Exploring Cloud-Based Terrain Generation Services

Lance Marrou, Glenn Carr
Leidos, Inc.
Orlando, Florida
Lance.R.Marrou@leidos.com,
Robert.G.Carr.JR@leidos.com

Keith Nielsen
PEO STRI
Orlando, Florida
keith.b.nielsen.civ@mail.mil

KEY WORDS: Common Operating Environment (COE), Terrain Generation Services (TGS), Cloud, M&S

ABSTRACT

The U.S. Department of Defense (DoD) Chief Information Officer (CIO) has committed to the adoption of the data center/cloud/generating force computing environment (DC/C/GF-CE) under the DoD Risk Management Framework (RMF). The U.S. Army (Army) long-term objective of transitioning to scalable and reliable cloud-based information technology (IT) services cannot be realized unless the services are approved and secured under the RMF.

Organizations are becoming increasingly reliant on information system services provided by external organizations to conduct important missions and business functions. The Army's numerous instantiations of applications, services, and hardware hosting locations add complexity to applications interoperability, lead to untimely data sharing between communities, perpetuate inefficient functional processes, and require significant resource investments. These external providers are often cloud-based services in the form of infrastructure, platforms, and software. The Army Cloud-Enabled Network Concept of Operations describes an operational framework for using cloud-enabled technology. A change is needed in how applications, data, and services are hosted to meet future warfighter needs and exploit the evolving, data driven, interconnected eco-system, despite resource constraints. Although this problem is being addressed for the Army's mission command areas through the Common Operating Environment (COE) initiative, our effort builds on the work of DC/C/GF-CE for modeling and simulation (M&S) communities of interest.

In this paper we document the experiment of extending a military network (.mil) into the commercial cloud (.com) under RMF on an Army program of record. We briefly describe how we leveraged other concurrent and previous work to establish our use cases for cloud-based terrain generation services. We identify lessons learned in adopting a cloud CE for M&S training applications, and initial analysis conducted related to geospatial data processing in the cloud CE. We conclude with recommendations of future M&S usage of these capabilities.

ABOUT THE AUTHORS

Lance Marrou is a senior systems engineer at Leidos in Orlando, Fla. Mr. Marrou received his master's degree in computer science from the University of Central Florida. He has been working with modeling and simulation systems since 1992 and has more than 25 years of experience in software and system design.

Keith B. Nielsen is a systems engineer for the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) on the U.S. Army Synthetic Environment Core (SE Core) program. Mr. Nielsen received his undergraduate degree in computer engineering from the University of Central Florida. Mr. Nielsen has more than 16 years of system engineering experience in modeling and simulation applications, with a specific focus on simulation protocols, synthetic natural environment, and cybersecurity.

R. Glenn Carr is a software systems engineer for Leidos in Orlando, Fla. He is currently the Information Systems Security Manager (ISSM) (contractor) for the SE Core program. He has over 22 years of experience with simulation and training systems from both the operation and the development sides in both the constructive and virtual realms.

Exploring Cloud-Based Terrain Generation Services

Lance Marrou, Glenn Carr
Leidos, Inc.
Orlando, Florida
Lance.R.Marrou@leidos.com,
Robert.G.Carr.JR@leidos.com

Keith Nielsen
PEO STRI
Orlando, Florida
keith.b.nielsen.civ@mail.mil

INTRODUCTION

The U.S. Army's (Army) numerous instantiations of applications, services, and hardware hosting locations add complexity to system architectures, lead to untimely data sharing between communities, and require significant resource investments. The Army needs to change how applications, data, and services are hosted in order to meet future warfighter needs and exploit the evolving, data-driven, interconnected eco-system. Although the Common Operating Environment (COE) is addressing this problem for the Army's mission areas, we are furthering the efforts of the data center/cloud/generating force computing environment (DC/C/GF-CE) in particular with respect to the various Modeling and Simulation (M&S) communities of interest. The Army envisions that the DC/C/GF-CE will meet the requirements for addressing these issues.

The U.S. Department of Defense (DoD) Chief Information Officer (CIO) has committed to the adoption of the cloud CE under the DoD Risk Management Framework (RMF). The Army's long-term objective of transitioning to scalable and reliable cloud-based information technology (IT) services cannot be realized unless the services are approved and secured under the RMF.

This paper describes work that has been done to help address a particular area of M&S within the guidelines of a cloud CE under RMF on an Army program of record (POR). Although there are websites and some other cloud-related capabilities authorized under RMF, none have been added to an existing domain as a true cloud-based extension, in order to leverage existing licenses and capabilities of the domain.

GEOSPATIAL DATA PREPARATION AND PRODUCTION

The particular area of M&S we address is a key performance parameter (KPP) of the Army's Synthetic Environment (SE) Core program that develops operational training terrain databases and 3D visual models to meet Warfighter operational training requirements. Based on the Army commitment to adapting to the cloud-based environments, it is clear that eventually synthetic environment generation capabilities must include cloud services, infrastructure, and concerns for further capabilities. Although there are several concerns, such as movement of large sources of terrain data and allocation of resources, a primary concern that is too often overlooked until the bitter end is the introduction of cybersecurity controls.

As with all other producers of terrain databases, SE Core has a significant investment in software tools and operating systems. The Army has enterprise licensing for Windows®[1], both desktop and server systems, and many programs have additional licensing. However, moving capabilities to the cloud often restricts access to those licenses. The cloud resources reside on some local networks hosted by the cloud service provider (CSP), such as Amazon Web Services (AWS)®[2] or Microsoft® Azure®. License servers outside of that area in a secured RMF environment will generally be inaccessible. While it is certainly feasible to purchase the cloud asset with the operating system (OS) included, this is effectively paying for the OS license twice. As an Army program, we already have licenses from the Army enterprise license list, but we need a method to access them from the cloud.

