**Medical Care Collection Fund (MCCF) Transaction Application Suite (TAS) Electronic Data Interchange (EDI)**

Deployment, Installation, Back-Out, and Rollback Guide

1.4



December 2018

Department of Veterans Affairs

Office of Information and Technology (OI&T)

**Revision History**

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 2018-12-05 | 1.4 | Updated to address review comments | John Innis |
| 2018-11-06 | 1.3 | Document Revision | David Betz |
| 2018-08-24 | 1.2 | Document Revision | David Betz |
| 2018-03-07 | 1.1 | Document Revision | Cheryl Lach |
| 2017-10-19 | 1.0 | Initial | David Betz |

**Artifact Rationale**

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

Table of Contents

[1 Introduction 5](#_Toc531780417)

[1.1 Purpose 5](#_Toc531780418)

[1.2 Dependencies 5](#_Toc531780419)

[1.3 Constraints 5](#_Toc531780420)

[2 Roles and Responsibilities 5](#_Toc531780421)

[3 Deployment 7](#_Toc531780422)

[3.1 Timeline 7](#_Toc531780423)

[3.2 Site Readiness Assessment 7](#_Toc531780424)

[3.2.1 Deployment Topology (Targeted Architecture) 7](#_Toc531780425)

[3.2.2 Site Information (Locations, Deployment Recipients) 10](#_Toc531780426)

[3.2.3 Site Preparation 10](#_Toc531780427)

[3.3 Resources 10](#_Toc531780428)

[3.3.1 Hardware 10](#_Toc531780429)

[3.3.2 Software 10](#_Toc531780430)

[3.3.3 Communications 11](#_Toc531780431)

[4 Installation 11](#_Toc531780432)

[4.1 Pre-installation and System Requirements 11](#_Toc531780433)

[4.2 Platform Installation and Preparation 11](#_Toc531780434)

[4.3 Download and Extract Files 11](#_Toc531780435)

[4.4 Database Creation 11](#_Toc531780436)

[4.5 Installation Scripts 11](#_Toc531780437)

[4.6 Cron Scripts 11](#_Toc531780438)

[4.7 Access Requirements and Skills Needed for the Installation 11](#_Toc531780439)

[4.8 Installation Procedure 12](#_Toc531780440)

[4.9 Installation Verification Procedure 12](#_Toc531780441)

[4.10 System Configuration 12](#_Toc531780442)

[4.11 Database Tuning 12](#_Toc531780443)

[5 Back-Out Procedure 12](#_Toc531780444)

[5.1 Back-Out Strategy 12](#_Toc531780445)

[5.2 Back-Out Considerations 12](#_Toc531780446)

[5.2.1 Load Testing 13](#_Toc531780447)

[5.2.2 User Acceptance Testing 13](#_Toc531780448)

[5.3 Back-Out Criteria 13](#_Toc531780449)

[5.4 Back-Out Risks 13](#_Toc531780450)

[5.5 Authority for Back-Out 13](#_Toc531780451)

[5.6 Back-Out Procedure 13](#_Toc531780452)

[5.7 Back-out Verification Procedure 13](#_Toc531780453)

[6 Rollback Procedure 13](#_Toc531780454)

[6.1 Rollback Considerations 13](#_Toc531780455)

[6.2 Rollback Criteria 13](#_Toc531780456)

[6.3 Rollback Risks 13](#_Toc531780457)

[6.4 Authority for Rollback 13](#_Toc531780458)

[6.5 Rollback Procedure 13](#_Toc531780459)

[6.6 Rollback Verification Procedure 14](#_Toc531780460)

**Table of Figures**

[**Figure 1: Schedule Snippet 7**](#_Toc531780461)

[**Figure 2: Targeted Architecture 8**](#_Toc531780462)

[**Figure 3: TAS API Kubernetes Implementation 9**](#_Toc531780463)

**Table of Tables**

[**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 5**](#_Toc531780464)

[**Table 3: Site Preparation 10**](#_Toc531780465)

[**Table 4: Hardware Specifications 10**](#_Toc531780466)

[**Table 5: Software Specifications 10**](#_Toc531780467)

# Introduction

This document describes how to deploy and install MCCF EDI TAS*,* as well as how to back-out the product and rollback to a previous version or data set. This document is a companion to the project charter and management plan for this effort. In cases where a non-developed Commercial Off The Shelf (COTS) product is being installed, the vendor provided User and Installation Guide may be used, but the Back-Out Recovery strategy still needs to be included in this document.

## Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom MCCF EDI TAS will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan also identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

## Dependencies

Data itself is stored in VistA. All Identity and Access Management services are provided by VA Identity and Access Management (IAM).

## Constraints

Microsoft Azure Government (MAG) is the target production environment. This environment is connected to the VA via an ExpressRoute connection. The application must maintain connectivity to VA IAM from the MAG environment.

