TIER: Production Candidate - Release 20161219 Report

(Continuous Release Pipeline)

December 19, 2016

Synopsis of the Current Release

Trust and Identity in Education and Research

Package Delivery

TIER Program: Team Report

Revision 2016.12.19

TIER Program Documentation

Contents

Introduction

On December 19, 2016, the Internet2 community released a Production Candidate of TIER Components (Trust and Identity in Education and Research). TIER is a program that addresses both a software delivery strategy and shared community practices developed by and for the research and education community. The "first look" release was issued in April 2016. The full report on the TIER formative work, prioritized requirements requested by the community, and an overview of the many contributors can be found in the Release One background document.

This new Production Candidate was produced by a Continuous Release Pipeline developed by the TIER Packaging Working Group. This pipeline is intended to provide an automated production system for evolving and supporting a user-friendly suite of TIER software.

This report highlights the primary goals for the pipeline, new features enabled in this release, a brief architectural overview of how the software is intended to work, and insights into additional features planned for releases.

This document contains a number of links to references. A complete list of these references is available on one wiki page.

Contents of the Release

The near-term goal of the TIER program is to enable more rapid adoption, consistent deployment and reliable update of the core Identity and Access Management (IAM) components most widely used by InCommon Federation participants. The ultimate goal of TIER is the integration of community-developed open-source trust and identity software components into a manageable and complete identity and access management suite, supported by common campus practices.

The release packages includes three open-source software components:

- Shibboleth Single Sign-On and Federating Software (Identity Provider Version 3.2.1 - Not for production)
- Grouper enterprise access management system (Version 2.3)
- COmanage Registry (Version 1.0.5)

These components are within Docker containers delivered (initially) as virtual machine images, which guarantees the software runs the same way every time in any environment. This containerized approach and the use of APIs will become more important as time goes on and these software tools become more integrated.

The containerized components are made available for testing and for your feedback to the TIER component architects. The VMs are intended for campuses that do not currently operate container-based applications. Production deployment of these virtual machines is not recommended at this time.

Release notes and installation documentation for each component can be found through links on the TIER Package Delivery page.

The long-term component release strategy converges on a "DevOps" (Development/Operations) model, leveraging Docker containers as the primary form of TIER component release. One of the best explanations of DevOps can be found here: https://theagileadmin.com/what-is-devops/. This particular perspective expresses the nuance that the TIER Working Group teams have had to navigate in constructing their response to the community requirements. Information specific to the TIER use of this process is in the blog post, The Landscape of TIER DevOps.

Continuous Release Pipeline

Objective(s)