If all data, tools, and access permissions were public and fully open source, then cybersecurity concerns would be minimal and RMF essentially not needed. However, that is never really the case, especially for Army training needs,

[1] Windows, Microsoft, and Azure are registered trademarks of the Microsoft Corporation within the United States and/or other countries.
[2] Amazon Web Services is a registered trademark of Amazon Technologies, Inc. within the United States and/or other countries.

which often require Distribution D or classified labeling. Cybersecurity protections must be considered; and to reduce long-term costs, they should be considered upfront rather than as an afterthought near project completion.

Source Data Considerations

Terrain data producers commonly acquire source data from many different repositories, most of which likely have distribution restrictions. Distribution Statement D is the common restriction which authorizes access for the U.S. DoD and U.S. DoD contractors only. Federal law restricts this data and violations can bring severe criminal penalties. There are also public and open source distributions of data and source code, but these have other problems. The flow diagram in Figure 1 illustrates some of the issues with different source geospatial datasets. The concept in this diagram is that there is a reasonably large amount of processing to perform on source data to get it into clean source data quality. The icons on each box roughly indicate the level of touch labor, where, at the worst case, a hand icon indicates significant touch labor; a person icon indicates an operator using one or more tools; and a gears icon indicates mostly automated processing.

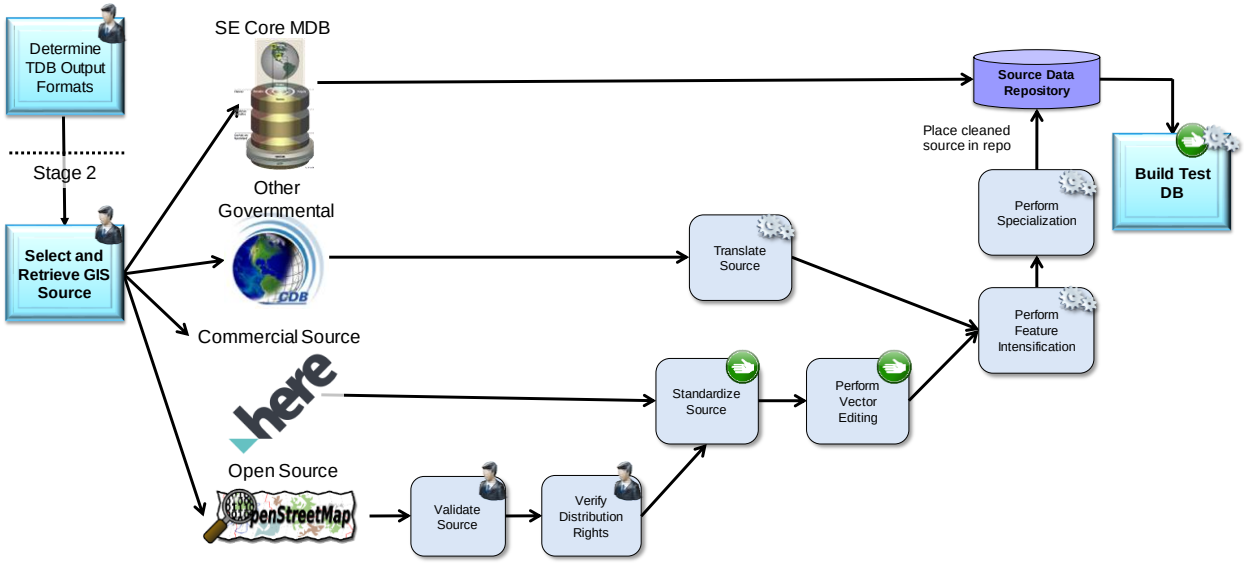

Figure 1. Source Data Preparation

At the top of the figure is a provider like SE Core and its Master Database (MDB) repository of clean source data. In the middle are commercial sources that still require processing such as translation to a common data model and additional simulation-specific functions for feature intensification and system specialization. Just below these commercial data providers are other governmental sources that need more than just translation (or mapping to a data model); they need some standardization and possibly significant vector editing (to include: alignment, cleaning, and digitization for missing features). Lastly are the open source providers which require validation and review of distribution rights (much of it can't be redistributed) before the processing from previous types of sources. Even the commercial and other governmental sources have distribution concerns, but the assumption for commercial is that you pay for the rights you and your customers require. If this means an enterprise level agreement with the DoD, such as with companies like Digital Globe®[3], then that's what is needed. (This can mean that the cost of commercial data far outweighs the cost of performing the translation, standardization, and other steps on open source repository data.)

Tools

The process of geospatial data preparation and production requires a large number of tools. These tools come from all domains, including government off the shelf (GOTS) (government purpose or full rights), commercial of the shelf (COTS), or open source tools. Undoubtedly, some geospatial data producers use proprietary tools (not for sale), but we have no method to analyze or access these and none were used in our work.

[3] Digital Globe is a registered trademark of Digital Globe, Inc. within the United States and/or other countries.

