The Consultative Committee for Space Data Systems

CCSDS RECOMMENDED PROCEDURES FOR CLOUD-BASED INTEROPERABILITY TESTING

CCSDS RECORD

CCSDS A13.1-Y-1

YELLOW BOOK

June 2018

The Consultative Committee for Space Data Systems

CCSDS RECOMMENDED PROCEDURES FOR CLOUD-BASED INTEROPERABILITY TESTING

CCSDS RECORD

CCSDS A13.1-Y-1

YELLOW BOOK

June 2018

AUTHORITY

Issue:	CCSDS Record, Issue 1
Date:	June 2018
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS). The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4).

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
E-mail: secretariat@mailman.ccsds.org

FOREWORD

This document describes lessons learned and best practices based on a pilot study between the National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA). The pilot study was to investigate the feasibility of performing interoperability testing utilizing cloud infrastructure. Upon successful completion of the pilot, it was decided to develop a Yellow Book documenting the best practices and lessons learned so other working groups within CCSDS could leverage cloud infrastructure to perform their interoperability tests. CCSDS working groups will be encouraged to leverage cloud based technologies going forward as it will be considered a best practice due to its effectiveness and efficiency.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Record is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the e-mail address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS A13.1-Y-1	CCSDS Recommended Procedures for Cloud-Based Interoperability Testing, CCSDS Record, Issue 1	June 2018	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

The purpose of this document is to specify a recommended practice for performing inter-agency CCSDS standards interoperability testing using cloud technologies. For many interagency test scenarios, use of cloud testing may simplify the creation of test environments and eliminate the need for perimeter access exceptions. This book contains the necessary information regarding planning, acquiring, and configuring cloud and related testing functions.

1.2 APPLICABILITY

This Yellow Book applies to any CCSDS interoperability testing that requires closed-loop/real-time interfacing between implemented systems (prototypes) of two or more entities (e.g., agencies). While some standards have been tested asynchronously by sending CCSDS frames via email, and others have been tested by creating perimeter firewall exceptions, using cloud technologies would permit testing an example such as a closed-loop/real-time interface involving transmitting data via the Command Operation Procedures-1 (COP-1), where a feedback loop is required.

This Yellow Book applies to all organizations within the CCSDS community that can use cloud technologies for testing.

1.3 RATIONALE

Based on the successful pilot project using cloud technologies by the CCSDS Systems Engineering Area (SEA) Security (Sec) Working Group (WG) (Sec WG) (see annex A), the CCSDS Engineering Steering Group (CESG) reached unanimous agreement that CESG should adopt this approach as a CCSDS recommended practice when performing inter-agency/interoperability testing.

2 BACKGROUND AND MOTIVATION

During the Consultative Committee for Space Data Systems (CCSDS) Security Working Group meeting in London in November 2014, the topic of interoperability testing between agencies was discussed. Several members of the Security Working Group described the difficulties they have experienced in the past performing point-to-point interoperability testing between two agencies. This had involved making special arrangements for servers located in a De-Militarized Zone (DMZ), or special access through agency firewalls. This was typically time-consuming, and required significant coordination with other entities. Closed-looped/real-time interoperability testing between CCSDS participating agencies has proven to be difficult at times because of the impact on security implementations (i.e., firewalls) by each agency. It has frequently been difficult to get firewall change requests approved, or new Virtual Private Network (VPN) tunnels established.

A more effective and efficient means to conduct interoperability testing was needed. With evolving technologies and agency polices, cloud-based technologies appear to be a viable solution to alleviate past interoperability issues between CCSDS participating agencies. The Space Data Link Security (SDLS) Working Group, with direct support from the Security Working Group, was chosen by the CESG to be a pilot for interoperability testing in the cloud. Based on the research and testing that was performed, this report describes the process followed, and some best practices discovered during the pilot cloud testing for CCSDS.

3 CONSIDERATIONS FOR TESTING IN THE CLOUD

3.1 OVERVIEW

Security considerations need to be accounted for when planning on using cloud resources to support CCSDS projects, and a good resource to understanding cloud is National Institute of Standards and Technology Special (NIST) Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (reference [C2]). NIST provides a solid foundation to consider when utilizing cloud technologies. However, outside of general good security practices, each agency within CCSDS will have its interpretation of the risks involved with cloud technologies, and polices on using cloud.

From a policy perspective, many CCSDS participating agencies have varying approaches when considering cloud usage. Annex B provides a sample of polices that were provided by agencies within the Security Working Group. This list is not all-encompassing of every agency within CCSDS, but merely a sample for informational purposes. Policies also change with time; therefore it is recommended to review the agency's latest polices when considering using cloud technologies to perform CCSDS work.

At the outset, it should be determined if a cloud deployment is even feasible from a policy and security perspective. Generally, within the context of CCSDS work, agencies are prototyping and performing testing to prove out public domain consensus standards that are under development. In most cases, the data and prototypes being developed are not sensitive. However, that is a case-by-case basis, and should be considered when determining if cloud testing is a feasible option. If the cloud is a feasible environment for a particular CCSDS project, then the following information, based on the pilot project by the Security Working Group, can be used as a guide/best practices.

The following subsections will outline steps to be taken in order to be successful when using cloud-based technologies to perform CCSDS interoperability testing. The following need to be considered when using cloud in the context of CCSDS:

- cloud deployment architecture (3.2);
- cloud provider (3.3);
- cost models (3.4) and procurement method (3.5);
- computing and storage resources costs (3.6);
- virtual machine deployment (3.7);
- virtual networking (3.8);
- virtual machine accessibility (3.9).

