**Appendix**

**Atlas Archvie System Design**

Contents

[D.1 INTRODUCTION 1](#_Toc81288684)

[D.1.1 System Overview 1](#_Toc81288685)

[D.1.2 Goals 2](#_Toc81288686)

[D.1.2.1 Short Term Goals 2](#_Toc81288687)

[D.1.2.2 Long Term Goals 2](#_Toc81288688)

[D.1.3 Scope 3](#_Toc81288689)

[D.1.4 Points of Contact 3](#_Toc81288690)

[D.2 EXCHANGE 2019 REQUIREMENTS 4](#_Toc81288691)

[D.2.1 Exchange Server Hardware 4](#_Toc81288692)

[D.2.2 System Diagrams 4](#_Toc81288693)

[D.2.3 Message Journaling 6](#_Toc81288694)

[D.2.4 Kemp Load Balancers 6](#_Toc81288695)

[D.2.5 Network Switches 7](#_Toc81288696)

[D.2.6 Backup and Disaster Recovery 7](#_Toc81288697)

[D.3 SERVER CONFIGURATIONS 7](#_Toc81288698)

[D.3.1 Operating System 7](#_Toc81288699)

[D.3.2 Group Policy 7](#_Toc81288700)

[D.3.3 Exchange Site Topology 8](#_Toc81288701)

[D.3.4 E-mail Flow 8](#_Toc81288702)

[D.3.5 Database Availability Groups (DAG) and Storage Design 8](#_Toc81288703)

[D.3.6 SMTP Relay 9](#_Toc81288704)

[D.3.7 MDS 9](#_Toc81288705)

[D.3.8 E-mail Client Design 9](#_Toc81288706)

[D.3.9 New Features 10](#_Toc81288707)

[D.3.10 Faxing 11](#_Toc81288708)

[D.3.11 Monitoring Tools 11](#_Toc81288709)

[D.4 MANAGEMENT 12](#_Toc81288710)

[D.4.1 Staffing 12](#_Toc81288711)

[D.4.2 Administrative Design 12](#_Toc81288712)

[D.4.3 Remote Management Tools 13](#_Toc81288713)

[D.4.4 Management Scopes 14](#_Toc81288714)

[D.5 USAMAIL EXCHANGE 2019 RACK DIAGRAM 15](#_Toc81288715)

[D.5.1 EXCHANGE 2019 – CEF-DC Layout 15](#_Toc81288716)

[D.5.2 EXCHANGE 2019 -- NOC Layout 16](#_Toc81288717)

[D.5.3 EXCHANGE 2019 – GI Lab Layout 17](#_Toc81288718)

1. INTRODUCTION

This document is the *Exchange 2019 System Design* document. It has been prepared for the United States Attorneys’ Office (USAO). This document provides specific information related to the design of the Exchange 2019 system. It is an Appendix to the *USA Messaging 2021 Upgrade Detailed Design* document.

* 1. System Overview

The United States Attorneys’ Offices (USAOs) is comprised of 94 Districts with offices spread across the continental United States, Alaska, Hawaii, Guam, Puerto Rico, and the U.S. Virgin Islands. The USAOs also include the Executive Office for the United States Attorneys (EOUSA). Headquartered in Washington, DC, the EOUSA performs management and liaison functions for the USAO.

Each of the 94 Districts is composed of between one and six sites. Within each District, one site is designated the District **Headquarters** (**HQ**) office, and the remaining sites are designated **Branch** offices. The number of users at each office ranges from 0 to 800.

The existing centralized e-mail messaging system is provided by Exchange 2013, split between data centers in Columbia, SC and Sterling, VA. There are six (6) active servers at each site with same-site failover capability, as well as failover to the other data center.

The USAO had been using a centralized Microsoft Exchange E-mail system since the implementation of the USAMAIL project which was completed in 2009. In 2019, the mailboxes hosted on the centralized system were migrated to Exchange Online, a service of Microsoft 365, in a highly secure Microsoft “tenant” dedicated to all DOJ components other than FBI.

The remaining “on Premises” Exchange system is dedicated to all functions not provided by the Exchange Online system. In brief, they are:

* Message Journal ingestion
* SMTP relay for on premises applications
* User provisioning
* External Email Address provisioning
* Maintenance of Mail Enabled Security Groups
* Expanding Non-synced Distribution Groups
* Remote Administrative Shell for Exchange Online

A full listing of on Premises Exchange functions can be found in the Requirements document.

The Exchange 2019 E-mail system will take advantage of changes and improvements that have occurred within Information Technology (IT) during the normal life cycle replacement of hardware and software elements in the USAOs.

