**VA Medical Care Collections Fund (MCCF)****Electronic Data Interchange (EDI)****Transactions Application Suite (TAS)**

Version 1.0

Deployment, Installation, Back-Out, and Rollback Guide



July 2018

Department of Veterans Affairs

Office of Information and Technology (OI&T)

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| July 22, 2018 | 1.0 | Document Revision | David Loban |

**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 1](#_Toc518310931)

[1.1 Purpose 1](#_Toc518310932)

[1.2 Dependencies 1](#_Toc518310933)

[1.3 Constraints 1](#_Toc518310934)

[2 Roles and Responsibilities 2](#_Toc518310935)

[3 Deployment 2](#_Toc518310936)

[3.1 Timeline 2](#_Toc518310937)

[3.2 Site Readiness Assessment 4](#_Toc518310938)

[3.2.1 Deployment Topology (Targeted Architecture) 4](#_Toc518310939)

[3.2.2 Site Information (Locations, Deployment Recipients) 7](#_Toc518310940)

[3.2.3 Site Preparation 7](#_Toc518310941)

[3.3 Resources 7](#_Toc518310942)

[3.3.1 Hardware 7](#_Toc518310943)

[3.3.2 Software 8](#_Toc518310944)

[3.3.3 Communications 8](#_Toc518310945)

[3.3.4 Schedule support line conference calls and invite required partiesDeployment/Installation/Back-Out Checklist 9](#_Toc518310946)

[4 Installation 9](#_Toc518310947)

[4.1 Pre-installation and System Requirements 9](#_Toc518310948)

[4.2 Platform Installation and Preparation 10](#_Toc518310949)

[4.3 Download and Extract Files 10](#_Toc518310950)

[4.4 Database Creation 10](#_Toc518310951)

[4.5 Installation Scripts 10](#_Toc518310952)

[4.6 Cron Scripts 10](#_Toc518310953)

[4.7 Access Requirements and Skills Needed for the Installation 10](#_Toc518310954)

[4.8 Installation Procedure 11](#_Toc518310955)

[4.9 Installation Verification Procedure 11](#_Toc518310956)

[4.10 System Configuration 11](#_Toc518310957)

[4.11 Database Tuning 11](#_Toc518310958)

[5 Back-Out Procedure 11](#_Toc518310959)

[5.1 Back-Out Strategy 11](#_Toc518310960)

[5.2 Back-Out Considerations 11](#_Toc518310961)

[5.2.1 Load Testing 12](#_Toc518310962)

[5.2.2 User Acceptance Testing 12](#_Toc518310963)

[5.3 Back-Out Criteria 12](#_Toc518310964)

[5.4 Back-Out Risks 12](#_Toc518310965)

[5.5 Authority for Back-Out 12](#_Toc518310966)

[5.6 Back-Out Procedure 12](#_Toc518310967)

[5.7 Back-out Verification Procedure 12](#_Toc518310968)

[6 Rollback Procedure 12](#_Toc518310969)

[6.1 Rollback Considerations 12](#_Toc518310970)

[6.2 Rollback Criteria 12](#_Toc518310971)

[6.3 Rollback Risks 12](#_Toc518310972)

[6.4 Authority for Rollback 13](#_Toc518310973)

[6.5 Rollback Procedure 13](#_Toc518310974)

[6.6 Rollback Verification Procedure 13](#_Toc518310975)

**Table of Figures**

[**Figure 1: Targeted Architecture 9**](#_Toc498414598)

**Table of Tables**

[**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 2**](#_Toc520113332)

[**Table 2: eBusiness Master Deployment Schedule 3**](#_Toc520113333)

[**Table 3: Site Preparation 5**](#_Toc520113334)

[**Table 4: System Specifications 5**](#_Toc520113335)

[**Table 5: Hardware Specifications 6**](#_Toc520113336)

[**Table 6: Software Specifications 7**](#_Toc520113337)

[**Table 7: Deployment/Installation/Back-Out Checklist 8**](#_Toc520113338)

# 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 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 IAM.

The MCCF EDI TAS is fully dependent on Microsoft Azure Gov Cloud in addition to the VA AITC to provide connectivity into VA private resources (eg. VistA). Within the Microsoft Azure Gov Cloud environment (MAG) there is a dependency on COSMOS DB for storage of data.

## 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.

MCCF EDI TAS is a web based application and must be compliant with NIST 508 and all other VA requirements for similar applications. Additionally, Users of MCCF EDI TAS authenticate into the system using VA supplied PIV cards and the VA IAM service. This provides role based access into the system.

