

Update to CCSDS Cloud Testing

**2016**

Brandon Bailey

NASA IV&V

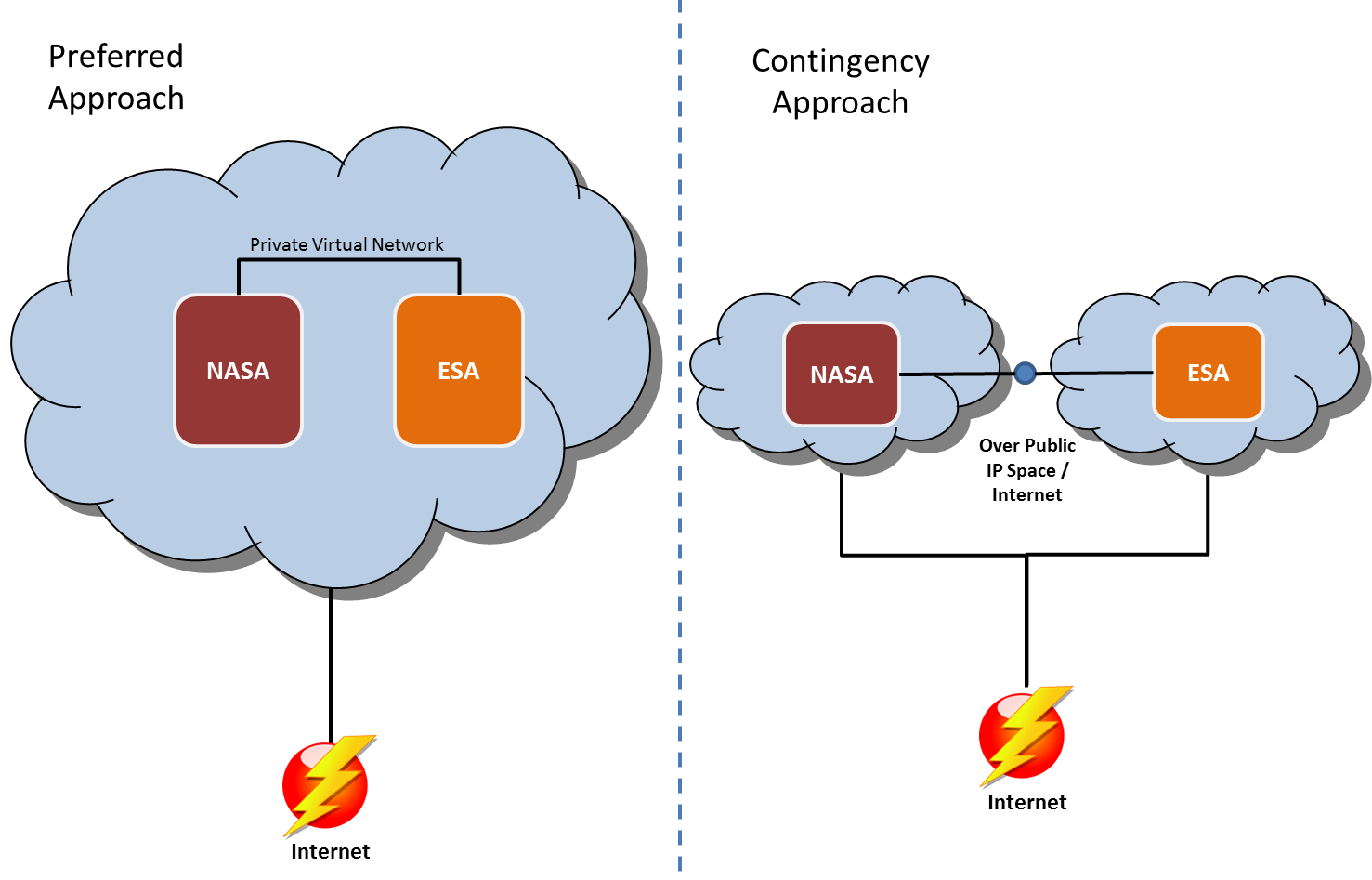
4/8/2016

****

**Cloud Research Summary**

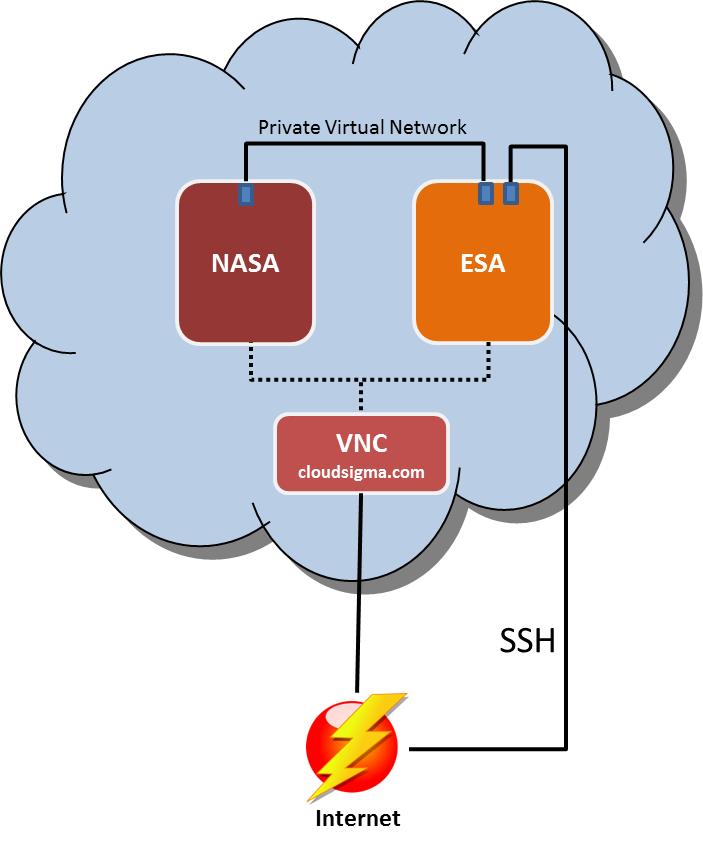
During the Consultative Committee for Space Data Systems (CCSDS) Security Working Group (SWG) meeting in London in November 2014, the topic of interoperability testing between agencies was discussed. Several members of the Security Working Group described the difficulties they have had in the past performing point-to-point interoperability testing between two agencies. It is difficult to get firewall change requests approved or new VPN tunnels established. A potential solution to alleviate these networking issues is to perform the interoperability tests in “the cloud”. In the Spring 2015 CCSDS meetings in Pasadena, CA it was disclosed at the opening plenary that the Space Data Link Security (SDLS) Working Group was chosen by the CESG to be a pilot study for interoperability testing in the cloud. A whitepaper (see Appendix A) was generated and presented in Darmstadt, Germany that discussed the different approaches for using “the cloud” to perform interoperability