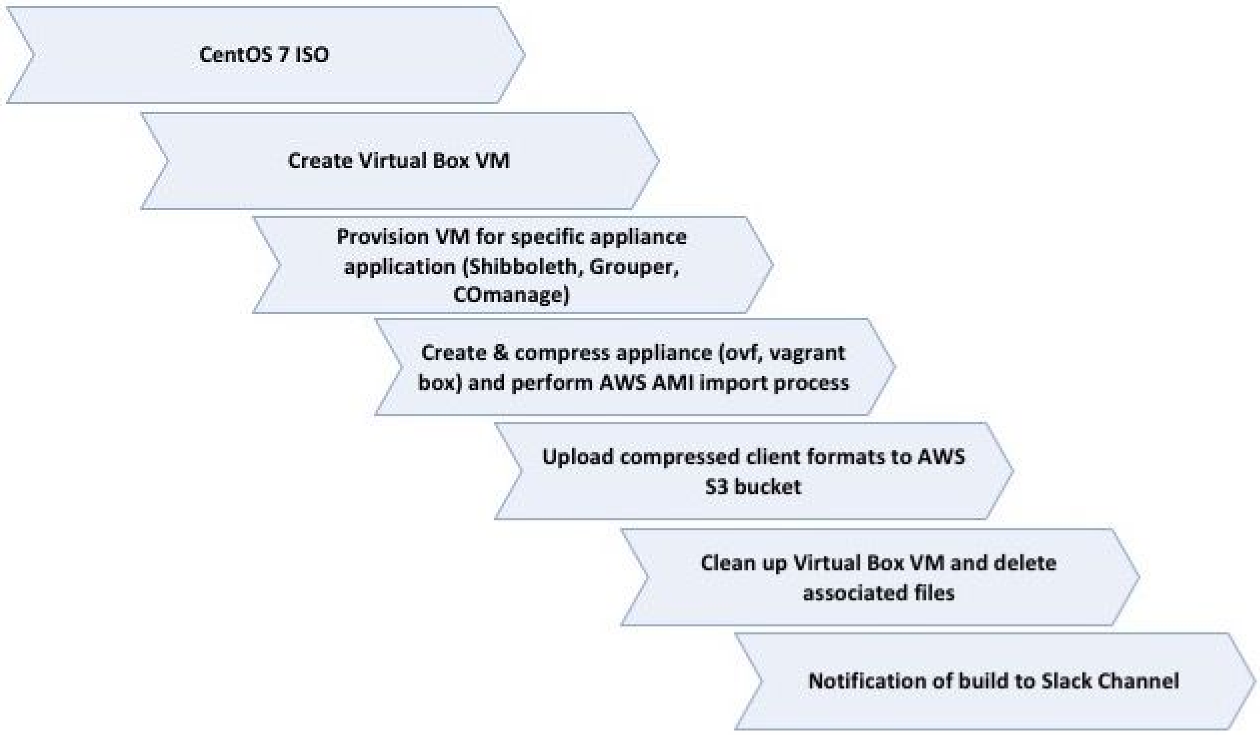
The overall model for the container-based distribution involves the creation of an automated build and test environment along with a set of virtual machine images that can be used to test and/or deploy the Docker containers. The automated build environment enables regularly scheduled updates to the production containers.

The objective and primary feature of the pipeline is to enable the implementer to achieve a running environment with the full suite of components in the shortest possible time. In addition to this turn-key objective, several other principles have been applied:

- Provide an upgrade path so implementors can take advantage of minor, but valuable, new features and capabilities without doing forklift replacement installations
- Include automated installation scripts to make installation and configuration as simple as possible
- Leverage as much existing work as possible (supports existing deployment and adoption)
- Narrow the toolsets (promotes maintainability)
- Utilize the container as a platform for the future (enhances maintainability and portability of the deliverables)
- Promote “sustainability and commitment of the team” (ensure that contract and support for the components are engaged as compensated participants)
- Fortification of the Federation’s operation (ensure that the trusted fabric of the federation is robust and future-focused)
- Utilization of development best practices (embrace best practices, consistently applied, across all components current and future)
    - Groundwork for continuous deployment and testing
    - Appropriate monitoring and feedback
    - Enabling community extensibility
- Serve as a foundation for future development of new features or modules allowing for strong API-based integration while supporting modularity at the core

Pipeline Architecture (Brief)

High Level Overview:

