Leveraging Cloud Computing Technology for LVC Training

Paul Dumanoir
Army, Program Executive Office for Simulation, Training and Instrumentation,
Project Manager, Integrated Training Environment
Orlando, Florida
paul.h.dumanoir.civ@mail.mil

Henry Marshall
Army Research Laboratory
Human Research and Engineering Directorate
Simulation and Training Technology Center
Orlando Florida
henry.a.marshall.civ@mail.mil

Robert Wells
Dynamic Animations Systems
Orlando, Florida
robert.a.wells@d-a-s.com

Jeff Truong
Effective Applications Corporation
Orlando, FL
jeff@effectiveapplications.com

ABSTRACT

Over the past years the Department of Defense and the Army have been working to accelerate toward wide-scale adoption of cloud computing for the potential cost saving and enhanced mission capabilities that it brings. The Live, Virtual, Constructive – Integrating Architecture (LVC-IA) is a Program of Record (POR), under the Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) Project Manager for Integrated Training Environment (PM ITE), which provides a net-centric linkage for existing Training Aids, Devices, Simulations, and Simulators in an ITE. To date the LVC-IA architecture utilizes a series of servers which are physically located in one or more fielding sites. Each instance of an LVC-IA system has to be individually installed and maintained at each site. Building and running these on site systems is complex and expensive. With each instantiation of LVC-IA for the new training sites, the capital and operating expenditures would simply multiply. A research effort was sponsored by PM ITE to evaluate the feasibility of leveraging cloud computing for LVC-IA. This paper summarizes the analysis conducted, architecture design, and prototype implemented from this research effort. The paper dives into the Information Assurance issues encountered and touches on processes from other Army programs as they relate to the Common Operating Environment (COE) Data Center/Cloud (DC/C) Computing Environment (CE). The paper also reports the comparative analysis results between an ITE with co-located LVC-IA versus an ITE with LVC-IA in the cloud. Finally the paper reports the challenges uncovered, lessons learned, and recommended way forward.

ABOUT THE AUTHORS

Paul Dumanoir is the Chief Engineer for the United States (U.S.) Army Product Manager for Warrior Training Integration (PdM WTI) under the Project Manager for Integrated Training Environment (PM ITE) at the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). He is currently the PM ITE Risk Reduction Test Bed project manager and has 26+ years of experience working in Army and Department of Defense simulation and training programs as Product Manager, Project Director, and Systems / Software Engineer. His current interests include component-based product-line engineering, enterprise architectures, and system of system integration and interoperability. He earned his Bachelor of Science in Electrical Engineering from the University of South Alabama in 1987 and his Master of Science. in Computer Systems from the University of Central Florida in 1991.

Henry Marshall is a Science and Technology Manager at the Army Research Laboratory, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC). His assignment experience spans across several agencies including Army, Department of Homeland Security (DHS), and Navy. His 30+ years with the Government have been spent assigned to leading edge simulation technology efforts in Modeling and Simulation (M&S) Architecture, law enforcement training, embedded training technology, Semi-Automated

Forces (SAF), and simulation software development and acquisition. He received a Bachelor of Science in Engineering degree in Electrical Engineering and a Master of Science degree in Systems Simulation from the University of Central Florida.

Robert A. Wells is a Project Engineer at Dynamic Animation Systems, Inc. He has led the development of the Risk Reduction Test Bed (RRTB) as part of the Advanced Simulation Systems Integration Modeling Interoperability Laboratory and Test Environment (ASSIMILATE) research effort. Mr. Wells has over 17 years of experience in the Modeling & Simulation (M&S) community and has managed a wide range of training systems within the industry. He has integrated Live, Virtual, and Constructive (LVC) components from the LVC Integrating Architecture (LVC-IA) program as well as core-system components from the LVC domains to include Homestation Instrumentation System (HITS), Aviation Combined Arms Tactical Trainer (AVCATT) & Close Combat Tactical Trainer (CCTT) SAF, and Joint Land Component Constructive Training Capability (JLCCTC) within the RRTB. He earned his Bachelor of Science degree in Computer Science from the UCF and his Masters in Business Administration from the Crummer Graduate School of Business at Rollins College.

Jeff Truong is a Principal Systems Engineer at Effective Applications Corporation. He has over 25 years of Systems/Software Engineering and Technical Management experience in distributed Modeling & Simulation systems, telephony/telecommunication systems, networking systems, and network management systems. Mr. Truong is currently a Systems Engineer working on various projects sponsored by the Army Research Laboratory, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC) as well as projects co-sponsored by STTC and the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) Project Manager for Constructive Simulation (PM ConSim).

