HOMELAND SECURITY
COMMUNITY OF BEST PRACTICES

Benefits, Best Practices, & Risks of Using Cloud Technologies

January, 2023

James Fountain, PMP CISM
james.fountain.7.ctr@us.af.mil

To enhance T&E science through multidisciplinary collaboration and deliver it to the DHS workforce through independent consultation and tailored resources.

About this Publication:
This work was conducted by the Homeland Security Community of Best Practices under contract FA8075-18-D-0002, Task FA8075-21-F-0074.

For more information:
Visit, https://www.afit.edu/HSCOBP/
Email, AFIT.ENS.HSCOBP@us.af.mil

Homeland Security Community of Best Practices
2950 Hobson Way
Wright-Patterson Air Force Base, Ohio

Version: 1, FY23

THEORY into PRACTICE

Table of Contents

Introduction

This document details aspects related to Test and Evaluation (T&E) in a cloud environment. The Department of Homeland Security's (DHS) 2019–2023 Information Technology Strategic plan includes a department-wide modernization initiative to adopt cloud-based computing. Unfortunately, the DHS Office of the Inspector General (OIG) noted most DHS system migration went to the cloud as-is without taking steps to maximize the benefits of cloud technologies (2020). While migration to the cloud has been taking place across government for many years, it is not without its challenges. This document is intended to help T&E practitioners transition from traditional T&E methods by presenting the benefits of cloud technology, providing best practices, highlighting risks, and illuminating areas for further research. Because the topic is so broad, this document should be used as an overview and reference tool rather than a "how-to" guide.

Background

The Homeland Security Community of Best Practices (HS COBP) held a research roundtable on the DHS critical research area of Cloud Technologies on October 26–27, 2022, which focused on cloud technology both *in* the cloud and *of* the cloud. Bertolino et al., (2020) emphasized the benefits of using cloud technology: "The cloud offers the opportunity to develop and maintain costly test infrastructures and to leverage on demand scalable resources for configuration...and performance…testing." Please note that this HS COBP document is predominantly focused on best practices for T&E *in* the cloud. However, as there is some overlap, some elements of testing *of* the cloud have been included.

The HS COBP Cloud Technologies Roundtable event included almost three dozen participants. Multiple areas of cloud technologies and their impact on DHS T&E were explored and reviewed over the two days. Key objectives for the event included:

- To review and identify key cloud technology T&E terms to ensure a collective use and understanding
- To define and differentiate testing 'in the cloud' vs. 'of the cloud'
- To determine methods that can be used and measured for testing *in* the cloud
- To identify and discuss testing *in* the cloud infrastructure
- To identify new or novel evaluation of testing *in* the cloud approaches and methods

While these objectives apply directly to cloud technologies, we cannot discuss testing *in* the cloud before first introducing the parallels to software testing.

Cloud testing is rooted in software testing. A recent study by Sogeti, Part of Capgemini sheds light on how software testing is approached across private industry. Over 1,600 IT executives from different global companies were surveyed on current practices and future trends in software quality and testing. According to the report,

- 73% of organizations already use environments deployed in the cloud and in relation to testing cloud-based applications,
- 63% of organizations mainly do performance testing,
- 62% of respondents mentioned security testing,
- 57% of organizations stated that assessing peak-load requirement was a common testing scenario, and
- 33% of respondents do not use any specific approach to test cloud-based applications.

(Saunders & Buenen, 2017)

When asked about software testing, most of the respondents spoke of their cloud environment and cloud related test efforts. This speaks to how deeply rooted cloud testing is already within industry. While cloud testing is similar to traditional software testing, it encompasses more. Cloud testing can refer to testing cloud resources, testing software in a cloud environment, or even using cloud-based tools for quality assurance testing (Chai, 2021).

