

# **Network Evaluation Lab - Infrastructure Review**

U.S. Army Information Systems Engineering Command  
Mission Engineering Directorate  
Fort Huachuca

Bruce Adamson

**Mission** - Manage the lab network infrastructure to safely permit multiple varying lab evaluations of vendor equipment.

**Composition** -

- Multiple Linux (Ubuntu and CentOS)
- Microsoft Windows
- Physical and virtual servers
- VMWare vSphere 6.5 virtual environment
- Cisco switches

**Network** -

- Defense Research Engineering Network (DREN)
- Layer-3 IPv4 routing
- Layer-2 Spanning Tree VLANs
- Multiple patch connectivity failover

**Scripts** - Automate various maintenance tasks across the servers, internally developed

# Linux Servers -

- Syslog - Ubuntu 20.04 (headless, physical)
  - Collects logging from all servers and devices
  - Uses GreyLog for sorting and displaying
- Netmon - Ubuntu 20.04 (headless, physical)
  - Collects SNMP (Simple Network Management Protocol) v3
  - Uses Zabbix
- DNS - Ubuntu 20.04 (headless, physical)
  - Provides name and time resolution services and synchronization
  - Uses bind and NTP (Network Time Protocol)
- Files - Ubuntu 20.04 (headless, physical)
  - Provides two multi TB storage shares
  - NFS (Network File System) and SMB (Shared Message Block)
  - Hosts all scripts

## Linux Servers (cont.)-

- Proxy - Ubuntu 20.04 (headless, physical)
  - Proxies all web traffic from the lab to the DREN
  - Uses squid
- LDAP - Ubuntu 18.04 (headless, physical)
  - Provides network authentication via Lightweight Directory Access Protocol to servers and switches, centrally
  - Also interfaces with Active Directory Domain Controllers
- ACAS - CentOS 7.0 (headless, physical)
  - Assured Compliance Assessment Solution
  - Scans all servers, matches results against compliance templates to ensure servers remain at required patch levels