Leveraging Cloud Computing Technology for LVC Training

Paul Dumanoir

Army Program Executive Office for Simulation, Training, and Instrumentation Project Manager, Integrated Training Environment

Orlando, Florida

paul.h.dumanoir.civ@mail.mil

Henry Marshall

Army Research Laboratory Human Research and Engineering Directorate Simulation and Training Technology Center

Orlando Florida

henry.a.marshall@us.army.mil

Robert Wells

Dynamic Animations Systems

Orlando, Florida

robert.a.wells@d-a-s.com

Jeff Truong

Effective Applications Corporation

Orlando, FL

jeff@effectiveapplications.com

INTRODUCTION

Over the past years the rate of adaptation of cloud computing by business enterprises has exploded. A recent article published by Forbes Magazine (Forbes, 2015) rounds up the various cloud computing forecasts and shows that the growth will continue well into the near future. The Department of Defense (DoD, 2012) and the Army (Army, 2015) also published their cloud computing visions and strategies due to the potential cost saving and enhanced mission capabilities that cloud computing brings.

As a joint initiative between the United States (U.S.) Army Research, Development and Engineering Command (RDECOM) Army Research Laboratory (ARL) Human Research & Engineering Directorate (HRED) Simulation & Training Technology Center (STTC) Advanced Simulation Branch (ASB) and the Program Executive Office for Simulation, Training, & Instrumentation (PEO STRI) Project Manager for Integrated Training Environment (PM ITE), a Risk Reduction Test Bed (RRTB) initiative was stood up as part of a larger STTC ASB program called Advanced Simulation Systems Integration Modeling Interoperability Laboratory and Test Environment (ASSIMILATE). The purpose of the test bed is to perform research on technologies and solutions that benefit the PM ITE portfolio which will eventually transition to the PM ITE Programs of Record (PoRs) without impacting their ongoing development and fielding efforts. It would also provide a base set of proven technologies that can help reduce technology risk on development programs.

One of the RRTB Research Topic objectives is to evaluate the feasibility of leveraging cloud computing for the Live, Virtual, and Constructive Integrating Architecture (LVC-IA) components and impacts related to Information Technology (IT) network infrastructure, simulation performance, and cyber security. The main focus was to explore the potential benefits, drawbacks and solution sets that enable components of the current LVC-IA systems to operate in a cloud environment while at least providing the same level of interoperability that currently exists in the LVC-IA system. In addition, another objective of this research was to investigate if and how the LVC- IA system can comply with the Army's Common Operating Environment (COE) Data Center/Cloud (DC/C) Computing Environment (CE) requirements. This LVC-IA cloud research effort consisted of analysis, design and prototype phases. This paper describes the results of the analysis and design phases. Paper also includes a description of the prototype phase which is planned for execution once the Interim Authority To Test (IATT) is approved to proceed into the prototype phase.

BACKGROUND

This section provides relevant background related to cloud computing models and the appropriate DoD/Army requirements as they apply to Government systems and systems of systems (SoS) like the LVC-IA and ITE.

The basis for the understanding of "what it means to be a cloud" was derived from definitions published by the National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST, 2011). NIST defined the following five Essential Characteristics of a cloud computing: (1) On-demand self-service- it's there when you need it, (2) Broad network access- available over the network, (3) Resource pooling- resources serve multiple customers, (4) Rapid elasticity- you get what you need, and (5) Measured Service – you only pay what you want. Based on our survey of Cloud Service Providers (CSPs), not all clouds exhibit all of these characteristics. In addition, according to NIST there are basically three Cloud Service Models: (1) Software as a Service (SaaS), (2) Platform as a Service (PaaS), and (3) Infrastructure as a Service (IaaS).

The Army Common Operating Environment (COE) Data Center / Cloud (DC/C) Computing Environment (CE) Architecture (Army, 2014) categorizes the applications (for cloud hosting) into two levels:

- **Cloud enabled applications** are virtualized and can run in the IaaS layer of the Cloud environment, but they do not support automatic scaling or use other features of the Cloud environment.
- **Cloud optimized applications** take full advantage of the cloud computing environment. Such applications may run in either the IaaS or PaaS layer. Multiple instances can run, and they support automatic horizontal scaling (both scaling up and down).

The Army COE Data Center/Cloud Computing Environment Architecture Compliance document (Army, 2014) describes the U.S. Army's objective of providing a broad range of high quality computing capabilities at reduced cost. The document contains "compliance statements" for two types of users:

1. For application owners who want to know what they need to do in order to be hosted in the Army's DC CE. These are the applicable criteria/requirements that we, as proxy for the application owner, evaluated in determining which LVC-IA components to move to the cloud.
2. For those who will build the DC CE. This is the largest part of the document. These compliance statements apply to the data center / cloud service providers.

There are various Federal, DoD, and Army documents on cloud strategy, CONOPS, and policies. The most relevant guidance for our research was related to the Cloud Security Model (CSM) and the Federal Risk and Authorization Management Program (FedRAMP).

