U.S. Air Force Active Directory and Exchange Migration

A White Paper

Brian Gibson

John Fair

www.tkcglobal.com

Managing one of the largest Department of Defense Active Directory and Exchange migrations ever.

In 2008, there were over 250 separate Air Force domains supporting 840,000 users and 1.9 million computing objects at 12 Major Commands (MAJCOM) worldwide. This configuration of many network "Islands" lead to standardization problems, skyrocketing operation,

maintenance and security costs and a lack of enterprise-wide cyber situational awareness—a key component of national defense. Airmen were required to submit new paperwork to request and create new accounts when traveling for military conferences, business meetings and schools, temporary duty assignments, or change of duty assignments. When changing duty assignments they also no longer had access to their old mail messages unless they backed up the messages prior to leaving the old location. A unified, Air Force-wide approach to vulnerability management was not possible and this contributed to an approximate $40 million annual bill to clean up cyber attacks. And information sharing between the Air Force, other military branches and intelligence agencies facing similar cyber issues and threats was complex and inefficient. Needed was a single, centrally managed network with enforceable policies and standards that would enable efficiencies in scale, security, cost and use. That network is the Air Force Network, or *AFNet*.

Involved at every stage of the migration

The goal of AFNet is to collapse all individual or standalone Air Force, Air Force Reserve and Air National Guard networks into a single global network under operational and management control of a single commander (Figure 1). This commander currently falls under the responsibility of the 24th Air Force Lackland Air Force Base, Texas, and will include support by two Network Operation and Security Centers (NOSC) located at Peterson Air Force Base (AFB), Colorado and the other at Langley AFB, Virginia. As part of the migration into the AFNet, mailboxes within the Continental United States (CONUS) sites are migrated into one of three area processing centers at Scott AFB, Illinois; Wright-Patterson AFB, Ohio or Joint Base Andrews, MD just outside of Washington, DC.

TKC Global is the prime contractor for all technical aspects within AFNet Microsoft Active Directory and Exchange (ADX) and other core service migration efforts. It also oversees the coordination between all migration team members. TKC Global utilizes a team of 78 system engineers on this initiative and is involved in every aspect of the migration, including:

- Initial design of the Air Force Active Directory forest (the highest level of organization in Active Directory).

- Advanced system engineering support of the Non Secure Internet Protocol Routing Network (NIPRNET) and Secret Internet Protocol Routing Network (SIPRNET) ADX environments.
- Support for user, group, e-mail, computer and file migrations from Base/MAJCOM ADX environments to the AFNet environment.
- Design, test and implement virtualization technologies.
- Migration of Air Force custom applications and Command and Control systems.
- Creating customized programs to modify data enabling commercial off the shelf applications to work effectively in Air Force environment (e.g. the User Mapping Tool).
- Server equipment hardware and software installation services.
- Network optimization and troubleshooting support for base level and enterprise data center network equipment and clients.
- Shutting down legacy environments.