# Roles and Responsibilities

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

| ID | Team | Phase / Role | Tasks | Project Phase (See Schedule) |
| --- | --- | --- | --- | --- |
| 1 | TASCore | Deployment | Plan and schedule deployment (including orchestration with vendors) | Planning |
| 2 | TASCore | Deployment | Determine and document the roles and responsibilities of those involved in the deployment. | Planning |
| 3 | TASCore | Deployment | Test for operational readiness | Testing |
| 4 | TASCore | Deployment | Execute deployment | Deployment |
| 5 | TASCore | Installation | Plan and schedule installation |  |
| 6 | TASCore, and VIP Release Agent | Installation | Ensure authority to operate and that certificate authority security documentation is in place | Deployment |
| 7 | TASCore | Installation | Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes |  |
| 8 | TASCore | Installations | Coordinate training | Deployment |
| 9 | TASCore | Back-out | Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out) | Deployment |
| 10 | TASCore | Post Deployment | Hardware, Software and System Support | Warranty |
|  |  |  |  |  |

# Deployment

The deployment is planned as an iterative rollout.

This section provides the schedule and milestones for the deployment.

## Timeline

The deployment and installation is scheduled to run to Q4 2019, as depicted in the master deployment schedule MCCF EDI TAS Strategic Roadmap in place as of Oct 2017.

Table 2: eBusiness Master Deployment Schedule

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **MCCF Build #** | **VIP Build #** | **TAS Release Version** | **VIP Dashboard Projected   Build Start** | **VIP Dashboard Projected Build Finish** | **IOC CD2 Approval Date** | **National Release CD2 Approval Date** | **National Release Start** | **Warranty Exp. Date** |
| **1** | **11** | **N/A** | **7/3/2017** | **10/3/2017** | **N/A** | **6/14/2018** | **6/22/2018** | **11/1/2018** |
| **2** | **16** | **N/A** | **9/25/2017** | **12/15/2017** | **N/A** | **6/14/2018** | **6/22/2018** | **11/1/2018** |
| **3** | **21** | **TAS v1.0** | **12/18/2017** | **3/9/2018** | **N/A** | **6/14/2018** | **6/22/2018** | **11/1/2018** |
| **4** | **26** | **N/A** | **3/12/2018** | **6/1/2018** | **11/9/2018** | **2/22/2019** | **3/1/20191** | **5/30/20191** |
| **5** | **31** | **TBD** | **6/4/2018** | **8/24/2018** | **11/9/2018** | **2/22/2019** | **3/1/20191** | **5/30/20191** |