There are three basic types of testing that can be performed *in* the cloud: functional, non-functional and cloud specific (TestingXperts, 2022). Functional and non-functional testing are similar to those performed in typical software tests. Functional tests can include end-to-end business flow, exploratory testing, data migration testing, automation testing, acceptance testing, integration testing, or compatibility testing. Non-functional testing may include performance testing, business requirement testing, or security testing. Lastly, there are cloud-specific types of tests such as disaster recovery testing, compatibility/browser performance testing, or multi-tenancy testing. For more details on any of these types of tests please see *Cloud-Based Testing: Benefits, Challenges, Types, and Tips* (Bryk, 2022) or *Overcome Challenges of Testing in Cloud Computing* (TestingXperts, 2022).

In addition to the types of tests that apply to cloud testing, there are certain techniques to test in a cloud environment. Software testing performed in the hosted cloud environment can be summarized into four core testing techniques (Siddiqui & Ahmad, 2016): Prioritization Techniques, Clustering Techniques, Load Distribution Scenarios, and Security Testing Mechanisms (Figure 1).

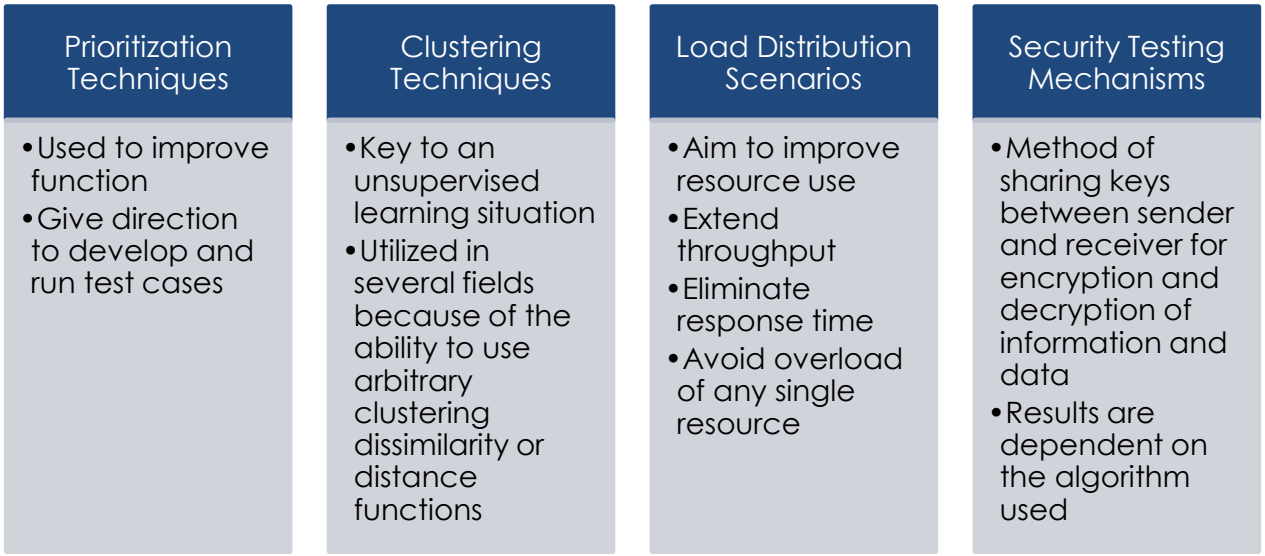

Figure 1

Four Core Testing Techniques

When looking at the presented benefits, best practices, risks, and future opportunities, consideration should be given to whether each applies to a specific type of test or test technique.

Cloud Environment Benefits

There is currently an organizational shift where more systems are being hosted in a cloud environment. So, what makes the cloud environment better than traditional hardware?

- Better return on investment due to the automation, flexibility, and scalability (and less overall resources required)
- Additional cost savings since less infrastructure is required for more accessibility
- Can be used from anywhere, as it is missing the physical restrictions, which improves collaboration
- Backups ensure less risk of data loss
- Added layers of security are available in a cloud environment
- Elasticity to drive a quicker testing response
- Reliability of testing processes, even during application mishaps or data breaches

Consider that the above list can be broken down further into the direct benefits of cloud testing.