Cloud Security Model (CSM)

The DoD Chief Information Officer (CIO) has designated Defense Information Systems Agency (DISA) as a key support function and enablement function of DoD Enterprise Cloud Services. DISA originally defined a Cloud Security Model (CSM) that consists of six information Impact Levels. The updated DoD Cloud Computing Security Requirements Guide (DoD, 2015) simplified from six to four information Impact Levels:

- Level 1: Unclassified Information approved for Public release
  This level is no longer used and has been merged with Level 2.
- Level 2: Non-Controlled Unclassified Information
- Level 3: Controlled Unclassified Information
  This level is no longer used and has been merged with Level 4.
- Level 4: Controlled Unclassified Information (CUI)
- Level 5: Controlled Unclassified Information
- Level 6: Classified Information up to SECRET

The Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Once a CSP completes the necessary FedRAMP Security Assessment Framework it will be designed as "FedRAMP Compliant." For our evaluation we

would choose the CSPs that are, or closed to be, FedRAMP Compliant and CSM compliant at Impact Levels 1 and 2 or higher.

LVC-IA CLOUD RESEARCH ANALYSIS PHASE

The main tasks performed under the analysis phase of this RRTB Cloud research were a feasibility analysis for migrating LVC-IA components to the cloud and comparative analysis of the FedRAMP compliant CSPs for our prototype.

LVC-IA Component Evaluation for Cloud Computing

The goal of this task was to identify the LVC-IA core components that would be most amenable to host in a cloud environment. A methodology was developed to rate each component on its affinity for being hosted in a cloud environment based on a number of different criteria. Those components rating highest against these criteria were deemed to be the most easily migrated into a cloud environment.

Each criterion was weighted with a numeric value to indicate its relative impact on functionality and provided a broader range of measurement. Each weight was assigned a numeric value that corresponded to a notional enumeration of 'LOW', 'MEDIUM' and 'HIGH', which translated numerically to '1', '3', and '5', respectively. For example, if a particular component partially meets a given criterion, the overall score takes this into account, assuming some but not all possible credit.

To calculate the applicability of a particular LVC-IA component to a given criterion, a numeric score was assigned and multiplied with the corresponding weight value. To simplify the scoring approach we only used numeric value that corresponded to a notional enumeration of 'LOW', 'MEDIUM' and 'HIGH', which translated numerically to '-5', '0', and '5', respectively. For example, General Criterion 12 Architecture Compliance considered how "well" a component met Army data centers architectural specification, and the scoring approach used provided an enumeration of "LOW", "MEDIUM", and "HIGH" to quantify that relationship. If the LVC-IA component scored "LOW," the approach met less than half of the requirements, and implementing such a capability would be significant code rework. If the LVC-IA component scored "MEDIUM," it met more than half of the requirements, but some content may not be understood. Finally, if it scored "HIGH," it fully supported all aspects Army data center architectural compliance.

Table 1 provides a summary description of each General Criterion. It also includes the weight given to each General Criterion in our approach and justification as to why that weight was assigned.

Table 1 – Software Component Evaluation Criteria Description

ID	Category	Criteria Summary	Weight	Weight Justification
1	Interface Characteristics	The component's interfaces allow latency introduced by the cloud environment and network topology.	MEDIUM	This is a normal weight.
2	Interface Characteristics	The component's interfaces are loosely coupled with other components.	LOW	While potentially producing less than optimum architecture, workarounds can be instantiated to deal with coupling issues.
3	Classification Level	The component's deployment within a cloud environment is consistent with overarching IA requirements.	HIGH	There is no alternative or workaround for components that are not compliant with security requirements.
4	Dependencies	The component's software, data and resource dependencies can be met in a cloud environment.	MEDIUM	This is a normal weight.
5	Commonality	The component's software is reusable and configurable for multiple users within a cloud environment.	LOW	Low commonality may create more copy/paste bloat that will affect supportability but workarounds in process and policy can make up for it in the short term.

6	Fault Tolerance	The component is tolerant of exceptional adverse conditions that may arise within a cloud environment.	HIGH	Solutions need to support the ability to understand faults that happen remotely and minimize their occurrence. The unknown location and nature of cloud make dealing with hidden faults difficult.
7	Scalability	The component has mechanisms to support scalability through prediction of resource needs and adjustment to changing usage demands.	HIGH	The remote and location transparent nature of the cloud makes dealing with capacity and scale at the edge difficult and complicates solutions.
8	Cohesion	The component offers a well-defined, cohesive capability.	MEDIUM	This is a normal weight.
9	Ease of Configuration	The component is easily configurable for use within a cloud environment.	MEDIUM	This is a normal weight.
10	Ease of Provisioning	The component provides mechanisms to provision itself within the cloud environment.	HIGH	Cloud solutions need to support auto-provisioning in order to be instantiated in a remote location transparent manner.
11	End User Requirements	The component minimizes its reliance on specific hardware devices or location-dependent resources.	HIGH	Dependencies on special or unique local resources at the point of use obviate the ability to be in a location transparent cloud topology.
12	Architecture Compliance	The component is compatible with Army's data center and cloud environment architectural specifications.	MEDIUM	This is a normal weight.