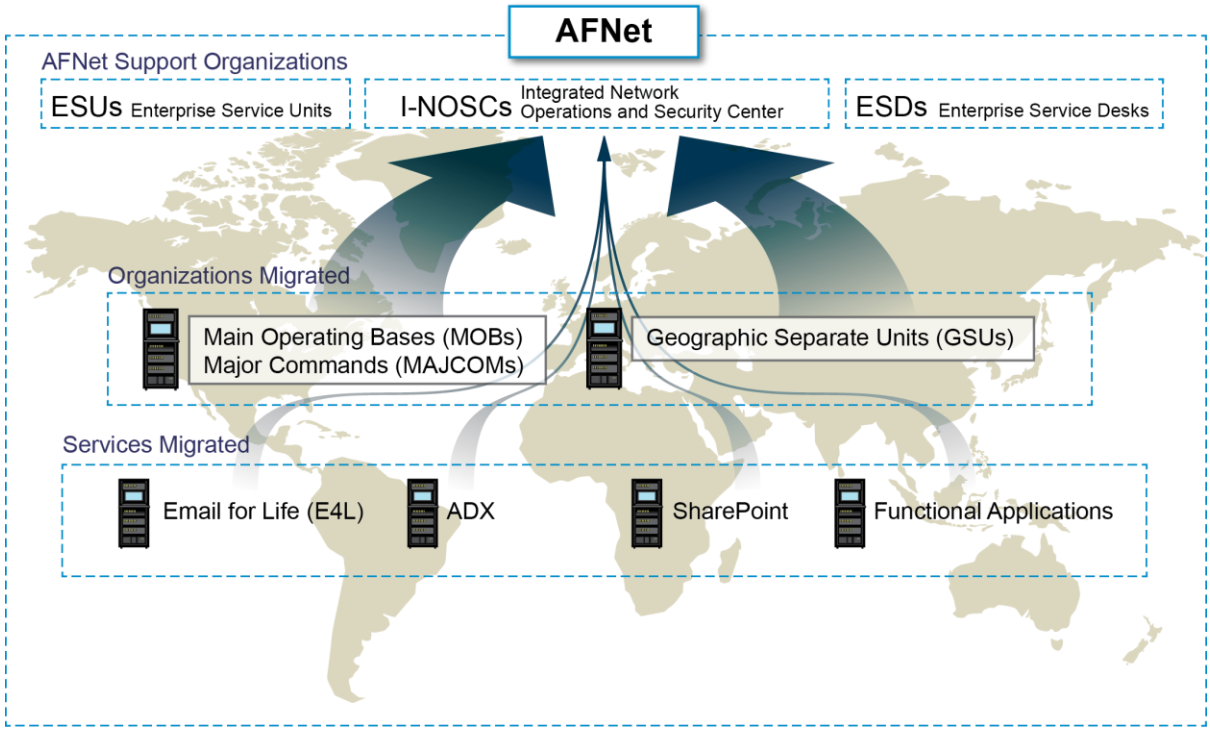

Figure 1: To collapse all individual Air Force networks into a single global network, AFNet migrates end user services from 250+ locations to central management support organizations under the control of a single commander.

A five step process

The Air Force ADX migration effort is carried out via a meticulously defined 250+ step process executed in five phases: *Assessment and infrastructure/Server build out, Pre-Migration, User Migration, Post Migration Clean-Up and Functional System Migration/Legacy System Shut Down (See Figure 2 at end of paper).*

Phase 1: Assessment and Infrastructure/Server Build Out

Phase 1 begins with a brief to base commanders on what's coming. Two-way trust must first be established between all participating domains to ensure that resource access and other components of the migration are handled properly. Working with Air Force personnel, the TKC Global team creates a master server list to determine what hardware/software is reusable and what components must be ordered. Schedules must be sufficiently flexible to accommodate order lead times. Site surveys are verified against infrastructure and power requirements and HVAC and floor space is made ready. Bandwidth and network boundary issues are resolved as are firewall port openings to the other bases we're connecting with. The infrastructure/server build team installs, configures and makes fully operational the hardware, including storage, network switches, SAN switches and servers. Virtualization solutions are designed, tested and deployed. Standard port security, firewalls and routing infrastructures are put in place. And migration pilot system lists are drawn up. EMC, Dell, NetApp, HP, Cisco, VMware and Hyper-V are technologies used in this phase among others.

Phase 2: Pre-Migration

This is basically a health check of the legacy environment to discover issues that could adversely affect its migration to a consolidated environment. Every mailbox is checked for a user account and "never logged on" and "inactive logged on" user accounts and computer objects are disabled. Antiquated log-on scripts are also deleted. All mailboxes are brought into the size limits of AFNet—VIPs 1GB, essential support personnel 500MB and all others 100MB. Group Policy Objects and Organizational and Security Units are reconciled and validated for proper placement and with appropriate naming standards in the new Active Directory forest. New log-on scripts are assigned and email distribution lists are scrubbed. At this point, new and upgraded servers are in place, configured and fully operational. TKC Global technicians provide training to the Computer Support Technician (CST) team on new post-migration processes and Standard Operating Procedures, especially with regard to the new Enterprise Service Desk (ESD) operations.

Properly documented certification and accreditation have been achieved and the support organization is prepared to take responsibility. Finally, selected pilot systems—two people from a fighter squadron or maintenance unit, for example—are first migrated to AFNet along with their functional systems. These users will test and use their systems for "normal" operations. This means their systems must perform exactly as they did before migration (e.g. in ordering bullets, jet fuel or spare parts) before the group's remaining members are migrated. Pilot users provide extensive feedback to the project team to assure the system meets all operational requirements. TKC Global works diligently with the Functional and Command and Control system owners to address any impact prior to migration to ensure that all critical services remain fully operational before, during and after migration. We do everything in our power to maintain this functionality while at the same time upholding the security posture of the network. All pre-migration technical and administrative checklists will be completed and validated by the ADX migration team. Checklists will be complete for all migrating environments.

