# VA Medical Care Collections Fund (MCCF)
# Electronic Data Interchange (EDI)
# Transaction Applications Suite (TAS)

# Production Operations Manual

**December 2018**

**Version 1.2**

**Department of Veterans Affairs**

## Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| December 4, 2018 | 1.2 | Corrected document title & version number; removed template table, but noted template version used in Revision History. | T. Nichols |
| November 15, 2018 | 1.1 | Added MCCF TAS Portal Start-up instructions to System Startup section. | Halfaker System Administration Team |
| July 22, 2018 | 1.0 | Initial version based on Template 1.6 dated March 2016. | MCCF EDI TAS |

Note: The revision history cycle begins once changes or enhancements are requested after the Production Operations Manual has been baselined.

# Artifact Rationale

The Production Operations Manual provides the information needed by the production operations team to maintain and troubleshoot the product. The Production Operations Manual must be provided prior to release of the product.

# Table of Contents


1. Introduction ..... 5
2. Routine Operations ..... 5
   2.1. Administrative Procedures ..... 5
      2.1.1. System Start-up ..... 5
         2.1.1.1. System Start-Up from Emergency Shut-Down ..... 5
         2.1.2. MCCF TAS Portal Start-up ..... 5
      2.1.3. System Shut-down ..... 4
         2.1.3.1. Emergency System Shut-down ..... 4
      2.1.4. Back-up & Restore ..... 4
         2.1.4.1. Back-Up Procedures ..... 5
         2.1.4.2. Restore Procedures ..... 5
         2.1.4.3. Back-Up Testing ..... 6
         2.1.4.4. Storage and Rotation ..... 6
   2.2. Security / Identity Management ..... 6
      2.2.1. Identity Management ..... 6
      2.2.2. Access control ..... 6
   2.3. User Notifications ..... 6
      2.3.1. User Notification Points of Contact ..... 6
   2.4. System Monitoring, Reporting & Tools ..... 6
      2.4.1. Dataflow Diagram ..... 7
      2.4.2. Availability Monitoring ..... 7
      2.4.3. Performance/Capacity Monitoring ..... 7
      2.4.4. Critical Metrics ..... 8
   2.5. Routine Updates, Extracts and Purges ..... 8
   2.6. Scheduled Maintenance ..... 8
   2.7. Capacity Planning ..... 8
      2.7.1. Initial Capacity Plan ..... 8
3. Exception Handling ..... 8
   3.1. Routine Errors ..... 9
      3.1.1. Security Errors ..... 9
      3.1.2. Time-outs ..... 9
      3.1.3. Concurrency ..... 9
   3.2. Significant Errors ..... 9
      3.2.1. Application Error Logs ..... 9
      3.2.2. Application Error Codes and Descriptions ..... 9
      3.2.3. Infrastructure Errors ..... 9
         3.2.3.1. Database ..... 10
         3.2.3.2. Web Server ..... 10
         3.2.3.3. Application Server ..... 10

3.2.3.4. Network ..... 10
3.2.3.5. Authentication & Authorization ..... 10
3.2.3.6. Logical and Physical Descriptions ..... 10
**3.3. Dependent System(s) ..... 11**
**3.4. Troubleshooting ..... 11**
**3.5. System Recovery ..... 11**
**3.5.1. Restart after Non-Scheduled System Interruption ..... 11**
**3.5.2. Restart after Database Restore ..... 12**
**3.5.3. Back-out Procedures ..... 12**
**3.5.4. Rollback Procedures ..... 12**
**4. Operations and Maintenance Responsibilities ..... 16**
**4. Approval Signatures ..... 18**

# 1. Introduction

This document describes how to maintain the components of the Medical Care Collections Fund (MCCF), Electronic Data Interchange (EDI), Transactions Application Suite (TAS) in the Microsoft Azure Government Cloud Environment (MAG), as well as how to troubleshoot problems that might occur with this product while in production. The intended audiences for this document are the IT teams responsible for hosting and maintaining the system after production release. This document is normally finalized just prior to production release, and it includes many updated elements specific to the hosting environment.

# 2. Routine Operations

The MCCF EDI TAS product is deployed in MAG, which provides all routine support of hardware and connectivity operations. The MCCF product software is managed via the Jenkins automated deployment tool on the MCCF FPC server.