3.2 CLOUD DEPLOYMENT ARCHITECTURE

3.2.1 GENERAL

Three options were considered during the pilot phase of CCSDS cloud testing. Not all of the advantages and/or disadvantages for each option are discussed in this document; only the high-level architecture is discussed, along with the probability of acceptance by each agency. It needs to be noted that when 'the cloud' is used, it means publicly routable cloud environments, and not cloud-based services hosted by government agencies behind their government firewalls. For example, the Government Cloud (GovCloud) instance within NASA is not being considered, because it does not solve the problem of getting firewall exceptions or separate VPNs established.

3.2.2 OPTION # 1: SHARED VIRTUAL MACHINE

In this option, all agencies share a single Virtual Machine (VM) to perform testing. The main benefit of this approach is that the test environment is totally self-contained, which allows all traffic to stay within a single virtual machine instance. In the event problems occur with interoperability testing, having everything on one machine can eliminate networking issues. However, the main issue with option #1 is that it may be difficult to convince the participating agencies to allow other agencies to have access (at the admin level) to machines containing their intellectual property. Additionally, it may be difficult to have the involved agencies agree on a single cloud provider. For these reasons, option #1 was not viable for the evaluated test, thought it might be for some tests. Figure 3-1 depicts option #1.

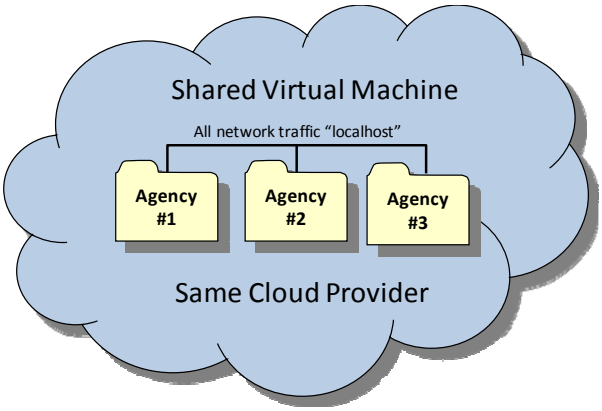

Figure 3-1: Shared VM Approach

3.2.3 OPTION # 2: SHARED CLOUD PROVIDER

In this option, all agencies share the same cloud provider but separate virtual machines are used to perform testing. The main benefit of this approach is that the test environment is totally self-contained within a virtual private network, which allows all traffic to stay within the virtual network. In the event problems occur with interoperability testing, having the

environments sharing a single virtual private network would eliminate networking issues. Option #2 eliminates the concerns about exposing intellectual property to other agencies; but one issue to overcome with this approach is getting the involved agencies to agree on a single cloud provider. For example, an agency may be restricted to a single provider or an agency may require a cloud provider to be certified (e.g., the US Federal Risk and Authorization Management Program, FEDRAMP). It may be difficult to achieve an intersection where a cloud provider is certified (e.g., FEDRAMP) and is also approved by the other participating agencies. There currently is not an internationally recognized standard for cloud technologies whereby a provider could get certified that is recognized by all CCSDS agencies. If agreement on a cloud provider between the participating agencies is possible, then option #2 is the ideal approach. Figure 3-2 depicts option #2.

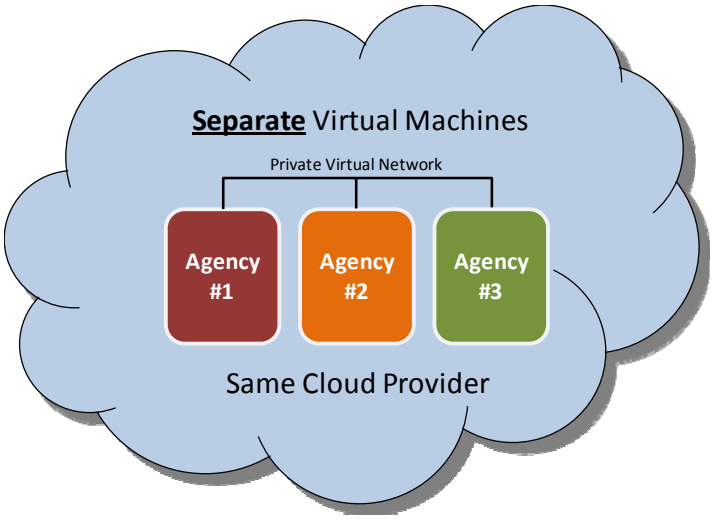

Figure 3-2: Shared Cloud Provider Approach

3.2.4 OPTION # 3: SEPARATE CLOUD PROVIDER

In this option, all agencies procure their own cloud providers and maintain their own virtual machines. This approach will alleviate some of the concerns discussed in options #1 and #2. Each agency will host its environment in the cloud provider of its choosing. This approach has advantages where the agencies cannot come to consensus on a single provider. The location of the data center is not an issue, and the funding mechanism can easily be handled by each participating agency. The disadvantages to this approach are the introduction of networking issues between the environments (latency, etc.), and the use of public IP space to pass information between virtual environments. Depending on the information being exchanged, the public IP space may not be a concern; it would need to be evaluated as part of the risk assessment to ensure sensitive unencrypted data is not being passed between agencies, but this is typically not the case for interoperability testing. For example, this would not be a concern for SDLS testing because the use of the SDLS protocol (reference [C1]) will keep the information secured during transmission. Figure 3-3 depicts option #3.