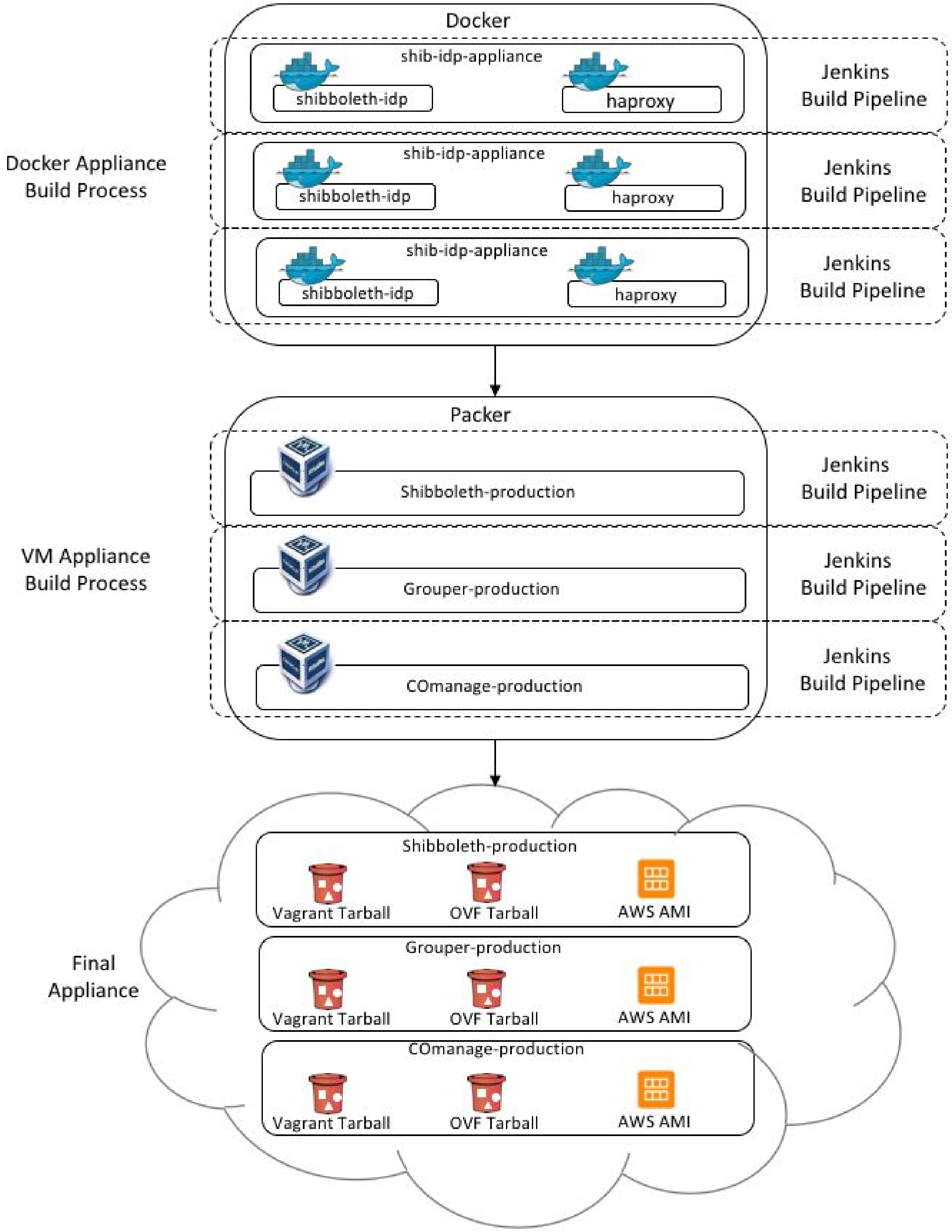

CentOS 7 ISO
Create Virtual Box VM
Provision VM for specific appliance application (Shibboleth, Grouper, COmanage)
Create & compress appliance (ovf, vagrant box) and perform AWS AMI import process
Upload compressed client formats to AWS S3 bucket
Clean up Virtual Box VM and delete associated files
Notification of build to Slack Channel

The build pipeline is designed to create an application appliance in the Open Virtualization Format , enabling an application to be quickly deployed as a preconfigured, runnable image. This process starts with a bare CentOS 7 image in the format of `.iso`, creates a local VirtualBox VM, provisions and configures the VM, creates tarballs (.ovf) and AWS AMI, cleans up and deletes the VM.

Jenkins CI (Continuous Integration) is an open source tool written in Java. Located at a server where the project's main build is created, Jenkins triggers a new build every time a user checks some changes into the source code, thus supporting the process of continuous integration for testing or development phases.

Hashicorp's "Packer" is then used for creating machine and container images for multiple platforms from a single source configuration.

Appliance Build Process Diagram



The pipeline can build AWS AMIs, however, the community teams have only tested the VirtualBox containers for the current release.

Community Experience: Hundreds of Person-Years

The TIER Program brings together what has been the independent direction of three independent development teams (Shibboleth Consortium, Grouper, COmanage) and two nascent development teams (Community IdP and Scalable Consent) to deliver a packaged suite of components. Moreover, it was deemed central to the mission that the deliverables be packaged and pre-configured to work well together in the context of the InCommon Federation. These activities also brought into focus a need to tend to the software, services and components upon which the InCommon Federation itself relies.