Trouble ticket resolution
With AFNet, helpdesks are transitioned from independently operated and managed entities at the base or MAJCAM level to a single virtualized Air Force information technology Enterprise Service Desk (ESD) geographically dispersed across four world-wide locations operating within one logical AIR Force network domain. These locations are Lackland AFB, Texas; Gunter AFB, Alabama; Ramstein Air Base, Germany and Hickam AFB, Hawaii. The ESD will field all unclassified network issues and outages for Air Force personnel and provide assistance 24/7/365. The ESD uses an Automated Call Distribution (ACD) system to allow intelligent routing of calls based on agent skills, location and/or availability. Most important, airmen now have just one number to call for help.

Phase 3: User Migration

User Migration is when the actual physical migration to the AFNet takes place for User Groups, Security Groups, Organizational Groups, email accounts, Group Policy Objects, workstations, Blackberry's and other mobile devises, public folders and Distribution Lists. This activity generally takes one to two months on average per facility, depending on its size and complexity.

At the onset of the project, we were migrating one base at a time. We soon learned that by splitting our team into specialized units (Assessment and Infrastructure/Server Build Out, Pre-Migration, User Migration, etc.), and assigning them the migration phases that are ready to be undertaken at any given base, we could begin migrating bases in parallel, thus accelerating program progress. We also established ways to identify potential issues prior to migration starting. This enabled us to migrate more quickly by eliminating issues that slowed down our synch and switch process.

Improving processes along the way
In addition to increasing the number of parallel migrations, we implemented an enhanced process of migrating the users' mailboxes called Remote User Collection (RUC). Before RUC, the Air Force migrated email accounts overnight or on weekends in blocks of 1,200 to 1,500 users. This involved a challenging process of continually synchronizing email in the legacy network with email in the AFNet for many weeks at a time. RUC enables us to migrate up to 5,000 users at a time by performing a simple "copy and switch" procedure. It also improves the success rates of these procedures from 85% to 97%.

VIP Migration
VIP classification differs between command types but generally includes General Officers, Senior Executive Service personnel, Group Command and Control personnel, Senior Staff Directors, Vice Commanders and Commanders. These are "hands on" migrations by the Computer Support Technicians and are made by appointment. It can be arranged for VIPs immediate support staff (secretaries, executives, etc.) to be migrated at the same time.

Career long email addresses

The most visible change AFNet brings to computer users across the Air Force is the change to a single email address (firstname.lastname@us.af.mil). This enables central management of these accounts. Regardless of the base or organization assigned—or if they're on TDY, deployed or Permanent Change of Station (PCS)—with their Common Access Card (CAC), users can sign on to any computer in AFNet to access their home station email, shared drives, etc. And this new address remains with users for the duration of their career, employment or affiliation with the Air Force. Account activation and de-activation is also eliminated greatly enhancing productivity.

Phase 4: Post-Migration Cleanup

Phase 4 is when the team traces out all inactive, disabled or expired user accounts, mailboxes and workstations that—for whatever reason—were not migrated in the previous phase. The user may have been on TDY, vacation, a business trip or deployed during migration. Also, accounts that may have gone obsolete for a long time may have expired without either the user or administrator knowing. There are many reasons they may have been left behind. Generally, about 100 of these instances occur per base. In Post-Migration Cleanup, the CST team goes into each area of Active Directory and Exchange and troubleshoots these objects and either deletes disables or migrates them into AFNet. A member of the TKC Global Post-Migration Cleanup Team will remain at the base until:

- All user accounts, machine accounts and email accounts are either deleted, disabled or migrated into the AFNet
- All mission systems fully operational at pre-migration are still operational and can be accessed
- Open trouble tickets have been reduced to less that 1%

Phase 5: Functional System Migration/ Legacy System Shutdown

This is the final phase of the migration process. Lasting approximately three months, this is when all legacy functional systems needed to support base operations are given new permissions and migrated into AFNet and the legacy network itself is decommissioned. Included in these functional systems are SharePoint, file and print servers, SQL servers, FTP servers, list servers, system management servers and any other server supporting day-to-day base operations. If a server is deemed unneeded for support base operations, it can be made available to the ADX Project Management Office (PMO) for possible reuse of hardware and server licenses.