## 2.1. Administrative Procedures

### 2.1.1. System Start-up

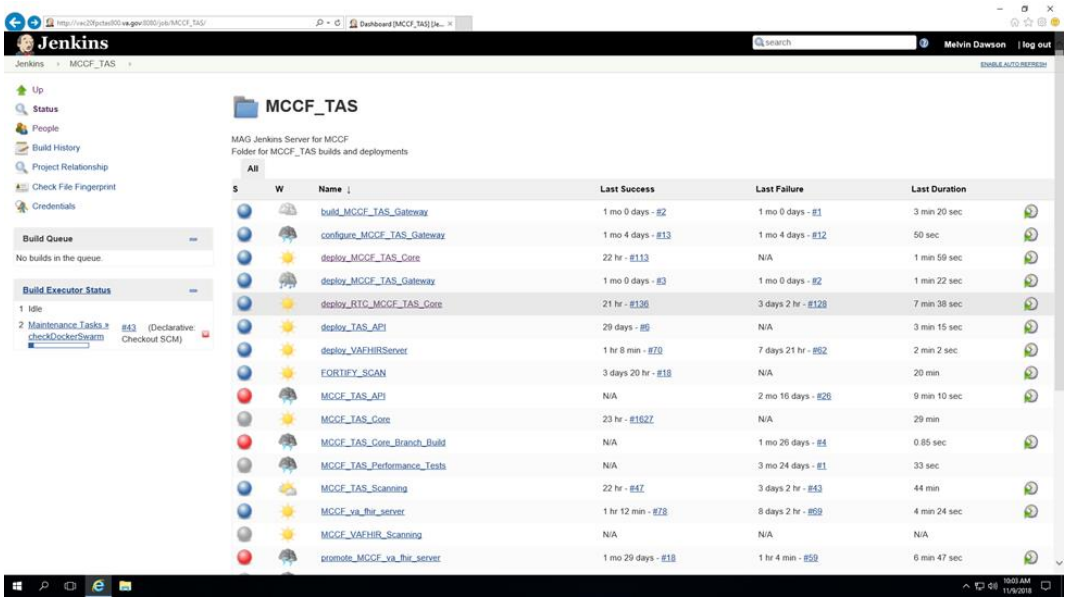
System start-up is performed within the MAG Administrative portal using the product owner's Azure Portal account. All MCCF systems and services are in a Microsoft Azure cloud environment and are designed to run at all times (if the clouds server is up, the MCCF servers will be up).

#### 2.1.1.1. System Start-Up from Emergency Shut-Down

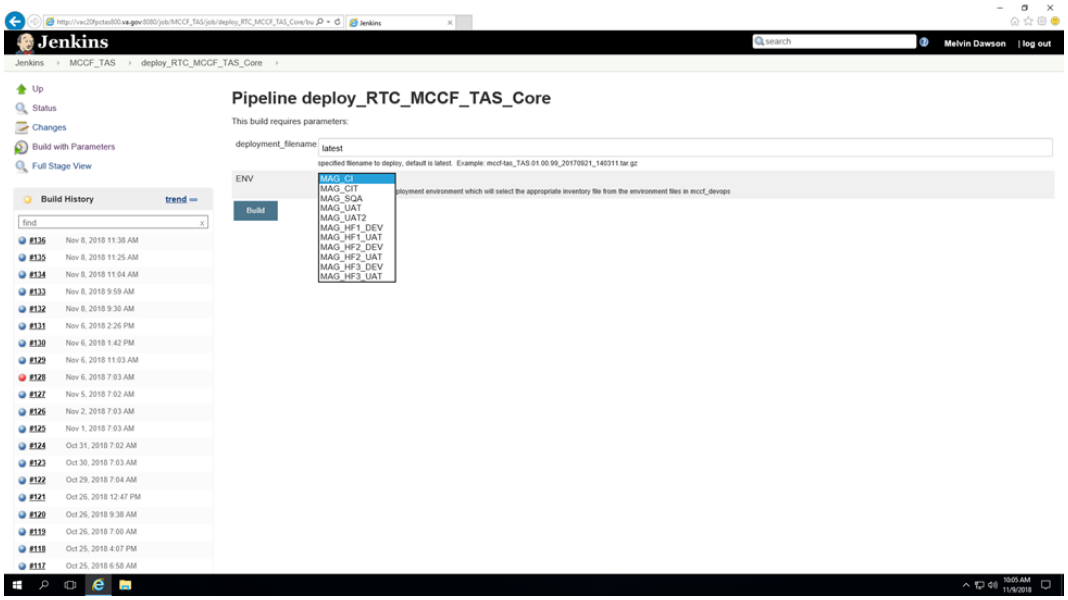
The MCCF product is deployed in the MAG environment. Operational emergency management is provided by the MAG environment.

