https://www.wallix.com/

WALLIX a fost dezvoltat pentru echipele tehnice care administrează infrastructura IT (servere, dispozitive de rețea și securitate etc.). Această soluție a fost concepută pentru a satisface nevoile de control al accesului și trasabilitate ale administratorilor de sistem.

Wallix Bastion include access control lists (ACL-uri) care constitue facilitate pentru administratorii care doresc să se conecteze la dispozitive de:

- verificarea detaliilor de autentificare furnizate de utilizator;
- verificarea drepturilor lor de acces la resursa în cauză;
- gestionarea parolelor conturilor țintă.

Wallix Bastion vă permite, să automatizați conectările la dispozitivele țintă pentru a spori securitatea sistemului

informatic prin prevenirea dezvăluirii detaliilor de autentificare a serverului.

Protocoalele acceptate în prezent sunt după cum urmează:

- SSH (and its sub-systems)
- TELNET, RLOGIN
- RDP and VNC
- RAW TCP/IP. Acest protocol permite redirecționarea conexiunilor TCP/IP locale pe stația client către un server țintă utilizând redirecționarea locală a porturilor TCP/IP. Proxy-ul SSH acționează ca un server SSH a cărui funcție este doar de a furniza redirecționarea locală a porturilor TCP/IP. Dacă un canal de sesiune shell este deschis la început, acesta va monitoriza apoi acțiunile de redirecționare efectuate.

WALLIX Bastion oferă o interfață Web compatibilă cu Internet Explorer, Chrome și Firefox pentru a monitoriza activitatea, conexiunile și pentru a configura componentele sale.

Poziționarea Bastionului WALLIX în infrastructura de rețea

Wallix Bastion este poziționat între un domeniu de încredere scăzut și un domeniu de încredere ridicat.

Domeniul de mare încredere este reprezentat de setul de dispozitive izolate de Bastionul WALLIX.

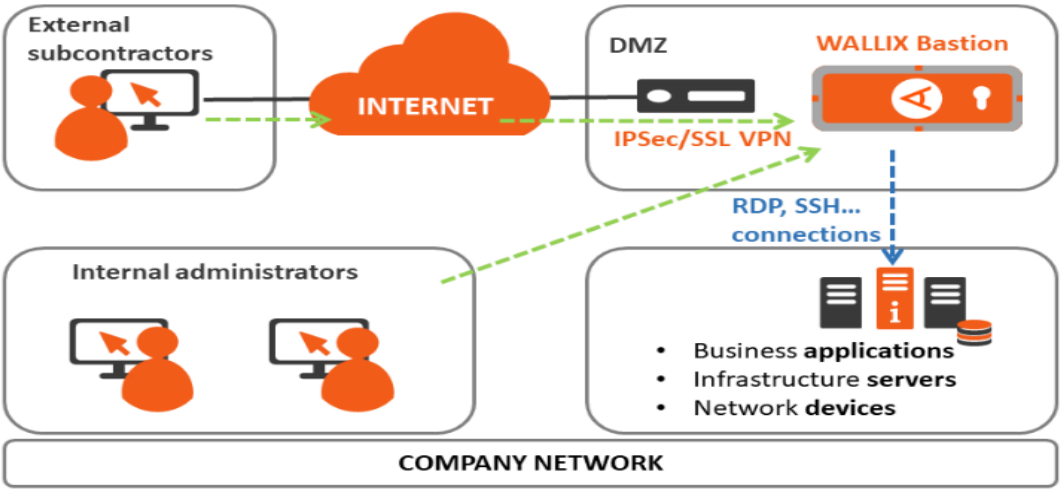
Aceste dispozitive și conturile lor conexe sunt numite "conturi țintă" în terminologia Wallix Bastion.

Domeniul de incredere scazut este reprezentat de populatia cu acces direct la Bastionul WALLIX:

- personalul companiei
- zona Internet

Pentru utilizatorii soluției, accesul la conturile țintă (în domeniul de mare încredere) este posibil numai prin WALLIX Bastion.

Figura 1. Bastionul WALLIX în infrastructura de rețea



Conceptul de ACL-uri wallix Bastion

WALLIX Bastion dispune de un motor avansat de gestionare a drepturilor care se bazează pe ACL-uri pentru a determina cine are acces la ce, când și cu ce protocol (protocoale).

