Enterprise Directory Services & Authentication

Information Exchange Forum
Session: #2
EDS&A

Robert Bachert
NETCOM 9th SC(A) G5
Army Enterprise EDS&A Overview

★ Will establish an Enterprise Directory Services and Authentication (EDS&A) Capabilities.
  • Army to implement an enterprise baseline.
  • This effort includes the standardization of the Army’s operating environment.
★ The objective is to make Army’s information technology infrastructure available and secure to authenticated user’s.
  • Provide users more flexibility and mobility
  • Enhance collaboration opportunities across the Army
★ NETCOM/9th SC(A) will acquire required equipment to implement, integrate, and support the EDS&A theater environments.
  • A phased approach will be used to implementation
  • Theater environments managed by 9th SC (A)
EDS&A Integrated Architecture Overview

Accountable Data Sources

- Other Approved User Accounts
- Military Personnel
- Civilian Personnel
- Contractor Personnel
- DEERS
- JPAS

- Operating Forces Domain
- Provision (EDSP) - as necessary

Data Wholesalers

- DMDC
- GDS/411
- NPE/.509

- Operating Forces Domain

Provision Army User Accounts, Certs & Attribute Updates with each Theater Forest

DISA Managed Identity Synchronization Service (IdSS)
- Personas
- Certifications
- Global Access List (GAL)
- Entitlements, etc.

Army Managed Forests

- 5 Theater Forests
  - Theater Forests and Domains
  - Users/Workstations
  - Service Entitlement
  - Functional Forests Migrated
  - Apps consolidation sync with ADCCP effort

- Army Managed Forests

1. CIO/G-6 Publish architecture
2. Requires Issue and enforcement of EDS&A Orders
3. Applications will be migrated under ADCCP consolidation

DMDC Batch Broker Service (BBS)

Federation Services ONLY
- CONUS
- EUR
- PAC
- SWA
- KOREA

Enterprise Directory Services

Provision Army User Accounts, Certs & Attribute Updates with each Theater Forest

Army Enterprise Application Service Forest (AEASF)
- Army Account Attributes
- Army scoped Apps
- Army Governance
- Direct PKE authentication

- Operating Forces Domain

DISA Managed Forests

- Operating Forces Domain

Enterprise Application & Services Forest (EASF)
- DoD Account Attributes
- DoD scoped Apps
- Enterprise Email
- Enterprise SharePoint

User Migration

Application Migration

Operating Forces Domain

Operating Forests (As needed)

Functional Forests

Operating Forces Domain

Extend - as necessary

Provision (EDSP) - as necessary

DMDC Batch Broker Service (BBS)

Federation Services ONLY

5 Theater Forests

- Theater Forests and Domains
- Users/Workstations
- Service Entitlement
- Functional Forests Migrated
- Apps consolidation sync with ADCCP effort

Army Managed Forests
Phase 0 – Pre-Active Directory Implementation Activities (e.g. Publish EXORD, Functional Forest Analysis / Collapse Plan (POA&M))

Phase 1 – Implement Tech Insertion & Global Footprint

Phase 2 – Enterprise Baseline Environment, 5 Theater Forests Upgraded to W2K8 R2

Phase 3 – Rationalize applications in support of ADCCP effort

Phase 4 – User Migration & Collapse Functional Forests (80%)

Capabilities Received:
- Common Operating Environment (COE)
- 100% 9th SC(A) NETOPS C2
- Single Identity
- Global Mobility/Collaboration

Windows 2K8 R2 AGM release is in the critical path to start this Phase.
Core Infrastructure Baseline for global environment. Deployment of Enterprise Management Capability (Complete by MAR 2012)

Phase 2 POA&M – Lead: NETCOM G5, support G3.
- Network standardization critical success factor
- AD Server 2008 R2 configuration
- All client machines Vista/Windows 7
- Out of Band Management (OOBM)
- Install Admin tools within OOBM environment
- Management Tools (NETOPS)
- NSA security risk mitigations fully implemented
- Decommission old theater equipment

EDS&A Administrative Roles & Responsibilities

- Enterprise Governance
- Enterprise Infrastructure Administration
- Sig Bde/ Installation Campus Administration
- Tenant Organization Administration
EDS&A Enterprise Governance

★ ARMY Cyber Operation and Integration Center (ACOIC)

• Drive the plan for strengthening the performance of the enterprise as defined by ARMY leadership
• Cascade strategy and goals down into the enterprise
• Providing organizational structures that facilitate the implementation of strategy and goals
• Ensure standards and policies are defined and enforced
• Drive adoption of Change Management within the Enterprise
• Measure IT performance within the Enterprise
Enterprise and Domain levels managed by 9th SC (A) and subordinate Signal organizations