Using the criteria and scoring approach described above, each LVC-IA's major architecture component was evaluated and scored quantitatively. Figure 1 depicts the findings in the bar graph to indicate the applicability of the component to a cloud environment. For example, for LVC-IA Exercise Portal, by adding up the weighted score (score assigned [-5, 0, or 5 for LOW, MEDIUM and HIGH respectively] times the weight assigned [1, 3, or 5 for LOW, MEDIUM and HIGH respectively]) for each criterion, we came up with the total weighted score of 195.

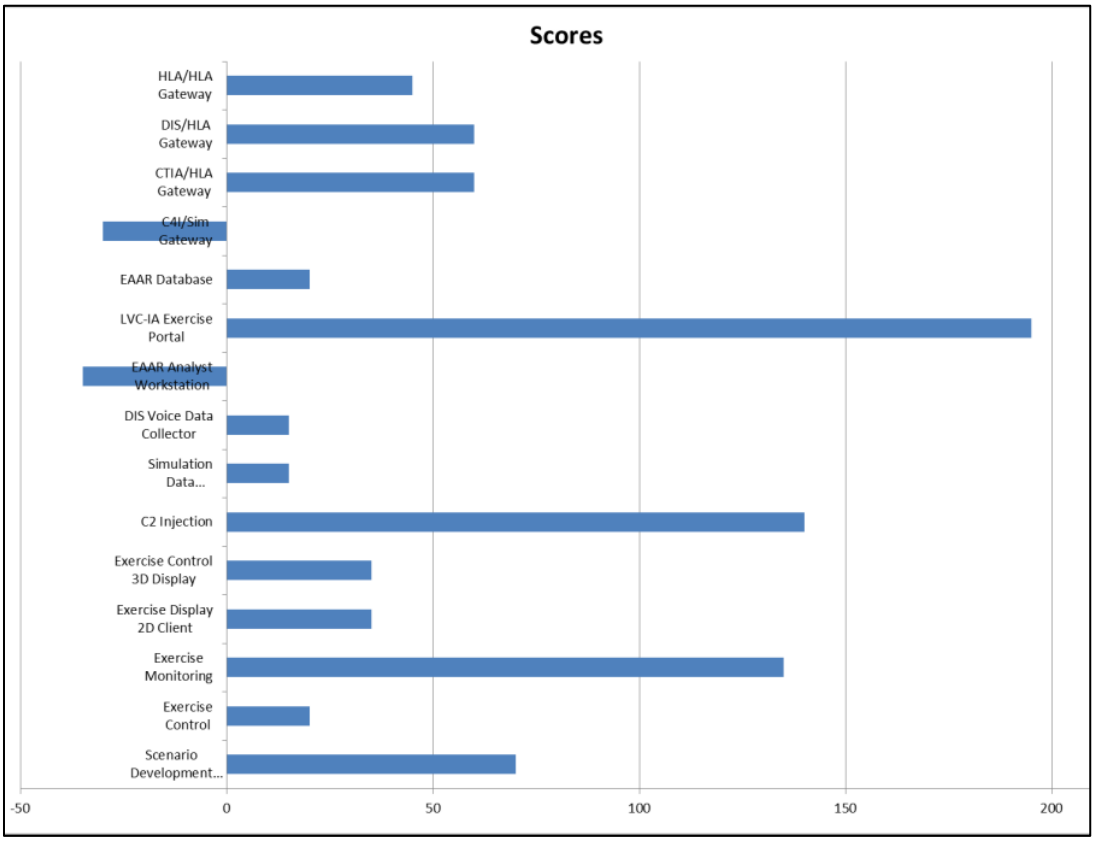

Figure 1 - General Criteria Summary of Scoring Results

The results of this analysis are somewhat predictable. The components with the highest scores are the good candidates for cloud-enabled. These are the components with some built-in cloud-optimization characteristics such as high tolerance for latency, loosely-couple interface with other components, and low dependency on other out-of-cloud components. The components with negative scores are not good candidates for cloud-enabled applications without cloud-optimization enhancements and/or having their out-of-cloud dependencies removed.

Cloud Service Providers (CSPs) Comparative Analysis

There are numerous commercial enterprises, who have either obtained, or are in the process of obtaining, the DoD CSM and FedRAMP accreditation. This comparative analysis task focused only on the CSPs that have achieved FedRAMP and DISA CSM compliance. The list of CSPs, used for this comparative analysis included the following candidates: (1) DISA milCloud, (2) Amazon Web Services (AWS), (3) Autonomic Resources (AR) Cloud Platform (ARC-P), (4) CGI Federal Cloud, and (5) VMWare/Carpathia. Table 2 provides a summary of our CSP comparative analysis and criteria used to select the CSP for the prototype phase. The information was gathered through Internet searches, emails, and teleconference with the organization points of contact. Note: data included in the table is representative of data captured at the time of the analysis and may not reflect latest data available.

