pacific region, the Asia Cloud Computing Association (ACCA, www.asiacloudcomputing.org) publishes a series of documents on cloud topics. Of these, the most interesting to me has been its recent report on financial service industry (FSI) regulations impacting cloud service providers and customers in markets in that area of the globe.[7]

In addition, beyond official standards and specifications, some formal SDOs publish overview documents on their own that aren't intended to set standards, but that serve as building blocks for future efforts. Such documents either survey overall considerations in a particular area or serve to establish common vocabularies and ontologies among concepts.

Formal SDOs and Compliance

The most formal of the international SDOs active in this area, as documented in earlier columns, are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunications Union-Telecommunications Standardisation Sector (ITU-T). So far, because of the complexity of the cloud technology space and its rapid pace of change, these organizations have limited most of their work to areas of general guidance, as mentioned earlier, and have issued few detailed specifications aimed at particular portions of the cloud technology spectrum.

The ISO and IEC operate a long-standing Joint Technical Committee 1 (JTC1) on Information Technology whose work is directly applicable to cloud computing. Within this work, its Special Committee 38 (SC38) on Cloud Computing and Distributed Platforms has been especially useful, although other special committees in JTC1 are also relevant. SC38 has, for example, published a cloud computing overview and vocabulary[8] and a reference architecture,[9] and has work in progress in the areas of service-level agreements, interoperability and portability, and dataflow across devices and cloud services. It has also issued formal ISO/IEC standards for the Open Virtualization Format (OVF)[10] and the Cloud Data Management Interface (CDMI),[11] each of which has been brought forward from other SDOs through JTC1's publicly available specification (PAS) process.

Some formal SDOs publish overview documents that aren't intended to set standards, but that serve as building blocks for future efforts.

Although participation in these groups' standards development activities is generally limited to officially delegated experts on behalf of national standards bodies, much of the committees' work is available for public view and comment throughout the development process, and browsing through the public information for each of the committees in

JTC1 can yield early insight into the activities and intended standardization efforts currently in progress.

In the ITU-T, Study Group 13 (SG13) is responsible for work on future networks including cloud computing, mobile, and next-generation networks. Its past activities have included standards to enable interworking between Ethernet and Multi-Protocol Label Switching (MPLS) networks. The group has also worked on standards to enable virtual private networks (VPNs) to work over optical, MPLS, IP, and other networks, and is actively pursuing standards for a wide variety of topics related to distributed, ubiquitous, ad hoc, virtualized, and software-defined networking. We'll cover topics related to cloud networking in the next issue of this magazine.

> There simply is no common zero-cost service level comparable to the Internet itself that's currently available in cloud service offerings.

SG13 has also specified functional requirements and architectures for networks supporting content delivery in IPTV, identity management, sensor networks/RFIDs, and related efforts toward international standards. It operated a Joint Coordination Activity on Cloud Computing (JCA-Cloud, www.itu.int/en/ITU-T/jca/Cloud/) from 2012 through 2015 to study cloud-related topics, which followed from a previous focus group on cloud computing (www.itu.int/en/ITU-T/focusgroups/cloud/). Its reports, however, are generally only available to active members.

As guidance-oriented documents such as these mature, there is a strong potential for rapid transition from standards to regulation and compliance issues, especially in areas related to privacy, security, data protection, financial transactions, and other sensitive areas that are already heavily regulated, such as health records. Previously produced ISO/IEC standards for data protection are already required for compliance by many governments, as detailed in some of the reports mentioned here. In addition, several cloud-relevant detailed specifications developed by other SDOs have been brought under the international standards umbrella by the JTC1 PAS process (see www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45020).

A Personal Interoperability Perspective: They're All Private Clouds

I'm a great admirer of the original NIST definition and subsequent work on cloud computing, and sometimes contribute to some of the public working groups and input processes NIST uses to assemble its reports. With full credit to the value of this work, I am nonetheless not a great fan of the classification that this work helped to popularize in labeling the differences between multitenant and single-tenant clouds as public, private, and hybrid.

In my view, these are all variations on private clouds, and the distinction between a public and a private cloud is simply that public clouds are private clouds to which you as a customer can gain access for a fee. They're only "public" in the sense that they're indiscriminate in terms of who can be a customer. Thus there's no such thing as a true public cloud.

We have public libraries and public parks, public walkways and public buildings. These are all "public" in a sense that no vendor-provided cloud can achieve. There simply is no common zero-cost service level comparable to the Internet itself that's currently available in cloud service offerings. Some vendors give out trial accounts, or allow low-level use of their services for extremely light workloads, but at the moment this never rises to the level of a general public utility that can be shared in a common way.

The closest thing that we have collectively at this time in cloud computing to a true public resource is the overall pattern for use of cloud services, which are most often implemented these days through RESTful API call sequence patterns and interchanges of data using a number of common protocols and formats. I've discussed this general pattern in previous columns.