**Enterprise Administrators**
- Forest Configuration Operators
- Replication Management Administrators
- Schema Administrators
- Security Policy Administrators
- Domain Controller Administrators

**Domain Administrators**
- Domain Configuration Operators
- Security Policy Administrators
- Domain Controller Administrators
- Replication Monitoring Operators
- DNS Administrators
- Service Admin Managers
- Backup Operators
Installation TLOU Administration

- Administration of Top Level Organizational Units (TLOU) is delegated by 9th SC (A) and subordinate Signal organizations to entities responsible for the function of administration of a set of AD resources
- TLOU(s) are not limited to physical sites and may include logical organizational entities that receive delegation of a subset of AD information infrastructure resources

Installation Tenant Organization Administration

- Delegation of Subordinate OU structure is authorized by TLOU Administrators for a given organization
PURPOSE

• To provide global remote administration of AD from identified Army Data Centers.
• To provide secure access to AD administrative applications and DC console access within the Army network and from the Internet.
• To provide an accessible, scalable, and highly available administration environment.
OOBM Logical Data Flow

Required Internal Ports:
- RDP (TCP 3389)
- LDAP (TCP 389)
- Kerberos (TCP/UDP 88)
- DNS (TCP 52)

1. User browses to OOBM Portal over HTTPS
2. User initiates HTTPS connection to OOBM Gateway with Admin Smart Card
3. RDP over HTTPS established to OOBM Gateway
4. RDP 3389 to Session Host Server
5. RDP 3389 over IPSEC to Managed Services and Systems

OOBM Logical Data Flow

Enterprise Services

3rd Party and AD Native Tool Sets

RD Connection Authorization Policies & RD Resource Authorization Policy

Administrator

User

Smart Card

Admin Smart Card

Connection Broker

Session Host Servers

Licensing

Authentication Traffic

RD Web Access and RD Gateway
An OU Administrator accesses a local workstation on any post, camp, or station globally.
The OU Administrator connects to the OOBM enclave via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS).
Once authenticated, the RD Connection Broker directs the user to a high assurance desktop on the RD Session Host managed by Theater Forest level administrators. The RD Session Host supports session load balancing and reconnection to existing sessions.
Using the high assurance desktop, approved native and third party tools can be accessed to perform Active Directory administration on replicas located anywhere within Theater. All traffic is secured end to end using IPSec.
OOBM Administrator Process Flow

UNCLASSIFIED

2011-08-23 (1445-1600)//Enterprise Directory Services & Authentication  IEF Session: #2, NETCOM/9th SC(A)  UNCLASSIFIED
In Phase 0, NETCOM and the Contractor build POA&Ms for each Functional forest to migrate to the theater enterprise. All applications have been identified & rationalized by Apr 2012 to support five theater managed environment and ADCCP.

Phase 3 POA&M – Lead: NETCOM G5, support G3.
- OPT Lead transferred to G3
- Plan will be incorporated into AD EXORD
- Plan will be aligned with ADCCP
- All Functional client machines Vista or Windows 7
- Identify any required extension of theater forest footprints
- Analysis of theater & Functional application based upon ADCCP rationalization criteria
- Define and coordinate functional POA&Ms for users and some applications to migrate into the 5-theater forest architecture

What is Application Binning?

★ The identification and consolidation of applications within the Army

★ Vision:
  • Reduce costs associated with Army applications
  • Provide common services to the larger Army community
  • Simplify location and presentation of services and data

★ Three Phases:
  • Discovery
  • Analysis
  • Consolidation
Discovery

★ Involves gathering information about applications, environment, and interdependencies

★ Critical Phase – Basis for subsequent decisions

★ Collecting Data:

• Definition of binning process informs discovery criteria
• Need usage, financial and technical data
• Minimize number of data calls
• Identifying owners and key data sources
• Adjusting for bias
• More than Active Directory aware applications

★ The Army does not track much of this data
Binning Applications

All applications are separated into three groups

Active Directory dependent applications: (These are applications that may or may not sit on a windows platform but rely on AD for authentication.

Active Directory aware applications: Applications that reside on a Windows-based member server but don’t require AD for authentication.