In deciding which tools to use on a particular project or, as with our case, on a DoD program of record, it is important to consider not just the cost aspects, but the cybersecurity to using them. Onboarding (bringing software onto the program) requires a different process for each type of software. GOTS often requires distribution agreements between the agencies and an evaluation to determine if the tools have undergone any sort of vulnerability review. Specifically, if a tool has a Certificate of Networthiness (CoN) or an Assess Only (under RMF) authorization, then it is much easier to onboard and is an important consideration for deployed systems. GOTS software that is not under current maintenance is problematic and may need to be treated differently, with more in-depth scans and review. Free and Open Source Software (FOSS) has significant advantages in cost, but has impacts in terms of onboarding and rights (some require that modifications be returned to the repository maintainer for review). Where a software originates also can affect its approval on a U.S. DoD system. FOSS requires static code analysis (SCA) reviews, which is a pervasive and time-consuming process. While SCA tools are good and help the process, there are often many issues found that need to be resolved (a big problem) or explained. To resolve an issue requires code development, which may have impacts on the license agreement as well as on updating to newer versions. COTS have direct costs for licenses and maintenance, but do not (normally) come with source code, making source code review impossible. Instead, the executables are vulnerability scanned upon onboarding every new version. COTS can also have the same origination problem as open source, such as when the Department of Homeland Security (DHS) directed all civilian government agencies to remove Russian-based Kaspersky Lab®[4] software from their systems within three months[5], and the DoD followed suit.

For our testing purposes, we adapted and reused several tools for the cloud-based terrain generation services (CBTGS) from the Army capability set: Synthetic (procedural) Imagery Processing Tool (SIPT), Rapid Unified Generation of Urban Databases (RUGUD), scatter, Real-time Imagery Processing Tool (RIPT), and modelization. We modified these tools where necessary to work within Applied Research Association's Assimilation of Sources for a Cohesive ENvironment Description (ASCEND) architecture and framework.

ASCEND provides a framework for tools to function as services and execute under workflows built within the architectural structure. This provides an abstraction layer above the cloud assets and lets the CBTGS operators and users define business rules to manipulate data and perform necessary job functions. ASCEND has several components that will not be explained in detail here, but are illustrated in Figure 2. In this figure, the workflow manager obtains jobs in an eXtensible Markup Language (XML) format and executes them. The execution is performed by allocating tasks to the service broker, which has one or more service managers to explicitly allocate services (tools such as modelization). Once the service is initiated, it is able to communicate directly back to the workflow manager for status, pause, restart, and cancel functions. The repository is the database of source data and the final output.

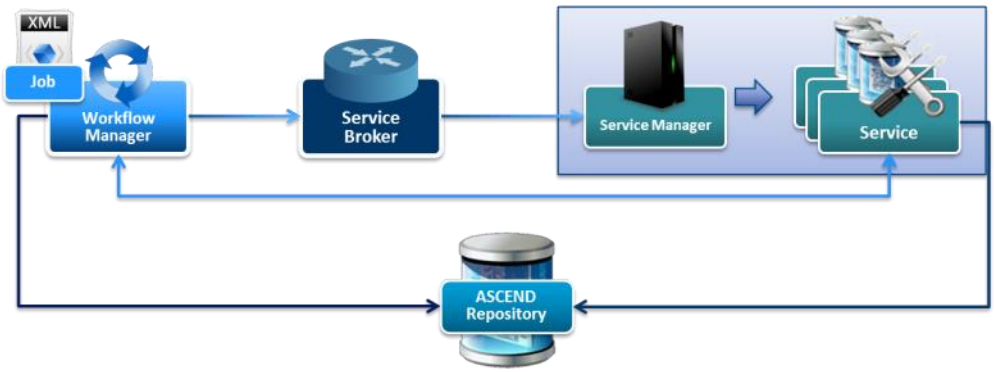

Figure 2. Relationship of ASCEND Framework Components

We logically separated the ASCEND repository into the Source Data Repository and the Terrain Database Repository (final output), as shown in Figure 3. In this figure, we have source geospatial information system (GIS) data on the left that logically is manipulated by CBTGS under authority of an operator and the results are placed in the terrain

[4] Kaspersky Lab is a registered trademark of AO Kaspersky Lab Close Corporation within the United States and/or other countries.

[5] https://www.nextgov.com/cybersecurity/2017/10/pentagon-scrub-kaspersky-defense-systems-following-dhs-ban/141978/

database (TDB) repository on the right. As illustrated and in our actual experimentation, we provide Objective Terrain Format (OTF), Unreal Engine4®[6] (UE4), and Night Vision Image Generator (NVIG) TDBs.

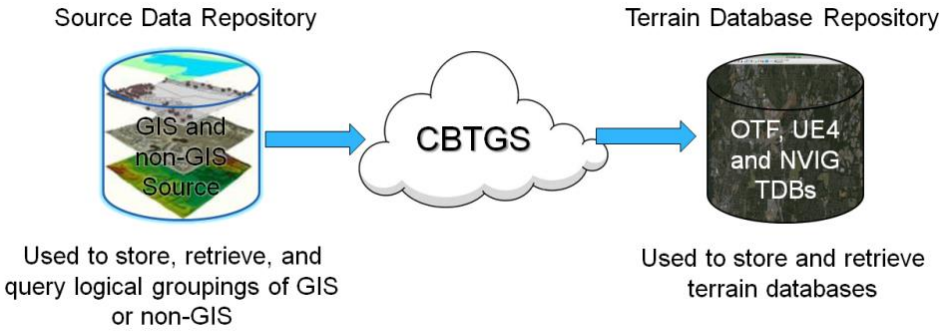

Figure 3. CBTGS Data Repositories

Scatter provides dataset feature intensification that enhances cleaned source to include the addition of simulation specific content, such as ground surface features to support simulation and training. The feature scatter process includes the expansion of aggregate feature data into individual feature representation. A feature expansion example would be the expansion of an areal built-up-region feature into individual building features of various types, or a treed tract into individual trees. Figure 4 shows a sample dataset before and after the scatter operation. Notice the enhanced building coverage over the data located primarily along the linear road features.

