CLOUD ONE

FAST
SECURE
STREAMLINED

Arcturus
(Cloud One DevSecOps Tools)

INTERIM AUTHORITY TO TEST (IATT)

TEST PLAN

Version 1.0

Prepared By:
Clarity Innovations

Controlled by: AFLCMC/HNII
CUI Category: CTI
Distribution D

POC: tracy.sims.2.ctr@us.af.mil
myrtle.hall.ctr@us.af.mil
kiyo.larson.ctr@us.af.mil

DISTRIBUTION Distribution Statement D: Distribution authorized to the Department of Defense (DoD) and U.S. DoD contractors only; administrative/operational use; 15 March 2013. Other requests shall be referred to AFLCMC/HNII IL6 AFB, MA 01731.

RECORD OF CHANGES

*A–ADDED M–MODIFIED D–DELETED

Version No.	Date	Section(s)	Brief Description	Author
1.0	5/15/2024		Initial Document	Clarity Innovations

SYSTEM INFORMATION

System Name	Arcturus Cloud One DevSecOpsTools
Version/Release	1.0
eMASS ID	11080
ITIPS	N/A
DITPR-DON #	N/A
DADMS #	N/A
Testing Dates	TBD
C1 Program Manager	Mr. Joseph Thorp, joseph.thorp@us.af.mil
Arcturus Program Manager	Mahika Saxena, mahika.saxena@us.af.mil
C1 Arcturus ISSM	Mr. Aaron Bowers, aaron.bowers.ctr@us.af.mil
Current Authorization Status	Unauthorized

APPROVED BY:

Contents

EXECUTIVE SUMMARY

Arcturus is a set of tools for hosting application code, testing and scanning applications, and deploying applications to the cloud within CloudOne. Arcturus works with customers to onboard them into Gitlab with project group creation and initial Jarvis pipeline configurations. The Jarvis pipeline builds, tests, scans, and deploys the application to the CloudOne cloud automatically.

Arcturus includes the CI/CD pipeline, runners, the three separate stages of build, test, and scan, and cloud delivery. The CI/CD pipelines are Continuous Integration (CI), Continuous Delivery (CD), and Continuous Deployment (CD) pipelines which automate phases of software development, from the build, to testing and scanning, through to release and deployment. Runners are machines, or VMs, configured and registered with GitLab which are provisioned to run the CI/CD jobs.

First, code is pushed to a GitLab repository, the build stage is triggered and code is compiled and ready for the next stage. During the test stage, all tests are run, including unit tests, UI tests, and functional tests. The scan stage includes scanning jobs that are used to help perform quality and security checks for an app. Once the test stage completes successfully, the delivery stage packages the compiled code, along with all its dependencies, into an artifact available for customer deployment into a specified landing zone. The Arcturus pipeline offers functionality to automate delivery of containerized systems to target distribution platforms onto Cloud One.

Arcturus is seeking a 1 year Interim Authority to Test (IATT).

PURPOSE

The purpose of this IATT Test Plan is to provide Rapid Cyber Acquisition (RCA) documented evidence that supports Cloud One's effort to obtain an IATT. The IATT is an integral part to obtaining an Authorization to Operate (ATO). The IATT results will provide a detailed technical record of the CNAP environment(s), as it pertains to vulnerability and risk management, and will provide the RCA Authorizing Official (AO) the ability to make an informed risk determination and authorization decision.

This IATT Test Plan will define the Arcturus environment, identify the applicable National Institute of Standards and Technology (NIST) 800-53 Rev 5 controls, Center for Internet Security (CIS) Benchmarks, Security Technical Implementation Guides (STIGs), and any other information necessary to accommodate a thorough and complete cybersecurity assessment.