### 2.1.2. MCCF TAS Portal Start-up

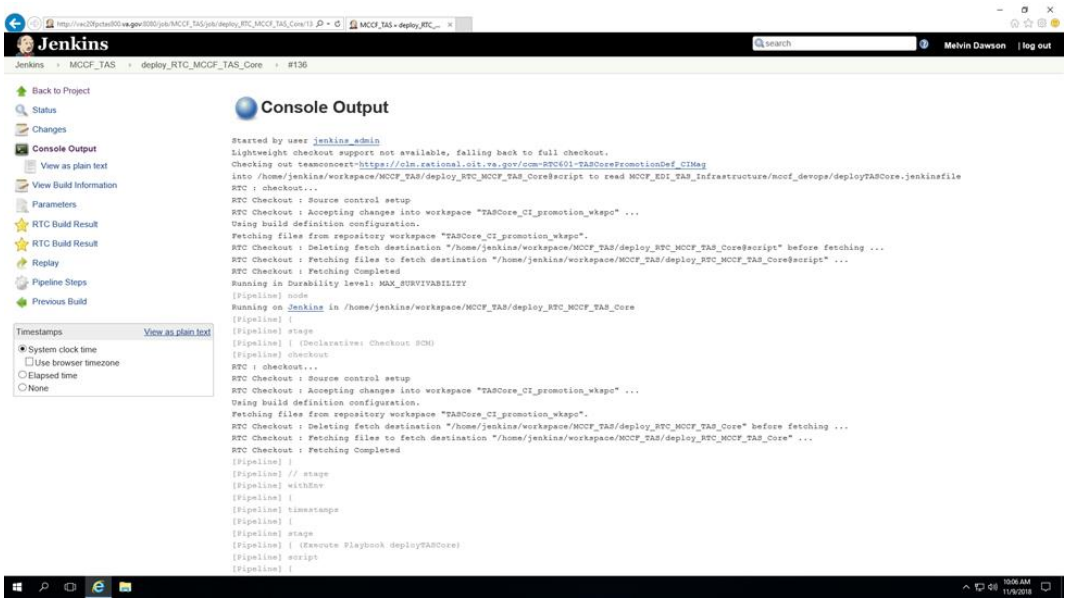
To start-up the MCCF TAS Portal application, run the deploy_RTC_MCCF_TAS_Core job in Jenkins to deploy the application to the specified PROD server by clicking on the Name link.

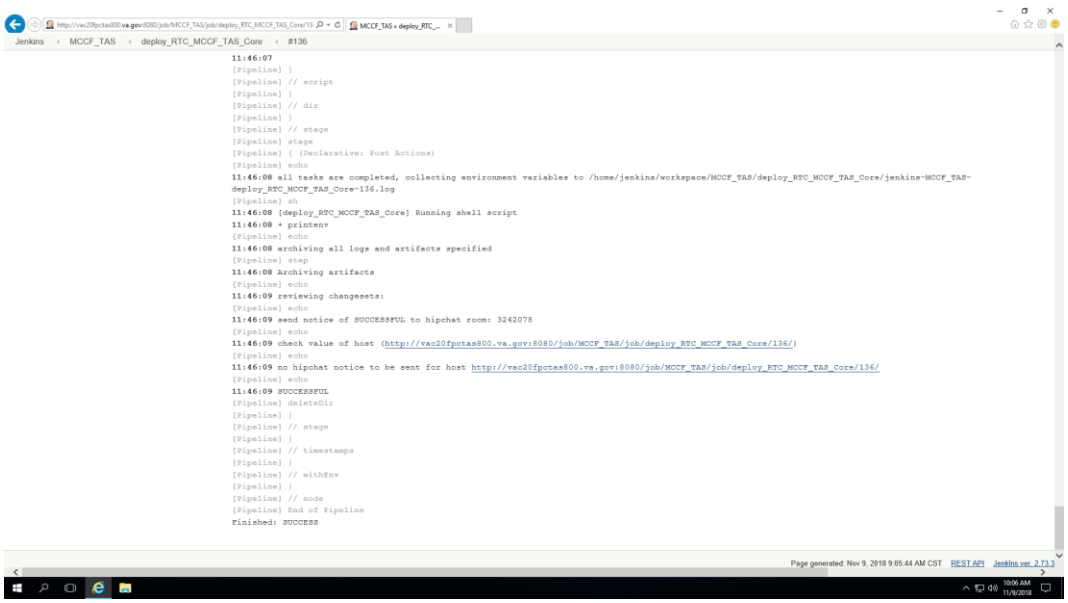



Next, you will be brought to the Pipeline deploy_RTC_MCCF_TAS_Core page. If not using the latest build, you can also specify deployment_filename (e.g., mccf-tas_TAS.01.00.247_20180604_092635.tar.gz) , which represents the name of file for a particular build's code (e.g Build 3, Build 5…) for the specific environment (ENV field) you want to deploy the code to.



Once all fields a appropriately populated, the build process is start by clicking the Build button, click on the orb at the top of the list on the left to open the Console Output page that will list the status of the deployment process. Continue to monitor until you receive a successful termination of the task.




NOTE: If there is a problem with the webserver, the Apache webserver may need to be restarted which can be done by a System Administrator. In this case, a System Administrator would start the webserver service/ daemon using the following command from a LINUX command prompt:

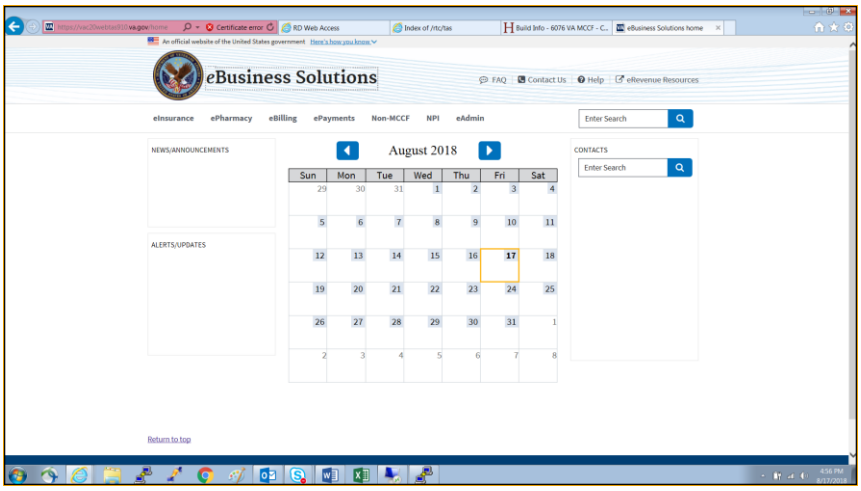
**systemctl start httpd**

The TAS Portal application will automatically be available either upon deployment using the deploy_RTC_MCCF_TAS_Core or by the restart of Apache.