Figure 4. Sample Dataset before and after Scatter

RUGUD is used to create the runtime-formatted target terrain databases and is composed of a series of plugins, each of which is callable by the ASCEND workflow manager. Aligning these tools in the proper series, together with the other tools, allows the CBTGS suite to generate the final TDBs from the provided source data. There are many components to the RUGUD toolset, but the primary ones of value to the reader will be the export tools for the three runtime database formats: Unreal Engine, NVIG, and OTF.

SIPT procedurally generates terrain and feature textures from source data based on feature classification and attribution. In this experimentation, we only integrated the capability to generate synthetic imagery from elevation

[6] Unreal, UE4, and Unreal Engine are registered trademarks and Unreal Editor is a trademark of Epic Games, Inc., within the United States and/or other countries.

and vector feature data, and not from runtime OpenFlight®[7] files (another capability of the tool). SIPT is a multi-machine, multi-process tool that automatically detects and scales to available nodes and processors. These relevant features facilitated integration into the ASCEND framework. Some examples of comparisons between real aerial imagery and synthetic imagery are shown in Figure 5. The top set of images highlight the negative aspect of cloud cover not removed from the imagery (which can be an expensive, time-consuming process). Several entities in a convoy are visible "above" the clouds because the imagery is on the ground. No clouds or any other unwanted artifacts are present in synthetic imagery. The bottom set of pictures is intended to demonstrate the high quality of the synthetic imagery in an important area like an airfield.

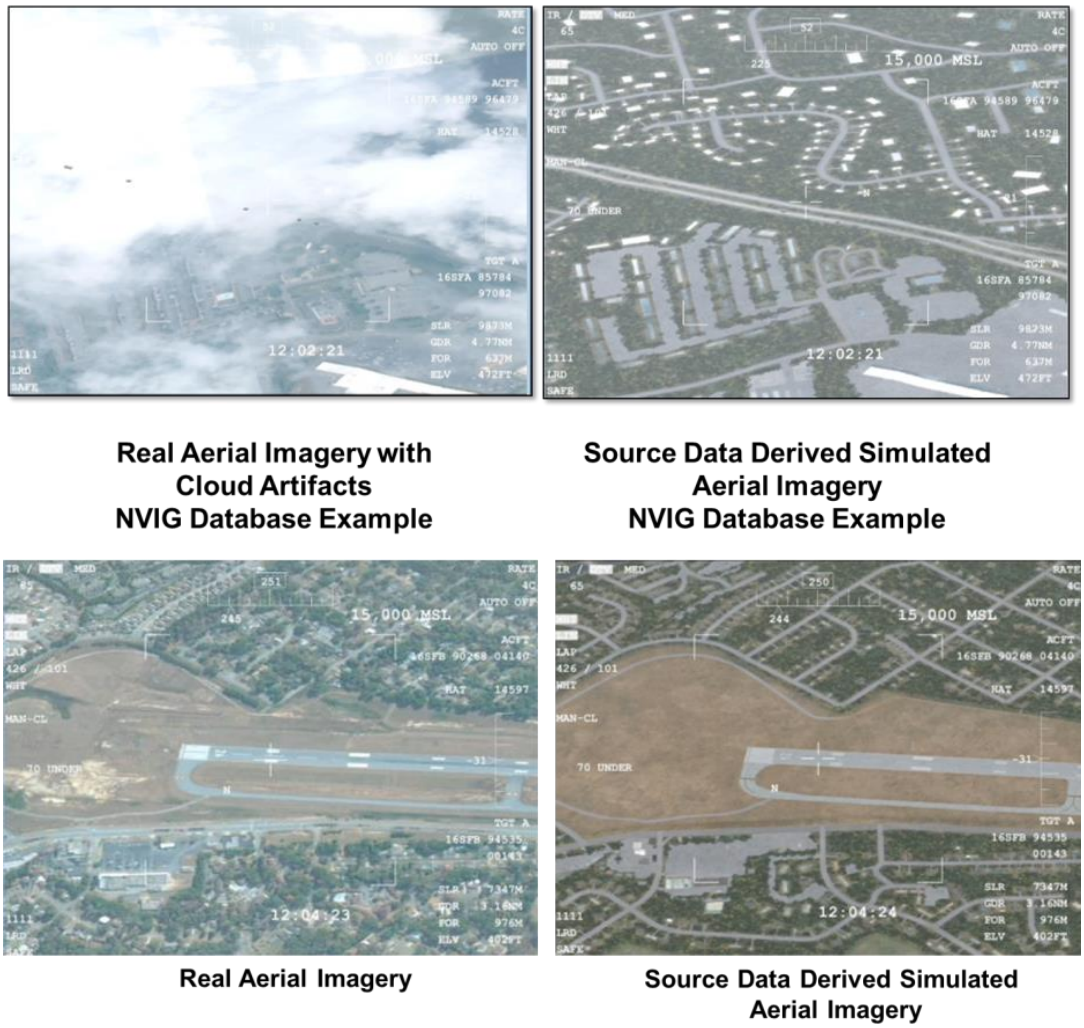

Figure 5. Real Aerial Imagery and Simulated Aerial Imagery Comparison

RIPT is a set of tools that can catalog and resample imagery, drape imagery onto OpenFlight content, or prepare imagery for NVIG database compilation. For cataloging imagery, the tool can automatically, or through user guidance, identify imagery of interest from large (double- or triple-digit terabyte) datasets and define prioritization between sources for image synthesis through resampling. Figure 6 provides a sample of the catalog capability as it finds the best images for use in the final mosaic, which can then be color balanced together for draping on polygon meshes.