Table 2 - CSP Comparative Analysis Summary

DoD Cloud Service Providers (CSP) Comparative Analysis (as of summer 2014)						
Provider / Product	**NIST Cloud Characteristics Compliance**(On-Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity, Measured Service)	**CSM/FedRAMP Compliance**	**Pricing (relative H/M/L)**	**Customer Responsiveness (relative H/M/L)**	**Support In-Cloud HLA and DIS?**	**Max Network I/F Supported per VM**
Autonotic Resource Cloud Platform (ARC-P) Community and Private Cloud	Complied with all.	AR has the following P-ATOs: **FedRAMP** P-ATO for IaaS (Community and Private) **FedRAMP** P-ATO (pending) for PaaS **DISA / DoD** P-ATO for impact levels 1 & 2 (Community and Private) **DISA / DoD** P-ATO (pending) for impact levels 3 & 4 (Community and Private)	Low	High	Yes	8
Amazon Web Services (AWS) GovCloud Government Community Cloud and AWS East/West US Public Cloud	Complied with all.	AWS GovCloud is compliant with many different IA controls. They have achieved compliance with **FedRAMP Impact Levels 1 and 2**, **DoD CSM Impact Levels 1 and 2,** FIPS 140-2, and ITAR. Additionaly AWS meets many of the NIST 800-53v3 controls that apply to CSM Impact Levels 3 - 5.	Low	Medium	No	2
DISA milCloud	Measured Service not addressed.	The milCloud infrastructure (vCloud / vSphere components) is currently accredited with an IATO. **A full ATO is scheduled for August 2014**. This is the "production" accreditation for the infrastructure.	Medium	Medium	No	Not disclosed
CGI Federal Cloud	Complied with all.	Receive **FedRAMP P-ATO by the JAB** on January 31, 2013. CGI was the second CSP and first large company to **receive a DoD P-ATO for impact levels 1 and 2.** CGI is actively working with DISA and SPAWAR to participate in DISA's Impact level 3 pilot.	High	Medium	No	Not disclosed
Carpatia/VMWare Virtual Cloud Government Service (vCGS)	Measured Service not complied.	Not available	N/A	Medium	Not tested	Not disclosed

LVC-IA Cloud Hosting Technical Challenges

There are a number of technical challenges in migrating the current LVC-IA to a cloud environment. We've held several technical interchanges with the CSPs to discuss these challenges. Some of these technical challenges and the CSP responses to these challenges are summarized below:

- LVC-IA and the core systems use the High-Level Architecture (HLA) and Distributed Interactive Simulation (DIS) for data exchange. Support for Multicast (MC) traffic used by HLA and broadcast (BC) traffic used by DIS between VMs in the cloud and from/to systems via external VPN connection is required.
    - AWS does not support MC or BC either within the cloud or site-to-cloud
    - CGI and milCloud "may" support but require custom work
    - ARC-P claimed that they can support but need to test and verify
- Ability to change Media Access Control (MAC) address for current HLA Run-Time Infrastructure (RTI) license is needed to avoid additional licensing cost
    - AWS does not support
    - ARC-P, CGI, and milCloud "may' support at the hypervisor level or require custom work
- Virtual Private Network (VPN) tunneling solution from our lab without Internet connection
    - Multiple options discussed
- Many LVC-IA Virtual Machines (VMs) are multi-homed and require multiple network interfaces in the current configuration. Some networks may need to be combined (i.e., Control/Backbone). Similarly, these VMs in the cloud would require multiple network interfaces.
    - AWS can only support up to two network interfaces per VM
    - ARC-P can support up to eight network interfaces per VM

Based on responses to our challenges, our selection was narrowed down between AWS and ARC-P as our possible choices for the prototype. Before making the final selection we needed to move on to the next phase to perform some initial technical evaluation.

LVC-IA CLOUD PROTOTYPE PHASE

The second phase of our project involved final technical CSP evaluation and selection, architecture design, and prototype implementation of LVC-IA in a cloud environment. The remainder of this paper describes the results of the CSP evaluation and selection and architecture design, since the prototype implementation was not completed at the time of paper submission.

HLA and DIS Tests in Cloud

We performed some basic HLA and DIS tests on the AWS and ARC-P cloud environments. The following sections summarize our test results.

To test the HLA multicast we needed to set up a federation with at least two federates. Since this was just a quick proof-of-concept test we decided to use the Modeling Architecture for Technology, Research, and EXperimentation (MATREX) in-house products: MATREX Run-Time Infrastructure Next Generation (RTI-NGmatrex); MATREX Federation Object Model (FOM); and MATREX Advanced Testing Capability (ATC) tool. The ATC instances were used as separate HLA/DIS federates. We set up two VMs in each cloud to run our simple HLA and DIS tests as depicted in Figure 2.