testing. Based on the research performed, below describes the work performed by the Security Working Group / Space Data Link Security Working Group to pilot cloud testing for CCSDS.

Recommendations for CCSDS projects looking to test in the cloud are to utilize one of the two approaches depicted below. 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 on which cloud providers can be utilized. Some agencies have a strict cloud policy while others do not and it depends on the data being hosted in the cloud. Using an ESA cloud provider as an example (CloudSigma), a rough order of magnitude estimate for two medium virtual machines resulted in a 30 day subscription cost of around $60 USD.

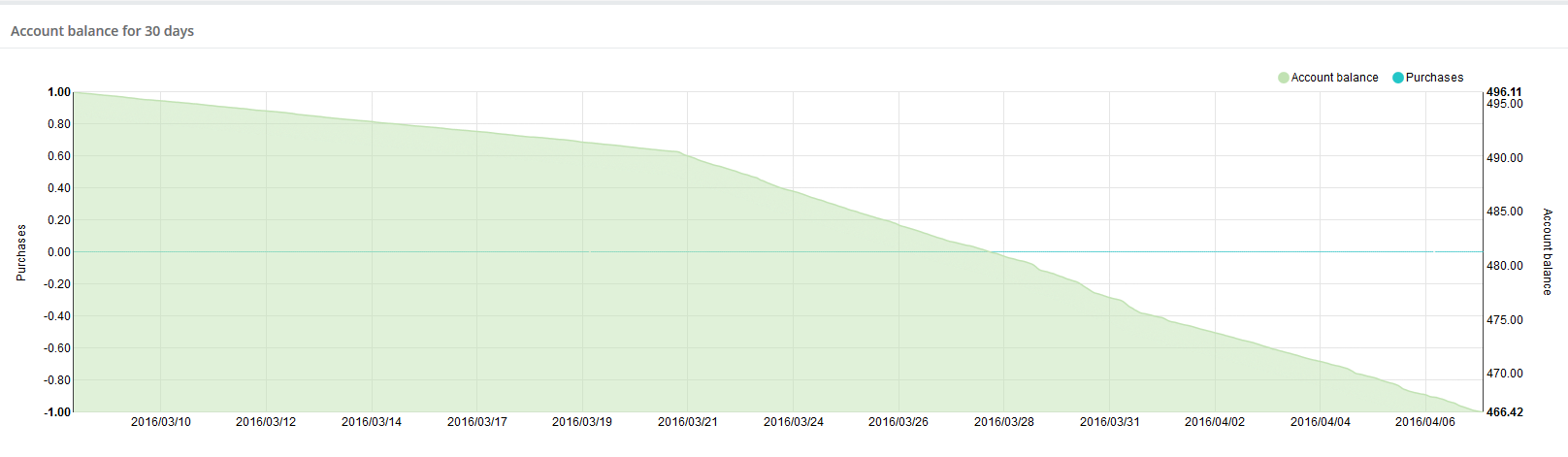


Since ESA already had CloudSigma on their approved cloud provider list, it was used for the pilot and will be used for future SDLS testing. From NASA’s perspective, they have a recently modified process ([ITS-HBK 2810. 02-05](https://nodis-dms.gsfc.nasa.gov/NASA_Wide/restricted_directives/OCIO_Docs/ITS-HBK_2810_%20%2002_05.pdf) - February 2016) for hosting NASA systems external from NASA which is being used for this effort.