TestingXperts (2022) list some of the foundational cloud testing benefits as (see Figure 2):

Scalability

- While leveraging a cloud-based testing platform, digital applications do not have to limit the number of users for performance testing
- Cloud performance testing is more realistic regarding types of visits, number of users, and geo-locations

Customization

- A cloud system can be used to emulate agency-centric environments
- Cloud testing enables the utilization of various permutations of test scenarios that include different configurations, web browsers, external devices, and operating systems

Remote Testing

- Cloud performance testing may be executed from anywhere the application is available enabling global scalability

Production Testing

- Tests are generally limited to the application test environment, but cloud performance testing can also be in production environments

Reduced Costs

- Using the cloud as a testing platform reduces the need for installation and maintenance configuration

Team Collaboration

- Cloud-based testing allows for inclusion of Development, Security, & Operations (DevSecOps) in workflows because of the collaboration between developers and testers
- Testers can spin up test environments with different configurations and data in the cloud, automate testing processes, integrate with development tools to provide fast feedback, and implement DevSecOps to help set up devices

Enterprise App Coverage

- Most applications are browser-based but enterprise apps often require higher computing capabilities
- Cloud-based testing enables effective testing with support for various internet or application protocols

Figure 2

Foundational Cloud Testing Benefits

There are additional benefits to cloud testing when combined with other software methodologies such as DevSecOps (Development, Security, and Operations). DevSecOps is a software development philosophy that integrates writing code with testing, securing, and deploying that code. DevSecOps can break down silos between the traditional roles of developers, security engineers, operation engineers, and quality assurance professionals and have them function as a team. Cross-functional teams work side-by-side with full ownership for the successful development, launch, and maintenance of their service. Continuous Delivery is the process of delivering the code that was integrated, built, and tested on regular intervals using automation. Agencies can produce more reliable software when it is time for deployment by setting the pass and fail criteria for testing, being ready for deployment early in the software development lifecycle (SDLC), and then using automated processes to check that the criteria are met. Not only does this practice help catch deployment issues early, but it also increases stakeholder support by supporting an agile workflow that allows for smaller and more frequent course corrections since the partially functioning product can be demonstrated to stakeholders (SecyDHS, 2022). Combining DevSecOps with cloud testing practices can greatly enhance the functionality and success of the software.

Cloud testing can also enhance the 'agility' of a software development process and is considered a good match to distributed agile teams (Akerele et al., 2013). The relative impact of cloud testing on agile development projects is detailed below:

- Feedback is vital in agile processes. Cloud testing significantly reduces the test cycle times of software projects and consequently, the deployment cycle. Cloud testing not only has a major impact on the time-to-market, but it also improves the flexibility of the system to accommodate changes and requirement creep.
- Cloud testing eradicates the problem of proximity in dispersed development teams. It bridges the geographical distance between global teams–enabling easy interchange and handover of feature development among teams as if they were collocated. Teams can now collaborate globally with a self-defined user interface.
- Every testing activity can be revealed and made visible in real time and accessed from anywhere via a custom URL for the organization.
- Cloud testing fully supports agility in testing by creating a welcoming platform for writing and importing automated scripts for functional testing. Cloud test platforms usually have plug-ins that allow the recording of the test activities to be analyzed after test completion. Valuable time can now be spent investigating new possible bugs instead of exhausting time running repeated tests manually. Cloud testing also provides an environment to concurrently run tests with different configurations on the same machine.
- Cloud testing encourages frequent changes to requirements as testing the modified system is possible anywhere. The effect (estimated finish date) of the frequent changes in the requirements and requirement creep is offset by the reduced test cycle achieved by cloud testing. Also, the scalability of the system makes it possible to test each iteration feature, as each iteration feature might require the ramping up and scaling down of the system requirements.
- Cloud testing also allows the quick ability to reproduce bugs for further analysis. This has been a major issue in traditional testing. There is a constant need to regenerate bugs that were detected in an environment for further investigation.