# Windows Servers -

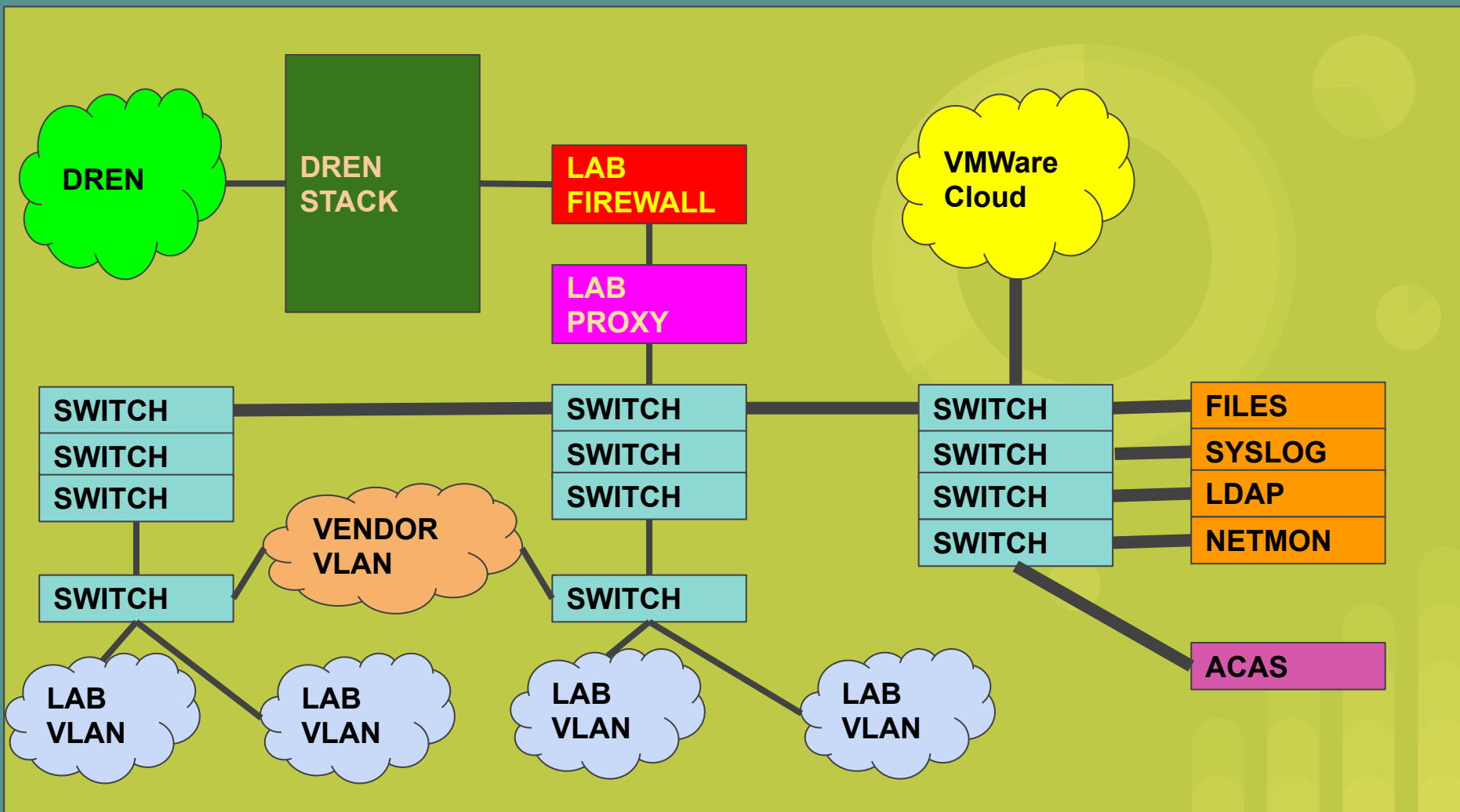
- Domain Controller 1 - Windows Server 2019 (physical)
  - Provides backup Active Directory services and authentication, interacts with LDAP
  - Implements group and user policy
  - Provides name and time services to Windows
- Domain Controller 2 - Windows Server 2019 (physical)
  - Provides primary Active Directory services and authentication, interacts with LDAP
  - Implements group and user policy
  - Provides name and time services to Windows
- WSUS - Windows Server 2019 (physical)
  - Windows Server Update Services pushes updates from DISA (Defense Information Systems Agency) repository

# Virtual Environment -

- VMWare vSphere 6.5 - ESXi servers (x16 clustered hosts) (physical)
  - Provides virtual environment
  - Managed by vCenter interface (x3 clustered hosts for control)
  - Contains 50+ virtual machines (Windows and Linux mix)
  - Cloud container spans all physical ESXi servers
  - RAM = 5.6 TB
  - Disk = 147.3 TB (SATA SSD)
  - CPU = 735 GHz (x320 Intel Xeon cores total)
  - Each physical server is multi-switch connected (x4 GB NIC, 1 per switch in stack), plus OOB (Out-of-band x2)