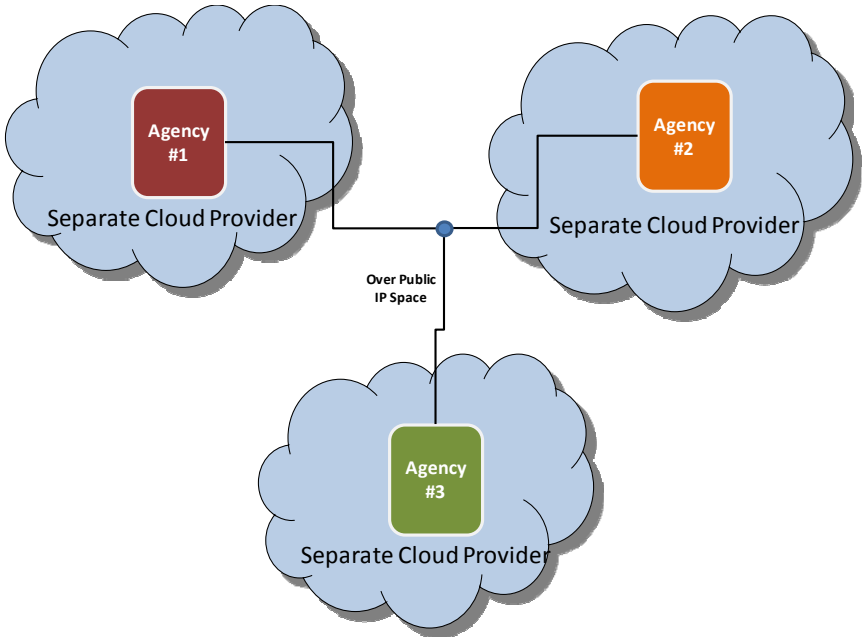

Figure 3-3: Separate Cloud Providers Approach

3.2.5 RECOMMENDED OPTIONS

CCSDS projects planning to perform interoperability testing in the cloud are recommended to utilize one of the two approaches, depicted below in figure 3-4. Utilizing the same cloud provider brings some policy challenges, but also eliminates some technical challenges. An example of a policy challenge is each agency's policy about which cloud providers can be utilized. Some agencies have a strict cloud policy, while others do not, and it may depend on the type and classification of data being hosted in the cloud.

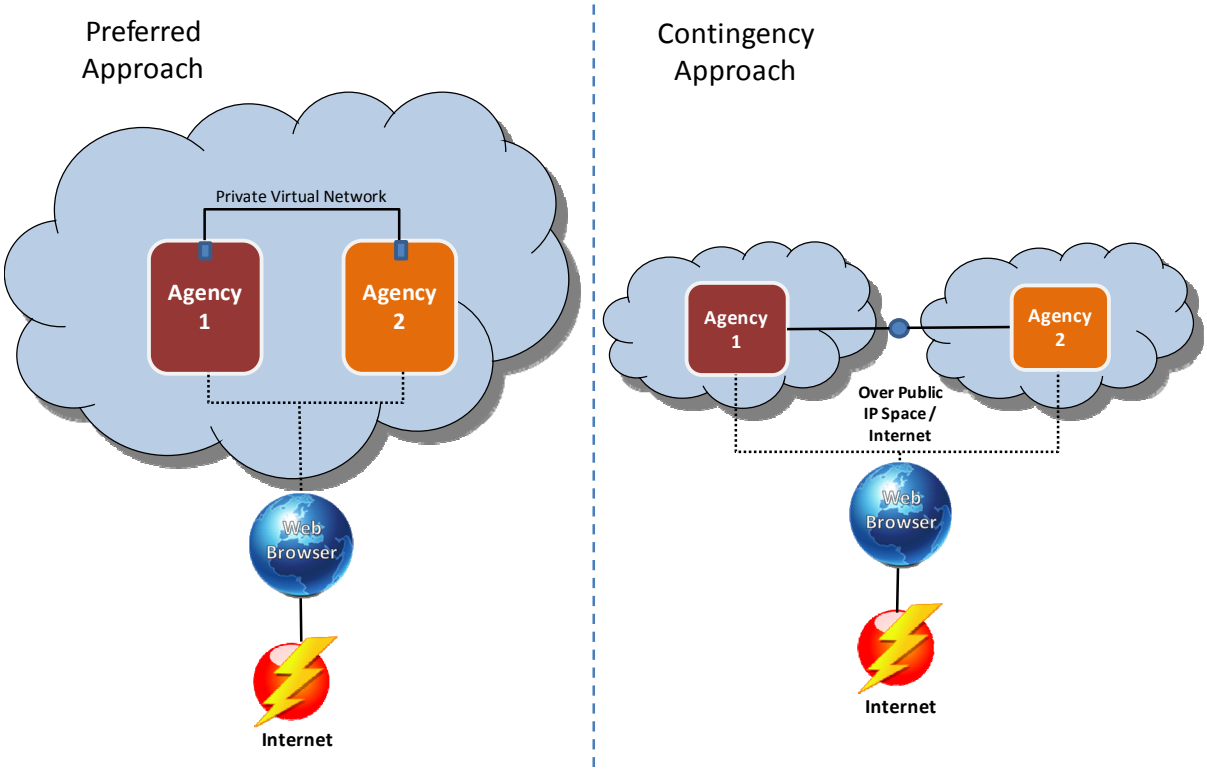

Figure 3-4: Best Approaches

Figure 3-4 depicts the two best options with the setup on the left being the preferred approach, option 2. Sharing the same cloud provider, interfacing on a private virtual network and using the web browser to interact with the VM is more secure (i.e., minimizes Internet exposure) and eliminates technical issues that have been experienced by previous CCSDS interoperability tests. The approach depicted in figure 3-4 on the left utilizes the same cloud provider with different virtual machines where the information passed between the two virtual machines occurs on a separate Virtual Local Area Network (VLAN). It is important to communicate with the cloud provider and ensure the capability is available to connect two virtual machines on an isolated VLAN. Using this approach, the virtual machines are not exposed to the Internet, thereby reducing the risk of external cyber-attacks. Each agency interacts with its virtual machine via a web browser using a Keyboard, Video, and Mouse (KVM) type of connection.