# Roles and Responsibilities

Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities

| **ID** | **Team** | **Phase / Role** | **Tasks** | **Project Phase (See Schedule)** |
| --- | --- | --- | --- | --- |
|  | TASCore | Deployment | Plan and schedule deployment (including orchestration with vendors) |  |
|  | TASCore | Deployment | Determine and document the roles and responsibilities of those involved in the deployment. |  |
|  | TASCore | Deployment | Test for operational readiness |  |
|  | TASCore | Deployment | Execute deployment |  |
|  | TASCore | Deployment | Plan and schedule installation |  |
|  | TASCore | Installation | Ensure authority to operate and that certificate authority security documentation is in place |  |
|  | TASCore | Installation | Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes |  |
|  | TASCore | Installation | Coordinate training |  |
|  | TASCore | Installation | Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out) |  |
|  | TASCore | Back-out | Hardware, Software and System Support |  |
|  |  |  |  |  |

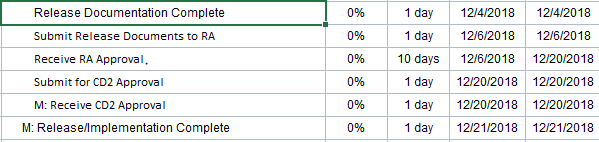
# Deployment

This section provides the schedule and milestones for the deployment.

## Timeline

The deployment and installation is scheduled to run in less than one hour, an estimated 30 to 45 minutes. The schedule snippet below shows the release timeline.

Figure 1: Schedule Snippet



## Site Readiness Assessment

Deployment is to the MAG environment. MAG regions include Iowa, Virginia, Arizona, and Texas. Deployment is to MAG virtual machines (“VM”).

This section discusses the locations that will receive the MCCF EDI TAS deployment.

### Deployment Topology (Targeted Architecture)

Deployment is to the MAG environment. MAG regions include Iowa, Virginia, Arizona, and Texas. Deployment is to MAG virtual machines (“VM”). The diagram below shows the high-level architecture.

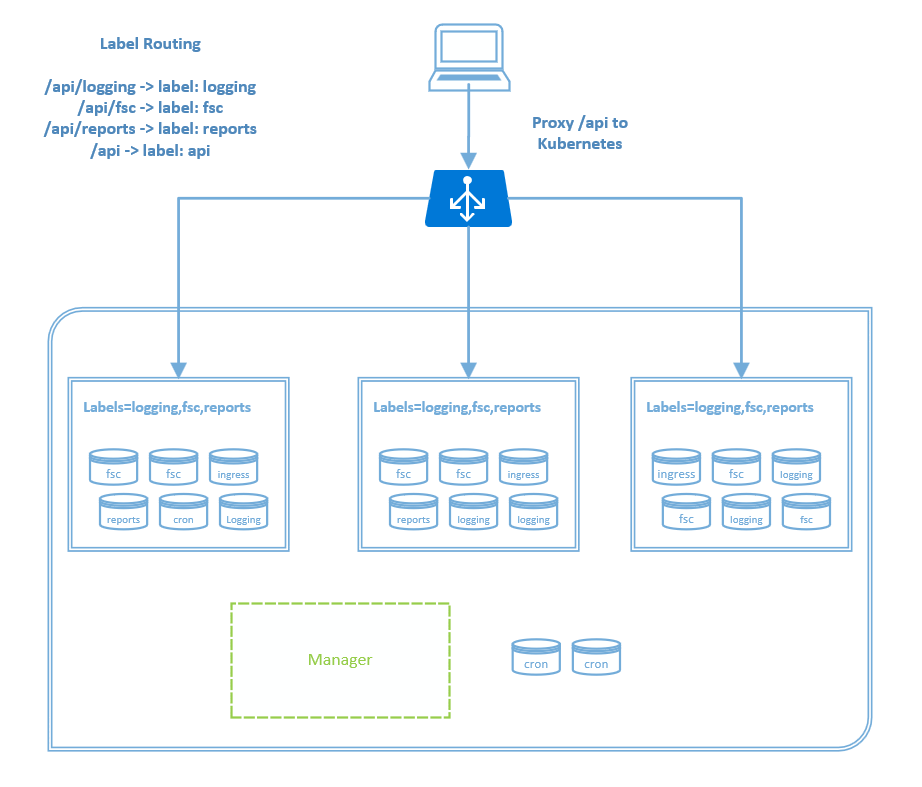
Figure 2: Targeted Architecture



TAS API instances are run with Kubernetes in a private orchestration cloud. Each underlying orchestration node is given a set of node labels. The orchestration manager will instruct the nodes to spin-up TAS API instances that relate to those labels. Ingress traffic is configured via a DaemonSet, allowing each system to be an orchestration ingress point. The orchestration cloud handles failover, name resolution, transport encryption, and load-balancing automatically.

Because the TAS API contains modules that can be individually activated, multiple instances of the TAS API can be deployed to maximize the computational abilities of any particular module. For example, the fsc module can be activated in one TAS API deployment while the logging module can be activated in another. As previously mentioned, these are spun-up on nodes instructed to handle traffic for those modules. The Kubernetes ingress controller will direct requests to the appropriate TAS API instance.