For the CCSDS cloud pilot and SDLS Extended Procedure interoperability testing, NASA and ESA utilized the approach depicted below.



NASA and ESA have their own separate virtual machines that were procured by the agency separately. This is an important point as from ESA’s perspective if NASA paid for the virtual machine then that brought in legal challenges where intellectual property transfers and licensing would need to be submitted. Therefore each agency deposited money in their CloudSigma account which will get billed as the virtual machines are used. As for billing, below depicts the cost burn down over the first month for NASA. This graphic is to demonstrate the low cost for performing the pilot of two separate agency communicating “in the cloud”. As you can see, the last 30 days costed approximately $34 USD.



If you take into account the labor that went into standing up the cloud and getting virtual machines imported and talking on a separate VLAN. It is estimated that it took 10 hours between meetings with NASA, ESA, CloudSigma, ESA management, NASA HQ 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 2 hours to take existing virtual machine from a particular agency and importing into the CloudSigma cloud.

**Tests Performed**

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

**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 straight forward as one would imagine due to what the cloud provider supported. In order to import the custom VMs the following was performed:

* Utilize “[ghost for Linux](https://sourceforge.net/projects/g4l/)” (G4L.iso) on the custom VM to create a compressed image (LZOP recommended compression)
* Create Linux VM (Ex. Ubuntu) on CloudSigma with two virtual hard disk
* Copy (Ex. SCP) the compressed custom image to the secondary hard drive
* Upload the G4L.iso to CloudSigma’s drive library and add the G4L drive to the VM
* Boot to G4L on the VM
* Restore image from secondary (Ex. /dev/sdb) drive to primary (Ex. /dev/sda)
* Reboot and now the VM on the cloud should be the custom VM and not the standard Linux VM

**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 was performed:

* On the ESA VM run the following bash script to connect the ESA VM to the NASA VLAN

#!/bin/bash

# CS account settings

username='david.koisser@esa.int'

location='zrh'

# Shared resource settings

name='shared-vlan'

vlan\_uuid='fc8ae8db-f91b-4c5c-ad11-3af3409035e0'

receiver\_username='brandon.t.bailey@nasa.gov'

receiver\_uuid='e7917a67-5a07-4f5d-95f6-27895082aca6'

# TAG Creation

data\_tag='{"objects": [{"name": "'${name}'", "resources": ["'${vlan\_uuid}'"]}]}'

echo "Creating tag: "${data\_tag}

curl \

-s --request POST --user ${username} \

--header 'Content-Type: application/json' \

-d "${data\_tag}" \

https://${location}.cloudsigma.com/api/2.0/tags/ > tag-output

tag\_uuid="`cat tag-output | awk 'match($0, /([0-9a-f-]{36,36})"\}\]\}$/, reg) { print reg[1]}'`"

# ACL Creation

data\_acl='{"objects": [{

"grantees": [{"email": "'${receiver\_username}'", "uuid": "'${receiver\_uuid}'"}],

"name": "'${name}'",

"rules": [{"permission": "LIST"}, {"permission": "ATTACH"}],

"tags": [{"uuid": "'${tag\_uuid}'"}]

}]}'

