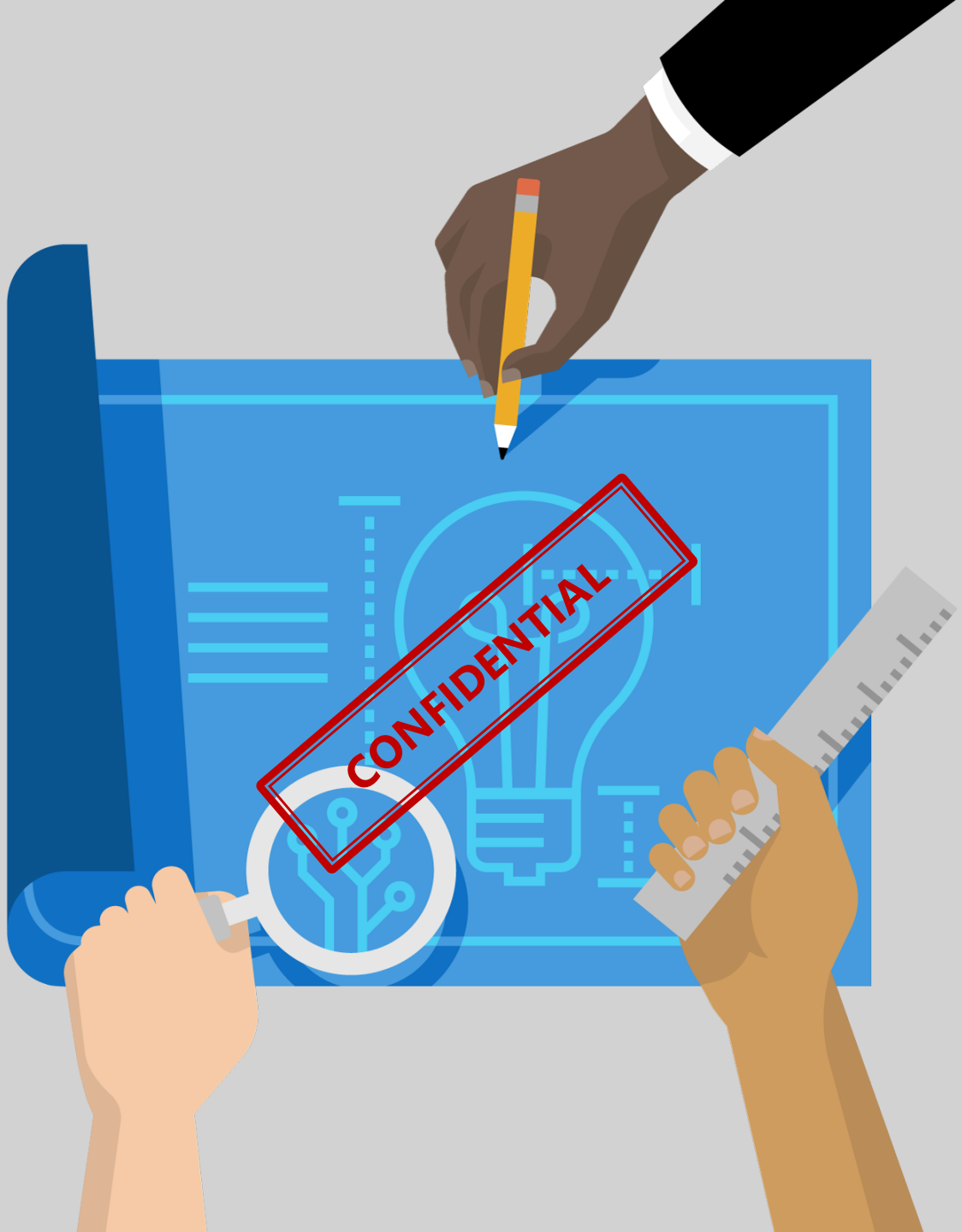
Microsoft

AT&T Modernization Application Assessment

ARMS (6450)

ADS Session

Application Assessment Team
Microsoft Services
Microsoft Corp.



ARMS - Current State

What was the objective?

- Assess application's current state
- Determine if application is a viable Azure cloud candidate
- Identify key elements for application modernization
- Propose a cloud architecture based on Azure PaaS/IaaS services

What is it?

- Accounts Receivable Management System – Collections (ARMS) for legacy B, S, and T wholesale and business retail customers
- Application provides the financial picture aged out to 120 days and backs off the open dispute amounts from the total receivable
- Supports SOX biller validation and AR results reporting
- Application is owned and used by Finance and Collections
- Has more than 55 Billing and Payment feeds

What are the technologies?

