MCCF

Deployment, Installation, Back-Out, and Rollback Guide

TAS.01.00.49



December 2017

Department of Veterans Affairs

Office of Information and Technology (OI&T)

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 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](#_Toc499285948)

[1.1 Purpose 5](#_Toc499285949)

[1.2 Dependencies 5](#_Toc499285950)

[1.3 Constraints 5](#_Toc499285951)

[2 Roles and Responsibilities 5](#_Toc499285952)

[3 Deployment 6](#_Toc499285953)

[3.1 Timeline 6](#_Toc499285954)

[3.2 Site Readiness Assessment 8](#_Toc499285955)

[3.2.1 Deployment Topology (Targeted Architecture) 8](#_Toc499285956)

[3.2.2 Site Information (Locations, Deployment Recipients) 9](#_Toc499285957)

[3.2.3 Site Preparation 10](#_Toc499285958)

[3.3 Resources 10](#_Toc499285959)

[3.3.1 Hardware 10](#_Toc499285960)

[3.3.2 Software 10](#_Toc499285961)

[3.3.3 Communications 10](#_Toc499285962)

[4 Installation 11](#_Toc499285963)

[4.1 Pre-installation and System Requirements 11](#_Toc499285964)

[4.2 Platform Installation and Preparation 11](#_Toc499285965)

[4.3 Download and Extract Files 11](#_Toc499285966)

[4.4 Database Creation 11](#_Toc499285967)

[4.5 Installation Scripts 11](#_Toc499285968)

[4.6 Cron Scripts 11](#_Toc499285969)

[4.7 Access Requirements and Skills Needed for the Installation 11](#_Toc499285970)

[4.8 Installation Procedure 11](#_Toc499285971)

[4.9 Installation Verification Procedure 12](#_Toc499285972)

[4.10 System Configuration 12](#_Toc499285973)

[4.11 Database Tuning 12](#_Toc499285974)

[5 Back-Out Procedure 12](#_Toc499285975)

[5.1 Back-Out Strategy 12](#_Toc499285976)

[5.2 Back-Out Considerations 12](#_Toc499285977)

[5.2.1 Load Testing 12](#_Toc499285978)

[5.2.2 User Acceptance Testing 12](#_Toc499285979)

[5.3 Back-Out Criteria 12](#_Toc499285980)

[5.4 Back-Out Risks 12](#_Toc499285981)

[5.5 Authority for Back-Out 13](#_Toc499285982)

[5.6 Back-Out Procedure 13](#_Toc499285983)

[5.7 Back-out Verification Procedure 13](#_Toc499285984)

[6 Rollback Procedure 13](#_Toc499285985)

[6.1 Rollback Considerations 13](#_Toc499285986)

[6.2 Rollback Criteria 13](#_Toc499285987)

[6.3 Rollback Risks 13](#_Toc499285988)

[6.4 Authority for Rollback 13](#_Toc499285989)

[6.5 Rollback Procedure 13](#_Toc499285990)

[6.6 Rollback Verification Procedure 13](#_Toc499285991)

**Table of Figures**

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

**Table of Tables**

[**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities 5**](#_Toc498415573)

[**Table 2: Master Deployment Schedule 6**](#_Toc498415574)

[**Table 3: Site Preparation 10**](#_Toc498415575)

[**Table 4: Hardware Specifications 10**](#_Toc498415576)

[**Table 5: Software Specifications 10**](#_Toc498415577)

# 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.

## 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 | Installation | 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 | Installations | Coordinate training |  |
|  | TASCore | Back-out | Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out) |  |
|  | TASCore | Post Deployment | Hardware, Software and System Support |  |
|  |  |  |  |  |

# 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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Product | Product Supported + Feature Description | FY17 | | | | FY18 | |
| **Q1 Oct/Nov/Dec** | **Q2 Jan/Feb/Mar** | **Q3 Apr/May/Jun** | **Q4 Jul/Aug/Sep** | **Q1 Oct/Nov/Dec** | **Q2 Jan/Feb/Mar** |
| **eBusiness** | **USD & P** |  |  | **1** | **1** | **0** | **0** |
| **Dev / UAT** |  |  | **1** | **1** | **1** | **0** |
| **IOC / Release** |  |  | **0** | **0** | **0** | **0** |
| **Warranty** |  |  | **0** | **1** | **1** | **1** |
| eBusiness Build 1 | SP update + TAS Portal Link to 2013 site |  | USD&P | Dev / UAT | Warranty |  |  |
| eBusiness Build 2 | TAS Link to ICB landing page ATO Support Arch Design Recommendation: Dynamic Nav feature to address multiple ATO challenges (this may be folded into the current scope of an existing Architecture Build) |  |  | USD&P | Dev / UAT | Warranty |  |
| eBusiness Build N | services to support eBilling TAS Build 1. |  |  |  | USD&P | Dev / UAT | Warranty |

## 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”).

Figure 1: Targeted Architecture



### 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 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.

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

Ansible will handle database creation, if required.

## Installation Scripts

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

## 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

## Installation Procedure

Ansible will handle all server software installations. There are no client components to install.

## 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

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).

# 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 docker 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.

## 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

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 |