1 Syncronized with ePharmacy Build 7 release

## Site Readiness Assessment

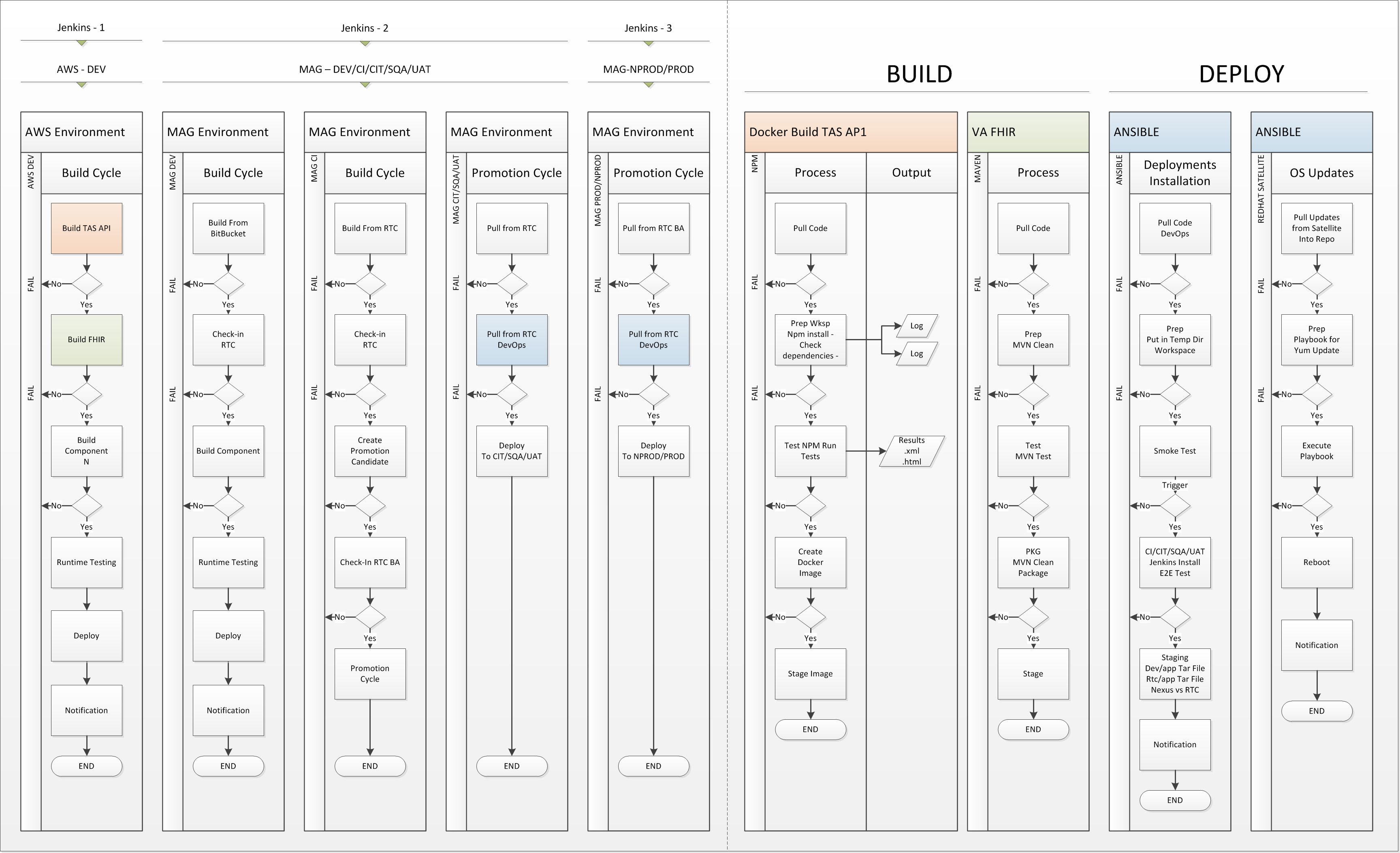
The MCCF EDI TAS project is deployed into Microsoft Azure Gov Cloud and as such, all mechanical and physical connections are considered to be part of the service. See Section 1.2 for additional details.

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

### Deployment Topology (Targeted Architecture)

The MCCF EDI TAS project is deployed into Microsoft Azure Gov Cloud and as such the deployment topology is left to the MAG environment.

Figure 1: Targeted Architecture



### Site Information (Locations, Deployment Recipients)

The MCCF EDI TAS project is deployed into Microsoft Azure Gov Cloud. The primary is located at Microsoft’s facility in the State of Virginia with a failover site planned for Austin, Texas.

### Site Preparation

The MCCF EDI TAS project is deployed into Microsoft Azure Gov Cloud and as such all site requirements are met and included in the subscription. 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

The MCCF EDI TAS project is deployed into Microsoft Azure Gov Cloud. Please refer to section 3.2.3 for additional details.

### Hardware

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

Table 4: System Specifications

| Server Function/Type | Host Name | Application Environment |
| --- | --- | --- |
| FPC | Vac20fpctas200 | Jenkins |
| Web (x2) | Vac20webtas210  Vac20webtas211 | Entry |
| App (x2) | Vac20apptas210  Vac20apptas211 | HAPIFHIR |
| DB | ? | COSMOS DB |
| Tableau | Vac20appmcf205 | Future |

Table 5: Hardware Specifications

| Site | MAG – VA | Microsft Azure VM Size |
| --- | --- | --- |
| Model | VM – FPC | LINUX Standard A2m\_v2  4vCPU+32GB RAM |
|  | VM – WEB | LINUX Standard A2m\_v2  4vCPU+32GB RAM |
|  | VM – APP | LINUX Standard A2m\_v2  4vCPU+32GB RAM |
|  | VM – DBS | LINUX Standard A2m\_v2  4vCPU+32GB RAM |

Currently the Microsoft Azure Gov Cloud subscription provides a maximum size virtual machine size of 20 v CPU’s and 140 GB RAM. However this sizing is irrelevant since storage is in COSMOS DB.

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 6: Software Specifications



The software required to be deployed into Microsoft Azure Gov Cloud is a LINUX System image obtained from the VA. All other required software is derived from either the VA Red Hat Satellite and/or the YUM Repositories and/or the MCCF product specific repositories on the FPC servers. COSMOS DB is supplied as a PaaS (Platform as a Service).