- Java 1.8, JSP, HTML, JavaScript, Apache Tomcat 8.5
- Microsoft® Visual C++ 2012 RTM Runtime Library, ActiveX
- Windows batch scripts
- IBM® Connect:Direct 4.7 for Windows
- Microsoft® SQL Server 2008 R2
    - SQL Server Integration Services (SSIS)
    - Data Transformation Services (DTS)
- Microsoft® Windows Server 2008 R2

Architecture

- Web Presentation Pattern:
    - Server-side script
- Layered Architecture
- Database Model:
    - Relational

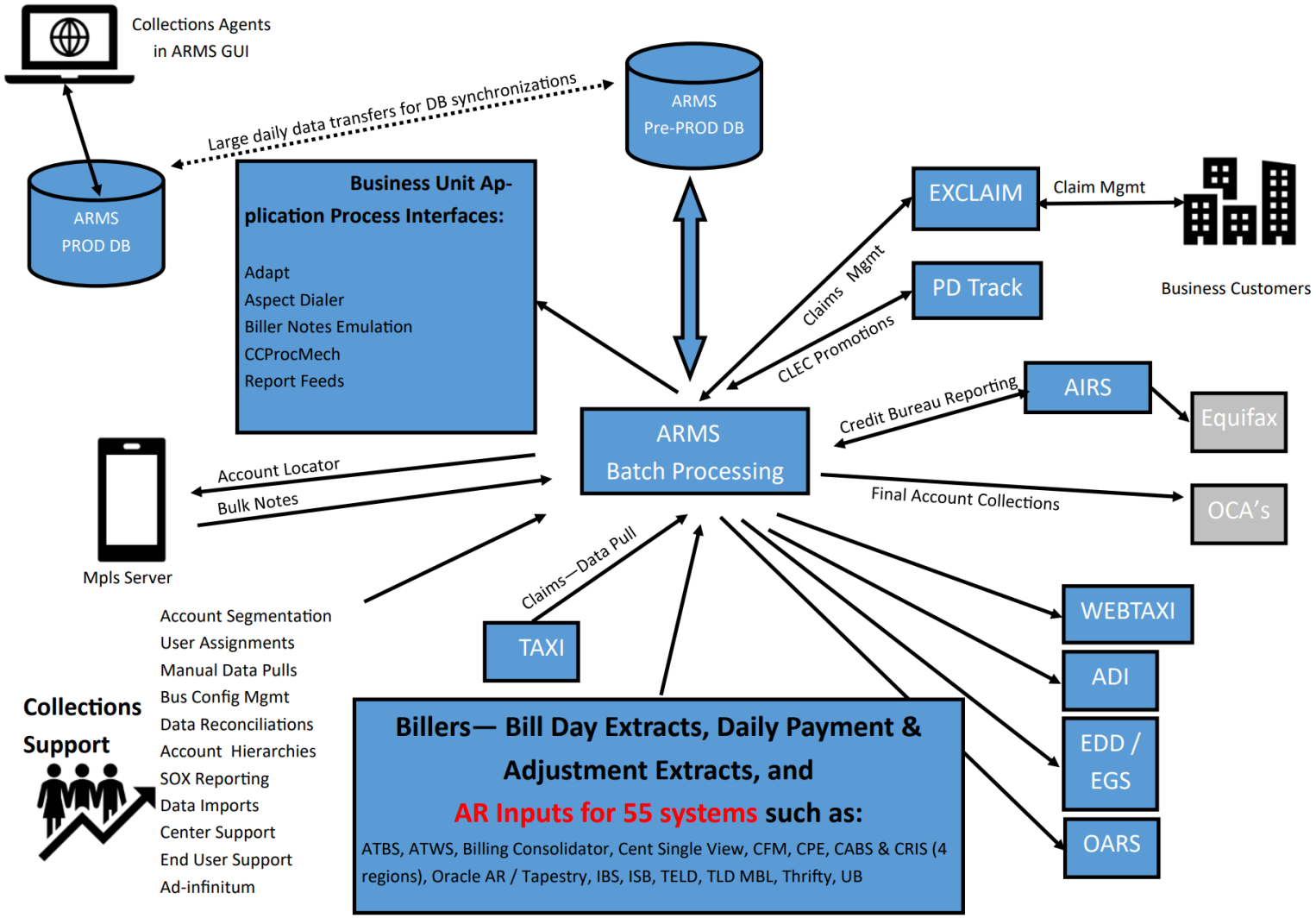
Deployment

- Deployment Pattern:
    - Two-tier deployment
- Performance and Reliability Pattern:
    - None