The TKC Global team provides one final check for users on the legacy network by unplugging the system's Domain Controllers (DCs) for 72 hours. Anyone using a DC for authentication will be denied access to that server and will notify the CST team. Once these incidents are resolved, the legacy DCs are permanently removed from the site, the domain is decommissioned and any remnant of it removed from all Air Force cyber communities. The network remains online to support the connectivity into the AFNet.

Keys to success

Base-wide communications is key

It is absolutely critical that an ADX migration of this size—with this much at stake—has a communications strategy that ensures all stakeholders are adequately informed. Briefings begin at the MAJCOM level six months prior to their migration and at Wing leadership 30-45 days prior to their migration. Cyber Readiness Reviews (CRR) obtains formal approval to proceed one day prior to migration. A series of emails are sent to the base 45, 30 and 15 days prior to migration start. This is followed by targeted emails to blocks of users 3-days and 1-day prior to their actual migration, followed then by Day After messages informing them of the change. The Air Force Portal, Air Force News Service, base newspaper articles, templates and FAQs provide general AFNet information and migration milestones. Fact sheets are distributed in open forums, conferences and conventions. Migration checklists provide stakeholders standard lists of tasks to prepare for migration. And SharePoint provides a centrally accessible repository of project information, updates, schedules and status.

Adapting COTS tools to unique Air Force environment

TKC Global created a custom build user mapping tool that enables commercial off-the-shelf migration software to work in the unique AFNet environment that includes target user accounts pre-populated for a previous initiative. Off-the-shelf migration tools simply aren't built to work in this type of environment, as they normally take the legacy account and create the target account during the migration process. We needed a way to match the legacy account with the user's appropriate target account. The new user mapping tool gave us this capability. It also has a logic built into it to identify known issues with accounts and help determine the appropriate match for dual users. An example of this is a Civil Service employee who also is a Reservist. This individual would have two accounts. The user mapping tool not only enables us to match the user to the target account, but also identifies this individual as a dual-role user and matches up the individual's account accordingly.

Reengineer as needed to meet the program's scale

It is important to note that many vendors' products have been engineered to scale to the AFNet level and higher. However, many have not been truly tested in a production environment for Active Directory and Exchange. TKC Global approached this issue by first fully understanding the best practices of each vendor's hardware, then closely monitoring the environment as we consolidated the users and mailboxes into it. We re-engineered as needed to adjust to the vast scale of this project. We found that some of the best practices were pushed to the limit and had to be adjusted to accommodate AFNet requirements.

Benefits of AFNet

AFNet consolidates all network operations, control and security under the 24th Air Force and its subordinate cyber units. This consolidation provides tremendous Air Force wide benefits in the areas of security, cost and standardization.

Security

- Provides Air Force-wide leadership a single picture of the Air Force network and cyber battlefield.
- Centralizes responsibility for vulnerability management yields significant improvements in ability to fight daily malicious intrusions through common virus protection, firewalls, permission approvals, patch pushes, etc.
- Standardizes Certification and Accreditation for vulnerability analysis.
- Reduces number of entry points for a dramatically smaller "attack surface."
- Frees network operators to "deny by default," by closing ports that traditionally have either shown mischief or shown no value to Air Force users.
- Enhances communication between Air Force installations provides greater opportunity to pinpoint threats and gauge their seriousness.
- Improves ability to manage user profiles and network access, freeing up vital human resources to focus on other critical network security tasks.

Cost

- Reduces necessary server footprint.
- Reduces personnel and cost needed to maintain multiple architectures.
- Reduces costs associated with HVAC and power.
- Reduces required testing environments.

Standardization

- Provides Air Force personnel with a single, career long e-mail address.
- Provides a common network look and feel.
- Standardizes applications and replaces myriads of legacy ones chosen to meet functional needs.
- Standardizes design simplifies operations and maintenance.
- Simplifies training—technicians no longer need to be trained on a new environment when moving to another base.
- Delivers a more predictable environment for collaboration and application configuration.
- Provides single sign-on from a CAC enabled computer and access anywhere within the AFNet with a single email address for an entire Air Force career.