Aceste ACL-uri constau din următoarele obiecte:

- utilizatori: adică utilizatori fizici ai WALLIX Bastion din directorul de utilizator intern și/sau extern;
- grupuri de utilizatori: un set de utilizatori
- dispozitive: adică dispozitive fizice sau virtualizate la care se solicită acces prin bastionul WALLIX
- conturi țintă: conturile declarate pe un dispozitiv sau pe o aplicație
- grupuri țintă: un set de conturi țintă
- aplicații: orice tip de aplicație și servicii care rulează pe un dispozitiv sau pe un set de dispozitive

În WALLIX Bastion, trebuie setată o autorizație pentru a acorda unui utilizator accesul la un cont țintă. Autorizațiile sunt declarate între un grup de utilizatori și un grup de conturi țintă (ceea ce înseamnă că fiecare cont țintă trebuie să aparțină unui

grup țintă și că fiecare utilizator trebuie să aparțină unui grup de utilizatori).

Autorizația permite utilizatorilor din grupul X să acceseze conturile țintă din grupul Y, prin intermediul protocoalelor A, B sau C.

Alte elemente sunt adăugate la aceste entități primare pentru a vă permite să definiți:

- intervale de timp de conectare
- caracterul critic al accesului la resursele-țintă
- dacă sesiunea este înregistrată sau nu
- tipul de procedură de autentificare a utilizatorului

De asemenea, puteți defini o serie de profiluri de administrator WALLIX Bastion, cu acces complet la caracteristicile Wallix Bastion sau drepturi limitate la anumite caracteristici. De exemplu, puteți defini că auditorii WALLIX Bastion vor accesa doar datele de audit sau vor permite administratorilor WALLIX Bastion să adauge/editeze utilizatori, să configureze administrarea sistemului, să gestioneze autorizațiile etc.

WALLIX Bastion dispune de un motor avansat de gestionare a drepturilor care se bazează pe ACL-uri pentru a determina cine are acces la ce, când și cu ce protocol (protocoale).

Aceste ACL-uri constau din următoarele obiecte:

- utilizatori: adică utilizatori fizici ai WALLIX Bastion din directorul de utilizator intern și/sau extern
- grupuri de utilizatori: un set de utilizatori
- dispozitive: adică dispozitive fizice sau virtualizate la care se solicită acces prin bastionul WALLIX
- conturi țintă: conturile declarate pe un dispozitiv sau pe o aplicație
- grupuri țintă: un set de conturi țintă
- aplicații: orice tip de aplicație și servicii care rulează pe un dispozitiv sau pe un set de dispozitive

În WALLIX Bastion, trebuie setată o autorizație pentru a acorda unui utilizator accesul la un cont. Autorizațiile sunt declarate între un grup de utilizatori și un grup de conturi țintă (ceea ce înseamnă că fiecare cont țintă trebuie să aparțină unui grup țintă și că fiecare utilizator trebuie să aparțină unui grup de utilizatori).

Autorizația permite utilizatorilor din grupul X să acceseze conturile țintă din grupul Y, prin intermediul protocoalelor A, B sau C.

Alte elemente sunt adăugate la aceste entități primare pentru a vă permite să definiți:

- intervale de timp de conectare
- caracterul critic al accesului la resursele-țintă
- dacă sesiunea este înregistrată sau nu
- tipul de procedură de autentificare a utilizatorului

OBSERVATIE: pentru a asigura implementarea cu succes a Bastionului WALLIX, va recomandam inventarierea:

- rolurile utilizatorilor care trebuie să aibă acces la conturile țintă
- rolurile utilizatorilor care trebuie sa administreze BASTIONUL WALLIX
- dispozitivele tinta si conturile tinta care trebuie accesate prin Bastionul WALLIX

Trebuie să puteți răspunde la următoarele întrebări pentru fiecare utilizator:

- are acest utilizator dreptul de a administra soluția și, în caz afirmativ, ce drepturi ar trebui să îi fie atribuite?
- acest utilizator trebuie să acceseze conturile țintă?
- când utilizatorul are dreptul să se conecteze?
- utilizatorul poate accesa resurse critice?

Trebuie să puteți răspunde la următoarele întrebări pentru fiecare dispozitiv țintă sau cont țintă:

- este acest cont țintă sau dispozitiv critic? (apoi, de fiecare dată când un dispozitiv critic este accesat, o notificare este trimisă administratorului)
- ar trebui să fie înregistrate sesiuni de utilizator pe acest cont?
- ce protocol (protocoale) pot fi utilizate pentru a accesa acest cont sau dispozitiv țintă?

WALLIX Session Manager

Această caracteristică specifică a WALLIX Bastion 8.0 este disponibilă în conformitate cu contractul de licență software.