[7] OpenFlight is a trademark of Presagis Canada Inc. and/or Presagis USA Inc. within the United States and/or other countries.

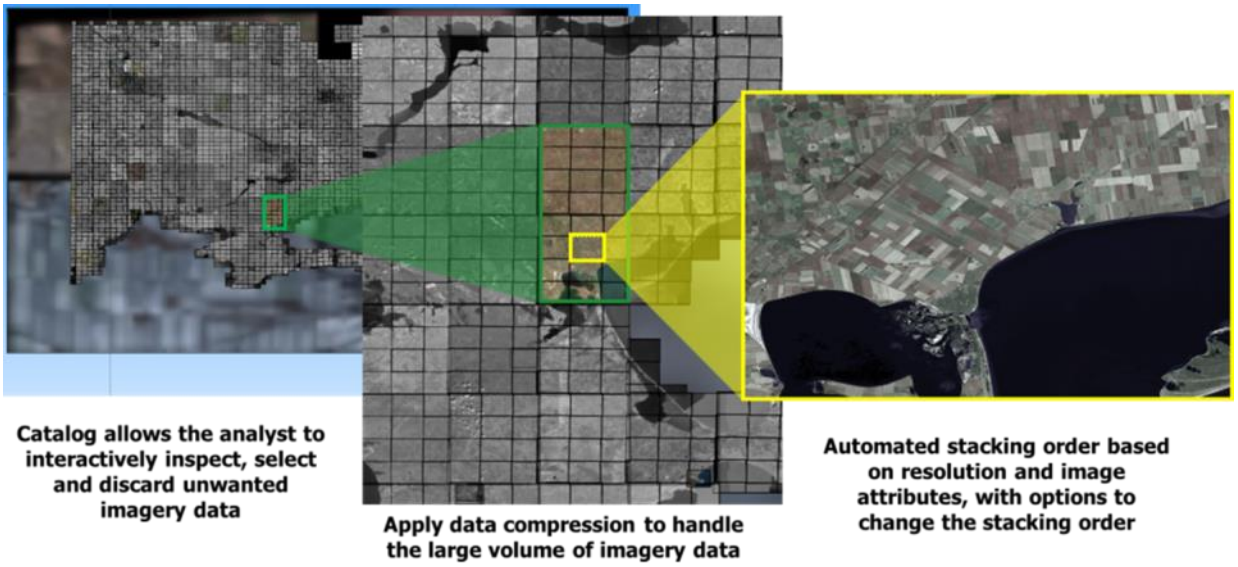

Figure 6. RIPT Imagery Catalog Example

The imagery catalog provides a texture- and context-based visual catalog to allow the user to visually inspect the full data set. This allows the user to find more opportunities to discard unwanted images. Stacking order (applied based on resolution and image attributes) and thumbnails are converted to atlases to allow interactive inspection. Figure 7 shows the process of collecting and preparing satellite imagery for runtime usage.

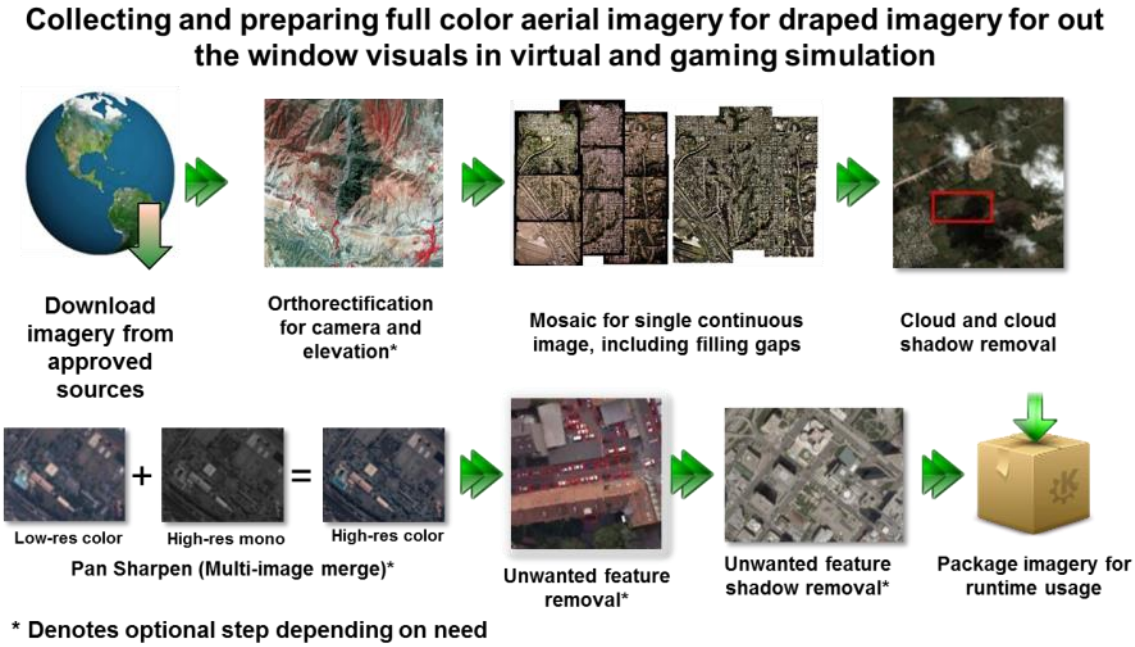

Figure 7. Collecting and Preparing Imagery

The Automated Feature Modelization Tool (Modelization) generates and assigns 3D models to the vector features based on the feature classification and the feature data attribution. The input consists of vector feature data representing areal building and linear road features. Based on feature attribution and user configuration, Modelization creates 3D visual models and replacement point and areal building features. The tool assigns each one of the point building features a corresponding 3D model. Through dialog control settings, the user controls the number of models. Figure 8 shows a procedurally generated building based on the areal footprint and feature attributes, within the Unreal® Editor.

