Ubuntu/CentOS 7 Desktop Scope of Support

Plans for modern linux desktop support.

Desktop Linux Distributions supported at SLAC

1. Recommended Linux Distribution: Ubuntu Long Term Support 18.04 or 20.04
    a. **Long term support** (LTS) releases are for 5 years.
    b. 18.04 = YY.MM of release date (released April 2018)
    c. It is possible to upgrade (complete reinstall NOT required) from one LTS distro to the next (eg, 16.04 -> 18.04 20.04)
2. CentOS 7 (2nd choice, alternative to Ubuntu LTS)
    a. Not the recommended first choice. Ubuntu LTS is preferred for the desktop.
    b. CentOS 7 is the final CentOS release to offer a 10 year support lifetime.
        i. CentOS Stream 8 will offer a 5 year lifecycle.
    c. End of Life date for CentOS 7 is June 2024
3. RHEL 6 is End of Life as of November, 2020.
    a. Older desktop hardware should be refreshed; Newer desktop hardware should be reinstalled with Ubuntu.

Desktop Linux Authentication Configuration

- Roadmap: Windows Active Directory will be used for authentication
    - This aligns with the SCS long term plan to reduce dependence on Unix Heimdal Kerberos, leverage the existing Windows AD Kerberos and LDAP infrastructure, and move towards a singe SLAC ID

Security Services/Features needed

These are taken directly from the SLAC MinSec Policy (which has 11 items that match the 11 items below)

These will be configured using Chef Configuration Management and Compliance scanning/reporting

1. Anti-virus Software
    a. Install and configure ClamAV (optional, since not in moderate enclave)
2. Application Patches
    a. Configure automatic updates for Applications via apt/yum config
3. Authentication
    a. Kerberos and SSH will be configured and used for encrypted authentication
    b. Use Chef Compliance to scan for any enabled insecure server protocols such as telnet and ftp
4. Logging
    a. Configure syslog to log to central syslog server, and enable logging locally to /var/log/everything
5. Network Services
    a. Check for inappropriate network services via Chef Compliance
6. Operating System Patches
    a. Configure automatic updates for OS patches via apt/yum
7. Passwords
    a. To deal with any local accounts that might get created on the desktop, we will configure local password quality checks and policies (expiration time, etc) according to SLAC password policy. Ideally Microsoft AD accounts will be used and no local accounts will be required.
    b. Global account password policies are handled by Active Directory, not the local desktop configuration. Windows AD passwords will be changed in the same way they are being done now.
8. Baseline Security Configuration
    a. CIS Level 1 Workstation Profile will be used (modified where appropriate)
    b. Chef Compliance scanning can report on compliance level for our baseline
    c. PDFs are available for the CIS Benchmarks for Ubuntu 16.04 and CentOS 7
9. Training
    a. No additional changes needed (same SLAC Training Assignments are required)
10. Security Scanning
    a. Local scanner account will be enabled to allow authenticated Nessus scans by Cyber Security team

11. Banner
    a. The SLAC DOE login banner will be configured

Stanford Minimum Security Standards

In order to align with Stanford Minimum Security Standards for Endpoints (defined as any laptop, desktop, or mobile device), there are some additional requirements, as documented on this link:

https://uit.stanford.edu/guide/securitystandards

1. Patching - Apply security patches within seven days of availability.
    a. Configure apt-get on Ubuntu to apply updates automatically
    b. https://help.ubuntu.com/lts/serverguide/automatic-updates.html
2. Whole Disk Encryption
    a. Ubuntu has an option for full disk encryption at install time.
    b. https://www.eff.org/deeplinks/2012/11/privacy-ubuntu-1210-full-disk-encryption
3. Malware Protection
    a. ClamAV or chkrootkit can be used on on Ubuntu for malware protection.
4. Backups
    a. Crash Plan (Stanford) on Ubuntu can be used
    b. Information: https://uit.stanford.edu/service/code42crashplan
    c. Download linux client pre-configured for Stanford Single Sign On: https://stanford.box.com/SU-SemiCustomized-CPPe-Install
5. Inventory
    a. Review and update SLAC netdb records quarterly.
6. Configuration Management
    a. Install SLAC's Chef for configuration management

Additional **Operating System Configuration** needed

These will be configured using Chef Configuration Management and Compliance scanning/reporting

1. NTP or Chrony client (network time synchronization)
2. DNS configuration (/etc/resolv.conf)
3. logrotate configuration
4. mailgateway (mail client configuration, eg, postfix)
5. sudo configuration (/etc/sudoers and/or /etc/sudoers.d/[filenames])
6. shells (install zsh and other valid shells)
7. unixadmins (sets up unix-admin logins and scanner account)
8. root (manage root password, remote root access via ssh keys, and root home environment)

Reference Documents

- Published SLAC Policies and Governance SLAC Controlled Documents page:
  https://docs.slac.stanford.edu/sites/pub/Pages/SLAC_Policies.aspx
- Unix Kerberos password quality checks (Linux Desktop 2.0 will use Windows AD instead of Unix Kerberos, but the Unix Kerberos policies are here for reference. The goal is to have alignment with password quality checks for Windows and Unix accounts)
  https://novel.slac.stanford.edu/twiki/bin/view/SCCS/IdentificationAuthentication
- Secure Computing at Stanford
  https://securecomputing.stanford.edu
- Minimum Security Requirements for Computing
  https://docs.slac.stanford.edu/sites/pub/Publications/701-I02-001-00_Min_Sec_Req_for_Comp.pdf
- Stanford MinSec cookbooks:
  https://uit.stanford.edu/guide/securitystandards/cookbooks
- How do I change my SLAC Windows password?
  https://portal.slac.stanford.edu/public/ITHelp/KB/Windows%20Password.aspx
- Configuration Management Procedures in the SCS twiki:
  https://novel.slac.stanford.edu/twiki/bin/view/SCCS/ConfigurationManagement

- SLAC Password Policy
  http://www2.slac.stanford.edu/computing/security/password/passwordpolicy.htm

- CIS Benchmarks
  CIS_Ubuntu_Linux_16.04_LTS_Benchmark_v1.0.0.pdf
  CIS_CentOS_Linux_7_Benchmark_v2.1.1.pdf
  CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v2.1.1.pdf
  CIS_Red_Hat_Enterprise_Linux_6_Benchmark_v2.0.2.pdf
  CIS_CentOS_Linux_6_Benchmark_v2.0.2.pdf

- Stanford UIT Linux Support/Not Supported Framework (DRAFT in Google Docs)
  https://docs.google.com/document/d/12YWkXekUBee4LHSy_FW9h5YOLFvQ2TW6o1X-iBqN5hc/edit?ts=5923468b#heading=h.ho5az6iazpu8

Related articles

Content by label

There is no content with the specified labels