To make this discussion relevant to the topic of

cloud migration, we can note both the existence of this pattern and the potential for over-reliance on cloud APIs as being the universal vehicle for interoperability. It's not enough to be able to say that cloud APIs are easy to adapt (because, for example, of their usual RESTful nature) and wire together. Realistically, APIs change, and incompatibilities can arise. Past and future versions of a particular approach, even from a single supplier, might not work or be compatible with each other.

Standards can help such interoperability to happen, but only if they're built in from the outset and positioned to be useful in the design of the methods for use of the services. A deliberate approach to designing protocols, APIs, and service control methods can help to create a true public resource out of the various private clouds that deliver these services.

Interoperability in this sense isn't an abstract concept, but the definite result of specific efforts designed to make common use of built-in capabilities that enable rapid interchangeability and selection among features of software from different providers without elaborate efforts by users. The guidebooks and white papers, vocabulary and ontology documents, and other landscape-describing efforts mentioned here are important references that should be consulted as part of any migration effort, and will help to set roadmaps to successful adoption and use of cloud services.

Further Exploration

For data to be retrievable and services truly to be interoperable, common frameworks must be agreed to and interoperability should be built in from the beginning. This will make the lives of future users, archivists, and historians easier, when it comes to do with data at least, and is an important element of making the cloud function as a common resource. Such an approach is also a natural precursor to making any type of migration easier in the cloud, whether into or out of multitenant environments, or between providers of cloud services.

Despite occasional attempts to patent or otherwise protect such calling sequences, APIs, and data exchange patterns, the character of the cloud as a common resource is driven by the need to keep such architectural features simple, and thus to enable multiple people to adopt them with the minimum possible effort. As the drive for simplicity of use comes to dominate even very sophisticated cloud services, standards will emerge to set roadmaps for future use and migration.

AS ALWAYS, THIS DISCUSSION ONLY REPRESENTS MY OWN OPINION. I'm interested in hearing your views and experience, and I'm sure other readers of the magazine would also appreciate such input. A roadmap for exploration in this area will be the most fun to develop, and will ultimately become more useful if it's developed collectively with rapid feedback between developers and users.

Please respond with your opinions on this topic or on those explored in previous columns. Let us know what you think, and please also include any news you think the community should know about the general areas of cloud standards, compliance, or related topics. We're always open to article submissions. I'm happy to review ideas for such submissions or for proposed guest columns. I can be reached for this purpose at alan.sill@standards-now.org.

References

1. Amazon Web Services, "Import an API into API Gateway," *Amazon API Gateway Developer Guide*, 2016; http://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-import-api.html.
2. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology Special Publication 800-145, 2011; http://dx.doi.org/10.6028/NIST.SP.800-145.
3. F. Liu et al., *NIST Cloud Computing Reference Architecture*, National Institute of Standards and Technology Special Publication 500-292, 2011; www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.
4. NIST Cloud Computing Standards Working Group, *NIST Cloud Computing Standards Roadmap*, National Institute of Standards and Technology Special Publication 500-291, version 2, 2013; www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf.
5. European Telecommunications Standards Institute, *ETSI Cloud Standards Coordination Final*

Report, version 1.0, 2013; www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF.
6. Standards and Interoperability for eInfrastructure Implementation Initiative, *SIENA Roadmap on Distributed Computing Infrastructure for e-Science and Beyond in Europe*, 2012; www.sienainitiative.eu/Pages/SelectedDocument.aspx?id_documento=f63de70f-7984-4dcd-9268-50eeadefb81a.
7. Asia Cloud Computing Association, *Report on FSI Regulations Impacting Cloud in Asia Pacific Markets*, 2015; www.asiacloudcomputing.org/images/research/ACCA_Report_-_Web.pdf.
8. International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Overview and Vocabulary*, ISO/IEC 17788:2014, 2014; www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60544.
9. International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Reference Architecture*, 2014; ISO/IEC 17789:2014, www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60545.
10. International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Open Virtualization Format (OVF) Specification*, ISO/IEC 17203:2011, 2011; www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59388.
11. International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Cloud Data Management Interface (CDMI)*, ISO/IEC 17826:2012, 2012; www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60617. (A newer version of this standard is under development at www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=70226.)

ALAN SILL *is interim senior director at the High Performance Computing Center at Texas Tech University, where he's site director for the US National Science Foundation Cloud and Autonomic Computing Center and adjunct professor of physics, and visiting professor of Distributed Computing at the University of Derby. Sill has a PhD in particle physics from American University. He's a senior member of IEEE and active participant in the Distributed Management Task Force and TeleManagement Forum, and he serves as president for the Open Grid Forum. He's a member of several cloud standards working groups, and national and international standards roadmap committees, and he remains active in particle physics and advanced computing research. For further details, visit http://cac.ttu.edu or contact him at alan.sill@standards-now.org.*