Această caracteristică permite administratorului să:

- identificarea utilizatorilor care sunt conectati la anumite dispozitive si monitorizarea activitatii acestora: sesiunile pot fi vizualizate in timp real prin interfata de administrare WALLIX Bastion Web sau descarcate pentru a fi vizualizate local pe statia de lucru a administratorului
- examinați activitatea înregistrată video dintr-o sesiune de utilizator privilegiată
- obțineți un acces direct la resurse utilizând clienți nativi, cum ar fi PuTTY, WinSCP, MSTC sau OpenSSH
- definirea și configurarea politicilor de conectare prin mecanisme disponibile pentru protocoalele RDP, VNC, SSH, TELNET, RLOGIN și RAW TCP/IP

Navigarea prin meniul interfeței Web

Menu	Sub-menu	Actions
My preferences		Change the user preferences See the section called “Setting your preferences”
My authorizations	**Sessions**	Display the user authorizations on sessions and access targets See the section called “User authorizations on sessions”

Menu	Sub-menu	Actions
	Passwords	Display the user authorizations on passwords and access the target credentials See the section called “User authorizations on passwords”
Audit	**Current sessions**	List connections and logouts See the section called “Current sessions”
	Session history	List closed connections and display session recordings See the section called “Session history”
	Account history	List the account activities See the section called “Account history”
	Approval history	List the current and expired approval requests See the section called “Approval history”
	Authentication history	List the primary authentications See the section called “Authentication history”
	Connection statistics	Generate connection statistics graphs See the section called “Connection statistics”
Users	**Accounts**	Manage and import (.csv file and LDAP directory) WALLIX Bastion users See the section called “User accounts”
	Groups	Manage and import (.csv file) WALLIX Bastion user groups See the section called “User groups”
	Profiles	Manage and import (.csv file) WALLIX Bastion user profiles See the section called “User profiles”
Targets	**Devices**	Manage and import (.csv file) target devices See the section called “Devices”
	Applications	Manage and import (.csv file) target applications See the section called “Applications”
	Domains	Manage and import (.csv file) global and local domains

Menu	Sub-menu	Actions
		See the section called “Domains”
	Accounts	Manage and import (.csv file) target accounts See the section called “Target accounts”
	Clusters	Manage and import (.csv file) clusters of jump servers See the section called “Clusters”
	Groups	Manage and import (.csv file) target groups See the section called “Target groups”
	Password vault plugins	Display the list of available external password vault plugins See the section called “External password vault plugins”
	Checkout policies	Manage password checkout policies See the section called “Checkout policies”
Authorizations	**Manage authorizations**	Manage and import (.csv file) authorizations between target groups and user groups See *Authorization management*
	My current approvals	Manage the current approval requests and provide answers See the section called “View the current approvals”
	My approval history	List the current and expired approval requests See the section called “View the approval history”
Session management	**Connection policies**	Manage authentication mechanisms for proxies (RDP, VNC, SSH, TELNET, RLOGIN and RAW TCP/IP) See the section called “Connection policies”
	Recording options	Manage options for session recording storage See the section called “Session recording options”
Password management	**Password change policies**	Manage password change policies See the section called “Password change policies”

Menu	Sub-menu	Actions
	Password change plugins	Display the list of available plugins for password change See the section called “Password change plugins”
Configuration	**Configuration options**	Configure specific WALLIX Bastion aspects (e.g. the GUI options, the RDP proxy, the SSH proxy, etc.) See *Appliance configuration*
	Time frames	Manage time frames See the section called “Time frames configuration”
	External authentications	Manage external authentication methods (LDAP, Active Directory, Kerberos, RADIUS) See the section called “External authentication configuration”
	LDAP/AD domains	Integrate user accounts via LDAP or Active Directory Import (.csv file) LDAP/AD domains and LDAP authentication mappings See the section called “Configuration of LDAP or Active Directory domain mapping”
	Notifications	Manage the notification mechanism See the section called “Notification configuration”
	Local password policy	Manage the local password policy See the section called “Local password policy configuration”
	Connection messages	Configure the message displayed on a banner when a user logs on to proxies See the section called “Connection messages”
	X509 configuration	Configure X509 certificate authentication See the section called “X509 certificate authentication configuration”
	API keys	Manage API keys See the section called “REST API key management”