Section 1: HARDWARE

Device	Manufacturer	Description
EC2	AWS	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud.
ECS - EC2/Fargate	AWS	Amazon Elastic Container Service (Amazon ECS) is a fully managed container orchestration service that helps you easily deploy, manage, and scale containerized applications.
S3	AWS	Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.
EBS	AWS	Amazon EBS allows you to create storage volumes and attach them to Amazon EC2 instances.
RDS	AWS	Amazon Relational Database Service (Amazon RDS) is a collection of managed services that makes it simple to set up, operate, and scale databases in the cloud.
ECR	AWS	Amazon Elastic Container Registry (Amazon ECR) is an AWS managed container image registry service that is secure, scalable, and reliable.
Inspector	AWS	Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
Secrets Manager	AWS	AWS Secrets Manager is a secrets management service that helps you protect access to your applications, services, and IT resources.
Systems Manager	AWS	AWS Systems Manager provides configuration management, which helps you maintain consistent configuration of your Amazon EC2 or on-premises instances.
VPC	AWS	Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.
SNS	AWS	Amazon Simple Notification Service (Amazon SNS) is a web service that makes it easy to set up, operate, and send notifications from the cloud.

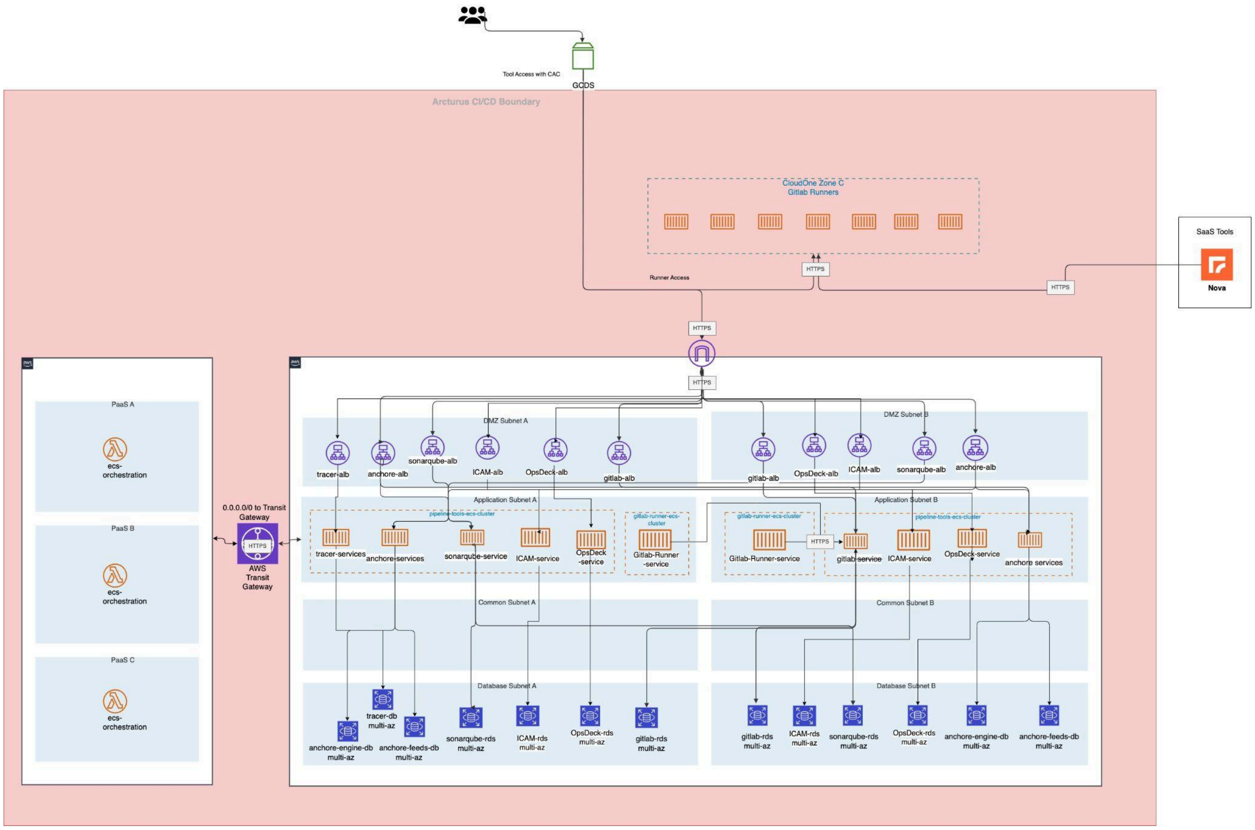
EventBridge	AWS	Amazon EventBridge is a service that provides real-time access to changes in data in AWS services, your own applications, and software as a service (SaaS) applications without writing code.
EC2 Auto Scaling	AWS	Amazon EC2 Auto Scaling helps you maintain application availability and lets you automatically add or remove EC2 instances using scaling policies that you define.
CloudWatch	AWS	CloudWatch enables you to monitor your complete stack (applications, infrastructure, network, and services) and use alarms, logs, and events data to take automated actions and reduce mean time to resolution (MTTR).
CloudWatch Logs	AWS	Amazon CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files.
CloudTrail	AWS	CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage.
Elastic Load Balancing - ALB/NLB	AWS	Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones.
KMS	AWS	AWS Key Management Service (KMS) gives you centralized control over the cryptographic keys used to protect your data.
IAM	AWS	AWS Identity and Access Management (IAM) can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.

