TACACS+ Server

Summary

TACACS+ is centralized identity access management that allows remote accessing of network devices with AAA (authentication, authorization, accounting) protocols.

Hostname: tacacs1.xxxx.xxxxxx.xxx

Access tacacs1.xxxx.xxxxxx.xxx through SSH and domain credentials (firstname.lastname and domain password). Must be in Domain Admins for sudo access.

Build Instructions

tacacs1.xxxx.xxxxxx.xxx was built on CentOS 7 using the following instructions: http://www.techspacekh.com/configuring-tacacs-plus-with-active-directory-user-authentication-on-rhelcentos-7/

Description	Steps

Create Yum repository to acquire tacacs-plus	# vim /etc/yum.repos.d/tacacs-plus.repo
	`[tacacs-plus]`
	`name=Tacacs Plus`
	`baseurl=http://li.nux.ro/download/nux/misc/el6/x86_64/`
	`enabled=0`
	`gpgcheck=1`
	`gpgkey=http://li.nux.ro/download/nux/RPM-GPG-KEY-nux.ro`

Install tac_plus	# yum -y --enablerepo=tacacs-plus install tac_plus
Install services to join server to domain	# yum -y install realmd sssd oddjob oddjob-mkhomedir adcli samba-common # yum -y install oddjob oddjob-mkhomedir sssd samba-common-tools # reboot
Discover dejero.local	# realm discover dejero.local *dejero.local* *type: kerberos* *realm-name: DEJERO.LOCAL* *domain-name: dejero.local* *configured: no* *server-software: active-directory* *client-software: sssd* *required-package: oddjob* *required-package: oddjob-mkhomedir* *required-package: sssd* *required-package: adcli* *required-package: samba-common-tools*

Join dejero.local	# realm join --user=xxxx.xxxxxxx dejero.local Password for xxxx.xxxxxxx:
Confirm join successful	# id xxxx.xxxxxxxx@dejero.local

Omit domain name for AD users	# vim /etc/sssd/sssd.conf
	`#use_fully_qualified_names = True`
	`use_fully_qualified_names =  False`
	# systemctl restart sssd

Create configuration file	# vim /etc/tac_plus.conf
	`key = <<LASTPASS>>`
	`accounting file = /var/log/tac.acct`
	`## Groups Definition ##`
	`group = NetworkAdmins {`
	`default service = permit`
	`login = PAM`
	`service = exec {`
	`priv-lvl = 15`
	`}`
	`}`
	`## Domain Users Access ##`
	`user = xxxx.xxxxxxx`
	`{ member = NetworkAdmins`
	`}`
	`user = xxxxxx.xxxxxxxxx`
	`{ member = NetworkAdmins`
	`}`
	`## Local Device Access ##`
	`user = xxxxxx {`
	`member = NetworkAdmins`
	`}`

Restart tac_plus service and enable it for system boot	# systemctl restart tac_plus # chkconfig tac_plus on
Add port to firewall	# firewall-cmd --zone=public --permanent --add-port=49/tcp