Once you have successfully deployed the code to the webserver, verify that it is up and operational. To do so, go to the webserver's homepage from a web browser using this format:

**https://[servername].va.gov**

Here is a screenshot of the TAS Portal homepage once it has been successfully started or restarted:




## 2.1.3. System Shut-down

The MCCF product is deployed in the MAG environment. Operational shutdown procedures are provided by the MAG environment. Additionally, the product owner's Administration personnel can initiate a MAG-specific shutdown using the Jenkins interface.

### 2.1.3.1. Emergency System Shut-down

The MCCF product is deployed in the MAG environment. Operational shutdown procedures are provided by the MAG environment. Operational emergency management is provided by the MAG environment.

## 2.1.4. Back-up & Restore

*The CosmosDB references in this section only apply to a future release of TAS that will contain CosmosDB. TAS v1.0 does not utilize a database.*

The MCCF product is deployed in the MAG environment, and stores all data – including PII, in CosmosDB, which is provided by the MAG in a SaaS model. As a result, all backup and restore operations are CosmosDB backup and restore operations. For more information, please refer to the link below:

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

Jenkins server resources , though stored under the /var/lib/jenkins directory, are also backed-up by blob storage in the Azure Cloud environment.

### 2.1.4.1. Back-Up Procedures

**Backup Schedule is TBD**

The following image illustrates periodic full backups of all Cosmos DB entities in GRS Azure Storage.

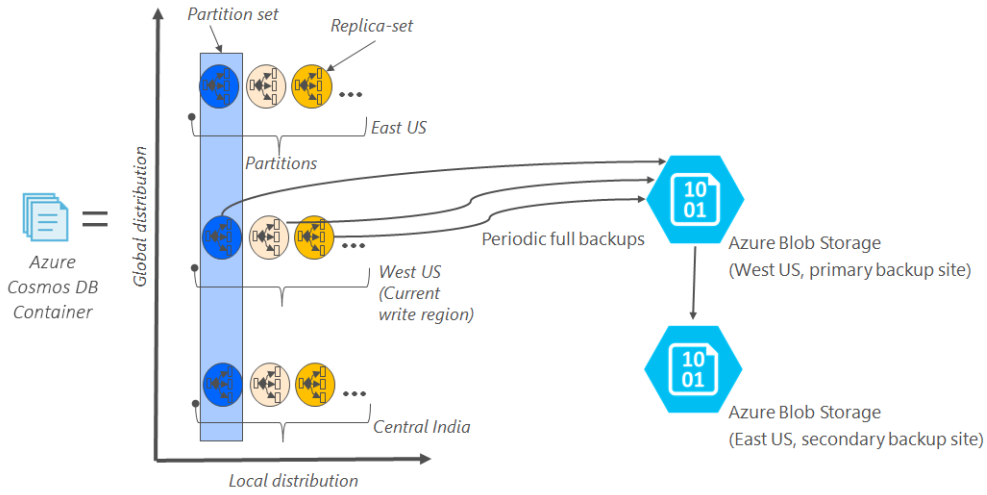



**Figure 1 - Backup Procedures**

**Backup retention period**

As described above, Azure Cosmos DB takes snapshots of data every four hours at the partition level. At any given time the last two snapshots are retained. However, if the collection/database is deleted, the existing snapshots are retained for all of the deleted partitions within the given collection/database for 30 days.

For SQL API, if users choose to maintain their own snapshots, the export to JSON option in the Azure Cosmos DB Data Migration tool can be used to schedule additional backups.

---

**Restoring a database from an online backup**

If a database or collection is accidentally deleted, the appropriate actions are to file a support ticket or to call Azure support to restore the data from the last automatic backup. Azure support is available only for selected plans only such as Standard. Developer, support isn't available with Basic plan. To learn about different support plans, see the Azure support plans page. If a need arises to restore a database because of a data corruption issue (this includes cases where documents within a collection are deleted), see handling data corruption as additional steps are required to prevent the corrupted data from overwriting the existing backups. For a specific snapshot of a backup to be restored, Cosmos DB requires that the data is available for the duration of the backup cycle for that snapshot.

### 2.1.4.2. Restore Procedures

The following link provides CosmosDB backup and restore operations

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

#### 2.1.4.3. Back-Up Testing

TBD

#### 2.1.4.4. Storage and Rotation

TBD

## 2.2. Security / Identity Management

The MCCF product subscribes to VA's IAM service to enable users to gain role-based limited access to the system using VA PIV credentials.