Figure 8. Procedurally Generated Building Model

All of the CBTGS tools are executed as services within the ASCEND service-oriented architecture (SOA) and thus were developed with Swagger®[8] (now OpenAPI™) interface definitions. All interface definitions were thoroughly tested, as were other necessary tool changes. Other infrastructure-related tools we used were ChefDK™[9], TerraForm®[10], AWS, VMWare vSphere®[11], operating systems such as Windows Server®[12] 2012R2, Windows® 10, Red Hat Enterprise Linux Enhanced Platform®[13] (RHEL®), GeoServer, One Semi-Automated Forces (OneSAF), Unreal Engine and Editor™, NVIG, Warfighter's Simulation (WARSIM), OpenSwan™[14], and CISCO®[15] components.

Virtualization

Virtualization is a different technology from cloud, though CSPs obviously make extensive use of virtualization capabilities. The main difference here is that the cloud itself hides the actual inner workings from the external network. If a user allocates a 4-core workstation from a CSP like AWS, this could be from a dedicated 4-core server or workstation or, more likely, from a much larger system, perhaps a 60-core server running virtualization software. Technology like suitcase clouds are simple semi-portable, small-sized virtualized systems. These typically, however, do not abstract the virtualization from the common user. In our experiments, we used both virtualized systems in our local network (for the great flexibility and convenience) and true cloud systems in AWS (very remote from our local network).

[8] Swagger is a registered trademark and OpenAPI is a trademark of Smartbear Software Inc. within the United States and/or other countries.
[9] ChefDK is a trademark of Chef Software, Inc. within the United States and/or other countries.
[10] TerraForm is a registered trademark of Urban Code, Incorporated within the United States and/or other countries.
[11] VMWare VSphere is a registered trademark of VMware, Inc. within the United States and/or other countries.
[12] Windows and Windows Server are registered trademarks of Microsoft Corporation within the United States and/or other countries.
[13] Enterprise Linux Advanced Platform and RHEL are registered trademarks of Red Hat, Inc. within the United States and/or other countries.
[14] OpenSwan is a trademark of Xelerance Corp within the United States and/or other countries.
[15] Cisco is a registered trademark of Cisco Technology, Inc. within the United States and/or other countries.

CLOUD ENVIRONMENT

Our primary goal for the experiment was to put terrain generation services in a cloud environment, not just virtualized. Virtualization has one very significant advantage, however. It is on the local network and thus inherits all of the cybersecurity controls of the dependent network. This makes it a lot easier to use legitimately, for both the controlled data and software. For our purposes, we needed to maintain control and protection, to the necessary extent possible, of the controlled but unclassified information (CUI) under Distribution D control. Because we had recently undergone RMF assessment and authorization (A&A) for an Army POR, and achieved both authorization to operate (ATO) and authorization to connect (ATC) to the Internet, we understood enough of what was needed to propose a solution as a test event to connect our military domain (.mil) to the CSP. This paper does not evaluate various cloud service providers, so our usage of AWS is not indicative of any support or promotion, it is simply a fact that we were more familiar with it and had some ability to leverage corporate assets and expertise.

There are many services offered by a local network and domain that are not available to standalone systems in a virtual private cloud (VPC). Accessing these services provided the real benefit of the approach developed in our experiment and documented in this paper. To access them, however, the workstations and servers instanced in the cloud needed to be joined to that domain. This effectively extended the domain boundary to those systems. The services we specifically targeted were authentication by the domain controller (DC), Defense Information Systems Agency (DISA) Assured Compliance Assessment Solution (ACAS) software suite (specifically, Nessus scanner), Host-Based Security System™[16] applications and support, and license management. The importance of each of these should be readily apparent to the reader, but it is critical to point out that access to license management is extremely powerful. This allowed us to not only reach back to the SE Core domain for OS licenses under the Army's enterprise agreements, but also to our commercial software without having to try to tediously peel off licenses and configure a license manager in the VPC itself. This way, the VPC can be more easily setup, brought down, and reconfigured as needed, providing the true cloud benefits of scalability and cost reduction.

The ability to obtain licenses through the military domain had another significant advantage. This gave us the immediate ability to reuse our validated and thoroughly tested baselined workstation and server images. These are RHEL images, and Windows 10 and Windows Server 2012R2 images that are based off Army Gold Master (AGM) baselines and further improved on SE Core to be fully RMF compliant under the corresponding application, OS, and specific product security technical implementation guidelines (STIGs).