Non-Windows based applications: Applications that don’t reside on a Windows-based member server and don’t use AD for authentication.
Application Migration Overview

DISA-Managed Army Enterprise Service Application Forest (AESAF)

DISA-Managed Army Enterprise Application Forest

Army Data Centers within Theaters

APPLICATIONS
Preparation for Migration

• **Identification and Bounding**
  – Gather necessary information about the application environment
  – Determine scope for migration iterations
  – Trace connectivity to determine architectures
  – Understand application linkage and user permission

• **Preparation**
  – Stage configuration changes for rapid execution
  – Communicate with users and schedule service interruptions
  – Document and rehearse changes

• **Movement**
  – Conduct per test
  – Migrate applications between environments during non-peak hours
  – Validate application functionality
In Phase 0, NETCOM and the Contractor build POA&Ms for each Functional forest to migrate to the theater enterprise. 80% of Functional migrated by 30 SEP 2012, remaining by Sep 2013.

Phase 4 POA&M – Lead: NETCOM G5, support G3.

- Execution of each Functional POA&M for users and some applications into the 5-theater forest architecture
- Plan will be incorporated into AD EXORD
- Plan will be aligned with ADCCP
- Dependant on POA&Ms for each functional forest (Phase 1)
- If a functional forest has an approved Enterprise Email waiver, they should also be granted a waiver for AD migration. This does not mean they are exempt from migration.
Federation Services providing global collaboration capabilities

- DISA Provide Application Authentication services
- Federation Services (FS) providing global collaborative access for web enabled applications
- Functional Forests collapsed into five theater
  AD Environment managed by 9th SC (A)

Active Directory Federated Services

Active Directory & Army Data Center Consolidation End State

9/2011  9/2013
Establish 5 Theater Forest standardized Active Directory Operating Environment

- Standard Configuration
- Standard OU Structure
- Standard GPO Management
- Standard Hardware Configuration
- Standard Configuration Management Processes across Theaters
- Standard Administration Tools and processes

Windows 2008 R2 Server environment

Windows 7 Desktop environment

Application Hosting criteria established

Agreed upon Functional Forest POA&Ms

60-80% of Function Forests collapsed

Establish an Out of Band Management (OOBM) environment
EDS&A Points of Contact

★ CIO/G6
  • AONS – COL Gary Langston / Jeff Gotherman
  • Cyber Dir – Ms. Tracy Traylor / Andre Townes
  • IRI – Mike Ramsey / Ted Schiller

★ Army Cyber Command
  • G-33: COL Max Duggan / Steve Mize

★ NETCOM
  • G3: COL Gerald Miller / Ernest Exum
  • G5: COL Daniel Matchette/ Robert Bachert / Stuart Wells
  • G8: Charlotte Calvert

★ Daily Operational Planning Team (OPT)
  • TELCON: 520-538-9890; 11:30 ET, 08:30 PT
Backup
Functional Forest Rationalization Process

1.) Consolidate Functionals
2.) Examine Users
3.) Users Tied to Apps?
   - No
   - Yes
   - 5.) Examine Theater DC Location and Capacity
   - 6.) Identify Users Tied to App
   - 7.) Kill App through Attrition
   - 8.) Can App be Cleaned?
   - 9.) App State
   - 10.) Extend Theater Footprint
   - 11.) Update App to ADCCP Standards
   - 12.) Extend Theater with Additional DCs
   - 13.) Migrate User Set to Theaters
   - 14.) Move App to Theater Environment
   - 15.) ADCCP Criteria?
   - 16.) Move App to DISA Environment
   - 17.) Shutdown DCs?
   - 18.) Shutdown Domain Controllers (DCs)
   - 19.) Shutdown Forest?
   - 20.) Review Remaining Users & Apps
   - 21.) Functional Consolidated

C2 (NetOps)
- Need shutdown dates in order
- Requires enforcement of orders
- Temporary extensions decided by NETCOM CG
- Integrate into enterprise CM process

User Migrations
Application Migrations
Shutdown Activities

2011-08-23 (1445-1600) // Enterprise Directory Services & Authentication
IEF Session: #2, NETCOM/9th SC(A)
Theater Rationalization Process

1.) Manage Theater Forests
2.) Users on Old DCs
3.) Tech Refresh Theater DCs
4.) Users utilize new DCs
5.) Examine Applications
6.) DC Verdict
   Reuse
   Dispose
7.) App State
   Dirty
   Clean
8.) Can App be Cleaned?
   Yes
   No
9.) Kill App through Attrition
10.) Rebuild and use in the Enterprise
11.) Send to Property Book Office
12.) Update App to ADCCP Standards
13.) Theater Forest Clean?
   Yes
   No
14.) ADCCP Criteria?
   Army
   DISA
15.) Clean App Remains in Theater
16.) Move App to DISA Environment
17.) Theater Managed Forests

- No Additional Forest Required
- Requires Enforcement of Orders
- Theater Forests End State Windows 2008R2