System-level (privileged) access to the systems is restricted to System Administrators, and utilizes the VA Centrify service to gain control access using VA PIV credentials.

https://vaww.strongauth.va.gov/RDWeb/Pages/en-Us/Default.aspx?reason=freeslots

### 2.2.1. Identity Management

Because ALL users and administrators gain access to the MCCF systems using VA PIV credentials, identity management is handled by the VA and its Active Directory (AD) infrastructure.

### 2.2.2. Access control

Users and administrators can gain access to the MCCF systems only by using VA PIV credentials, either via the IAM or via Centrify services provided by the VA.

## 2.3. User Notifications

All relevant users are notified via email of upcoming system changes and outages within an acceptable and reasonable period of time prior to the scheduled event(s). An email distribution list created by the product owner, is used to send these notifications to the appropriate contacts.

### 2.3.1. User Notification Points of Contact

Notifications will be sent to the personnel identified by the product owner. As noted in 2.3., an email distribution list created by the product owner, is used to send these notifications to the appropriate contacts.

## 2.4. System Monitoring, Reporting & Tools

Performance and other system monitoring services are provided by the Cloud Provider.
https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview

## 2.4.1. Dataflow Diagram

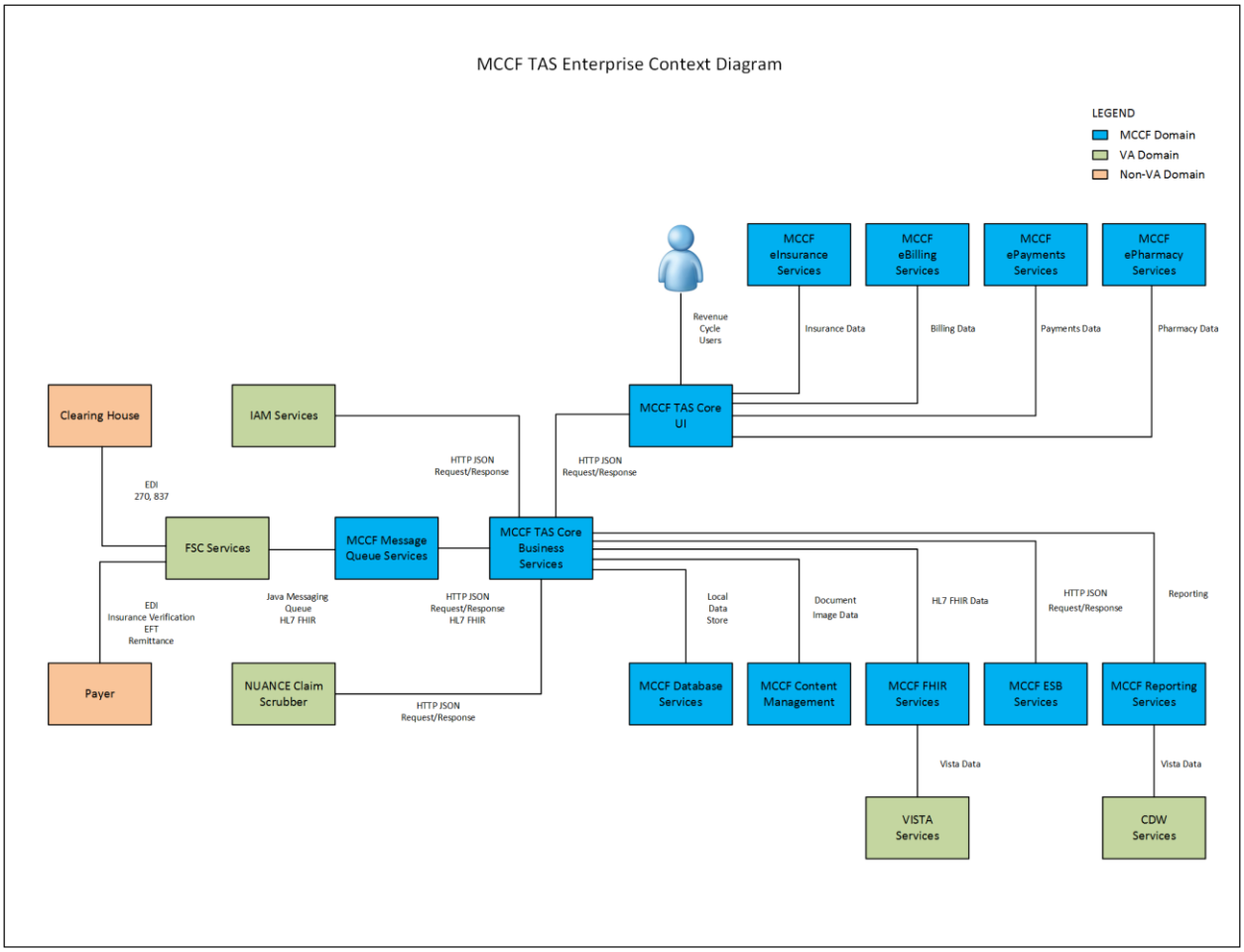



**Figure 2 - Dataflow Diagram**

## 2.4.2. Availability Monitoring

Availability monitoring is performed within Azure. Please refer to the Microsoft Azure link below for more information:

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview

## 2.4.3. Performance/Capacity Monitoring

Performance/Capacity Monitoring of our systems can be performed locally, via the Azure Cloud Management Portal and can be scaled up relatively easily. As noted above, please refer to the Microsoft Azure link below for more information:

https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview

### 2.4.4. Critical Metrics

TBD

## 2.5. Routine Updates, Extracts and Purges

TBD

## 2.6. Scheduled Maintenance

The MCCF product has been developed, and is operationally maintained using an Agile continuous deployment methodology. As a result, there is no set schedule of maintenance other than one that may be utilized as chosen by the product owner, which is the Microsoft Azure cloud services provider. AITC performs monthly software updates. The product teams perform MAG (Dev/Test) updates after VA environments are updated.

## 2.7. Capacity Planning

Required analysis is completed to identify and define the achievable QoS levels for applicable capacity and performance metrics, and to determine how these will be monitored and enforced; QoS levels to be delivered will be those that are either at least equal to corresponding industry benchmarks or those that reflect situational specifics of the information technology in question. **Applies to MCCF once the MCCF Detailed Application Design and performance requirements are finalized.**

Capacity measures include those from the processing, utilization, and concurrency rates for system components.

### 2.7.1. Initial Capacity Plan

| Server Environments | Sku | Type | Compute type | vCPUs | GB RAM | Data disks | Max IOPS | Local SSD | Premium disk support | Notes |
|---|---|---|---|---|---|---|---|---|---|---|
| **FPC, APP, WEB, DBS** | A4m_v2 | Standard | General purpose | 4 | 32 | 8 | 8x500 | | SSD | With the exception of the FPC servers, these servers are in build specific staging environments for testing. Not the active development environments. |
| **Tableau** | DS13_v2 | Promo | Memory optimized | 8 | 56 | 32 | 32000 | 112 GB | SSD | The is a Windows server and is a stand-alone enviroment. |

**Figure 3 - Server Environment within Azure**

# 3. Exception Handling

The MCCF product has been designed and deployed using an Agile methodology. The MCCF product is primarily a web-based product, and errors and defects can be detected by the system or reported by end-users. In both instances, remediation can be completed quickly and efficiently through the Agile delivery process.

The MCCF API runs in a Docker cluster, which sends errors and exceptions to the syslog area (/var/log/…) directory of the system.

## 3.1. Routine Errors

The MCCF product will report runtime errors and other detected system anomalies via email to a pre-defined (product owner defined) group. Because MCCF is designed with the Agile methodology, defects can be identified and mitigated quickly by the appropriate development and/or operational teams.

### 3.1.1. Security Errors

The MCCF product will report runtime errors and other detected system anomalies via email to a pre-defined (product owner defined) group. Because MCCF is designed with the Agile methodology, defects can be identified and mitigated quickly by the appropriate development and/or operational teams. Security violations will come from Centrify or IAM environments.

### 3.1.2. Time-outs

Time-out and other connection-related security functions are managed and controlled by the VA-provided credentialing (IAM or Centrify) as noted above.

### 3.1.3. Concurrency

TBD

## 3.2. Significant Errors

The MCCF product is primarily deployed in the MAG environment. As a result, most hardware and connection-level errors will be managed by the Microsoft Azure cloud services provider. Software issues will usually generate error messages that the system operators may consult to determine their root-causes.

### 3.2.1. Application Error Logs

The MCCF product is primarily a web-based application. The system logs for the webserver, and other supporting applications are located in Linux-standard locations (/var/log) which are visible to the Jenkins administrator.

### 3.2.2. Application Error Codes and Descriptions

The MCCF product does not generate product-specific error codes.

### 3.2.3. Infrastructure Errors

The MCCF product is primarily deployed in the MAG environment. As a result, infrastructure errors will be referred to the cloud provider for remediation.

#### 3.2.3.1. Database

The MCCF product uses the MAG-supplied CosmosDB database in a SaaS mode. As such, all database errors will be referred to the cloud provider for remediation.

### 3.2.3.2. Web Server

The MCCF product is primarily a web-based application. The system logs for the webserver and other supporting applications are located in Linux-standard locations (/var/log) which are visible to the Jenkins administrator.

### 3.2.3.3. Application Server

The MCCF Application Servers provide HAPIFHIR services to the MCCF web application. Log files for this server are located on the responsible application server, and are located in the Linux-standard locations (/var/log) which are visible to the Jenkins administrator.

### 3.2.3.4. Network

The MCCF project is primarily deployed into the MAG environment. Network maintenance and configuration are a part of the cloud provider service.

### 3.2.3.5. Authentication & Authorization

The MCCG product authenticates users with VA-provided mechanisms (IAM and Centrify), each of which provides its own authentication and authorization logging.