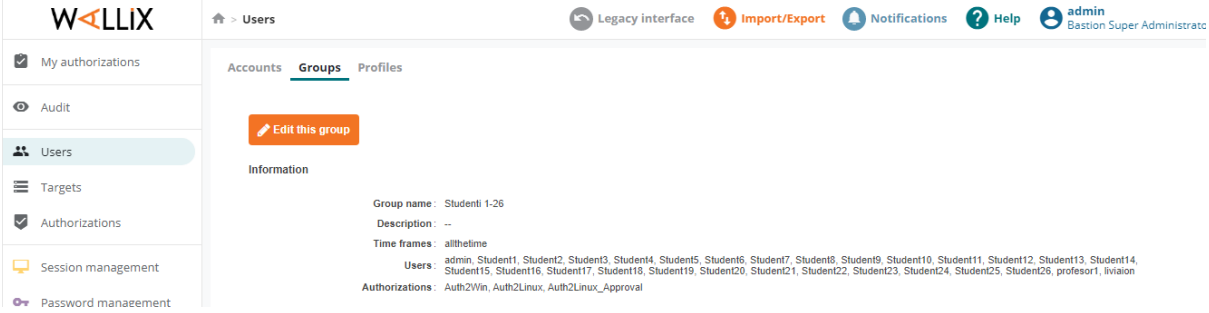
Menu	Sub-menu	Actions
	License	Display and update license key See the section called “License”
	Encryption	Set the encryption protection See the section called “Encryption”
	Audit logs	Display the content of the "wabaudit" file See the section called “System logs”
System	**Status**	Display general information on system status See the section called “System status”
	Network	Configure network settings See the section called “Network”
	Time service	Configure time service settings (NTP) See the section called “Time service”
	Remote storage	Manage remote storage of session recordings See the section called “Remote storage”
	SIEM integration	Manage routing of logs to other network devices See the section called “SIEM integration”
	SNMP	Manage the SNMP agent See the section called “SNMP”
	SMTP server	Configure the mail server for notification sending See the section called “SMTP server”
	Service control	Define service mapping with network interfaces and WALLIX Bastion services to be enabled/disabled See the section called “Service control”
	Syslog	Display the content of the "syslog" file See the section called “System logs”
	Boot messages	Display the content of the "dmesg" file See the section called “System logs”
	Backup/Restore	Save and restore a WALLIX Bastion configuration

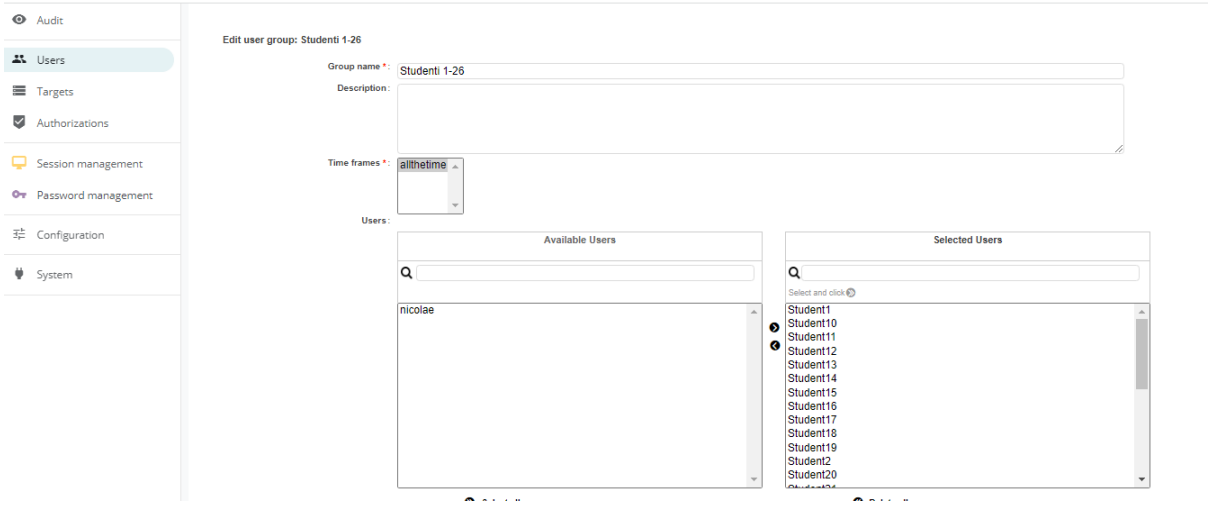
Menu	Sub-menu	Actions
		See the section called “Backup and Restoration”
Import/Export	**CSV**	Import data from a .csv file Export data as a .csv file, a .zip or .tar.gz archive See: the section called “User accounts”, the section called “User groups”, the section called “User profiles”, the section called “Devices”, the section called “Applications”, the section called “Domains”, the section called “Target accounts”, the section called “Clusters”, the section called “Target groups”, the section called “Add an authorization”, the section called “Configuration of LDAP or Active Directory domain mapping”
	Users from LDAP/AD	Import users from an LDAP or AD directory See the section called “User accounts”