echo "Creating acl: "${data\_acl}

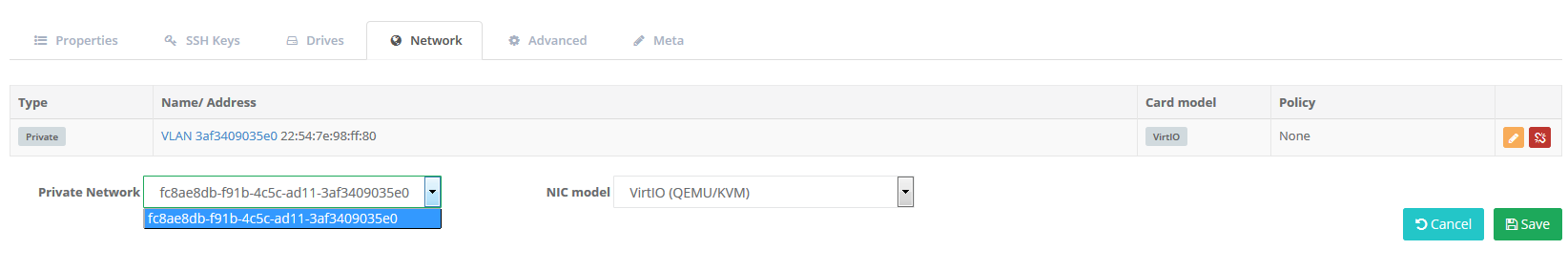
curl \

-s --request POST --user ${username} \

--header 'Content-Type: application/json' \

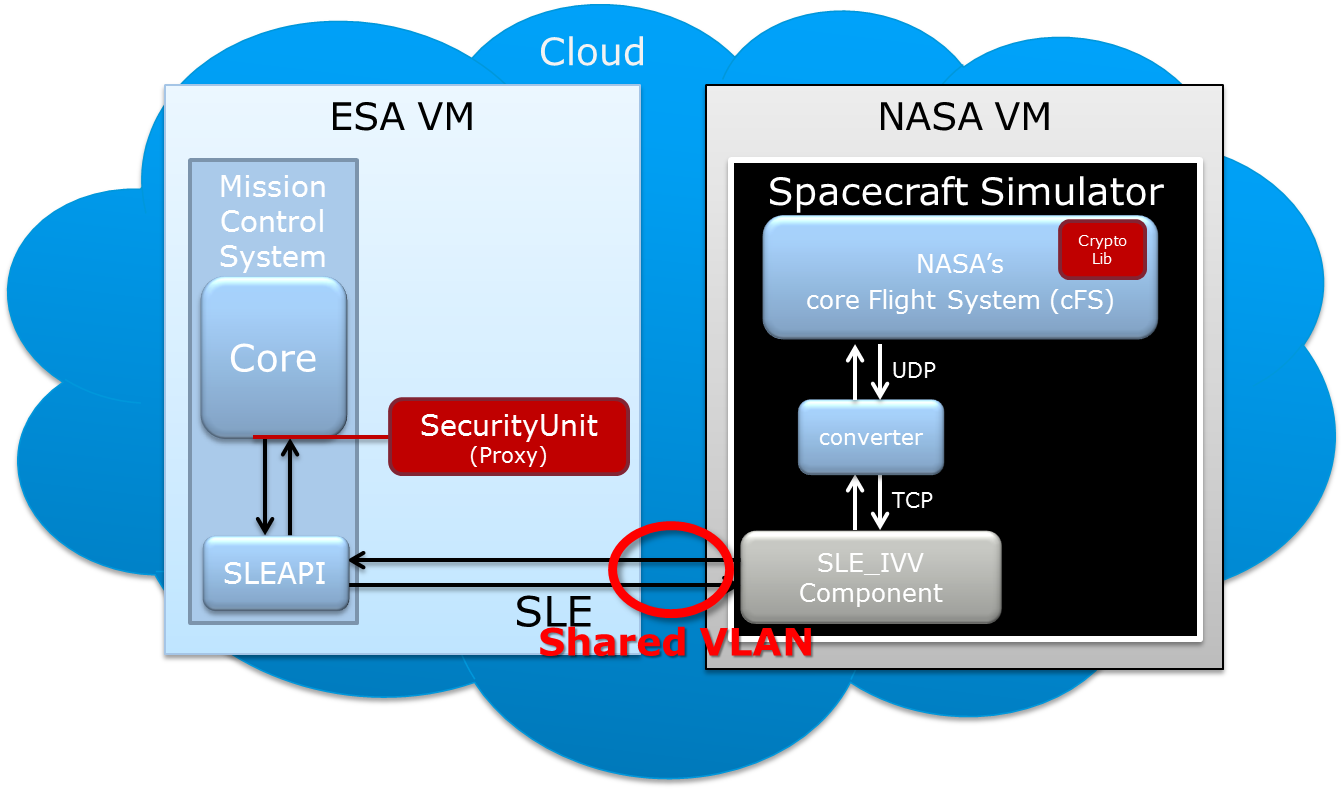
-d "${data\_acl}" \

https://${location}.cloudsigma.com/api/2.0/acls/ > acl-output

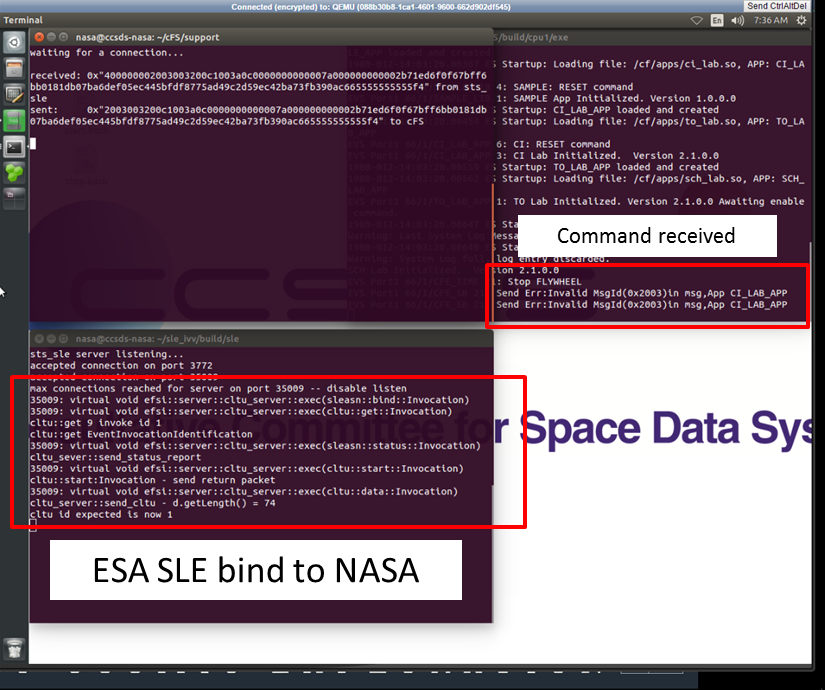
* In the GUI, confirm the shared VLAN is present and connect the VM to it
* Start the VM and ensure the adapter is present and assign IP address on same subnet
  + ifconfig
  + ifconfig eth0 192.168.21.3
* Issue the ping command to confirm traffic can traverse