Figure 3: TAS API Kubernetes Implementation



### Site Information (Locations, Deployment Recipients)

Deployment is to the MAG environment. MAG regions include Iowa, Virginia, Arizona, and Texas. Deployment is to MAG virtual machines (“VM”).

### Site Preparation

Deployment is to the MAG environment. Microsoft handles all physical resources, including power, racks, cooling, etc. MAG must be logically, not physical prepared. Preparation will include firewall configuration and identity and access management configuration.

The following table describes preparation required by the site prior to deployment.

Table 3: Site Preparation

| **Site/Other** | **Problem/Change Needed** | **Features to Adapt/Modify to New Product** | **Actions/Steps** | **Owner** |
| --- | --- | --- | --- | --- |
| N/A | N/A | N/A | N/A | N/A |

## Resources

### Hardware

The following table describes hardware specifications required at each site prior to deployment.

Table 4: Hardware Specifications

| **Required Hardware** | **Model** | **Version** | **Configuration** | **Manufacturer** | **Other** |
| --- | --- | --- | --- | --- | --- |
| VM | N/A | N/A | N/A | N/A | N/A |

Please see the Roles and Responsibilities table in Section 2 for details about who is responsible for preparing the site to meet these hardware specifications.

### Software

The following table describes software specifications required at each site prior to deployment.

Table 5: Software Specifications

| **Required Software** | **Make** | **Version** | **Configuration** | **Manufacturer** | **Other** |
| --- | --- | --- | --- | --- | --- |
| RHEL | N/A | 7.3 | N/A | N/A | N/A |

Please see the Roles and Responsibilities table in Section 2 above for details about who is responsible for preparing the site to meet these software specifications.

### Communications

MAG provides monitoring and notification features which can be used to alert technicians of an error.

# Installation

## Pre-installation and System Requirements

The MAG environment must be setup for deployment to occur. A valid and usable Red Hat Enterprise Linux (RHEL) 7.3 VM image must be available for technicians to deploy VMs. Domain Name Service (DNS) must be accessible. Centrify must be in place to allow authentication.

## Platform Installation and Preparation

For each full deployment of the system, the frontend, the services deployed into an orchestration cloud, HAPI-FHIR, and MAG services must be configured.

Ansible will handle automated installation and deployment of each component.

Before MAG installation, each component is checked in the EDE environment.

## Download and Extract Files

Ansible will handle all software installations. Software will come from private, not public, VM repositories.

## Database Creation

Non-VistA-related databases are hosted in Cosmos DB inside MAG. These are infrastructure components that are setup via sysadmins.

## Installation Scripts

Ansible will handle all software installations. Software will come from private, not public, VM repositories.

## Cron Scripts

Cron runs nightly scripts. These run processes to copy data for reporting.

## Access Requirements and Skills Needed for the Installation

MAG policies require individuals to have specific permissions for each MAG resource. To create a VM, a user must have the Virtual Machine Contributor role

## Installation Procedure

Ansible will handle all server software installations. There are no client components to install. The steps to install TAS version 1.1 are as follows.

1. Login to the Jenkins server
2. Click on the MCCF\_TAS link
3. Click on the “deploy\_RTC\_MCCF\_TAS\_Core” link
4. Enter “MAG\_PROD” into the ENV field
5. Enter the TAS v1.1 filename of “mccf-tas\_TAS.01.00.1517.20181108\_103103.tar.gz” into the deployment\_filename field.

## Installation Verification Procedure

Each layer of the application has a set of tests which validate the performance of that layer’s functionality. This occurs prior to deployment. A health monitoring service endpoint exists to check system status. MAG uses the health monitoring service endpoint to monitor status and provide notifications of system issues.

## System Configuration

Ansible will handle all server software installations and configuration.

## Database Tuning

Databases are hosted in Cosmos DB, Azure SQL Database, or are Azure Storage Tables. These are managed services that do not require systems-level administration.

# Back-Out Procedure

MAG is largely driven by immutable deployments. New versions of applications should go to new deployments; in-place upgrades should never take place. This nullifies the concept of a back-out procedure; instead, it’s a pointer change.

For non-VistA services, this will entail the creation of new orchestration containers with a new version tag with a pointer change to new containers. For front-end work, this will entail deployment of a new build with a pointer change to the new index.html and resources.

Back-out is a pointer change to previous versions. This is a built-in feature of orchestration.

## Back-Out Strategy

N/A See section 5.

## Back-Out Considerations

N/A See section 5.

### Load Testing

N/A

### User Acceptance Testing

N/A

## Back-Out Criteria

N/A See section 5.

## Back-Out Risks

N/A See section 5.

## Authority for Back-Out

N/A See section 5.

## Back-Out Procedure

N/A See section 5.

## Back-out Verification Procedure

N/A See section 5.

# Rollback Procedure

N/A

## Rollback Considerations

N/A

## Rollback Criteria

N/A

## Rollback Risks

N/A

## Authority for Rollback

N/A

## Rollback Procedure

N/A

## Rollback Verification Procedure

N/A