Scenariu de laborator

Profesor

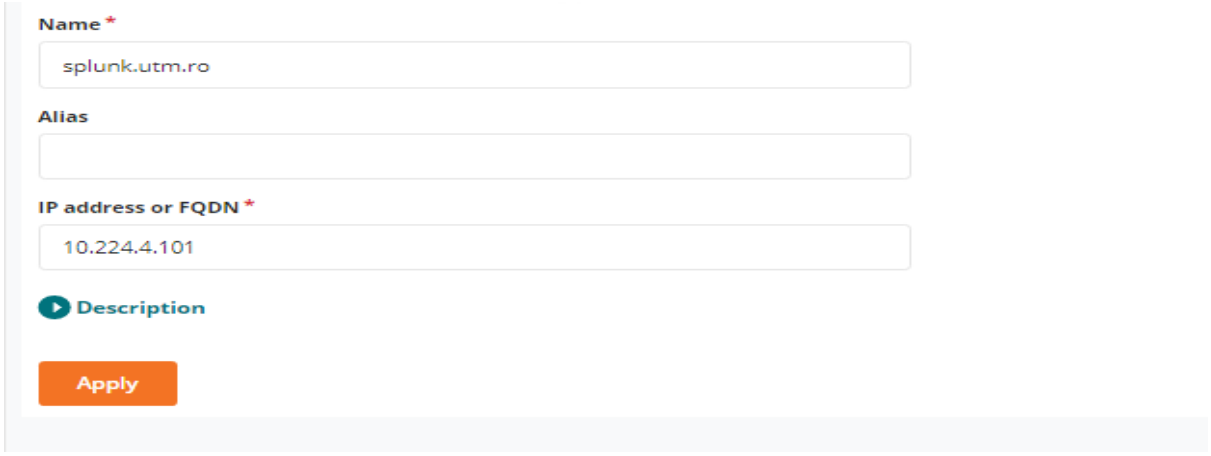
1. Verifica faptul ca toti userii student1-26 fac parte din grupul Studenti1-26 si adauga studentii/userii care nu sunt in grup



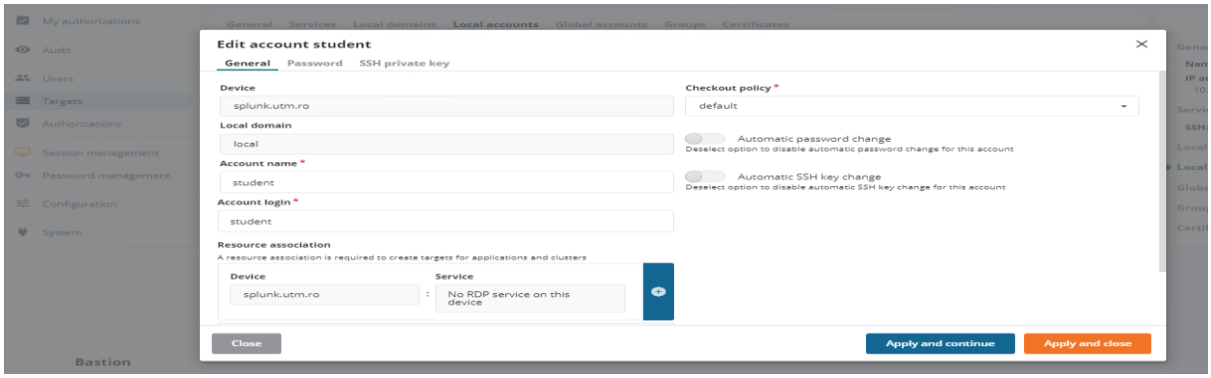


2. Se adauga “Targets” (servere la care sa avem acces privilegiat)

Se alege +Device

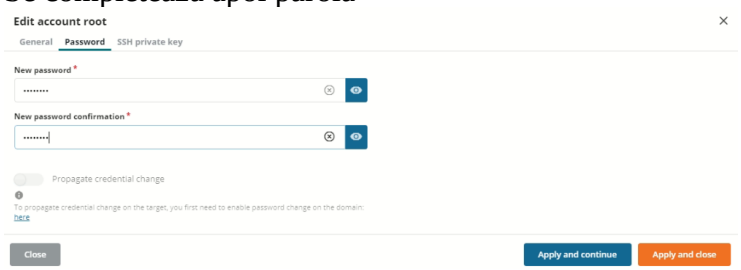


Se defineste un “Local Account”