The following productivity issues are present under the current Exchange 2013 System:

* SMTP relay is load balanced through DNS, leading to unrecoverable relay failures in certain Java programs that do not store and forward failed relays.
* Excessive number of servers (once needed for mailbox storage) lead to unnecessary system complexity.
* Lack of storage space on local drives causing server unavailability.
* Hardware limitations (especially speed of drives) causing delays in Journaling.

With the introduction of Exchange 2019, the United States Attorneys have the opportunity to improve the E-mail system and provide better service to the organization.

* 1. Goals

The goal of the Exchange 2019 system is the continued e-mail service for all USAO and integration with all messaging-related components.

* Having a workable Exchange Management Shell to run user provisioning commands.
* Having a reliable SMTP relay
  + Internal
  + External
* Having a load balanced Federation System for O365
* Synchronizing existing Mail Enabled Security Groups, and other Mail Enabled Groups nested into them
* Maintaining usdoj.gov addresses so that they become the user’s Identity for the PIV card system.
* Reliable Skype meetings
* Envelope Journaling that captures the exact content of each sent/received message, including bcc and Group Membership
  1. Scope

The scope of this project is the migration from the existing Exchange 2013 system to the Exchange 2019 system. EOUSA will refresh the USAMail server hardware by installing new servers and hardware load balancers.

* 1. Points of Contact

| **Name** | **Organization/Title** | **Phone** | **Email** |
| --- | --- | --- | --- |
| Mark Fleshman | EOUSA CIO | 202 252-6246 | Mark.Fleshman@usdoj.gov |
| David Atkins | OAS Federal Project Manager | 202 252-6277 | David.Atkins@usdoj.gov |
| Joaquin Santos | GI Technical Director | 202 252-6386 | Joaquin.Santos@usdoj.gov |
| Aynura Mammadova | GI Project Leader | 202 252-6375 | Aynura.Mammadova@usdoj.gov |
| Jonathan Reiser | GI Senior Network Engineer | 202 252-6373 | Jonathan.Reiser@usdoj.gov |
| Phillip Hylton | GI Senior Technical Writer and Editor | 202 252-6362 | Phillip.Hylton@usdoj.gov |

1. EXCHANGE 2019 REQUIREMENTS

This section identifies the minimum hardware and software requirements for the servers that will comprise the USA Messaging system. It also identifies requirements for other messaging systems related to Exchange 2019.

* 1. Exchange Server Hardware

All server hardware requirements are based on vendor deployment guidelines, best practices.

CEF-DC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | **In Cabinet** | **ILO** | **Prod NIC** | **MAC Addresses** | **Switch Ports** |
| **USAHUBSML241** | F13 | 10.200.2.96 | 10.200.1.96 | 48-df-37-e1-f0-f0 | 21 (USAHUBNIDF2003/4) |
| **USAHUBSML242** | F13 | 10.200.2.97 | 10.200.1.97 | 48-df-37-e1-9f-a0 | 23 (USAHUBNIDF2003/4) |

NOC

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server** | **In Cabinet** | **ILO** | **Prod NIC** | **MAC Addresses** | **Switch Ports** |
| **USAHUBSML141** | 3A803 U38-39 | 10.200.194.210 | 10.200.16.85 | 48-DF-37-E1-7B-A0 | 36 (USAHUBNIDF1001) |
| **USAHUBSML142** | 3A803 U36-37 | 10.200.194.211 | 10.200.16.86 | 48-df-37-e1-f0-b8 | 37 |
|  |  |  |  |  |

* 1. System Diagrams

Refer to Section 3.1 of the USA Messaging 2021 Upgrade Detailed Design for a detailed diagram of the network connections to and from the USA Messaging 2021 environment (including Exchange 2019).

The following diagram represents the current Exchange 2013 Production environment.

**Figure 2-1. *Current Exchange 2013 Production Environment* diagram**



**Figure 2-2. *Exchange 2013 Production Environment* diagram**

* 1. Message Journaling

EOUSA continues to use message Journaling, specifically the type of Journaling that originates at the Database level (as opposed to a rule on the Transport). The ProofPoint Enterprise Archive system will be used to ingest from the Journaling mailbox and store the USAMail 2014 Compliance archive and will provide Archive Search and LitHold services. See *Appendix I* of the *USAMail 2014 Detailed System Design* for complete details about ProofPoint and Journaling.

* 1. Kemp Load Balancers

To optimize connections from clients, EOUSA will use four Kemp X15 Load Balancers (one pair in each datacenter), which will evenly distribute requests from clients to the Client Access ports on the Exchange 2019 servers.

* 1. Network Switches

The Exchange 2019 servers will connect directly to Cisco Nexus 5k switches

The Kemp X15 Load Balancers will connect directly to Cisco Nexus 2k Fabric Extenders.