**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 via SLE and sending commands. Below depicts the setup for SLE test.

****

The test was to send command (TC) from ESA to NASA over the shared VLAN using SLE. Below depicts NASA’s response to receiving the command from ESA. Currently not all features are implemented (Ex. COP-1) but this proved the concept that testing can be performed in the cloud.



**Summary**

The cloud pilot was deemed successful and can be used as proof of concept for future interoperability testing for CCSDS working groups. The cloud setup described herein will be used to perform the SDLS Extended Procedure interoperability testing. This pilot proved that testing in the cloud is a low cost, efficient option for CCSDS working groups to interface their implementations. This approach could possibly decrease the amount of time to perform interoperability testing as agencies will not have to wait until the technical meetings every six months or get bogged down with IT security and firewall modification requests.

**Introduction**

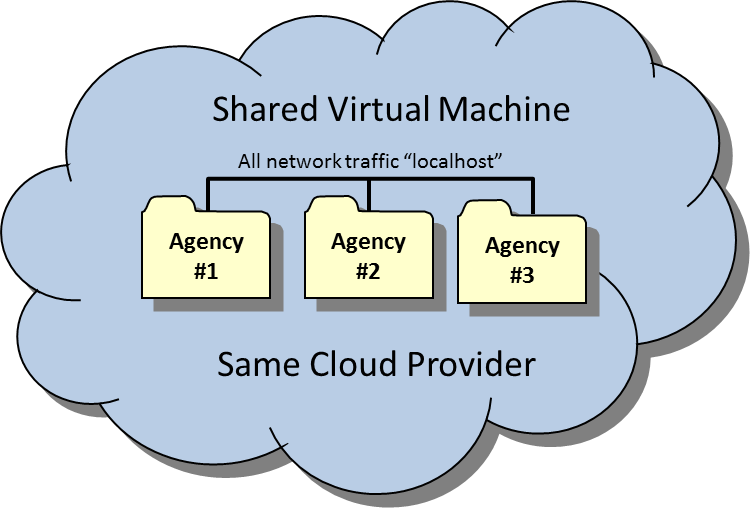
During the Consultative Committee for Space Data Systems (CCSDS) Security Working Group (SWG) meeting in London in November 2014, the topic of interoperability testing between agencies was discussed. Several members of the SWG described the difficulties they have had in the past performing point-to-point interoperability testing between two agencies. It is difficult to get firewall change requests approved or new VPN tunnels established. A potential solution to alleviate these networking issues is to perform the interoperability tests in “the cloud”. In the Spring 2015 CCSDS meetings in Pasadena, CA it was disclosed at the opening plenary that the Space Data Link Security (SDLS) Working Group was chosen by the CESG to be a pilot study for interoperability testing in the cloud. This paper will discuss the approach the SDLS WG will take for performing SDLS Extended Procedures within the cloud. This paper will not discuss establishing a general purpose CCSDS cloud testing environment. The results from SDLS pilot could be used to determine the feasibility of CCSDS cloud testing environment. The pilot will be attempting to solve the SDLS working group’s specific problem for interoperability testing the SDLS extended procedures.

**Approaches**

Three approaches have been discussed within the SWG and SDLS working groups on how to perform testing in the cloud. It needs to be noted that when discussing “the cloud”, it is the publically routable cloud environments and not cloud based services hosted by government agencies behind their government firewalls. For example, the GovCloud instance within NASA is not being considered because it doesn’t solve the problem about getting firewall exceptions or separate VPNs established.

**Approach # 1:** All agencies share a single virtual machine to perform testing. The main benefit of this approach is the test environment is totally self-contained which would allow all traffic to stay within a single virtual machine instance. In the event problems occurred with interoperability testing, having it all on one machine would eliminate networking issues from the equation. However the main downfall of this approach is two-fold. It is unlikely the involved agencies would agree on a single cloud provider to host the machines but the main issue with approach #1 is it would be a hard sell to the participating agencies that other agencies would have access (at the admin level) to machines containing their intellectual property. Due to these reasons, approach #1 will not be pursued by the SDLS WG.