The contingency approach in figure 3-4 on the right, option #3, utilizes two different cloud providers and incurs more risk. The virtual machines from the respective agencies would be exposed to the Internet and thereby have a high exposure to cyber-attack. Therefore additional controls would need to be put in place, such as host-based firewalls and/or host-based intrusion detection to lock down communications and only allow the necessary ports and protocols inbound and outbound. In the contingency scenario, all the traffic traverses public IP space and, if unencrypted, could be subject to eavesdropping. However, in most cases the data being utilized during CCSDS testing is non-sensitive test data; therefore eavesdropping may not be a concern.

3.3 CLOUD PROVIDER

Depending on the participating agencies, the cloud provider selection could be driven by a multitude of factors (e.g., policy, location, technical capability, cost). Annex B contains information on some of the CCSDS participating agencies' approved cloud providers or polices on cloud. Cloud technologies and agency polices are evolving, and each CCSDS participating agency should contact its appropriate cloud point of contact during planning to verify that the data presented in table B-1 is applicable and up to date.

A best practice is to utilize the same cloud provider when possible because it reduces cyber risk, as the communication between the virtual machines happens locally on a private virtual network. Additionally, each agency should procure its own cloud service via a combined procurement, to eliminate intellectual property or legal concerns.

3.4 COST MODELS

The cost for cloud utilization varies depending on the cloud provider. Some cloud providers are time-based subscriptions, while others operate with a 'pay-as-you-go' model. The subscription model simply purchases virtual machines of a certain size for a fixed amount of time. Based on experience with the pilot, which used the subscription model, the subscription model would not be the preferred approach. It is recommended to procure cloud services using the pay-as-you-go model. Experience has demonstrated that performing testing within a fixed window can be difficult, especially when piloting new technologies and working with different agencies. Therefore a best practice is to establish a balance with a cloud provider and pull from that balance as used (i.e., pay-as-you-go). For example, establish a balance of 500 United States Dollars (USD) with a cloud provider, and the balance will be reduced as the virtual machines are used. Depending on the rules and regulations for the agencies involved, one agency can procure the cloud services on behalf of the other. However, the pilot study revealed that some agencies have strict rules on this, and each agency had to procure its own service. In general, to mitigate any potential legal issues, it is recommended that each agency procure its own service.

3.5 PROCUREMENT METHOD

Depending on the agency's procurement regulations, procuring services from the cloud provider can be as easy as a credit card purchase or it might require a full purchase order with substantial paperwork and oversight. Each agency will have to work within its procurement rules, but the most efficient approach is simply procuring the desired amount of computing resources by establishing a balance (e.g., 500 USD) with a cloud provider and burning down the balance over time using the most efficient cost model (i.e., on-demand or subscription) for the particular implementation.

3.6 COMPUTING AND STORAGE RESOURCES COSTS

The first important factor to consider associated with the cost of cloud technologies is the technical specifications of the required resources, which includes the Central Processing Unit (CPU), Random-Access Memory (RAM), and Storage. Network throughput can be a factor as well. The second factor to consider is the required uptime for each virtual machine. The longer the machines are operating, the higher the cost. Based on experience with the cloud pilot, uptime can be reduced to only when testing is occurring, which is different from most standard cloud implementations (i.e., web servers) where the machines are required to be on at all times. The ability to pay-as-you-go, and only power-on the virtual machine when testing, can make the cloud approach extremely cost effective.

Below describes an example comparison between two costing models and the two approaches discussed earlier. When using the subscription model, the cloud provider projects 24x7 usage and applies a discount for bulk purchase, whereas the pay-as-you-go model assumes only 160 hours of usage (8 hours/day for 20 working days). Most cloud providers charge more for the pay-as-you-go model but the required uptime for interoperability testing in most cases will be relatively low. However, it is recommended that each agency perform its own cost comparison to ensure the most cost-effective approach. The main difference between the two approaches is the level of cyber risk involved. Directly exposing virtual machines to the Internet with limited protection (i.e., only cloud provider firewall) is a risky proposition, unless proper controls are implemented.

Costs associated with the example, for 1 month of cloud services for a small-to-medium virtual machine (2 CPUs, 2 gigabytes of RAM), are 27 USD for a subscription and 8 USD for on-demand use (i.e., 160 hours of use).

3.7 VIRTUAL MACHINE DEPLOYMENT

As described in the cloud deployment architecture section, each participating agency will more than likely use separate virtual machines, versus sharing a single virtual machine, to eliminate intellectual property or legal concerns. When deploying virtual machines to the cloud, two options are available: (1) building from scratch on a fresh operating system, or (2) migrating an existing virtual machine into the cloud. For more complex environments, the most efficient option is to migrate an existing virtual machine (or convert an existing physical machine to a virtual machine, and then migrate). Migrating a preconfigured machine eliminates the setup time, which often can be a lengthy process. However, in some instances, redeploying on a fresh operating system can occur with minimal effort, and in those instances migration should be avoided.

If migration is the preferred approach, the following should be considered when deploying or even selecting a cloud provider. The cloud provider will have to support uploading custom virtual disk images. Not all cloud providers provide this capability; therefore it should be considered upfront when selecting the provider. Additionally, it is beneficial for the provider to support the ability to upload an International Organization for Standardization (ISO) 9660-compliant disk image for use, since that allows for uploading a custom operating system, or

even full virtual machine migration. Annex subsection A2.2 provides detailed instructions on how to import a full virtual machine using an ISO.