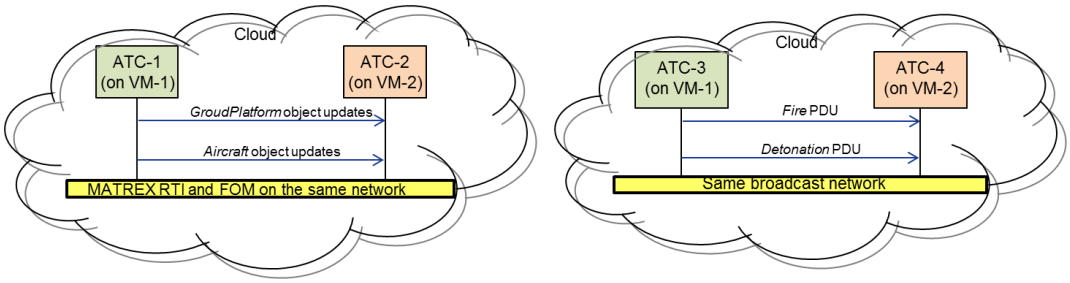

Figure 2 – HLA and DIS Test Architecture

AWS Test Results

We first tested the HLA and DIS interoperability between instances of ATC running on the same VM. These tests passed with no issue. Next we proceeded to test the HLA and DIS data interoperability between instances of ATC running on different VMs within the same virtual network in the cloud. The tests FAILED and confirmed that AWS does NOT support multicast within its cloud as they indicated. Since intra-cloud DIS data exchange does not work, we chose not to proceed with Site-to-Cloud HLA/DIS tests via VPN tunnel.

ARC-P Test Results

We repeated the same HLA and DIS tests done in the AWS environment using the VMs set up on the ARC-P. The results were better: the HLA and DIS interoperability tests between instances of ATC running on the same VM as well as running on different VMs within the same virtual network in the cloud all PASSED. The tests confirmed that ARC-P does support HLA/DIS multicast/broadcast within its cloud as they claimed. The next step in our technical evaluation plan was to repeat the similar HLA tests but have a federate on our site exchanging data with another federate hosted in the cloud via VPN tunnel. AR had previously indicated that this should work but later decided NOT to support due to security concern.

CSP Selection for Prototype

Based on our initial technical evaluation, ARC-P resulted as the better choice for our prototype. Their IaaS service is more flexible and it addresses more of our LVC-IA/ITE requirements/challenges than the other candidates and they had been very responsive in supporting us during the entire evaluation period.

Cloud Computing Architecture Design

The LVC-IA architecture uses a series of Joint Simulation Bus (JBUS) based gateways that maps different LVC protocols to/from a common data model called Common Data Definition (CDD). This architecture allows the ITE (LVC) core systems to interoperate without requiring any major adaptation on their parts.

Our initial cloud computing design for the prototype was based on a LVC-IA architecture baseline which used HLA as its main data transport backbone. Since our CSP technical evaluation concluded that using HLA site-to-cloud was not feasible, we decided to look at a newer version of LVC-IA, being developed by the POR, as the architecture baseline for our cloud architecture design.

Since this newer version of LVC-IA has a requirement to support distributed operations at remote sites interoperating with home station, this newer architecture version uses Enterprise Service Bus (ESB) and Java Messaging Service (JMS) technologies to implement a data backbone transport service called the Data Model Transport Channel (DMTC). DMTC transports the serialized CDD messages between systems and sites eliminating the need for HLA/DIS multicast/broadcast (LVC-IA CDR, 2014). This architecture lends itself better for cloud hosting since this DMTC feature reduces the number of translation hops compared to the HLA-based backbone used in previous LVC-IA versions. There are still some LVC-IA components that use a HLA-based backbone but the main data exchange with the virtual systems (in the home station or remote sites) is accomplished via JMS. Figure 3 shows a high-level architecture view of an unclassified instance of this newer LVC-IA version located in the STTC RRTB lab.