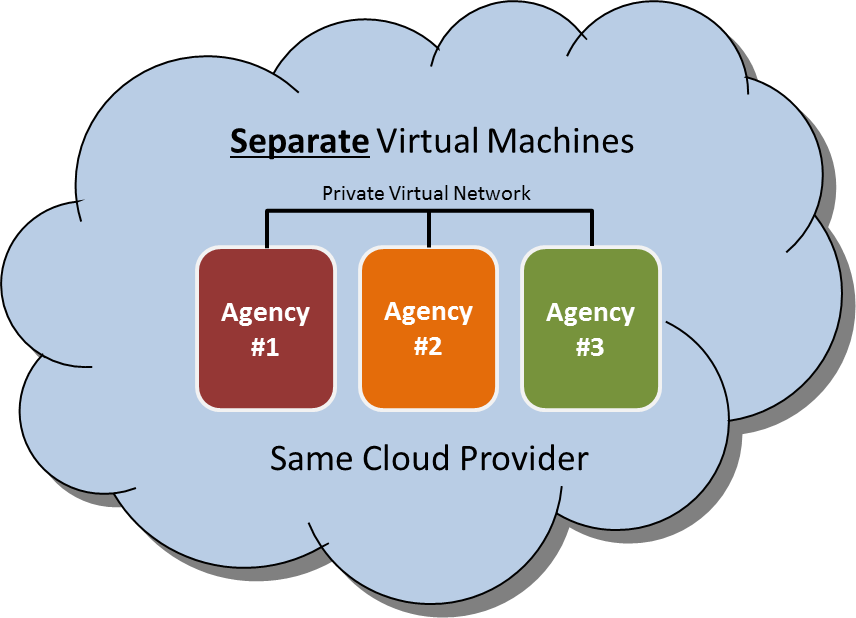
Figure 1 depicts approach #1



**Figure 1: Shared VM Approach**

**Approach # 2:** All agencies share the same cloud provider but different virtual machines to perform testing. The main benefit of this approach is the test environment is totally self-contained within a virtual private network which would allow all traffic to stay within the virtual network. In the event problems occurred with interoperability testing, having the environments sharing a single virtual private network would eliminate networking issues from the equation. Approach #2 eliminates the concerns about exposing intellectual property to other agencies; however similar to approach #1 the downfall of this approach is it will be unlikely the involved agencies would agree on a single cloud provider. For example, an agency may be restricted to a single provider (i.e. DLR). Similarly NASA requires their cloud providers to be FEDRAMP certified which is a US Government specific certification. If agreement between any of the participating agencies can occur, approach #2 would be the ideal approach. Further research is needed to fully eliminate this approach for SDLS testing. For example, for SDLS Extended Procedure testing NASA and ESA are currently slated to perform the testing and if they could agree upon a cloud provider (i.e. Amazon, VMware,etc.) and are not bounded by which data center (US or Europe) the information resides then approach #2 may be valid.