SLAs & NFRs

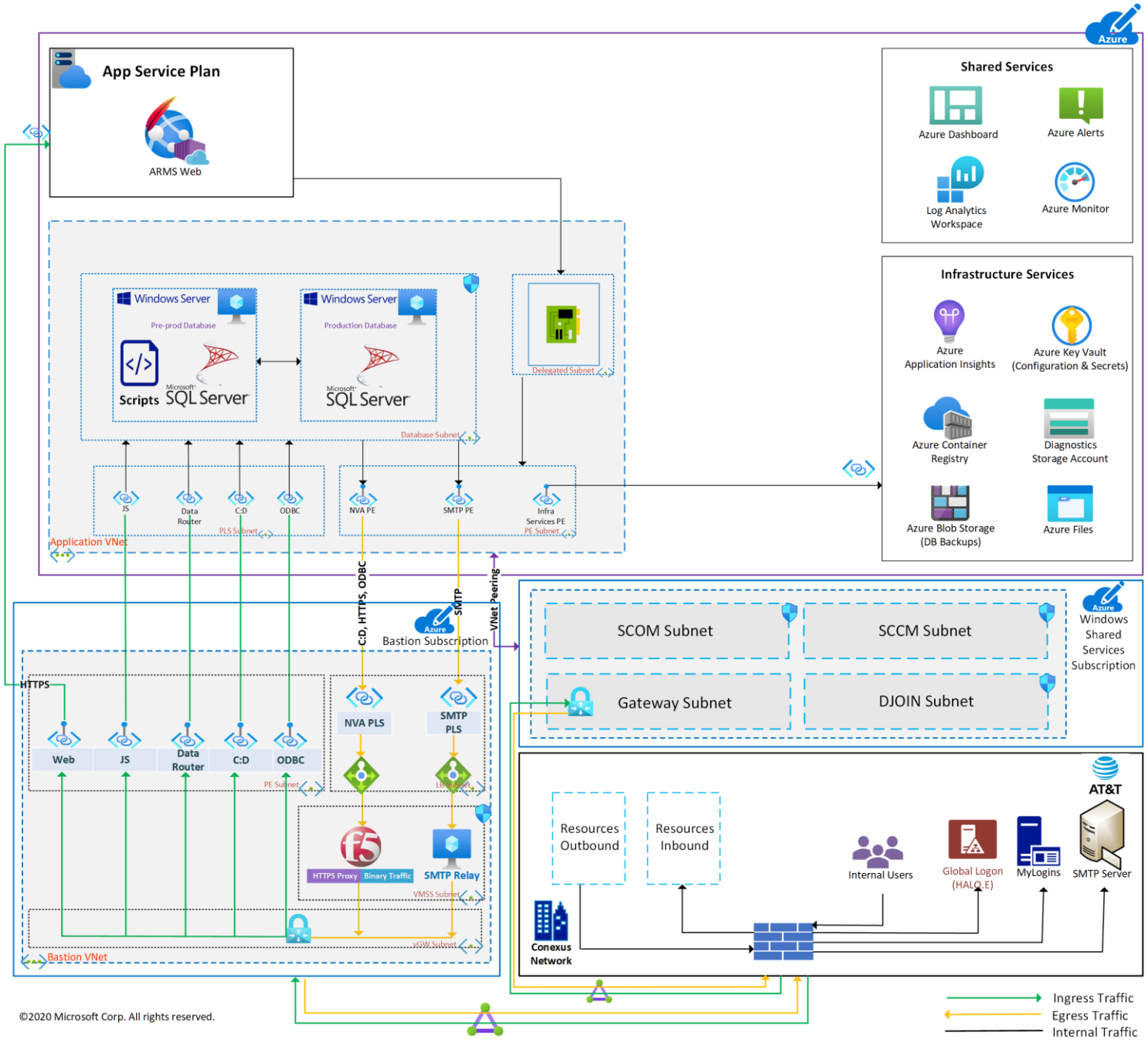
- Mission critical application
- No defined performance & scale SLAs
- MOTS DR & HA Objectives:
    - DR RTO <= 14 days
    - DR RPO <= 72 hours
    - DR Recovery Type: 2B
    - HA Profile: Silver
- ~850 total users
- ~275 concurrent users