- Cloud testing creates synergy by being fully supportive of agile development techniques such as the Test-Driven-Development. Automatic unit tests are written to fail, pass, and refactor–all *in* the cloud.

Best Practices

While not applicable to all areas, the following best practices gathered from the roundtable and industry might be useful for a variety of DHS T&E cloud testing activities:

- Performing testing more periodically. Test labs in cloud hosted environments typically sit idle for long periods, consuming capital, power, and real estate. Research indicated that approximately 50% of the infrastructure earmarked for testing is underutilized. This provides opportunities for programs to re-verify performance (Meadors, 2022).
- Traditionally, testing has been limited to websites (maybe a single browser) or desktop applications. With the advent of multiple devices, the testing spectrum has widened. Take advantage of the plethora of options available to test faster (Meadors, 2022).
- Improper cloud usage, for novice organizations, may sometimes increase costs as there are limited configurations available. Organizations should perfectly analyze their needs before committing to a cloud vendor to optimize cost. Also, project teams and test teams should thoroughly plan the environment usage from assembly to utilization to disassembly (Meadors, 2022).
- The T&E organization should add more personnel to the team with better utilization of organizational resources to support other mission areas (Meadors, 2022).
- Some of the available load-generating apps work across cloud platforms but verifying the compatibility of such tools with the application architecture is essential. By evaluating the latest load testing tools and models, key features such as bandwidth simulation, upload / download speeds, etc., can be accurately represented to understand the load limits (TestingXperts, 2022).
- Choose the load testing tools that include features such as analytics, reports, and scheduling. By focusing on leveraging automation and scheduling, the DevOps teams can avoid overworking production systems while testing and scheduling the ongoing load tests. Once the tests are completed, these tools share comprehensive reports with the respective stakeholders so that everyone has a clear picture of how the app is performing (TestingXperts, 2022).
- It is often difficult to identify a root cause in the case of possible reasons for poor app performance. By testing both inside and outside the firewall, the load test plan should find and fix performance bottlenecks (TestingXperts, 2022).
- Merely exposing the app to high loads until failure may not generate a realistic scenario. This is also true when using similar types of devices, browsers, bandwidths, or OS. By simulating real conditions in the load testing environment an agency should be able to provide a diverse range of test scenarios, keeping the user load at a base level with different configurations (TestingXperts, 2022).
- To maximize the value of cloud performance testing, teams must prioritize the bugs. Once the data and insights are available, testing teams should strategically take actions to achieve the maximum return on investment from testing efforts (TestingXperts, 2022).
- Performance tests are often focused on servers and clusters. However, these tests should measure the human element (users) as well. Cloud performance testing should consider members of the eventual application for comprehensive test results (TestingXperts, 2022).

Challenges/Risks

Any discussion of cloud testing methods needs to be balanced with an understanding of the associated risks. As described below, understanding, analyzing, and dealing with possible risks within the hosting cloud environment are also critical in ensuring successful T&E methods (Akerele et al., 2013):