The network team will configure each switch with Port Channels to support network teams (and the resulting doubled throughput) on each of the two connected servers the Load Balancer in each datacenter.

* 1. Backup and Disaster Recovery

[CommVault]

1. SERVER CONFIGURATIONS
   1. Operating System

The base operating system, Windows 2019 Server, will be installed in accordance with *Appendix A01* of the *Implementation Plan for Exchange 2019*.

* 1. Group Policy

The USAO plans to utilize Group Policy Objects (GPOs) as a tool to manage the users and computers in the usa.doj.gov domain more effectively. The USAO will develop GPOs that address security and management requirements, and they will apply them to Organizational Units (OU), which contain users and computers. The USAO will also implement domain-level and domain controller policies that will enforce specific security in the domain.

The specific Group Policy to be applied to the Exchange 2019 servers (that is, to the Organizational Unit which contains them) shall be based on a merger of the security hardening policies recommended by the National Institute of Standards and Technology (NIST), and exceptions known to be necessary for Exchange Servers (for example the ability to start the .Net TCP Port Sharing service. The Group Policy, thus derived, will then be applied to an Active Directory Organization Unit containing the Exchange 2019 server objects. That Organizational Unit is called usa.doj.gov/HUB/Servers/OAS-Servers/USAMailExchange

* 1. Exchange Site Topology

The USAO uses Active Directory Site Links to route messages. All of the Exchange 2019 servers and Load Balancers will be located in Columbia, SC and Sterling, VA, which are two geographically dispersed locations on different subnets. SMTP relays will be routed through the JMD ProofPoint messaging gateway system but Exchange DB data replication will be routed through a 1GB line between the two locations.

* 1. E-mail Flow

Most E-mail starts at the Outlook client, connected to a mailbox in the Exchange Online system, and is processed by that system’s back end. Most of the traffic generated in Exchange Online does not touch USA Messaging 2021, but there are important exceptions:

* Journal Envelopes, whose purpose is detailed in Appendix \_\_\_\_.
* Messages sent to Distribution Groups whose memberships are not synced to Exchange Online.

SMTP relay emails (including EVOIP Voice Mail messages) are sent from the applications that relays to the load balancer, thence to the ProofPoint Gateway, and thence to mailboxes in Exchange Online (or, rarely, to external recipients).

* 1. Database Availability Groups (DAG) and Storage Design

The Exchange 2019 system will continue the Database Availability Group (DAG) design feature, but with only on purpose: the redundancy of the Journal mailboxes.

The DAG members also monitor each others’ condition, and the condition of their databases, through the private network. Replicating data from one data center to another is more challenging; a router must be involved and the replication traffic must use bandwidth that is shared by other traffic between the data centers.

* 1. SMTP Relay

Authorized systems will be able to use one of the Exchange 2019 servers for SMTP relay to send email from their application.

The list of authorized systems is expected to change over time. Since adding new authorized systems can have security, storage and network traffic implications, Network Operations shall only enable systems to relay if those systems have been vetted through a service ticketing process.

The NOC shall, from time to time generate a report listing the authorized systems. The report thus generated shall be available to the persons designated in the Project Management Plan as being responsible, at any level, for USA Messaging 2021 maintenance. The report shall not be accessible outside of that scope. Upon request, for example from a District which has a legitimate purpose for requesting, the NOC shall confirm the presence or ability of a particular IP address on the list of authorized systems.

* 1. MDS

The Exchange 2019 system will connect to JMD’s MDS system for GAL synchronization. All external email addresses will be created and/or deleted by JMD based on the sync information. GAL syncs will occur every weeknight.

An account, USAHUB-MDS, shall exist for the sole purpose of servicing MDS. The USAHUB-MDS account is a member of only one group, Domain Users, but shall also be granted specific Active Directory rights consistent with the following:

* The ability to create new Contacts within the boundaries of the DOJ MDS Contacts Organizational Unit.
* The ability to write specific properties (e.g. SMTP addresses) to mail-enabled Users.

The password to the USAHUB-MDS account shall be known to the administrators at JMD who operate the MDS sync.

* 1. E-mail Client Design

No client connections will be allowed into the Exchange 2019 system unless permitted through a proper USAVON process. All client connections are supposed to connect to Exchange Online.

* 1. New Features
  2. Faxing

EOUSA will continue to provide RightFax, in the NOC datacenter only, so that client machines will be able to use the native RightFax client to send faxes, and so that Districts with a business need to receive faxes may do so.