Current State – Architecture



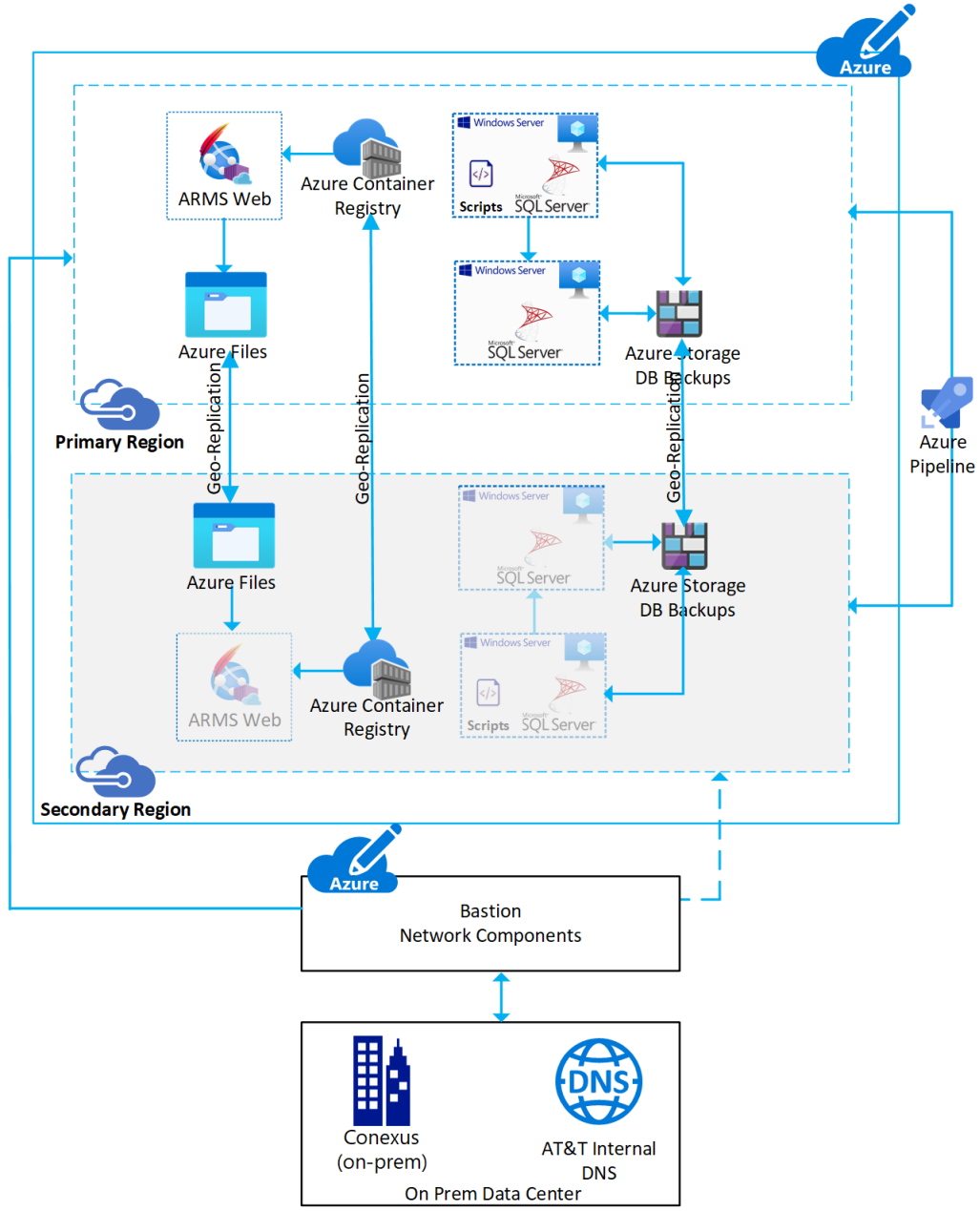
Modernization Approach

Cloud Architecture



Disaster Recovery

- Azure Active/Passive region configuration proposed to meet “2B” DR objective
- Primary Azure region resources will be provisioned upfront
- Secondary Azure region resources will be provisioned using Azure pipelines as needed
- Geo-Replication will be leveraged for Azure Files (data feeds), Azure Storage (DB backup) and Azure Container Registry (Docker images)
- Manual switch over to Secondary environment



Presentation

- Refactor JSP code to plain HTML with JavaScript
- Leverage Apache HTTP Server 2.4.46
- Deploy application to Azure Web App for Containers (RHEL 7.7)