3.8 VIRTUAL NETWORKING

The virtual networking setup is important, and the cloud provider's capability should be considered before selecting a provider. Depending on the deployment architecture, selected multiple virtual networking options are available. The ability to securely transfer information to and from the virtual machine (e.g., SeCure Copy [SCP] or Secure File Transfer Protocol [SFTP]) is necessary, but the best practice is to have this as an on-demand capability, to limit Internet exposure.

When communication between two virtual machines is required, a best practice, as described in 3.2.5, is the ability to connect two or more virtual machines on an isolated VLAN to establish a local connection. It is important to ensure with the cloud provider that two machines purchased by different customers can be interconnected on the same VLAN. This is likely to require assistance by the cloud provider.

When setting up the virtual networking a best practice is to only in rare cases expose the virtual machines directly to the Internet. This will reduce risk of cyber-attack.

3.9 VIRTUAL MACHINE ACCESSIBILITY

If direct Internet connection (i.e., Secure SHell [SSH] access) is only limited to rare cases, then accessibility needs to be considered as well. Utilizing a web based KVM connection to interact with the virtual machine, instead of a direct Internet connection, is ideal. Most cloud providers provide a web based KVM feature to interact with the VM. Subsection 3.2.5 provides additional information.

ANNEX A

CCSDS CLOUD PILOT – ESA AND NASA EXAMPLE

A1 INTRODUCTION

The following annex provides a cloud testing example in the form of the case study by the SDLS working group/Sec WG working group for testing the Space Data-Link Layer Security Protocol Extended Procedures. In this case study, ESA and NASA were the two agencies performing the testing. Using the option #2 approach depicted earlier, NASA and ESA had to navigate Information Technology (IT) Security polices to come to an agreement on the same cloud provider. In the case of NASA, there is a process (reference [C5]) for hosting IT systems/Information external to NASA. Therefore the fact that it was cloud based had no bearing on the approval process. In the case of ESA, its polices are more stringent on hosting systems externally, especially on the cloud. Therefore the decision was to utilize one of ESA's approved cloud providers.

For the CCSDS cloud pilot and SDLS Extended Procedures (reference [C4]) interoperability testing, NASA and ESA utilized the approach depicted below in figure A-1.

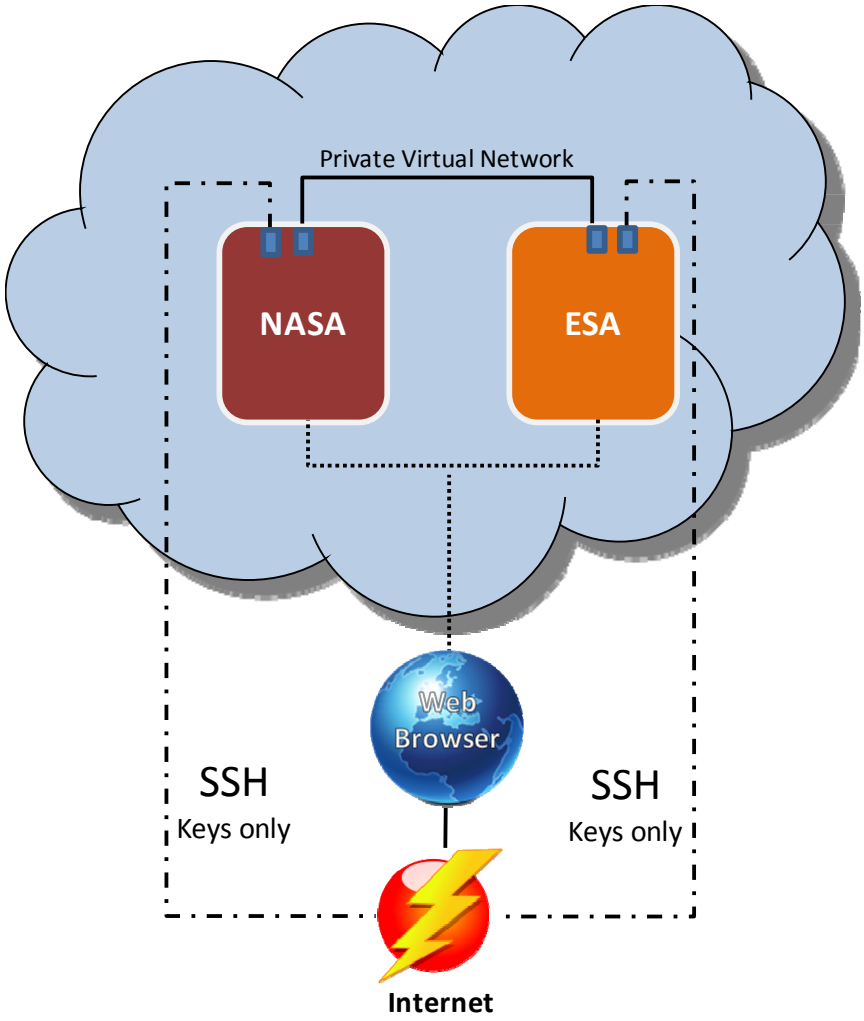

Figure A-1: NASA and ESA Pilot Cloud Setup

NASA and ESA had their own separate virtual machines, which were procured separately. This was an important point since, from ESA's perspective, if NASA paid for the virtual machine, then that brought in Intellectual Property Rights (IPR) challenges. Therefore each agency deposited money in its cloud account, which got billed as the virtual machines were used. This means that each agency has full control over its virtual machine. As for billing, figure A-2 depicts the cost burn down over the first month for NASA. Figure A-2 demonstrates the low cost for performing the pilot study of two separate agencies communicating 'in the cloud'. As can be seen, for the first 30 days it costs approximately 34 USD. This is higher than the projected 8 USD mentioned in 3.6 but it results from high utilization in the beginning stages of the activity. ESA's cost would be similar.