Section 2: SOFTWARE

Software Type	Vendor	Name	Version
Version Control / Pipeline Orchestrator	Gitlab	Gitlab	16.11.2-ee - manually updated following new releases
Software Scanner	Sonarsource	SonarQube	10.4
Software Scanner	OWASP	OWASP Dependency Check	9.0.9

Software Scanner	Anchore	Anchore	5.2.0
Software Scanner	Aqua Security	Trivy	0.48.1
Software Scanner	Checkmarx	KICS	1.7.12
Software Scanner	Gitleaks LLC	Gitleaks	8.18.2
Infrastructure as Code	HashiCorp	Terraform	1.7.5
CLI tool	AWS	AWS CLI	2.15.32
CLI tool	Mirantis	Docker	24.0.7
SBOM creation	Anchore	Syft	1.1.0
Artifact Storage	Sonatype	Nexus Repository Manager	3.67.1
Pipeline Orchestration	GitLab	Gitlab Runner	16.2.1
Java Build Framework	Apache	Maven	3.9.6
Javascript Build Framework	OpenJS Foundation	Node.js	20.11.0
Scripting Language	Python	Python	3.8

Section 3: SYSTEM TOPOLOGY DIAGRAM



Updated 4/24/24

Section 4: TEST SCHEDULE & LOCATION

Table 1 outlines the schedule for this test effort. This schedule will assist in excluding unforeseen delays.

Milestone	Estimated Completion Date
TBD	TBD

Table 1. Test Schedule

Section 5: TEST MEASURES/CASES

The operational Arcturus performance criteria for use cases are specified below.

The Arcturus test cases are outlined below: Pipeline app liation outline validation pass/failure What is being tested?

- To evaluate the performance of the …solution using current infrastructure and…?
- To evaluate user experience….?
- What is being considered a successful test?

Step	Action	Expected Result	Pass /Fail	Comments
1	Integration with the CAC token works correctly as the Single Sign-On (SSO) authentication mechanism.	Users are able to use their CAC or ECA certificate to authenticate to Arcturus Tools	Pass	Successful_Login.mov
2	Ensure users can access the Arcturus via https://gitlab.test.cce.af.mil	Authenticated users can access Arcturus Tools and Documentation	Pass	Successful_Login.mov
3	Test to ensure access is restricted to ONLY authorized users and groups as defined by SSO provider	Users not approved to use Arcturus tools cannot access Arcturus tools	Pass	UnauthorizedAcces…
4	Ensure Data-at-Rest (DAR) and Data-in-Transit (DIT) are encrypted	All Data At Rest and Data In Transit is encrypted	Pass	S3Encryption-DAR.… , RDSEncryption-DA… , ALB-TLS-DIT.png

5	Authorization: Identify any issues related to role privilege, enforcement, and attempt to bypass authorization restrictions.	Users cannot elevate their privileges	Pass	(Users cannot access admin area)
6	Manual/automated assessment of the IL5 Zone A environment using CIS Benchmarks and STIG checklists.		Pass	https://drive.google.com/file/d/18b7KeJtxWAv6YZ4ZtEVYVbR5UkCfYECj/view?usp=drive_link
7	Perform vulnerability scanning of Arcturus (list tools)	Arcturus tools suite are subject to applicable scanning, Trivy and KICS.	Pass	This will be covered by section 6
8	Test unauthorized access by use of a dummy non-authorized account to attempt to perform tasks which are not allowed by the group/permission set of provisioned accounts.	Unauthorized users cannot access Arcturus Tools	Pass	UnauthorizedAcces…
9	Onboarding an application	App team is onboarded to GitLab and their respective group has been created	Pass	Arcturus_Customer…
10	Create a group for the application	App team is onboarded to GitLab and their respective	Pass	Arcturus_Customer…
11	Team lead has ownership and adds member (demo)	App team leaders are assigned the Owner role within their group	Pass	Arcturus_Customer…
12	Deploy cluster to house application in the cloud deployed to landing zone (demo)	Landing Zone and Cluster are deployed to customer landing zone	Fail (Works on GC)	Arcturus_Demo.mp4