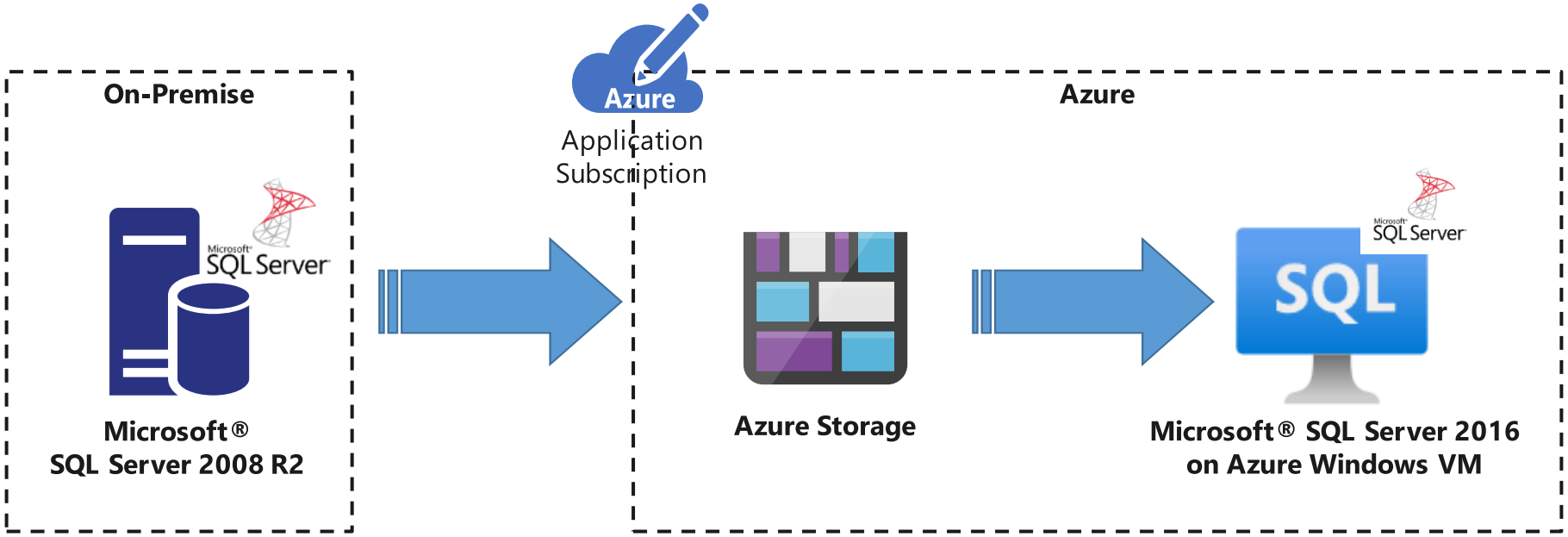
Batch Processing

- Deploy batch scripts to Azure Windows VMs (Microsoft® Windows Server 2016)
- Migrate Data Transformation Services (DTS) packages to SQL Server Integration Services (SSIS) 2016 on Azure Windows VM (Microsoft® Windows Server 2016)
- Port SQL Server Integration Services (SSIS) packages to SQL Server Integration Services (SSIS) 2016 on Azure Windows VM (Microsoft® Windows Server 2016)
- Port SQL Server Agent jobs to SQL Server 2016 on Azure Windows VM (Microsoft® Windows Server 2016)
- Leverage Azure Files

Data Tier

Requirement	Comments
Data Encryption at Rest and in Transit	Data encryption will be configured as per ASPR (AT&T Security Policy and Requirements). **In-Transit**: Microsoft® SQL Server database secures customer data by encrypting data in motion with Transport Layer Security. Microsoft® SQL Server database always enforces encryption (SSL/TLS) for all connections. **At-Rest**: Transparent Data Encryption (TDE) with customer-managed key helps protect Microsoft® SQL Server database against the threat of malicious offline activity by encrypting data at rest. TDE encrypts the entire database using an AES encryption algorithm, which doesn't require application developers to make any changes to existing applications.
High Availability	Application has Silver HA Profile. Microsoft® SQL Server database in Azure Windows VM has built-in availability SLA of 99.9%. Database backups stored in geo-replicated Azure Blob storage will be restored in case of a local outage.
Disaster Recovery	Application has 2B DR Recovery Type. Database backups stored in geo-replicated Azure Blob storage will be restored in case of a disaster.
Backup and Retention	Microsoft® SQL Agent Jobs will be utilized to backup databases and these files will be stored on Azure storage.
Database Maintenance	Microsoft® SQL Server and the Microsoft® Windows operating system provide utilities that let you view the current condition of the database and to track performance as conditions change.
Data Migration	Native backups (.bak files) from on-premises network share will be moved to Azure storage. These backup files will be restored on the Azure VM Microsoft® SQL Server database. SQL Server Integration Services (SSIS) packages will be migrated using SSDT/ Visual Studio

Database Migration Workflow (One-Time)

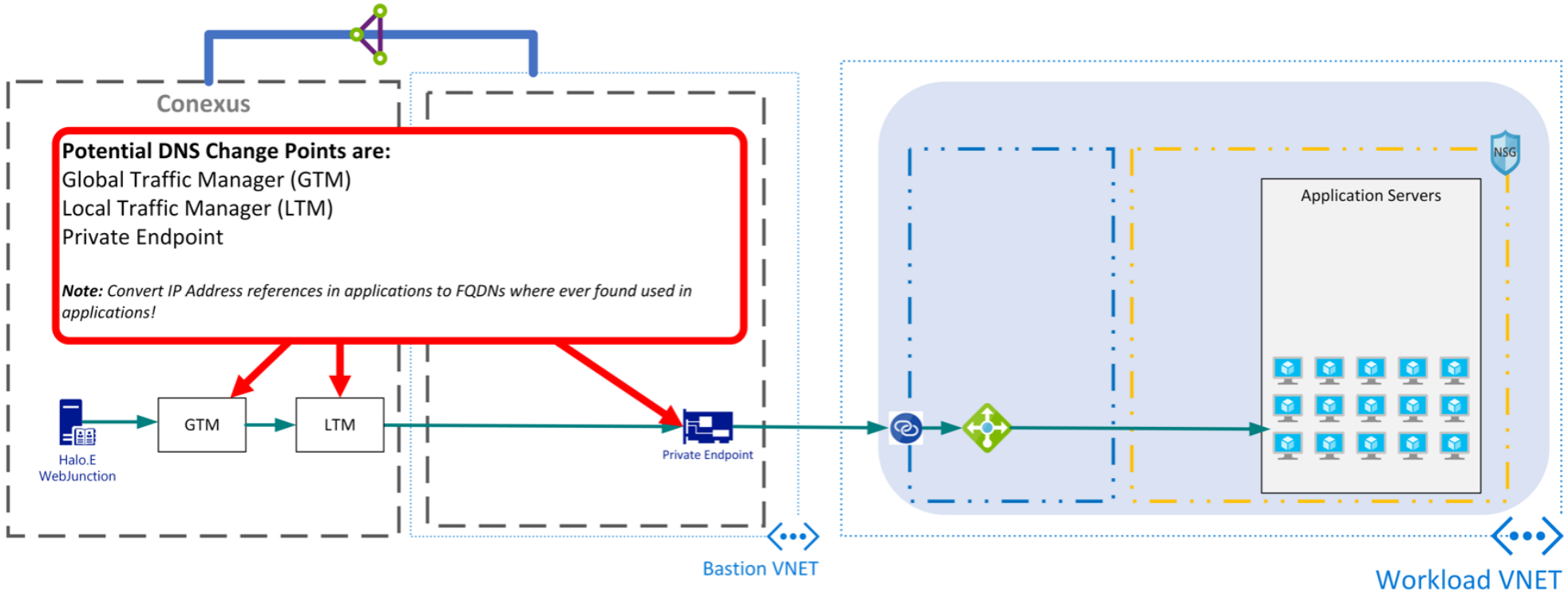


1. Full backups are provided in network share
2. Backup files will be uploaded to Azure storage
3. Full backups will be restored to Microsoft® SQL Server on Azure Windows VM