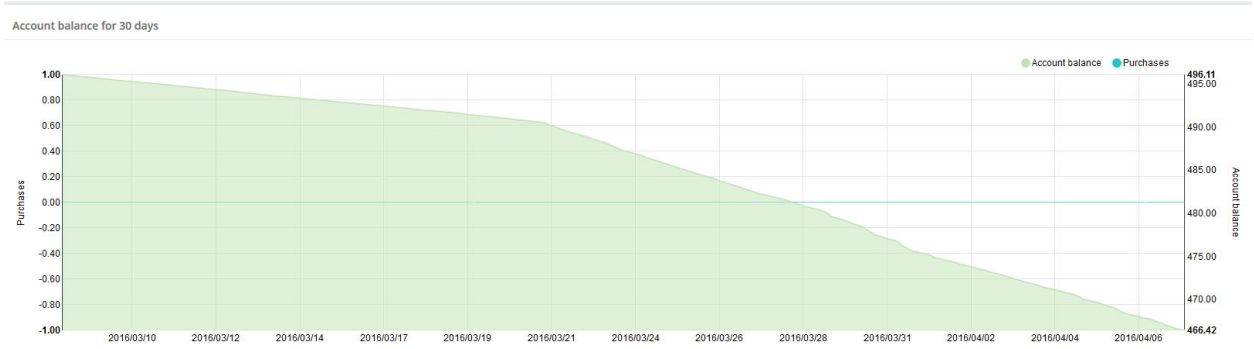

Figure A-2: Cost Burn SDLS Pilot for One Month

Taking into account the labor that went into standing up the cloud and getting virtual machines imported and communicating over an isolated separate VLAN, it was estimated to have taken around 10 hours, which included meetings with NASA, ESA, the cloud provider, ESA management, and NASA headquarters' management. This would not be the case in the future, since both agencies have successfully piloted this capability. It is estimated to take less than two hours to take an existing virtual machine from a particular agency and import it into the cloud.

A2 TESTS PERFORMED

A2.1 OVERVIEW

This annex subsection describes the tests performed to claim success for the CCSDS cloud pilot.

A2.2 TEST CASE #1: IMPORT CUSTOM VM

The initial test for the pilot was to import a custom VM for each agency. This test was not as straightforward as one would imagine, because of what the cloud provider supported. The option existed to import a raw disk image, but because of size limitations, this was not a feasible option. In order to import the custom VMs, the following was performed:

- utilization of 'ghost for Linux' (G4L.iso) on the custom VM to create a compressed image (Lempel-Ziv-Oberhumer Packer [LZOP] recommended compression).
- creation of Linux VM (e.g., Ubuntu) on the cloud with two virtual hard disks.
- copying of (e.g., SCP) the compressed custom image to the secondary hard drive.
- uploading of the G4L.iso to cloud drive library and add the G4L drive to the VM.
- booting to G4L on the VM.
- restoring image from secondary (e.g., /dev/sdb) drive to primary (e.g., /dev/sda).

– rebooting; at this point the VM on the cloud should be the custom VM and not the standard Linux VM.

A2.3 TEST CASE #2: BASIC PING TEST

The second test performed was to ensure network traffic could traverse the isolated VLAN between the two custom VMs. The following tests were performed:

– on the ESA VM, running of a Bourne Again Shell (BASH) script provided by the cloud provider to connect the ESA VM to the NASA VLAN;

– in the user interface, confirmation that the shared VLAN is present and connection to the VM; assignment of the Internet Protocol (IP) address 192.168.21.2;

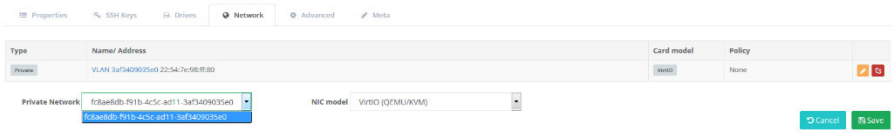

Figure A-3: VLAN Selection

– starting of the VM, ensuring the adapter is present, and assigning the IP address on same subnet:

  • ifconfig,

  • ifconfig eth0 192.168.21.3;

– issuing the ping command to confirm traffic can traverse the subnet: ping 192.168.21.2

A2.4 TEST CASE #3: CONNECT VIA SLE

The final test before claiming success for the pilot was connecting the ESA ground system simulator to NASA's flight system simulator using the Space Link Extension (SLE) service protocol, and sending commands. Figure A-4 depicts the setup for SLE test.