- It is a common illusion that cloud-computing testing is generally cheaper. Ongoing intrinsic costs associated with cloud testing should include the cost to support privacy regulation policy as well as cost to build auditing processes in the system and recovery service cost.
- It is a good practice to hold regular meetings with the cloud test vendor to highlight any areas of concerns, risks, or issues that might arise. This is unlike the on-premises sites where there is a governance system to ensure compliance. This risk can be mitigated by emphasizing compliance on the contract agreement and strictly outlining the organizations' specific policies.
- The testing processes of the service provider might not be following the principles governing the agency's organization. Service providers usually have separate regulations governing their operations and infrastructure management. This might be difficult to verify even when specified in the Service Level Agreement (SLA) due to the limitation of the agency's involvement in cloud vendor's activities. Vigorous testing should be performed and aimed at determining the cloud environment's risk level for security, scalability, reliability, and performance. These tests should be fully run before an agreement or update is signed with the cloud provider and before executing any test.
- A major risk factor is the learning curve of the testers using the Domain-Specific Language (DSL) of the service provider's platform (if any). Metrics such as defect density, test coverage, etc. should be closely monitored while remaining alert to any demonstratable risk level of variability in the system performance.
- A major risk in cloud testing revolves around security–especially when the agency's data will be stored along with the production environment *in* the cloud. The utilization of a vendor platform creates risk because agencies may cede control of the platform and data to the vendor. This risk is exacerbated when a part of the cloud services is federated to a third party by the hosting cloud vendor. In the event the service provider terminates the service provision due to financial or strategic reasons, the user could potentially be in trouble if a 'plan B' is not in place.
- There is also a major risk when the testing activities are completely outsourced to a cloud test service provider. The cloud vendor's personnel could be easily 'tapped' for information about the development organization's product and be offered a reward for such an act.
- The breakdown of the testing platform server entirely paralyses the testing activities. The risk of this occurrence affects not only the testing activities but all other activities dependent on the testing phase. Hence, the server needs to be up and running as well as being always available to prevent this period of inactivity. Running availability tests before choosing the vendor can help reduce this risk.

Test execution risks: Test area managers need be on the lookout for issues applying particular T&E methods *in* the cloud. These challenges can include (Bertolino et al., 2020):

- Establishing a test environment that properly replicates user applications, especially with field devices, could impact levels of configuration, network operations, or storage management that remain a non-issue in single hosted cloud applications. Additionally, limits to the T&E methods application in field situations could further impact successful Verification

& Validation (V&V) activities and results.
- Data privacy, driven by regulatory compliance, or cloud vendor operational constraints established back within the base SLA can cause their own risks. The test team's operational metrics may be negatively impacted by the need for cloud operations to comply with their own operational security standards, as well as allow the agency to operate their own test scripts or V&V activities.
- Risks associated with load balancing and bandwidth management may also arise given application changes across multiple environments while testing is underway or during the life cycle of application usages for a given delivery approach.
- Synchronization issues may arise when performing testing across multiple cloud vendors or even within a changing hosted cloud environment. T&E methods may not be meant to span multiple devices or field applications. These also cause complexities in security synchronization as public vs hybrid cloud hosting also may have a negative impact on successful V&V activities by inhibiting consistency in evaluation and uniform certification.

Recurring risks: There are also certain risks which tend to reoccur and could negatively impact any T&E method (Bertolino et al., 2020):
- The complexity of applications and infrastructures that are deployed and tested *in* the cloud is increasingly higher thus impacting how testing is completed and tracked.
- Existing T&E techniques do not consider specific cloud environment features, e.g., heterogeneity, scalability, load balancing, communication, frequent failures, and synchronization between distributed test managers. This can impact the types of tests that can be used and how testing can be implemented.
- The construction of a test environment *in* the cloud is often tedious, time-consuming, and complex, which can impact sizing of the allocated virtual machines or result in unbalanced loads. This has a negative impact on test execution since it can cause low resource utilization or increased response time.
- In non-functional testing (e.g., load, performance, or stress testing), factors such as network bandwidth or workload could impact V&V activities which impacts test evaluation.
- Costs are often under-estimated, especially for the computational resources needed to properly configure the environment DSL of the service provider's platform.

Future Opportunities

As a result of the HS COBP hosted roundtable on Cloud Technologies, participants brainstormed new or innovative approaches on T&E *in* the cloud. This included a list of questions which are expected to drive additional research:

Low Impact, High Relevancy
- What equities/ownership interests in cloud development and testing need to be allocated to the relevant communities?
- What guidance is appropriate for acquisition programs defining the T&E boundary and attack surface for cloud-based systems?
- How can organizations best implement cloud technologies?
- What are the benefits of moving a legacy system to the cloud?
- What agency acquisition strategy should be developed for cloud testing?
- On what platforms do we need to test the system to reach a desired confidence level?