Cross-cutting Concerns

Identity

- Global Logon Authentication (HALO)



Authentication

- Implements Global Logon

Authorization

- Application uses MyLogins for User Access Control (UAC)

Encryption

- ASPR-compliant encryption of data at rest and data in transit
- All web traffic over HTTPS TLS 1.2
- Azure Files communication is encrypted by default using SMB 3.0

Communications

- Azure resources will be deployed within an Azure Virtual Network to enable secure communication with each other and on-premises networks
- Subnets will be used to segment the VNet address space into segments that are appropriate for the application
- Secure resources within subnets using Network Security Groups
- Filter network traffic between subnets using Network Security Groups
- All Azure PaaS services will leverage Azure Private Link
- Leverage Azure Bastion subscription to control and secure communications between Azure and AT&T data centers

Integrations

Dependencies (1 of 5)

Source App	Target App	Upstream	Downstream	Protocol
ARMS (6450)	ACIS (3940)	X		Connect:Direct
	AIM (2397)	X		Connect:Direct
	AIRS (3809)	X		Connect:Direct
	AspectAOD (20943)	X	X	Connect:Direct
	ATBS (13806)	X		Connect:Direct
	ATWS (21685)	X		Connect:Direct
	BEST (17599)	X		Connect:Direct
	Billing Consolidator (14972)	X		Connect:Direct
	CABS-AIT (3935)	X		Connect:Direct
	CABS-N (23308)	X		Connect:Direct

Dependencies (2 of 5)

Source App	Target App	Upstream	Downstream	Protocol
ARMS (6450)	CABS-PB (1178)	X		Connect:Direct
	CABS-SE (20977)	X		Connect:Direct
	CABS-SW (1174)	X		Connect:Direct
	CASH (15860)	X		Connect:Direct
	CENET (2022)	X		Connect:Direct
	CENT (20616)	X		Connect:Direct
	CIA ABS (13585)	X		
	CPE Billing (5337)	X	X	
	CRIS (7882)	X		Connect:Direct
	CRIS CASH (1551)	X		Connect:Direct

Dependencies (3 of 5)

Source App	Target App	Upstream	Downstream	Protocol
ARMS (6450)	DCS (13804)	X		Connect:Direct
	ECS (14883)	X	X	Connect:Direct
	EDD (17689)	X	X	Data Router
	EXECUBILL (17020)	X		
	GISDN (18756)	X		
	ISB (14084)	X		Connect:Direct
	JDE (12627)	X		
	Oracle ART (16350)	X		Connect:Direct
	PD Track (19255)	X		Connect:Direct
	RBS (3958)	X		

Dependencies (4 of 5)