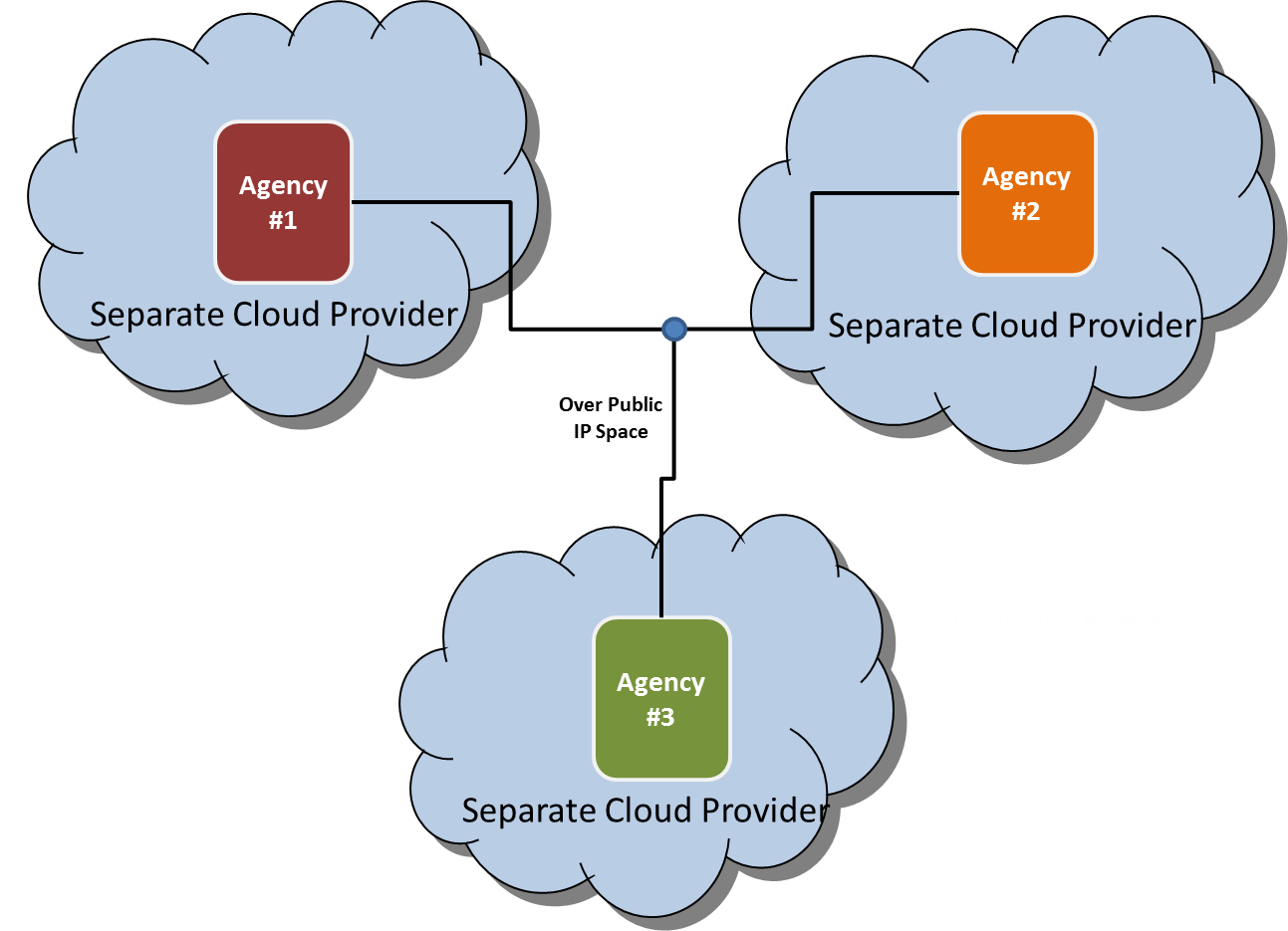
Figure 2 depicts approach #2



**Figure 2: Shared Cloud Provider Approach**

**Approach # 3:** All agencies procure their own cloud provider and maintain their own virtual machines. This approach will alleviate the concerns discussed in approach #1 and #2. Each agency will host their simulation environment in the cloud of their choosing. This approach is the cleanest for multiple reasons. No agency has to come to consensus on a provider, the location of the data center isn’t an issue, and the funding mechanism can easily be handled by each participating agency. The cons to this approach are the introduction of networking issues between the simulations (latency, etc.) and the use of public IP space to pass information between simulation environments. The public IP concern isn’t much of a concern for SDLS testing because the use of the SDLS protocol will keep the information secured during transmission.

Figure 3 depicts approach #3

****

**Figure 3: Separate Cloud Providers**

**Agencies Policies on Cloud**

Each Agency has different policies with respect to hosting information on the cloud. This is the main reason why a single cloud provider is unlikely to be a reasonable approach. For example, Agency X only allows for Agencies to use local in-country cloud providers. This may not work if NASA is involved due to their FEDRAMP requirements.

**Cloud Providers**

The follow table will list a sampling of the available cloud provider for each agency within the SDLS Working Group. This list is not all inclusive for all agencies but it lists the providers considered as a part of this pilot.

|  |  |  |
| --- | --- | --- |
| Agency | Cloud Provider | Comments |
| NASA | Amazon Web Services (AWS)  VMware vCloud Government Service (vCGS)  Other(s) | NASA has multiple avenues using AWS as the provider. AWS is FEDRAMP certified.  vCGS was recently FEDRAMP approved.  There are other FEDRAMP approved vendors but for the purpose of this paper and pilot only AWS and vCGS were considered. |
| 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. |
| CNES | No restrictions as long as they meet IT security policy/requirements | CNES has some Software as a Service (SaaS) contracts and are investigating Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).  Cloud usage is not forbidden within CNES, but as any technology, it has to answer to our 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 ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information).  CNES does not have any restrictions regarding the provider, as long as it answers 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 their host government department – BIS (Business Innovations & Skills). As such, they have had no involvement with the Cloud and have no policies about it. |
| DLR | T-Systems | T-Systems does not look feasible for CCSDS interoperability testing;  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, once IT approval was give, it would be necessary to check with the legal department to see if there are any problems with export control. |