High Impact, Low Relevancy

- Should new government-wide standards be created, or should the government adopt the evolving industry standards?
- What elements of a cloud service are appropriate for verifying that providers are meeting their contractual performance and reliability obligations?
- What test factors should drive migration from a legacy hardware host to a hosted cloud platform?
- What workforce development is needed to enable cloud deployment?
- Who should take ownership for deciding the audience and amount of workforce development?

High Impact, High Relevancy

- How can we implement DHS doctrine for cloud hosted database testing that can support enterprise resilience evaluations?
- How do we mitigate Cloud Service Provider ownership and software ownership / provenance risk?
- When is the optimal time to bring in members of the testing team to system development?
- How do cloud-based systems interoperate with other systems, whether cloud-based or not?
- What is the best approach to request standardization of software as a service (SaaS), infrastructure as a service (IaaS), or platform as a service (PaaS) for cloud test and evaluation?
- What cloud-specific acceptance criteria need to be traced in T&E strategy briefings and Integrated Evaluation Framework (IEF)?
- What are the criteria for deploying DHS product development on dedicated cloud platforms to protect mission data?
- How can we help programs that are new to the cloud get started quickly and rigorously with testing? E.g., what goes into a cloud testing template?

References

Akerele, O., Ramachandran, M., Dixon, M. (2013). Testing in the cloud: Strategies, risks and benefits. In: Mahmood, Z., Saeed, S. (eds) *Software Engineering Frameworks for the Cloud Computing Paradigm* (pp. 165-185). Computer Communications and Networks. Springer, London. https://doi.org/10.1007/978-1-4471-5031-2_8

Bertolino, A., De Angelis, G., Gallego, M., Garcia, B., Gortázar, F., Lonetti, F., & Marchetti, E. (2020). A systematic review on cloud testing. *ACM Computing Surveys, 8*(5), pp. 1–43. https://doi.org/10.1145/3331447

Bryk, A. (2022, May 20) *Cloud-based testing: Benefits, challenges, types, and tips*. Apriorit. https://www.apriorit.com/qa-blog/548-cloud-based-testing

Chai, Wesley (2021, Feb). *Definition: Cloud testing*. TechTarget. https://www.techtarget.com/searchstorage/definition/cloud-testing

Meadors, R., (2022, Nov 7). *Roundtable 4-Cloud Technologies.* Wright Brothers Institute.

Saunders, P., Buenen, M. (2017). *World Quality Report 2017-2018*. Sogeti, Part of Capgemini. https://www.sogeti.com/explore/reports/world-quality-report-2017-2018/

Siddiqui, T., Ahmad, R. (2016). A review on software testing approaches for cloud applications. *Perspectives In Science(8),* pp. 689–691. https://www.sciencedirect.com/science/article/pii/S2213020916301999?via%3Dihub

TestingXperts (2022, Oct 25). *Six best practices for cloud performance testing*. TestingXperts. https://www.testingxperts.com/blog/cloud-performance-testing

TestingXperts (2022, Jul 1). *Overcome challenges of testing in cloud computing*. TestingXperts. https://www.testingxperts.com/blog/overcome-challenges-of-testing-in-cloud-computing/

U.S. Dept. of Homeland Security, SecyDHS (2022). *Cloud Security Technical Reference Architecture.* U.S. Digital Service, Cybersecurity and Infrastructure Agency (CISA) and Federal Risk and Authorization Management Program (FedRAMP)*(2),* pp. 1–70. https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

U.S. Dept. of Homeland Security, DHS-OIG (2020). *Progress and Challenges in Modernizing DHS IT Systems and Infrastructure.* U.S. Department of Homeland Security, Office of Inspector General, pp. 1–40. Report # OIG-20-61. https://www.oig.dhs.gov/reports/2020/progress-and-challenges-modernizing-dhs-it-systems-and-infrastructure/oig-20-61-aug20