## Network -

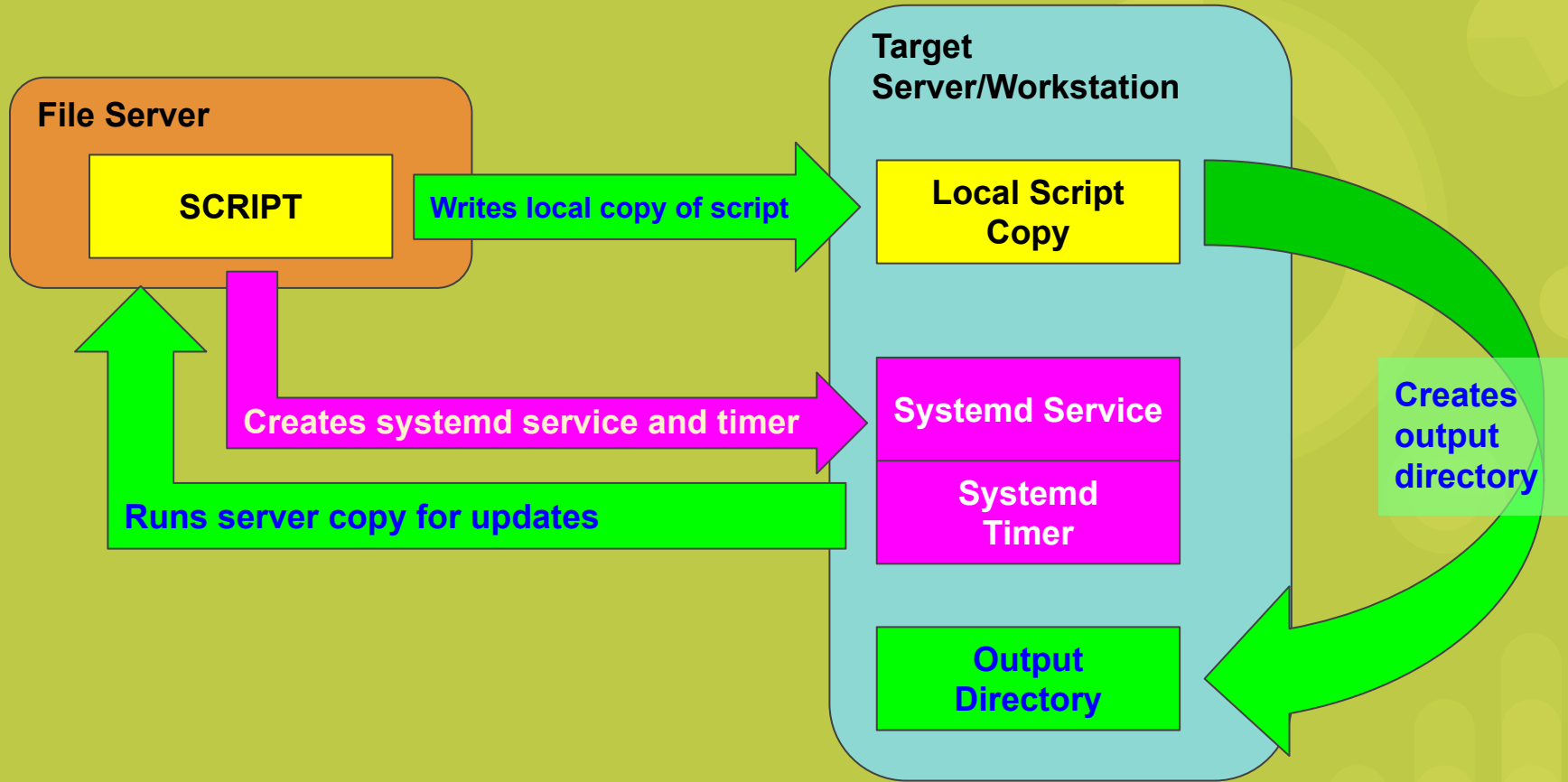
- Firewall - Physical
  - Provides packet-filtering and flow-filtering
- Switches - Layer-3 Cisco
  - Gigabit Ethernet Copper (x48 RJ-45 ports)
  - 10 Gigabit Ethernet Fiber (x4 fiber module ports)
  - Switch management access controlled by LDAP, restricted to elevated accounts only, logged by syslog
- NICs - Network Interface Cards (RJ-45 copper)
  - Linux physical servers are multi-path connected using **ifenslave** (x4 Gigabit NICs), striped across 4 stacked Cisco switches (one NIC per switch)
  - Windows servers are similarly connected
  - Switch side uses LACP (Link Aggregation Control Protocol) to bond multiple NICs into one connection





# Scripts -

- Backup - “ServerBooks”
  - Sets systemd timers
  - Acts like cron job to backup server
- Update - “AutoUpdate”
  - Sets systemd timers
  - Acts like cron job to update server
- ProxyAdBlock - “AdBlockDownload”
  - Acts like cron job to reach out to external URL to download AdBlock list and update proxy server
- UnlockAccount - “AoLRUnlock”
  - Acts like cron job to unlock local Account of Last Resort every 15 minutes
  - If account is locked, wait 15 minutes
- Build Scripts - Run on new setup (one time)
  - Set of different scripts to install the service or client needed
  - Ex. LDAP client, LDAP server, Syslog server, etc.





**QUESTIONS?**