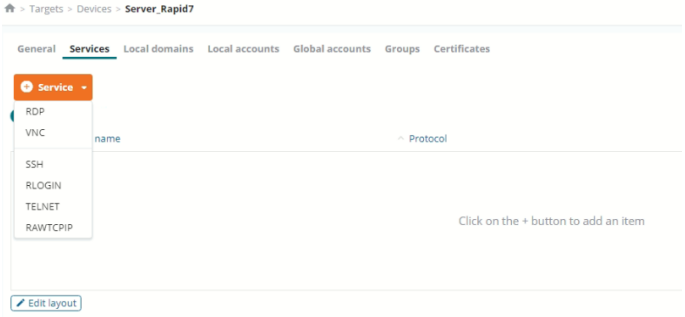
Apply and Continue

Se completeaza apoi parola

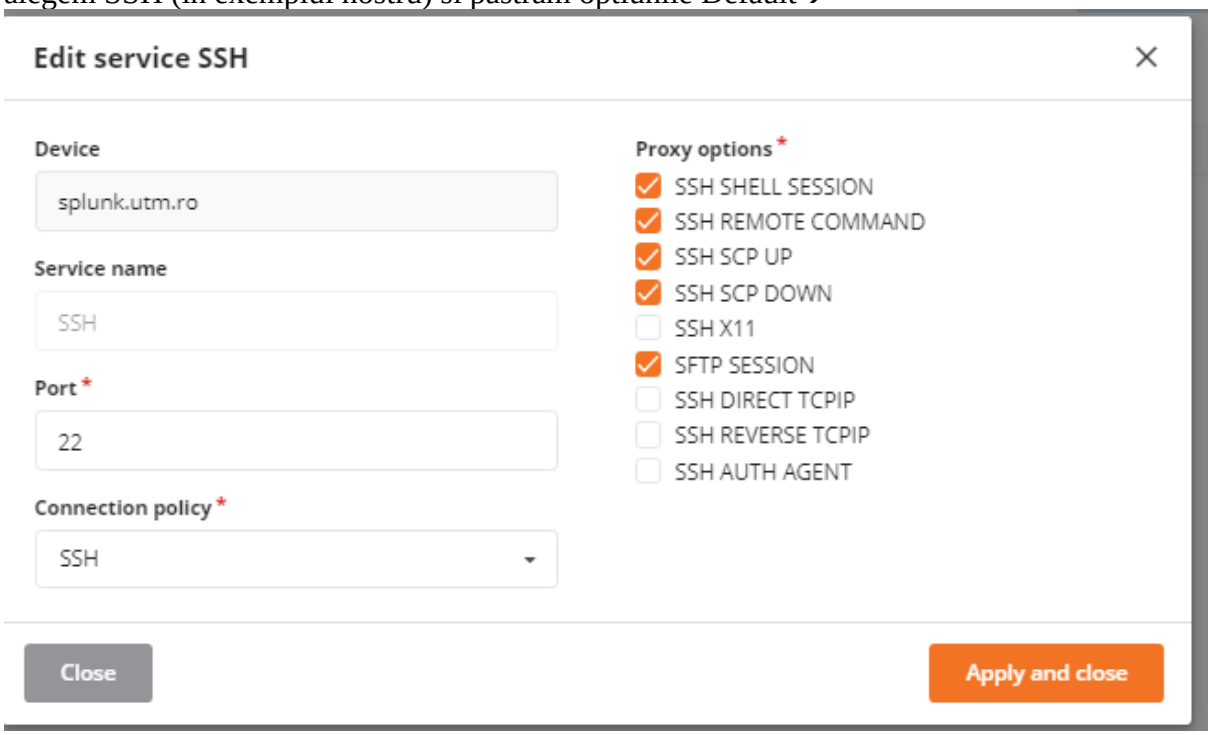


Avem: un server (Target), un user (student) si definim metoda de conectare la targets (SSH, este RDP, este TELNET, etc …)