### 3.2.3.6. Logical and Physical Descriptions

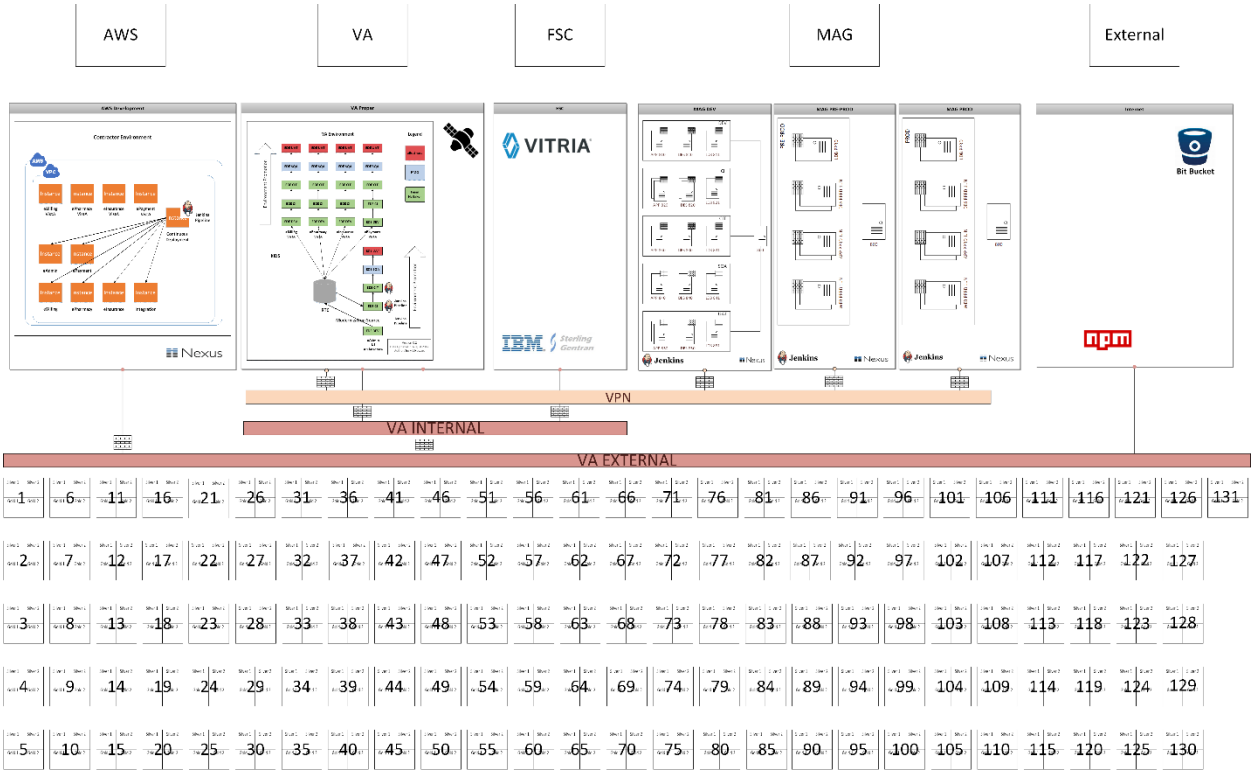



**Figure 4 - MCCF Physical Architecture**

## 3.3. Dependent System(s)

TBD

## 3.4. Troubleshooting

TBD

## 3.5. System Recovery

The MCCF product is primarily deployed in the MAG environment which does not support a system recovery option. Instead, system components (or the entire MCCF system) are deleted (destroyed) and re-built as needed. NOTE: unlike some cloud environments, the MAG does NOT support the restarting of a VM with another disk image. Instead a NEW VM must be created should it be desired that an older image/snapshot be used for a system.

### 3.5.1. Restart after Non-Scheduled System Interruption

Systems might restart because of issues within the VM itself or due to an application anomaly. The workload or role that's running on the VM might trigger a bug check within the guest operating system. To determine the reason for the crash, view the system and serial logs for Linux VMs. Once the issue has been found and resolved, the Linux VM can be restarted via the Azure Cloud Portal Dashboard using an automated script. Below is an example:

To restart a VM using the Azure portal, select your VM and click the **Restart** button as in the following example:

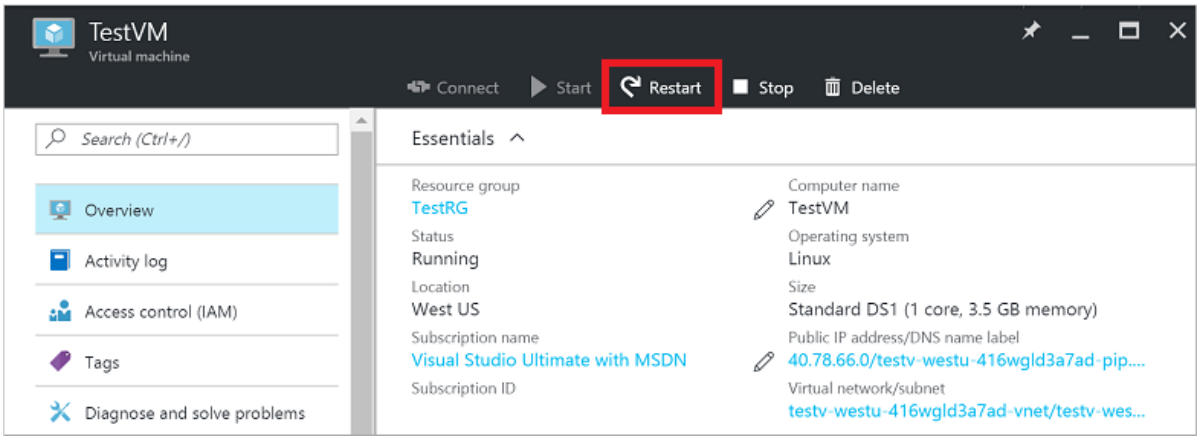



**Figure 5 - Azure Portal**

There are few cases where our VMs are rebooted due to planned maintenance to the underlying infrastructure. Being impactful to the availability of our VMs hosted in Azure, The following represents cases that are impactful to the availability of VMs hosted in Azureare and are available to use:

- Notification sent at least 30 days before the impact.
- Visibility to the maintenance windows per each VM.
- Flexibility and control in setting the exact time for maintenance to impact your VMs.

The **Pre-emptive Maintenance Window** provides the flexibility to initiate the maintenance on our VMs. By doing so, one can determine when VMs are impacted, the sequence of the update, and the time between each VM being maintained.

### 3.5.2. Restart after Database Restore

TBD

### 3.5.3. Back-out Procedures

There are no back-out procedures. If a system is running an undesired MCCF product revision, it can be either re-built or re-deployed from the Jenkins console.

### 3.5.4. Rollback Procedures

The CosmosDB database is provided SaaS. Rollback Procedures are therefore provided by the cloud provider.

# 4. Operations and Maintenance Responsibilities

The following table contains a description of the operations and maintenance roles and responsibilities.

| Role & Brief Description | Assigned Organization (Pillar and Sub-office) | Contact Information |
|---|---|---|
| Tier 0: Local End User Support (e.g. Automated Data Processing Application Coordinator (ADPACS)) | N/A – This is not a desktop application. Browser configuration requirements will be published and URL. We do not provide local end user support. | N/A |
| Enterprise Service Desk Tier 1: Provide first contact resolution via Knowledge Documents retained in CA Service Desk Manager.<br>NOTE: The MCCF EDI TAS PjM is coordinating with the ESD to integrate TAS support. | ITOPs (Enterprise Service Desk) | 855-NSD-HELP (855-673-4357) |

| Role & Brief Description | Assigned Organization (Pillar and Sub-office) | Contact Information |
|---|---|---|
| Tier 2: The second level of service provider functions, which include problem screening, definition, and resolution. Service requests that cannot be resolved at this level in a set period of time are elevated to appropriate service providers at the Tier 3 level. | Release 1 – MCCF EDI project team is supporting.<br>FSC is currently determining level and type of support.. | ESD Tickets escalated to Tier 2<br>For initial release, ESD will not be integrated into support.<br>POC: Toby Rudik or Jim Plastow |
| Tier 3: The third level of service provider functions, which consist primarily of problem identification, diagnosis, and resolution. Service requests that cannot be resolved at the Tier 2 level are typically referred to the Tier 3 for resolution. | Release 1 – MCCF EDI project team is supporting.<br>FSC is currently determining level and type of support | ESD Tickets escalated to Tier 3<br>For initial release, ESD will not be integrated into support.<br>POC: Toby Rudik or Jim Plastow |
| Receiving Org/Sustainment Manager: Coordinates ongoing support activities including budget reporting, contract management, and technical risk management during O&M.<br><br>** If applicable, include key details such as whether this individual will be reviewing deliverables from an O&M contract. | Release 1 – MCCF EDI project team is executing as Receiving Organziation.<br>FSC is transitioning into the Receiving Organziation role for subsequent releases | POC: Toby Rudik or Jim Plastow |
| COR ** Check with the Contracting Officer to determine if a certified COR is required and at what level during O&M. | EPMO | POC: TBD |
| Contracting Office | Technical Acquisition Center (TAC) | POC: TBD |

### *RACI Matrix*

MCCF Operations and Maintenance Res

# 4. Approval Signatures

REVIEW DATE: *<date>*

SCRIBE: *<name>*

CHRISTAN M GOVICH 467073

Digitally signed by CHRISTAN M GOVICH 467073
Date: 2018.12.12 09:55:06 -05'00'

Katrina Tuisamatatele or Designee
Health Portfolio Director

Frank C. Annecchini 1132102

Digitally signed by Frank C. Annecchini 1132102
Date: 2018.12.06 13:52:49 -06'00'

Frank Annecchini
Product Owner

Jimmy J. Medrano 122258

Digitally signed by Jimmy J. Medrano 122258
Date: 2018.12.06 10:53:14 -06'00'

Jimmy Medrano
Receiving Organization POC

TOBY S. RUDIK 338177

Digitally signed by TOBY S. RUDIK 338177
Date: 2018.12.06 11:45:38 -06'00'

Toby Rudik
Operations Support POC