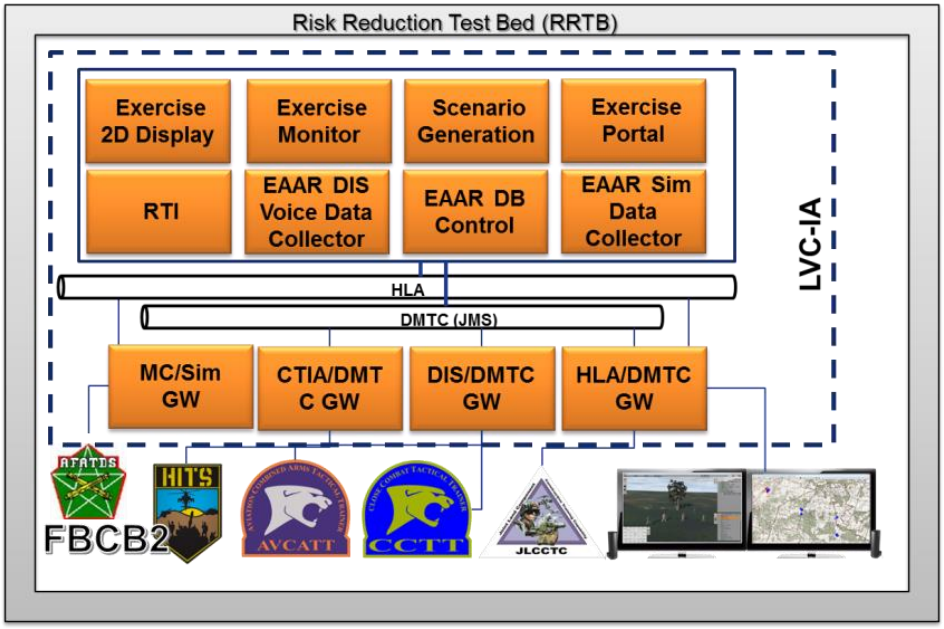

Figure 3 Newer version of LVC-IA instantiated at the RRTB

Since site-to-cloud multicast is not feasible we had to look at architecture options that allow JMS to be used. This meant that most of the legacy core systems that will be located at local sites will have to communicate with components of LVC-IA in the cloud using VPN tunnels. Figure 4 shows our initially planned LVC-IA cloud prototype architecture.

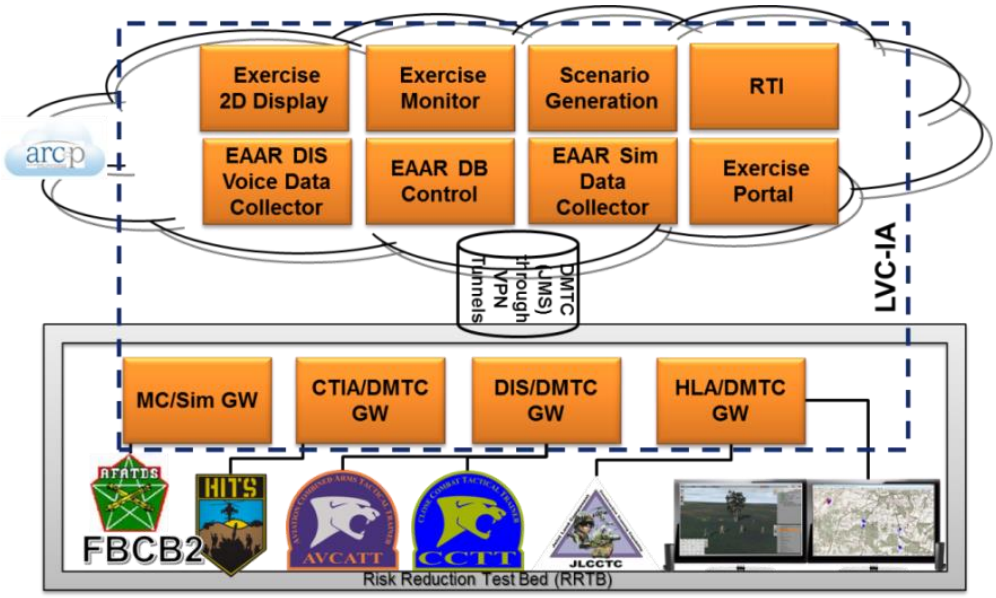

Figure 4 – Initially Planned LVC-IA Cloud Prototype Architecture

Cloud Information Assurance (IA) Challenges

The newer version of the LVC-IA, being used by our cloud research did not receive its Authority to Operate (ATO) in a Closed Restricted Network (CRN) until several months into our research schedule. Even with the accreditation, this version of LVC-IA is not authorized to operate in any open network or cloud environment (Connected Restricted Network). Therefore, our team had to work with PEO STRI and STTC cyber security professionals to

obtain an Interim Authority To Test (IATT) before the first LVC-IA component could be uploaded to the cloud. This IATT process consisted of many lengthy steps and dependencies. Some critical dependencies are listed below.