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.

If the system is down, or the application isn’t responding correctly due to other extenuating circumstances, the following actions should be taken:

* Determine if the system (servers) or if the software is not responding

a) Is the server up and available?

b) Is just the application or functionality of the application that is not resonding?

* Notify the appropriate support personnel of the incident and document the incident following processes regarding System Outage Notification
* Notify the user community that the system and/or software is unavailable

### Schedule support line conference calls and invite required partiesDeployment/Installation/Back-Out Checklist

TASCore and its components are provided as SaaS (Software as a Service). When the software is deployed, it is installed at the same time; however, because this is SaaS, a back-out plan is not utilized. If the application isn’t responding correctly, or if other business line functionality isn’t performing, the software can be redeployed to a prior version for any of the business line functions, which should cause only minimal impact.

Table 7: Deployment/Installation/Back-Out Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| Activity | Day | Time | Individual who completed task |
| Deploy |  |  |  |
| Install |  |  |  |
| Back-Out |  |  |  |

# Installation

## Pre-installation and System Requirements

The VA must provide a MAG (Microsoft Azure Gov Cloud) Subscription with sufficient capacity for the listed hardware (Virtual Machines) and software (COSMOS DB). Additionally, the VA must provide connectivity from the VA network to MAG in addition to providing the COSMOS DB which resides in MAG, thus, the MAG environment must be setup for deployment to occur. A valid and usable RHEL 7.3 VM image must be available for technicians to deploy VMs. 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, each Node service, Mule ESB, HAPI-FHIR, and Elasticsearch must be installed.

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

The instructions related to standing up MAG for the MCCF EDI TAS are contained in this document:



## Download and Extract Files

All MCCF EDI TAS software is derived from the VA satellite and MCCF repositories. All software deployment is managed by the Jenkins Continuous Integration automation tool which meet existing VA requirements.

## Database Creation

The MCCF EDI TAS utilizes the COSMOS DB which is Software as a Service (SaaS).

## Installation Scripts

The installation of MCCF EDI TAS is managed by the Jenkins Continuous Integration automation tool. The scripts required to install are contained in this document:



## Cron Scripts

No Cron scripts required as of this writing.

## 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.

All required access MCCF EDI TAS is managed through the VA’s IAM (Identity and Access Management).

## Installation Procedure

The installation of MCCF EDI TAS is managed by the Jenkins Continuous Integration automation tool. The scripts required to install are contained in this document. See section 4.5 for Jenkins Installation Script.

## 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.

The steps required to verify the installation of MCCF EDI TAS are TBD

## System Configuration

The MCCF EDI TAS is hosted in MAG

## Database Tuning

Database designers should ensure Elasticsearch (“ES”) dynamic mappings are not used, that schema is defined explicitly, and that mapping types are appropriate for their function.

Database administrators should ensure ES nodes are within proper memory and CPU thresholds (e.g. GET /\_nodes/stats).

The MCCF EDI TAS database is SaaS provided by MAG.

# Back-Out Procedure

There is no Back-Out Procedure for MCCF EDI TAS due to the fact that the MAG environment does not provide a facility to modify an existing VM (virtual machine) to roll-back or back-out software. Instead, the system must be deleted/destroyed and rebuilt with the desired MCCF state.

## 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

Refer to Section 5 (Back Out Procedure) of this document. Due to the fact that COSMOS DB running in MAG is the repository for MCCF EDI TAS, the rollback procedure would be performed in MAG. Refer to the following link that provides further information on Automatic online backup and restore with Azure Cosmos DB:

<https://docs.microsoft.com/en-us/azure/cosmos-db/online-backup-and-restore>

## 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

Template Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| March 2016 | 2.2 | Changed the title from Installation, Back-Out, and Rollback Guide to Deployment and Installation Guide, with the understanding that Back-Out and Rollback belong with Installation. | VIP Team |
| February 2016 | 2.1 | Changed title from Installation, Back-Out, and Rollback Plan to Installation, Back-Out, and Rollback Guide as recommended by OI&T Documentation Standards Committee | OI&T Documentation Standards Committee |
| December 2015 | 2.0 | The OI&T Documentation Standards Committee merged the existing *“Installation, Back-Out, Rollback Plan”* template with the content requirements in the OI&T End-user Documentation Standards for a more comprehensive Installation Plan. | OI&T Documentation Standards Committee |
| February 2015 | 1.0 | Initial Draft | Lifecycle and Release Management |