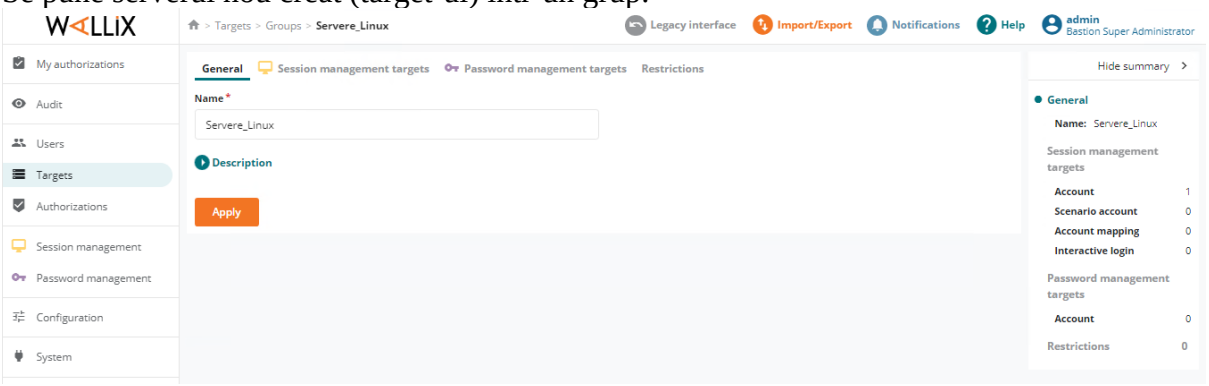
Services→



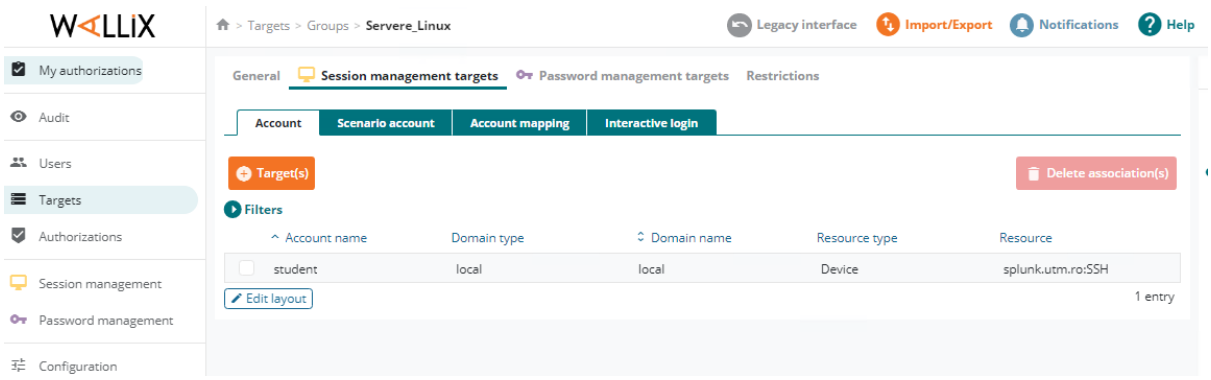
alegem SSH (in exemplul nostru) si pastram optiunile Default→

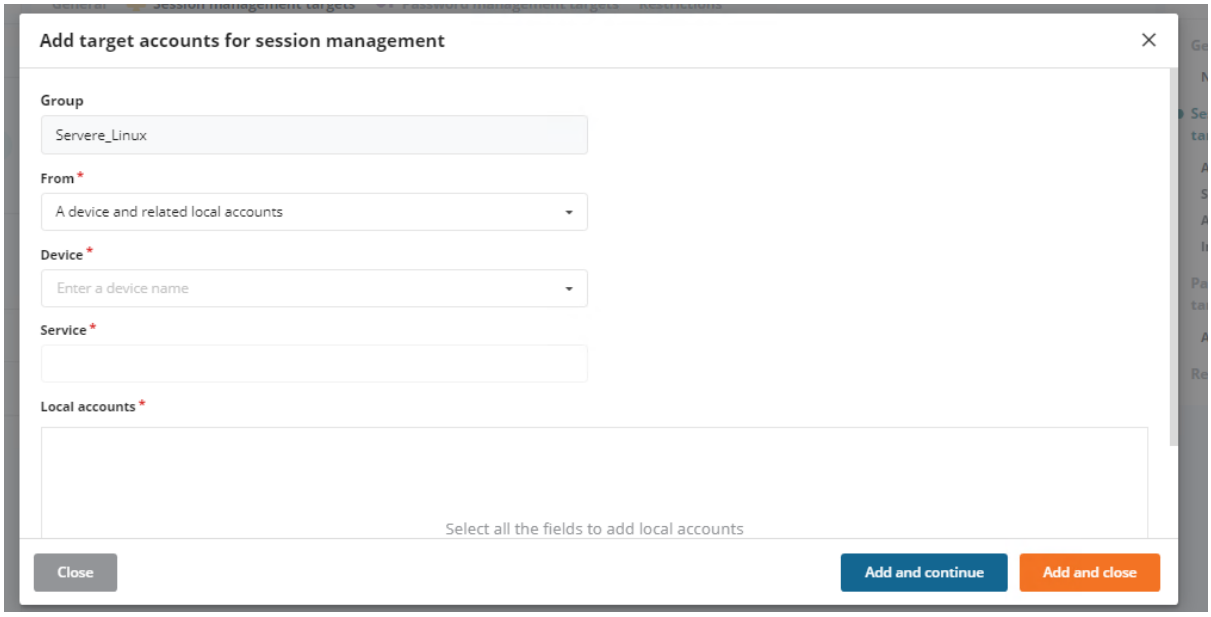


Se pune serverul nou creat (target-ul) intr-un grup.