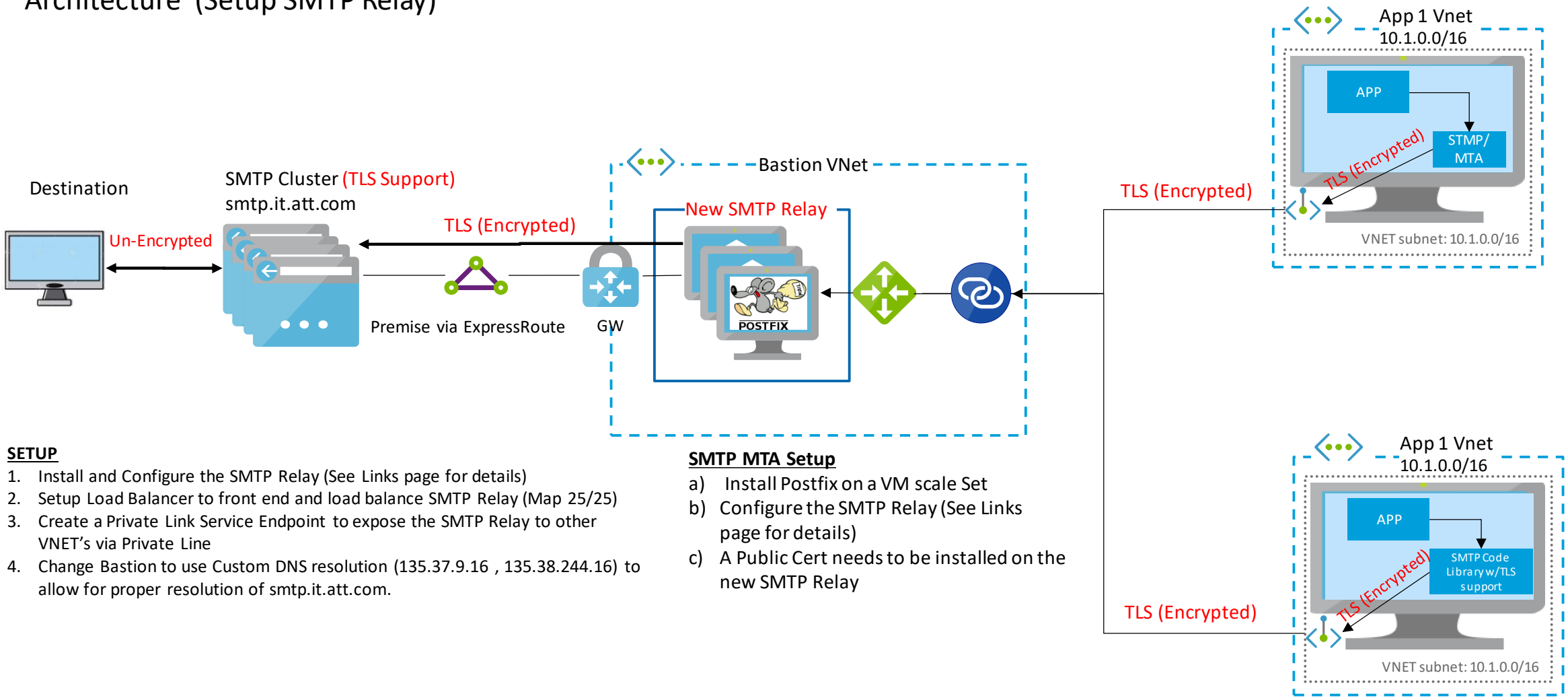
Source App	Target App	Upstream	Downstream	Protocol
ARMS (6450)	RPMS (13490)	X		
	SDN-ONENET (13715)	X		
	TAXI (578)	X	X	Database Connection ODB
	THRIFTY - AS400 (13261)	X		Connect:Direct
	TLD-PROD (7547)	X		Database Connection ODBC
	UNIVERSAL BILLER RESULTS (14191)	X		Connect:Direct
	VTNS (13440)	X		
	WEBTAXI (8685)	X	X	Database Connection ODBC
	ADAPT (21656)		X	Connect:Direct
	AIRS (3809)		X	Connect:Direct

Dependencies (5 of 5)

Source App	Target App	Upstream	Downstream	Protocol
ARMS (6450)	ASLA (28558)		X	Data Router
	ATT MACS (8182)		X	
	CCAX (19704)		X	
	CCProcMech (21030)		X	Connect:Direct
	ExClaim (10427)		X	Database Connection ODBC
	LRS (8937)		X	
	WEBPHONE (13924)	X		Tabular Data Stream (TDS)
	MPLTOOLS (24511)	X		Tabular Data Stream (TDS)
	OARS (14273)		X	Connect:Direct

Integration (SMTP)

Architecture (Setup SMTP Relay)



SETUP

1. Install and Configure the SMTP Relay (See Links page for details)
2. Setup Load Balancer to front end and load balance SMTP Relay (Map 25/25)
3. Create a Private Link Service Endpoint to expose the SMTP Relay to other VNET's via Private Line
4. Change Bastion to use Custom DNS resolution (135.37.9.16 , 135.38.244.16) to allow for proper resolution of smtp.it.att.com.

SMTP MTA Setup

a) Install Postfix on a VM scale Set
b) Configure the SMTP Relay (See Links page for details)
c) A Public Cert needs to be installed on the new SMTP Relay

Integration (Connect:Direct & Data Router)

- IBM® Connect:Direct Secure Plus for Windows 4.7 to be installed on Azure SQL Server VM
  - NVA rule will be defined for connectivity to on-premises systems using Connect:Direct
- AT&T Data Router Publisher will be leveraged for publishing the files to Data Router

DevOps

Operations & Monitoring

- Application Insights will be used to monitor the availability, performance, and usage of web applications
- Azure Monitor for Containers will be used to monitor containers
- Azure Monitor for VMs will be used to monitor VM processes, dependencies, setting alert rules and sending notifications.
- Leverage System Center Operations Manager (SCOM) on Windows Shared Services Subscription for monitoring Microsoft® SQL Server

Performance, Scalability & Load

- Application implements the following performance and scalability patterns:
  - Not Available
- Performance
  - Not Available
- Load
  - Maximum Number of Users: ~850
  - Concurrent Users: ~275
  - Database Size: ~1 TB

Note: AT&T Application Team will need to perform a performance / load test baseline prior to modernization

Application Lifecycle

- Azure DevOps GIT repository will be the source control

Deployment

- Implement Infrastructure as Code (IaC) using:
  - Terraform automation tool to easily manage infrastructure as code
  - Automate builds and deployments using Azure CI/CD pipelines to Azure
- Deployment will target two (2) Azure subscriptions:
  - Pre-prod: Dev, Test, and Pre-Prod environments
  - Production: Production environment