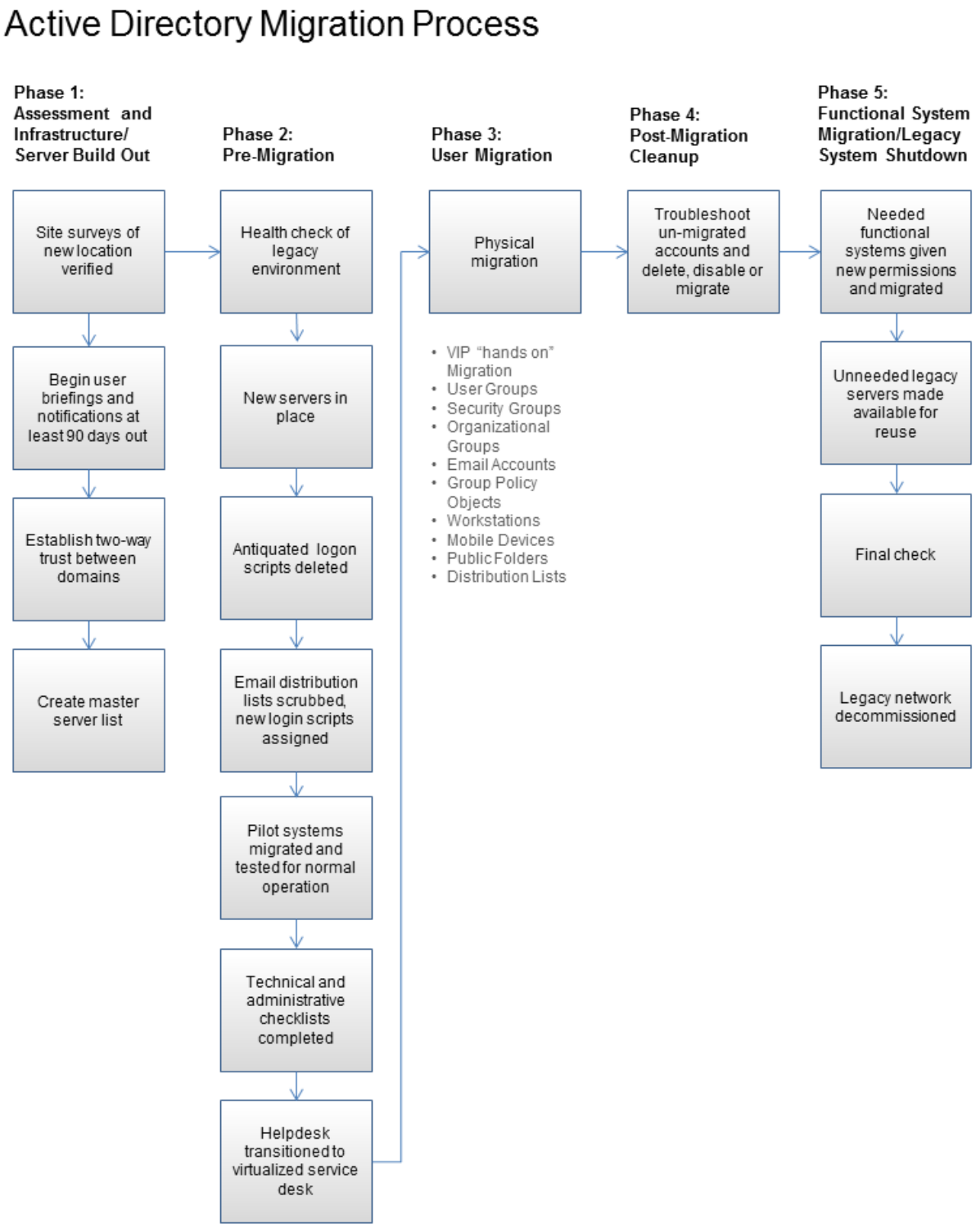

Figure 2: While all base migrations follow the same 5-step process, time to completion varies with size and scope. On average, Assessment, Infrastructure Build Out and Pre Migration requires 120 days, Pre-Migration 2-8 weeks, Post-Migration Cleanup 2 weeks and Functional System Migration/Legacy System Shutdown 1-6 months.

Operational Headquarters
13873 Park Center Road, Suite 400N
Herndon, VA 20171
571.323.5200
info@tkcglobal.com

www.tkcglobal.com