The TIER working groups (Packaging, APIs and Data Structures, Security and Audit, Registry, Components, Ad Hoc Advisory Architecture) represent the marshaling of community expertise with more than 100 active, contributing participants that collectively represent hundreds of years of IAM and campus experience. Without these teams, many important elements may have been overlooked as we developed the container, documentation, community outreach, partner engagement, campus engagement and many other strategies which have arisen from these fast-paced discussions.

Releases "Now and Next"

With this release of the TIER software, we will have ended the "big bang" approach to releases and going forward we will make new functionality, patches and features available as soon as they are ready. To that end, the team goal is to have a continuously integrated and tested version of the combined suite "at the ready" for download, test and deployment in predetermined cycles. Continuous integration means that the entire component suite can be upgraded at the pace and along timelines most suitable to the campus deployment teams.

The plan continues to be evolving the core infrastructure to enable significant future functionality and ease of use wherever possible. The list below identifies some of what has been instituted as well as the visionary goals that have been requested of the TIER Program. The range of goals includes some aspirational objectives, but many are achievable in the foreseeable future:

- Now in place or partially in place:
    - Instantiation of continuous integration / test and build
    - Consolidation of all development efforts into the GitHub architecture which enables many other capabilities
- Upcoming and/or Planned:
    - Instrumentation to better understand TIER adoption
    - Refinement of the existing container system
    - Definition and publication of upgrade / update path for campuses such that a refresh to current components can be performed as seamlessly as possible
    - Improvement and reorganization of updated documentation (by role/activity)
    - Implementation of a multi-component self-contained-IAM infrastructure to support simple usage scenarios.
    - Re-deploy our component tracking and management within federation-enabled and updated versions of JIRA and Confluence.
    - Definition and encapsulation of an operational "entity registry" which contains the identities of both "people" and "things."
    - Further realizing the vision of enabling campuses to instantiate a multi-VM based TIER Workbench tied together with TIER APIs, and capable of onboarding users, managing their accounts, credentials, affiliations and privileges, and providing them access to federated Service Providers. This is where the work of the API and Entity Registry Working Group is headed though acknowledging that the working groups are not the engineering teams who must ultimately make the proper implementation choices.

With an eye toward the future, we also need to support the provisioning of a continuously patched and consistent software package.

Feedback and Support

The key to success for the TIER Program will be adoption by the campus community. Our efforts to ensure that the container and deployment environments are right can only be measured through campus feedback. The experience of every adopting campus will inform the changes and course corrections as we move forward.

We are very interested in your feedback. Please go to the web page, "TIER Questions, Comments, and Feedback" for information about providing comments and for support contact information.

Staying Informed

Relevant TIER Lists

Currently, we have the following broad community-facing TIER-related lists where discussion about the TIER Release *could* occur:

- TIER-adopters (Subscribe to TIER-adopters) (Send a Message to TIER-adopters) discussions for/by implementers of TIER components
- TIER-Investors (Subscribe to TIER-Investors) (Send a Message to TIER-Investors) CIO and their identified IAM staff/ architects
- TIER-Investor-CIOs (Subscribe to TIER-Investor-CIOs) (Send a Message to TIER-Investor-CIOs) Investing CIOs only
- TIER-Architecture (Subscribe to TIER-Architecture) (Send a Message to TIER-architecture) architecture discussion for TIER
- TIER-Discussion (Subscribe to TIER-Discussion) (Send a Message to TIER-Discussion) general discussion for TIER
- In addition, if you wish subscribe to the TIER Newsletter please use the TIER Newsletter Subscriber Enrollment Form

Although the hypertext links above are provided to automatically perform this task, you may subscribe to any of these lists by sending an e-mail message as follows:

To: pubsympa@internet2.edu
Subject: subscriber <NameOfMailList> <MyFirstName> <MySurname>

Body of message can be whatever you want but if you do it right, the mail list manager will ignore it and your subscription in the mail list manager will auto-enroll you!