Cybersecurity under Risk Management Framework (RMF)

Our goal was to receive formal approval by the government authorizing official (AO) with recommendation by the government cybersecurity staff for us to put the CBTGS capability in an external CSP. The plan of approach was to document the full capability as a child Enterprise Mission Assurance Support Service (eMASS) entry to the SE Core program. We developed the necessary additional documentation and submitted to the government AO as an interim authority to test (IATT) event. During the approval process, based on discussions including the Program Executive Office for Simulation, Training and Instrumentation (PEO STRI) Chief Information Officer (CIO) office and Army Network Enterprise Technology Command (NETCOM), the decision was made that an IATT was still needed but to be self-certified by the agency due to it being considered a closed restricted network (CRN) (only connected via VPN). Thus, routing and approval through NETCOM was not

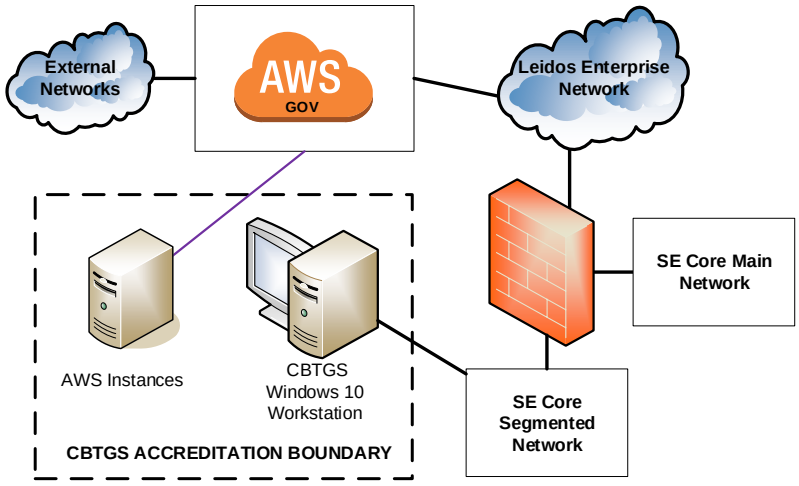

Figure 9. CBTGS Block Network Diagram

[16] DISA's Host-Based Security System is created by McAfee.

completed and with the PEO STRI CIO Cybersecurity approval recommendation, the AO approved the work under the RMF package for a suitable timeframe.

Figure 9 shows the high-level block network diagram for the CBTGS RMF approval package. The currently accredited SE Core boundaries under the ATO received in 2017 are depicted on the right side as the SE Core Main Network with a Cisco Adaptive Security Appliance (ASA) firewall separating the SE Core Segmented Network (reference the enclave STIG for more information on zone designations). Within the segmented zone are allocated lab assets and a switch connecting to a new workstation for the experiments authorized under the CBTGS Information Assurance Posture Assessment Checklist (IPAC). The ASA routes through the Leidos enterprise network via an Internet Protocol Security (IPsec)-encrypted, Federal Information Processing Standards (FIPS) 140-2 compliant, Internet Key Exchange (IKE) v2 virtual personal network (VPN) tunnel. This connects to an AWS GovCloud instance containing the virtual machine instances and configurations needed for the experiment.

Figure 10 provides a more detailed diagram of the CBTGS network. In this figure, we illustrate some of the services that are now available to the workstations and servers instanced in the Cloud, as described above: license management, HBSS, ACAS, and authentication. The IPsec tunnel connects from the SE Core ASA to the AWS OpenSwan. This was a significant undertaking and, per the Cisco engineer, connecting these systems via an IKEv2 VPN had not been successful in 48 previous attempts. Had we known this prior to this effort, we may have attempted a different solution; our attempt was successful and recorded in the online Cisco notes for future efforts. At the time of the experiment, AWS did not offer a GovCloud marketplace, so we could not quickly purchase a virtual ASA that would make the VPN connection trivial. Once connected, workstations and servers were able to join the SE Core domain using the Linux®[17] AWS instance (no license needed) and obtain its RHEL license through the SE Core network. Another key component in the design was that we utilized the Leidos enterprise Multi-Protocol Label Switching (MPLS) network, which has a direct connect to the AWS GovCloud. Although a common enterprise architecture among large corporations, this path provided a tunnel from SE Core (a .mil domain) to the AWS GovCloud without going through the Internet. This design provided a significant measure of security and followed the layered defense approach required by DISA guidelines as it provided a layer of insulation and a very robust security stack in protection. Not included in this design was an approach to allow the cloud assets to access the Internet. This is because, for an experiment, we connected to the segmented network, which, by its definition, does not have Internet access. In formal implementation, the cloud instances would join directly to the Zone B network and have additional services and resources at their disposal (including access to the sizeable storage systems on SE Core).