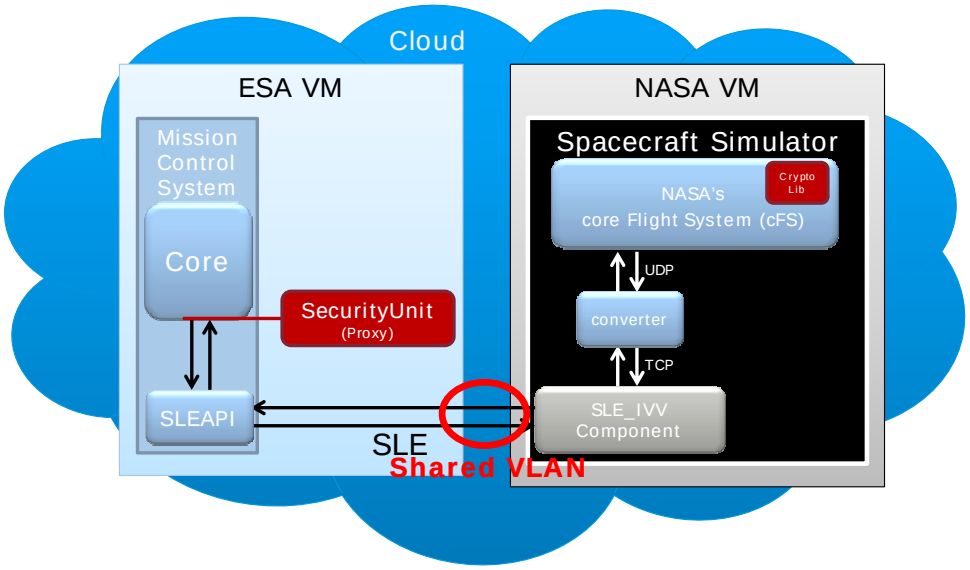

Figure A-4: NASA and ESA SDLS Pilot Environment

The test was to send telecommands from the ESA Mission Control System (MCS) to the NASA Spacecraft over the shared VLAN, using the SLE Forward-Command Link Transfer Unit (F-CLTU) service component and a space link simulator/protocol converter. Figure A-5 depicts the NASA Spacecraft response to receiving the command from ESA.

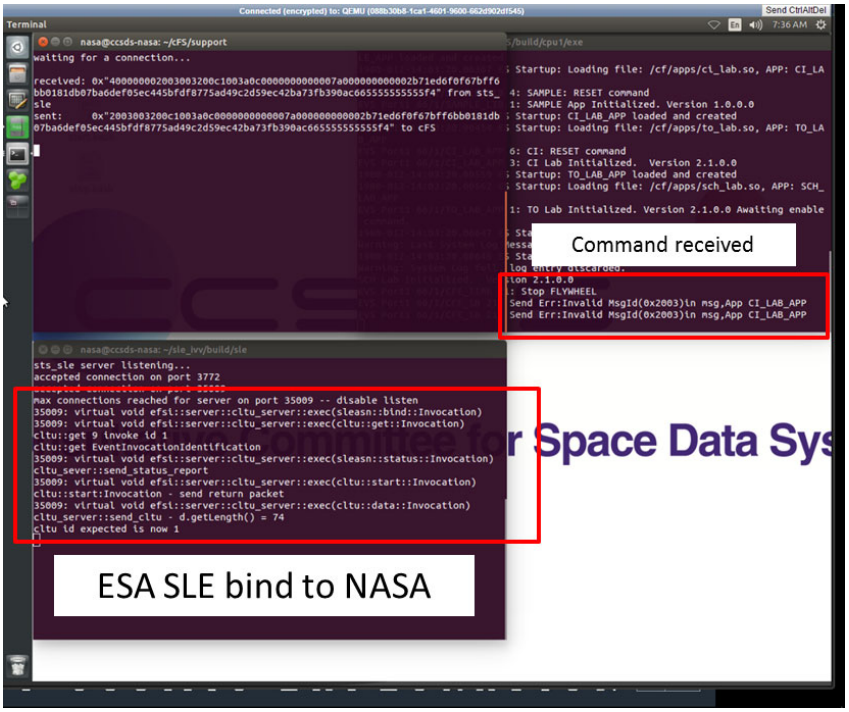

Figure A-5: SLE Bind Between NASA SLE and ESA MCS (NASA Side)

Figure A-6 below shows the same NASA SLE connection to the ESA MCS.

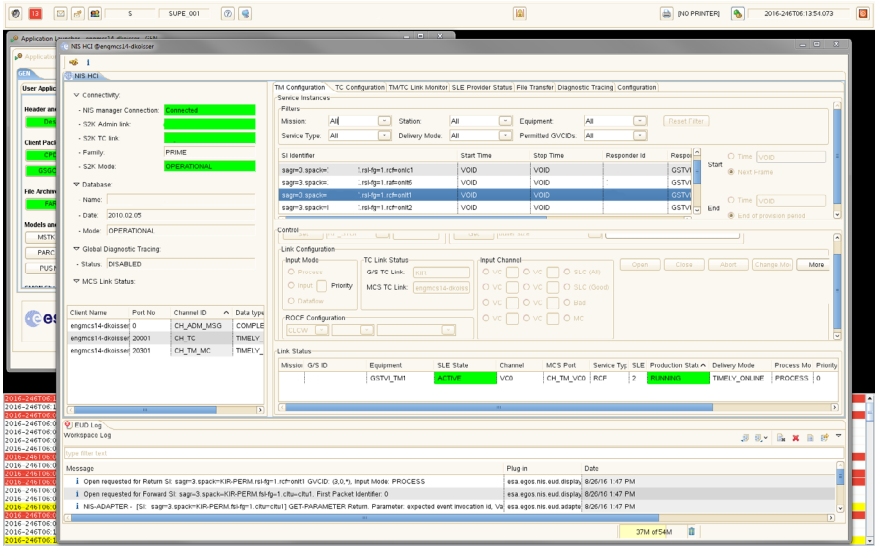

Figure A-6: SLE Bind Between ESA MCS and NASA SLE (ESA Side)

The SLE bind and the passing of telecommands from one simulator to the other meant a successful cloud pilot, as it proved the concept of machine-to-machine communication in the cloud. However, this Yellow Book does not contain the exhaustive testing performed between ESA and NASA to verify the SLDS protocol and extended procedures. The SDLS Extended Procedures Yellow Book (reference [C3]) contains the detailed information on each test performed using the aforementioned cloud environment.