- LVC-IA software version used in our research must include full information assurance accreditation to be used as the initial accredited baseline in the RRTB
- Any changes to the initial accredited LVC-IA software version, in support of the cloud research, must be scanned and documented in the IATT package submitted for approval
- All LVC&G core systems and mission command systems used in our research must be updated to the latest version with their own accreditation

Prototype Implementation

Once the IATT is approved, we will proceed with our cloud prototype implementation using the ARC-P cloud environment. Our plan is to experiment with different options of placing different LVC-IA components in and out of the cloud, evaluate performance impacts, and make and document necessary changes to the LVC-IA software to accommodate our prototype cloud architecture. We will provision the VMs in our cloud environment and set up all the networking required per our design. Once the VMs and networking are set up, we will gradually upload the components to the cloud. As each part of the architecture component is set up, interoperability tests will be performed to ensure that the components can communicate between different Virtual Local Area Networks (VLANs) per our design. Once our cloud environment is set up, we will proceed with the integration of other LVC-IA components and core systems located in our lab with the LVC-IA components in the cloud. We will adapt the Long Haul Gateway to connect the core systems with the LVC-IA-in-the-cloud through VPN tunnels.

As for test methodology employed, we've developed a test plan that includes the relevant test cases from the LVC-IA End-to-End test plan. Other than functional verification tests we will focus on the technical performance measurements (TPM) tests and compare the results between non-cloud and cloud-enabled environments. Some of the tests in our test plan include (will be repeated for non-cloud and cloud-enabled environments): entity reflection tests between the LVC systems, maneuver and fire engagement tests between the LVC systems, situational awareness reflection tests from LVC entities on mission command systems (MCS), latency tests between the LVC systems, and network throughput tests between the LVC systems. We'll also record bandwidth usage and cost of running LVC-IA in a cloud based on usage.

Since IATT approval was not received until this paper was finalized, the prototype implementation results will be shared in a subsequent opportunity.

SUMMARY AND PATH FORWARD

To align with the DoD and Army cloud computing strategies and visions, this research examined the feasibility of cloud-enabled components of LVC-IA while maintaining the same level of interoperability with the ITE core systems in remote sites. Our research uncovered some technical challenges with the cloud environment for the current LVC-IA systems that required some re-architecting and adaptations. There were many challenges for the legacy HLA- and DIS-based federations to migrate as-is to operating in a cloud. The most notable challenge was that most cloud environments did not support intra-cloud or site-to-cloud HLA multicast and DIS broadcast. We learned from our project that the increased cyber security / IA requirements also presented many challenges for cloud migration. Organizations which want to migrate their LVC systems to the cloud should allow enough time and resource in their planning.

To realize the full benefits of the cloud a goal would be to cloud-optimize the LVC-IA applications and as much ITE core systems as possible. With cloud-optimized applications we can evolve from hosting LVC-IA on an IaaS cloud, to providing additional platform services in a PaaS layer, and ultimately, to providing LVC simulation (software) services in a SaaS layer. Various cost-benefit analyses are currently being conducted to assess the cost-benefit tradeoffs of migrating LVC-IA and other ITE systems to the cloud. In addition, since several conditional dependencies impact an organization's ability to use commercial CSPs, LVC-IA and ITE SoS are assessing these conditions against the Risk Management Framework (RMF) requirements of their system. Even if the LVC-IA and/or other systems within the ITE SoS are not ultimately targeted for cloud migration or optimization, the research

conducted under this initiative will provide important data points for decision makers as they plan for technology insertion into the existing ITE SoS or future programs like the Synthetic Training Environment.

Currently, other RRTB initiatives, such as the Live Synthetic Training and Test & Evaluation Infrastructure Architecture ((LS TTE IA) activity, are exploring next generation architectural constructs which align with Army COE Data Center /Cloud Computing Environment objectives and technologies. The LS TTE IA is a cloud-enabled Service Oriented Architecture proof of concept with an expressed goal of supporting both the Training and the Test & Evaluation communities. LS TTE IA designers are investigating, via active prototyping and coordination with various development teams, the feasibility of COE compliance and suitable for hosting within the COE Data Center/Cloud Computing Environment. (Dumanoir et al., 2015). These initiatives provide a key platform for risk reduction on current and future Army PORs.

REFERENCES

United States Army. (2015). *Cloud Computing Strategy*, v1.0, March 2015

United States Department of Defense (DoD). (2015). DoD Cloud Computing Security Requirements Guide (SRG), Version 1, Release 1, 12-January-2015

United States Department of Defense (DoD). (2013). *DoD Enterprise Cloud Strategy Documents*, v.94, 15-MAY-2013

United States Army Program Executive Office for Simulation, Training and Instrumentation (PEO STRI). (2013). *LVC-IA v2.0 Critical Design Review*, November, 2013

National Institute of Standards and Technologies (NIST). (2011). *NIST Definition of Cloud Computing*, SP 800-145, September 2011

Forbes Magazine Online Edition. (2015, January 24). *Roundup of Cloud Computing Forecasts and Market Estimates*. Retrieve from the Forbes Magazine website: http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/

Dumanoir, P., Barie, S., Crutchfield, R., Grippin, B., Willoughby, M., Wittman, R. (2015). Live Synthetic Training and Test & Evaluation Infrastructure Architecture (LS TTE IA) Prototype. For publication I/ITSEC 2015.