Assumptions & Risks

Assumptions

- The Architecture depicted is based on the available and approved AT&T Azure patterns at the time of the Modernization Assessment. Newer Azure services and patterns may have been introduced since the Modernization Assessment was complete. Please refer to the latest approved Azure patterns before implementation
- Versions of all proposed technologies are based on recommended technologies in BOM version 4.2
- IBM® Connect:Direct® Secure Plus for Microsoft Windows 4.7 supports encrypted transport using TLS 1.2 and AES-256 encryption
  https://www.ibm.com/support/knowledgecenter/SS4PJT_6.0.0/cd_unix/cdunix_secplus/CDU_TLS_and_SSL.html
- No functional enhancements are being considered
- Build-ready source code will be provided by AT&T for application modernization
- AT&T App Owners will coordinate on-premises application/database encryption configuration change. No effort will be included as part of the Azure modernization estimate
- Bastion vNet will be configured with SMTP relay using AT&T architectural patterns
- Application team will provide test cases and will execute user acceptance tests
- No performance SLAs defined
- Performance Testing is timeboxed to 80 hours planning, and 160 hours execution (1 resource). Performance Test is limited to 1 round of testing and includes up to 2 scenarios

Assumptions (continued)

- Application team will cleanup retired and redundant code in ARMS web application before modernization
- Desktop application has not been assessed. We recommend that the desktop application be rewritten as a web-based application using Angular 9 and Spring Boot REST APIs
- AT&T will update configurations for any on-premises components or external applications pointing to Azure services
- Required Azure subscriptions and software licenses will be provided by AT&T
- One (1) data migration will be performed into the Pre-prod environment
- Deployment to production environment will be performed by AT&T and/or its delegates
- Additional effort will be required for modernization for any components/dependencies that have not been identified during the assessment
- Test environments used for assessment are representative of production environments
- Per the MOTS database, the proposed solution will decommission the following on-premises servers/VMs:
  - Web-application – 1 VM, 1 Server
  - Database – 3 Servers

Risks

- External applications may not support encrypted communication

Summary

Technology Mapping (1 of 3)

Components	Current Technology	Mapped Technology	Implementation Details
ARMS Web Application	Microsoft® Windows Server 2008 R2, Apache Tomcat 8.5, JSP, Java 8.0.1, HTML, JavaScript	Azure Web App for Containers (RHEL 7.7) with Apache HTTP Server 2.4.46, HTML, JavaScript	- Leverage Apache HTTP Server 2.4.46 - Clean-up the JSPs to plain HTMLs
Batch Processing (SSIS)	Microsoft® SQL Server Integration Services 2008 R2 (SSIS) Packages	Microsoft® SQL Server Integration Services (SSIS) hosted on Azure Windows VM (Microsoft® Windows Server 2016)	- Update batch scripts from Windows Server 2008 R2 version to Windows 2016 version - Upgrade SSIS Packages from Package Deployment Model to Project Deployment Model - Migrate existing SQL Server Integration Services packages to Azure Windows VM (Microsoft® Windows Server 2016)
Batch Processing (DTS)	Microsoft® Data Transformation Services (DTS) Packages	Microsoft® SQL Server Integration Services (SSIS) hosted on Azure Windows VM (Microsoft® Windows Server 2016)	- Update batch scripts from Windows Server 2008 R2 version to Windows 2016 version - Migrate DTS packages to SSIS on Azure Windows VM (Microsoft® Windows Server 2016)

Technology Mapping (2 of 3)

Components	Current Technology	Mapped Technology	Implementation Details
ARMS Database • Production (collection, collection_history) • Pre-production (collection, collection_backup, collection_investigation, collection_archive)	Microsoft® SQL Server 2008 R2 on Microsoft® Windows Server 2008 R2	Azure Windows VMs (Microsoft® Windows Server 2016), Microsoft® SQL Server 2016	- Backup and restore on-premises SQL Databases to Microsoft® SQL Server 2016 hosted on Azure Windows VM (Microsoft Windows Server 2016) - Make required changes to support application
Connect:Direct	IBM® Connect:Direct 4.7 for Windows	IBM® Connect:Direct 4.7 for Windows	- Deploy IBM® Connect:Direct 4.7 for Windows
AT&T Data Router	AT&T Data Router on Windows Server 2008 R2	AT&T Data Router on Windows VM (Microsoft® Windows Server 2016)	- Deploy AT&T Data Router for Windows
Application Secrets and Configuration Files	Local configuration files and code files	Azure Key Vault	- Refactor configuration read in code to work with Azure environment & Azure Key Vault - Code to read application secrets will be refactored to work with Azure Environment & Azure Key Vault
Application Logging	Local file system	Application Insights & Alerts	- Provision and configure Application Insights so that application logs can be logged in one place but still can be queried independently - Configure Azure Monitor and Azure Alerts for common operational alerts

Technology Mapping (3 of 3)

Components	Current Technology	Mapped Technology	Implementation Details
Local File System	Windows File System	Azure Files	- Configure Azure Files storage - Update existing batch code to interact with Azure Files - Enable Geo-Redundant Storage
Develop Deployment Plan and Pipeline	Manual	Azure DevOps	- Using Terraform scripts (Infrastructure as Code) to automate provisioning of new environments - Create CI/CD pipeline on Azure for Dev, Test and pre-production environments - Develop Deployment Plan and/or artifacts to support automated cloud deployment

Thank you!