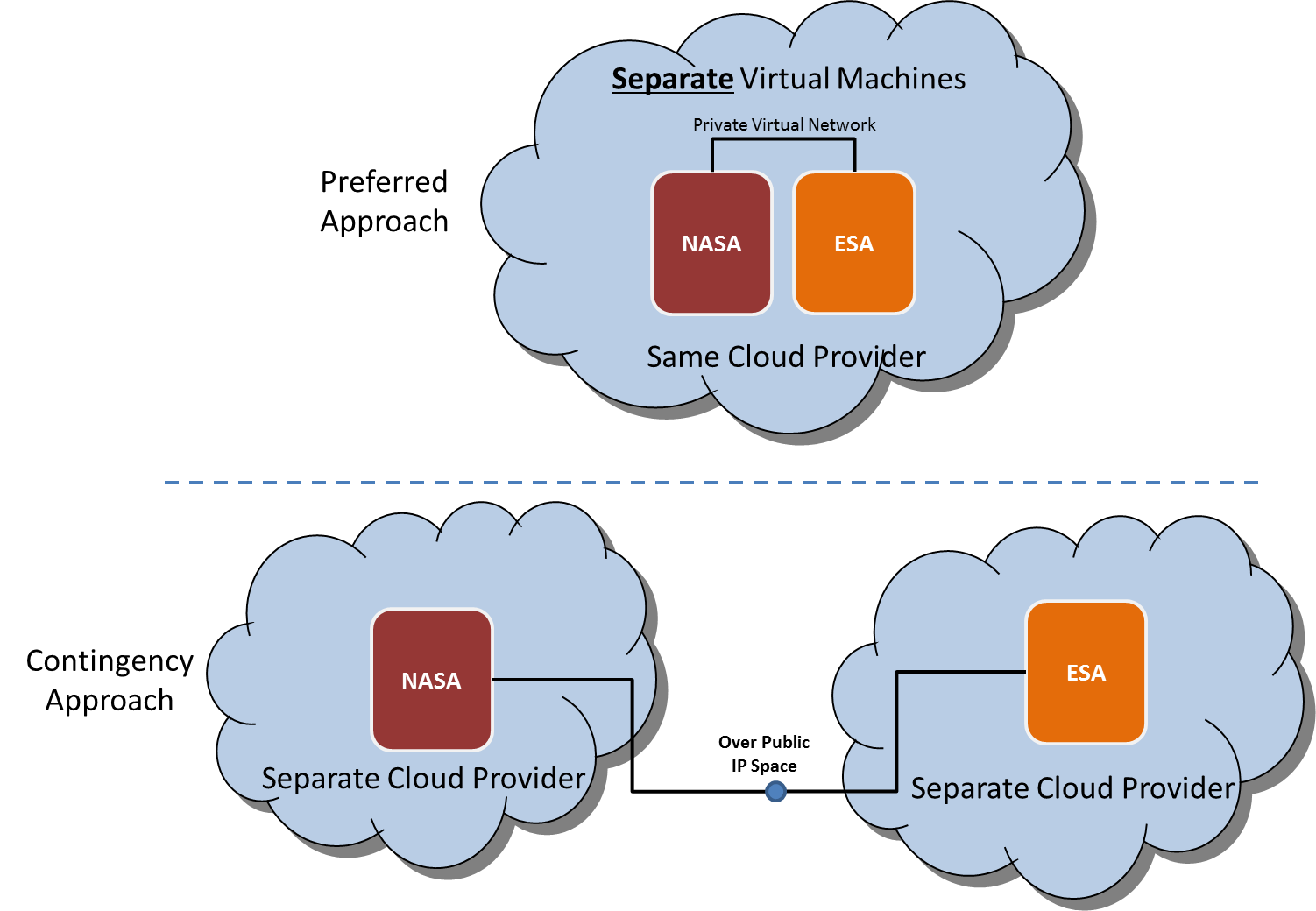
**Plan for SDLS Extended Procedure Testing**

Considering the three approaches outlined above and the fact ESA and NASA are slated for SDLS Extended Procedure testing, approach #2 will be investigated first. If it is determined that ESA and NASA cannot come to agreement on a cloud provider, approach #3 will be employed as a contingency plan (see Figure #4). SDLS Extended Procedure testing is likely a year away; but each agency agreed to pilot the cloud based testing concept in preparation for the SDLS Extended Procedure testing.

The initial pilot will be:

* NASA stand up virtual machine on cloud and perform necessary configuration (ensure NASA can deploy packages, update packages, upload simulations components, etc.)
  + This includes getting through NASA’s approval process for cloud based hosting
* ESA stand up virtual machine on cloud (ensure ESA can deploy packages, update packages, upload simulations components, etc.)
  + This includes getting through ESA’s approval process for cloud based hosting
* Establish communications between the two virtual machines and perform basic communication tests that would representative of real time connection between simulated ground an d spacecraft

If the above objectives are met, then it is reasonable to assume that from a cloud infrastructure perspective that SDLS Extended Procedure testing can be performed when the time comes.



**Figure 4: Pilot for SDLS Extended Procedure Testing**

**Conclusions**

The conclusions to be drawn from performing the initial pilot will provide a basis for the SDLS working group to make an informed decision on the feasibility of using the cloud to perform interoperability of the SDLS Extended Procedures. The results of the pilot will also provide a basis for future work on establishing a CCSDS general purpose cloud computing interoperability environment.