Connect: Operations in Army Cloud Computing

Speakers: CW4 Carrie McLeish, CW4 Taylor Wells, CW3 Joe Hamm

Moderator: CW5 Todd M. Boudreau

September 10, 2013
Description:

• This panel will discuss advantages and challenges of Army Cloud Computing.

• The presentation will look at the Army’s transition to LandWarNet 2020 (LWN2020), support of core warfighting capabilities in the Joint Information Environment (JIE), tactical and strategic cloud services, and security of data at rest and in transit.

• The presentation will be followed by a Q&A session.
We Must Train as We Fight
Deploy Little to No Notice Anytime, Anywhere in Austere Environments
Installations as a Docking Station
Modernized From Strategic Core to the Tactical Edge
Single Secure Network
Incorporate Echelons Above Army Requirements
Centralized Management and Decentralized Execution

The Network is Key to a Smaller, More Capable, Better Trained Expeditionary Army

Future

- Reduced Costs for Data Centers and Applications
- Improved Interoperability for Better Coordination and Information
- Improved User Satisfaction and Mission Success
- Faster, More Responsive Capability Deliveries to Warfighters
- Improved Security to Reduce Cyber Threats
- Faster Adoption of Commercial IT Breakthroughs
LandWarNet 2020 and Beyond
What We Are Investing In . . .

Network Capacity (Connect and Operate)

Enterprise Services (Share)

NetOps & Security (Access and Defend)

NetOps and Security

Environment

Joint

Enterprise Services

NetWarNet 2020
And Beyond

Network Capacity

UNCLASSIFIED
Security Architecture Overview
(DoD Top Level Architecture (TLA))

- Army CIO Guidance: Eliminate Security Infrastructure at Installations
- Heavy Security Stack for Core Data Center: Leverage with MPLS to Protect Installation Processing Node (IPN)
- MPLS & Traffic Management Schema will Ensure Latency to Core Data Center OR IPN is Never >60ms for Intra-Region & Never >100ms (Worst Case) Inter-Region within CONUS
- Potential 97.5% Reduction in Security Stacks Over the Currently Employed Solution Set
- DISA SSA Team: Approach is Consistent with JIE Goals
- Reduce CONUS Enclaves from 78 Down to One Instantiated with Sub-Regions
Multi-Protocol Label Switching (MPLS)
The Value of Virtual Traffic Management

★ Virtual Traffic Management - Not Infrastructure Dependent
★ More Interstate Lanes; **Real Power** is the ‘New’ Lanes Are ‘Smart’
★ Connects to Available 10Gb DISN & Supports 100+ Gb as Capacity Becomes Available
★ Uses Data-Carrying Switch That is Highly Scalable & Protocol Agnostic – Path Learning Mechanism
★ CIO/G6 Teaming with PEO EIS to Execute

★ Benefits:
  • Speeds Up Traffic Flow and Easier to Manage
  • Better Reliability and Increased Performance
  • **For the First Time**, We Can Put all Classification Levels on the Same Transport

Army Purchased Enough MPLSs in FY12 to Field 30 Largest CONUS Installations
Balance Modernization & Sustainment – Flexibility Through Capabilities

Network Operations & Security
- Single Identity
- Authentication Service
- Thin/Zero Client
- Continuous Monitoring
- Mobile Security (BYOD)
- Net Ops

Network Capacity
- Transport
- Data Center
- Voice, Video, IM, Presence
- Web 2.0 (milSuite)
- Collaboration

Enterprise Services
- Messaging (Email)
- Ent Svc Desk
- Content Management
- Collaboration

BMA: ERPs
- Centralized Accounting
- Supply, Maint, Property Personnel & Pay Mgt

WMA: Tactical Deployed
- 7 BCTs
- 4 BCTs
- 4 BCTs
- 4 BCTs
- 4 BCTs

FY XX
- Installations
- X Data Centers
- X Data Centers
- X Data Centers
- X Data Centers
- X Data Centers

LandWarNet 2020 and Beyond
Modernization Through Capability Sets (Initial Strategy)

Network Mission Area (NMA) Capability Sets Ensure Synchronization
Stay Connected

www.flickr.com/ArmyCIOG6

www.facebook.com/ArmyCIOG6

twitter.com/ArmyCIOG6

CIOG6.Army.mil

www.youtube.com/ArmyCIOG6
Why the Joint Information Environment (JIE)?

- Exploding technologies
- Demanding scope
- Increasing threat
- Decreasing budget
- Demanding efficiencies

“Together, we will strengthen the DoD by delivering the agile and secure information capabilities needed to enhance our nation’s combat power and decision making.”
--Teresa M. Takai, DoD CIO
What is the Cloud?

- Cloud Enabled Network Operations supports Unified Land Operations
- Deployment Models: public, private, community and hybrid (NIST)
- Service Models: SaaS, PaaS, and IaaS
- Connection States: Disconnected, Intermittent and Low Bandwidth (DIL)
- Tactical and Strategic
• The 26 June 2012 DoD CIO designation memo specifies that DISA will perform cloud brokerage functions to achieve IT efficiencies, reliability, interoperability, and improve security and end-to-end performance by using cloud service offerings. DoD Components will acquire cloud services through the Enterprise Cloud Service Broker (ECSB) or obtain a waiver from the DoD CIO designated review authority (i.e., the GIG Waiver Board).

• Responsibilities:
  – manage the use
  – performance and delivery of cloud services
  – negotiate relationships between cloud providers and cloud consumers
Cloud Computing Myths

Myth 1: Virtualization is cloud computing

Virtualization is the technology that enables cloud computing

Myth 2: The tactical edge will lose complete administrative access to their services

Administrative control is still being discussed and is part of the agreement between the Enterprise Cloud Service Broker (ECSB) and the unit requesting services.
Myth 3: Thin client/zero client is cloud computing

a. Thin client provides minimal computing power but does have a hard drive

b. Zero client extends the bus of the computer across the cloud and has no hard drive, no drivers, etc.
Phases of Deployment
• Deployed Tactical Network hosts crucial applications and services on the Local Area Network (LAN) to support continued operations while operating a Disconnected, Intermittent, and Low Bandwidth (DIL) environments

• Are we providing a buffet to our adversary?
Information Protection

• Protect the data that is saved locally
• Protect the data in transit to and from the cloud
• Protect the data at the ECSB Enterprise Cloud Service Broker
Protection Methods

- Full Disc Encryption
- Zero Removable Media
- Access Control
- Tactical PKI