13	Pipeline files are created	Pipeline file is created to point to Jarvis Pipeline	Pass	Arcturus_Demo.mp4
14	Code pushed to Gitlab and tests the application	Customer is able to transfer code to gitlab by referencing Arcturus Documentation	Pass	Arcturus_Demo.mp4
15	Application scans results	Application is scanned via the Jarvis Pipeline	Pass	Arcturus_Demo.mp4
16	Container is built	Application is built into a container	Pass	Arcturus_Demo.mp4
17	Sonarqube scan results and all subsequent changes made	Application is scanned by Sonarqube via the Jarvis Pipeline	Pass	Arcturus_Demo.mp4
18	Application can be deployed to the cloud on test and production environment	Container and IAC deployment stages only occur in test or prod branches	Pass	Arcturus_Demo.mp4
19	Merge request with necessary approvals is required to promote application	Merge request rules are in place in order to ensure necessary approvals are met to promote code to environments	Fail? (Need to configure still)	Arcturus_Demo.mp4

Section 6: SECURITY TEST OBJECTIVE

This test will ensure technical compliance with applicable security controls can be achieved while testing the functionality and operational capabilities. Verification Method (VM); Test (T); & Observation (O)

Required Actions	Expected Results	Actual Results	Comments	Pass/Fail
Container Scans	No Medium or higher vulnerabilities	Containers are kept up to date with product	See artifact for details on each	Fail (Although we cannot control the containers, we

	exist in containers used by Arcturus.	guidelines/best practices.	container results	keep them up to date)
Pipeline IaC Scans	No Medium or higher vulnerabilities exist in IaC used by Arcturus.	No Medium or higher vulnerabilities exist in IaC used by Arcturus.	See artifact for details on each pipeline iac scan results	Pass
AWS Inspector Scans	No vulnerabilities on Cloud Service Provider being used exist	AWS Inspector is still being provisioned for SwiftShield	https://jira.tools.cce.af.mil/browse/C1AFCCE2-87740	Fail (AWS Inspector is not running yet)

Section 7: REPORTING

Deliverables on all test objectives will be documented and kept by the Information System Security Manager (ISSM). Deliverables described above may include:

- Network Health Assessment
- Raw and remediated scan reports

Section 8: TEST REPORT

The test Report provides an overall technical, managerial, and operational security examination of the system and will identify the results of the testing and the recommended improvements to correct failed controls. This report will summarize security findings, address whether security requirements specified in the Test Plan were successfully implemented and identify the impact of open findings. The Test Report will provide insight on the security posture of Arcturus on this effort. All results will be documented within the Enterprise Mission Assurance Support Service (eMASS) record in support of final AO Authorization determination. All marking, transmission, receipt, handling, and processing of sensitive or classified data/information shall be performed in accordance with DoD 5200.1-R.

ACRONYMS

Acronym	Definition
AO	Authorizing Official
ATO	Authorization to Operate
AWS	Amazon Web Services
CD	Continuous Delivery
CD	Continuous Deployment
CI	Continuous Integration
CIS	Center for Internet Security
CLI	Amazon Command Line Interface
CNAP	Cloud Native Access Point
EBS	Amazon Cloud Block Storage
ECR	Amazon Elastic Container Registry
ECS	Amazon Elastic Container Service
EC2	Amazon Elastic Compute Cloud
eMASS	Enterprise Mission Assurance Support Service
IAM	Identity and Access Management
IATT	Interim Authority to Test
KMS	Amazon Key Management Service
NIST	National Institute of Standards and Technology
OWASP	Open Worldwide Application Security Project
RCA	Rapid Cyber Acquisition
RDS	Amazon Relational Database Service
STIG	Security Technical Implementation Guides
S3	Amazon Simple Storage Service