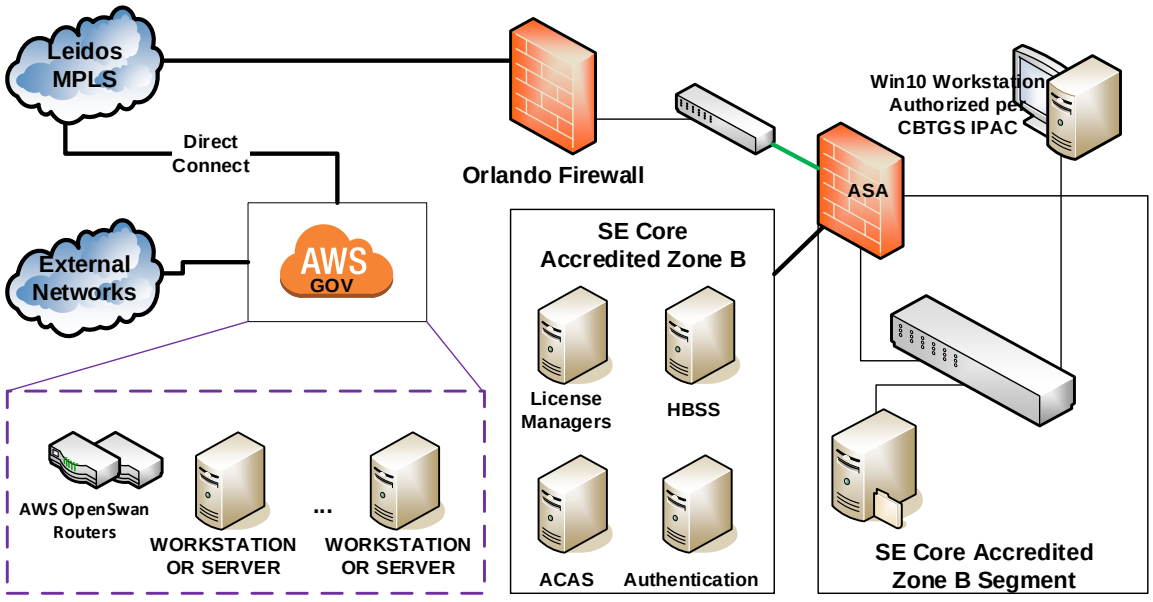

Figure 10. CBTGS Detailed Network Diagram

[17] Linux is a registered trademark of Linus Torvalds within the United States and/or other countries

Lessons Learned

There are several lessons learned from this experiment that are useful to share to the broader community.

- Start cybersecurity approval early and have it in place, ready to implement. Along these lines, work closely with the government ISSM and the CIO office as needed to get early buy-in and recommendations
- Plan ahead with the government ISSM office for the exact approval mechanism (e.g., IATT, is NETCOM needed) and what will work for the given task. This can significantly affect cost and schedule
- Onboarding of software, if necessary, should be in consideration at the beginning of the design phase
- RHEL is easier to configure from an unlicensed cloud instance than from Windows. However, we had difficulty in the remote display and may need additional, licensed software for this capability
- After this experiment, AWS and other CSPs began to offer a marketplace in the GovCloud. Utilization of the correct equipment and software will save time and effort
- Due to security concerns, there is little visibility into the bootstrap within the CSP. This hampered our investigation into the instantiation of Windows machines that needed to reach back for licensing of the OS. To resolve this, a plan should be made upfront for official CSP support.
- Copying virtualized images over networks can be a tedious process and although not normally required often, if you're debugging the image itself (to get it to boot), this can be seriously detrimental. The obvious solution is a much faster network, but perhaps some additional time on minimizing the size of the image would help.

Cost

Specific costs will not be disclosed here as they're dependent upon the CSP and any agreements in place with the organizations requiring the services. However, in general, the cost to perform this experiment in terms of the equipment and software was very low. Due to the design, we either used open source software (e.g., OpenSwan) or were able to reach back into SE Core for our commercial licenses. The instances we chose on AWS GovCloud weren't super high (we chose c3.4xlarge or c3.2xlarge), and overall the cost was about as expected.

Performance

Performance within the cloud was reasonable, but, could be improved. The ping time between the SE Core network and the instanced workstation joined to the domain was about 85ms. The network infrastructure, however, has a relatively low bandwidth and it is in the process of being upgraded. Despite the low bandwidth, we were getting secure copy speeds of about 72Mbps. The direct connect provided us with only four hops between our network and the OpenSwan router, while through the Internet the estimate is over 30 (unsure because most route nodes do not respond when the time to live (TTL) is set for its node for the trace route). The process that took the most time during the experiment, as expected, was transferring data to and from the cloud instance. We primarily experienced this issue when uploading new virtualized images.

CONCLUSION

For future (follow-on) work, the CBTGS eMASS package will be extremely useful as a delta ATO on the program, or even as a template on other DoD programs requiring RMF and cloud capabilities. All of the cybersecurity artifacts were uploaded in the eMASS package and are available for review and download by the Government, although since the closing of the previous program we have archived and removed the package itself from the online eMASS system. Further review and discussion between the program ISSM, CIO office, and NETCOM are needed to clarify requirements and final approach.

An additional concern from the Government Cybersecurity Office was that it does not have a contractual service agreement directly with Amazon for this task. Future approval for a delta ATO would require some service level agreement (SLA) between the Government and the CSP. The options for this agreement need to be explored with agreement and approval from the Cybersecurity Office.

Figure 11 shows an example output of the final capability. This is shown in the Unreal Editor and is an airfield within the Pacific Northwest database. Of note here, we have included a number of 3D moving models (mostly airplanes and helicopters) that were built on program. All of the buildings and other static geometry were procedurally generated by the Modelization tool and the imagery is the procedural imagery.

Figure 11. Example in UE4 for Gray Army Airfield Joint Base Lewis-McChord (JBLM)

ACKNOWLEDGMENTS

Special acknowledgment is made to the staff at Cisco for helping setup the tunnel between the periphery program firewall and the CSP OpenSwan. Additional acknowledgment goes to the team members on the effort, our program subcontractor and Government support, and to AWS for their support for the RMF approval.

REFERENCES

U.S. Army Enterprise Cloud Computing Reference Architecture, Version 1.0 29 Sep 2014, CIO/G-6 Enterprise Reference Architecture Series.
Memorandum, Under Secretary of the Army, 9 June, 2014, subject: Migration of Army Enterprise Systems/Applications to Core Data Centers.
ASA(ALT) Common Operating Environment Data Center/Cloud Computing Environment Architecture Compliance. Version 2.0. 18 September 2013.
Live, Virtual & Constructive Training and Test & Evaluations Enterprise Architecture Capability Objectives. Draft MITRE Technical Report. 2013.
Program Executive Office (PEO) Enterprise Information Systems (EIS) Enterprise Computing (EC). http://www.eis.army.mil/ec/ec-program-initiatives.