A3 CCSDS CLOUD PILOT SUMMARY

The cloud pilot was successful and can be used as proof of concept for future interoperability testing for other CCSDS working groups. The cloud setup described herein was used to perform the SDLS Extended Procedures interoperability testing but the SDLS Extended Procedures Test Report (reference [C3]) will provide for more details. This pilot proved that testing in the cloud is a low cost, efficient option for CCSDS working groups to interface their implementations. This approach is likely to significantly decrease the amount of time it takes to perform interoperability testing, since agencies will not have to wait until the technical meetings every six months, or get bogged down with IT security and firewall modification requests.

ANNEX B

AGENCY POLICIES ON CLOUD

Each Agency has different policies with respect to hosting information and systems in the cloud. This is the main reason why a single cloud provider can be difficult to achieve. For example, Agency X allows the use of only local/in-country cloud providers. This may not work if an agency has certain requirements (i.e., FEDRAMP) that must be met. Table B-1 is a sample set of cloud polices from agencies within the Security Working Group. These are policies on cloud technologies at the time of the development of this document, and the latest agency policies should be reviewed when planning the use of cloud on CCSDS projects. Cloud technologies and agency polices are evolving, and each CCSDS participating agency should contact its appropriate cloud point of contact to verify that the data presented in table B-1 is applicable and accurate.

Table B-1: Agencies Cloud Policy

Agency	Cloud Provider	Comments
NASA	--	NASA's Enterprise Managed Cloud Computing (EMCC) organization is an Agency-level program, managed by the Computing Services Program Office (CSPO). EMCC on boards cloud providers for NASA use. Currently, only Amazon Web Services have been approved by EMCC. However, as described within this document, NASA also has a process for hosting IT systems outside of NASA's firewall (reference [C5]), which is recommended for the purposes of CCSDS testing.
	Amazon Web Services (AWS)VMware	NASA has multiple avenues using AWS as the provider. AWS is FEDRAMP certified.
	vCloud Government Service (vCGS)	vCGS was recently FEDRAMP approved.
	Other(s)	There are other FEDRAMP approved vendors, but for the purpose of this paper and pilot only AWS and vCGS were considered. (See https://www.fedramp.gov/marketplace/compliant-systems/ for more information.)
ESA	Interoute Cloud Sigma OBS	Getting cloud services with these providers should be achievable. These providers specifically stated compliance to specific requirements on security & privacy.

Agency	Cloud Provider	Comments
CNES	No restrictions as long as they meet IT security policy/requirements	CNES has some Software as a Service (SaaS) contracts, and is investigating Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Cloud usage is not forbidden within CNES, but as with any technology, it has to meet NASA security requirements established by risk analysis. Test software in the scope of CCSDS should not be an issue. CNES has to follow security guidelines from the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). CNES does not have any restrictions regarding the provider, as long as it conforms to the security plan and can deal with CNES's procurement process and contracts.
UK Space Agency	None	The UK Space Agency uses the same networks as its host government department – Business Innovations & Skills (BIS). As such, it has had no involvement with the Cloud, and has no policies about it.
DLR	T-Systems	The possibility exists that if a cloud provider has a 'comparable security level' to T-Systems, DLR Central IT Security may approve the use of a different cloud provider. However, if IT approval were given, it would be necessary to check with the legal department to see if there are any problems with export control.

ANNEX C

REFERENCES

[C1] *Space Data Link Security Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-1. Washington, D.C.: CCSDS, September 2015.

[C2] Wayne Jansen and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing*. National Institute of Standards and Technology Special Publication 800-144. Gaithersburg, Maryland: NIST, December 2011.

[C3] *Space Data Link Security (SDLS) Extended Procedures Interoperability Test Report*. CCSDS Internal Report. Forthcoming.

[C4] *Space Data Link Security Protocol—Extended Procedures*. Issue 0. Proposed Draft Recommendation for Space Data System Standards (Proposed Red Book), CCSDS 355.1-R-0. Washington, D.C.: CCSDS, June 2018.

[C5] *Security Assessment and Authorization: External Information Systems*. ITS-HBK 2810.02-05. Washington, DC: NASA, October 24, 2012.

ANNEX D

ACRONYMS

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AWS	Amazon Web Services
BASH	Bourne Again Shell
BIS	Business Innovations & Skills
CCSDS	Consultative Committee for Space Data Systems
CESG	CCSDS Engineering Steering Group
CLTU	Command Link Transfer Unit
CNES	Centre National d'Etudes Spatiales
COP-1	Command Operation Procedures-1
CPU	Central Processing Unit
CSPO	Computing Services Program Office
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DMZ	de-militarized zone
EMCC	Enterprise Managed Cloud Computing
ESA	European Space Agency
F-CLTU	Forward-Command Link Transfer Unit
FEDRAMP	Federal Risk and Authorization Management Program
G4L	Ghost for Linux
GovCloud	Government Cloud
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Standardization Organization
IT	Information Technology
KVM	Keyboard, Video and Mouse

LZOP	Lempel-Ziv-Oberhumer Packer
MCS	Mission Control System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
RAM	Random-Access Memory
SaaS	Software as a Service
SCP	Secure Copy
SDLS	Space Data Link Security
SEA	Systems Engineering Area
SEC	Security
SFTP	Secure File Transfer Protocol
SLE	Space Link Extension
SSH	Secure Shell
US	United States
USA	United States of America
USD	United States Dollars
vCGS	VMware vCloud Government Service
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VPNs	Virtual Private Networks
WG	Working Group