There are two RightFax servers, one hosting the RightFax hardware (an expansion board with incoming/outgoing phone lines provided by the Telecom department) and the other hosting the RightFax application. The consolidated SQL cluster at the NOC hosts the RightFax database. Users with mailboxes are automatically able to send faxes courtesy of the Captaris Sync Module, which synchronizes between Active Directory and the RightFax database and adds and deletes users on an nightly basis.

All RightFax received faxes, and fax notifications, will be facilitated by the SMTP relay.

* 1. Monitoring Tools

EOUSA will continue to use a system that actively monitors the performance of the Exchange systems and alerts the NOC (by Instant Message if necessary) if unacceptable performance thresholds are reached.

1. MANAGEMENT

All IT equipment belonging to the USAO is housed in physically secure locations. General operations and maintenance of the USAVON system will be performed by DOJ employees and contractors with an in-depth knowledge of Windows Active Directory and Exchange at an enterprise level. The use of strong authentication is planned for all privileged administrator accounts.

* 1. Staffing

Operations and maintenance of the USAVON system within the USAOs will be accomplished through a three-tiered approach. In Tier One, operations and maintenance will be provided by the Systems Managers (SMs) in each district. Every Systems Manager is a government employee and as such, each undergoes a security investigation as a condition of employment. The Systems Managers will perform the daily operations and maintenance tasks required to maintain the USAVON equipment and software within their specific district. Access rights will be delegated to the Systems Managers as needed to allow them to perform their duties.

In Tier Two, operations and maintenance will be provided by the TechOne hotline, which is part of the USAO. The TechOne hotline is staffed by contractors, and they provide operations and maintenance support to the Systems Managers throughout the districts. Specific roles and responsibilities will be assigned to the TechOne engineers, and administrative rights will be delegated as appropriate.

The USAO Network Operations Center (NOC) will manage the USAO infrastructure equipment that will be located at the NOC (Columbia, SC) and at the CEF-DC at Sterling, VA The NOC will manage Active Directory (AD), Exchange, Networking equipment, Anti-Virus signature/engine updates, centralized Enterprise Management, remote access, electronic faxing (RightFax) and other designated centralized services.

When a Systems Manager in a district is unable to perform the daily operations and maintenance, an engineer will be contacted at the TechOne hotline to provide assistance. That assistance will be provided verbally via telephone, via the remote management tools, or by a visit to the site itself.

* 1. Administrative Design

The USAO utilizes a District-based administration model. Resources belonging to the District are managed by the District Systems Manager. This management model will continue for Exchange 2019 resources (inasmuch as they interact with the Exchange Online system). Rights will be delegated to District SMs to manage the remaining on premises Distribution Groups for their District. District SMs will be able to create and delete mailboxes in the Exchange Online system, because those rights integrate with Active Directory. District SMs will also be able to *manage* Exchange Online objects (mailboxes, mailbox delegation, mailbox folder permissions, distribution groups that are native to Exchange Online) because those rights are delegated to them by the Exchange Online administrators.

* 1. Remote Management Tools

The remote management tools available to the Systems Managers and TechOne are:

* Active Directory Users and Computers (ADUC)
* Exchange Management Shell (based on Windows PowerShell)
* Exchange Administration Center (EAC)
* Exchange Online Administrative Center (EAC)
* Exchange Online PowerShell Module

There is no Management Console in Exchange 2019.

Refer to the *O365 Systems Managers Operations Guide* for details on the procedures available to the Systems Managers and TechOne.

The tasks specifically for the NOC include:

|  |  |  |
| --- | --- | --- |
| **Task** | **Tool** | **Comments** |
| Create Distribution Group | Exchange Online EAC or PowerShell |  |
| Assign Distribution Group Owner | Exchange Online EAC or PowerShell |  |
|  |  |  |

The tasks for the Districts include:

|  |  |  |
| --- | --- | --- |
| **Task** | **Tool** | **Comments** |
| Create User | USAID.GOV |  |
| Create Mailbox | USAID.GOV |  |
| Verify Mailbox Size (single user) | Exchange Online EAC |  |
| Verify Mailbox Size (all District users) | Exchange Online PowerShell Module |  |
| Manage Distribution Group (on Premises) | On Premises EAC |  |
| Manage Distribution Group (Online) | Exchange Online EAC |  |

* 1. Management Scopes

Management Scopes are the mechanism by which appropriate rights are granted to the Districts. Those scopes, in EOUSA, are the Districts’ Organizational Units.

1. USAMAIL EXCHANGE 2019 RACK DIAGRAM
   1. EXCHANGE 2019 – CEF-DC Layout

Updates to this diagram must be reported to EOUSA’s Points of Contact at the CEF-DC.

* 1. EXCHANGE 2019 -- NOC Layout

* 1. EXCHANGE 2019 – GI Lab Layout