La acest grup nou creat adaugam “Targets”



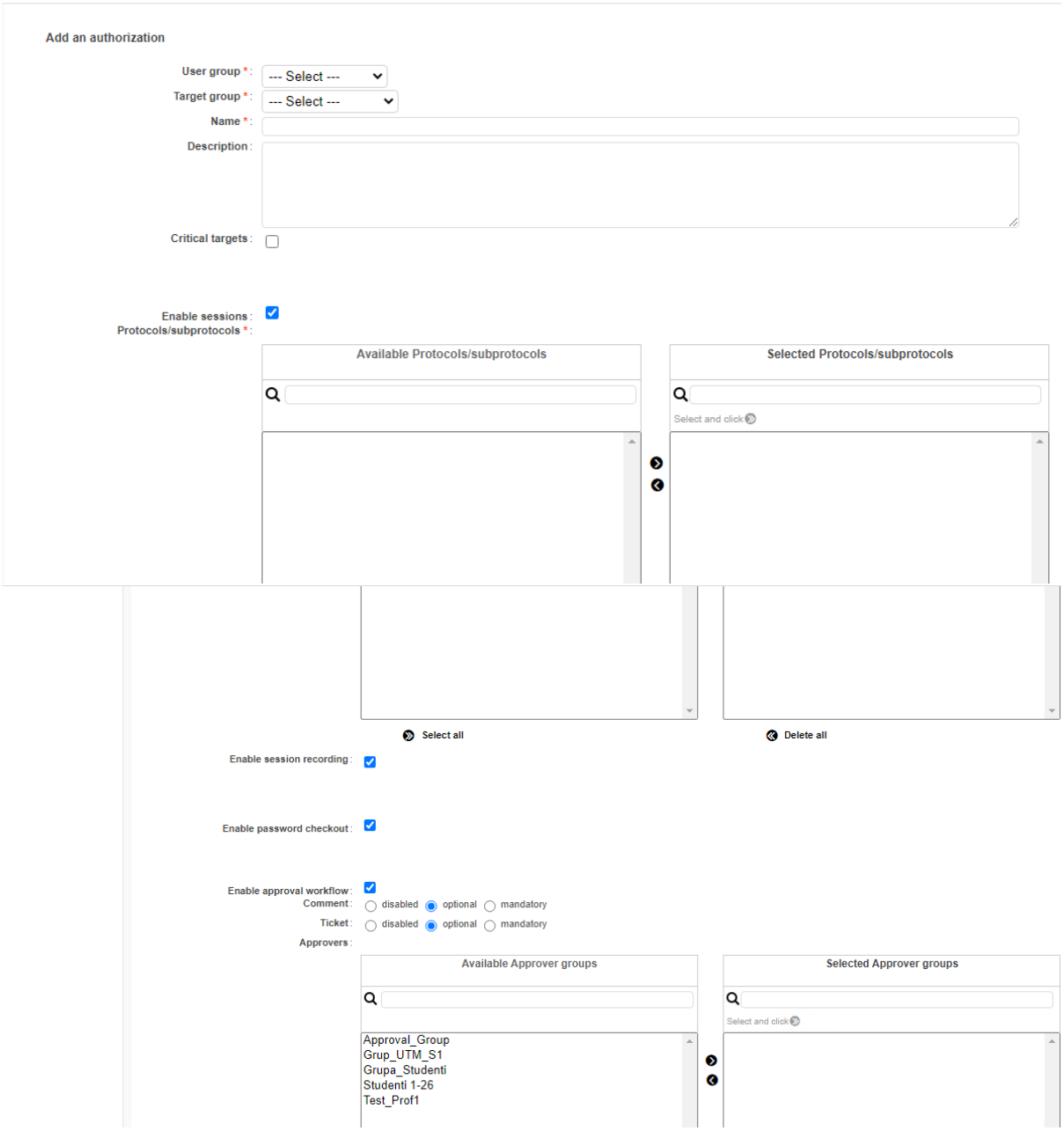


Apoi→Add and close

Concluzie: Am creat un grup (Servere_Linux), la care am adaugat un Targets (Servere_Linux) cu precizarea metodei de autentificare (SSH)

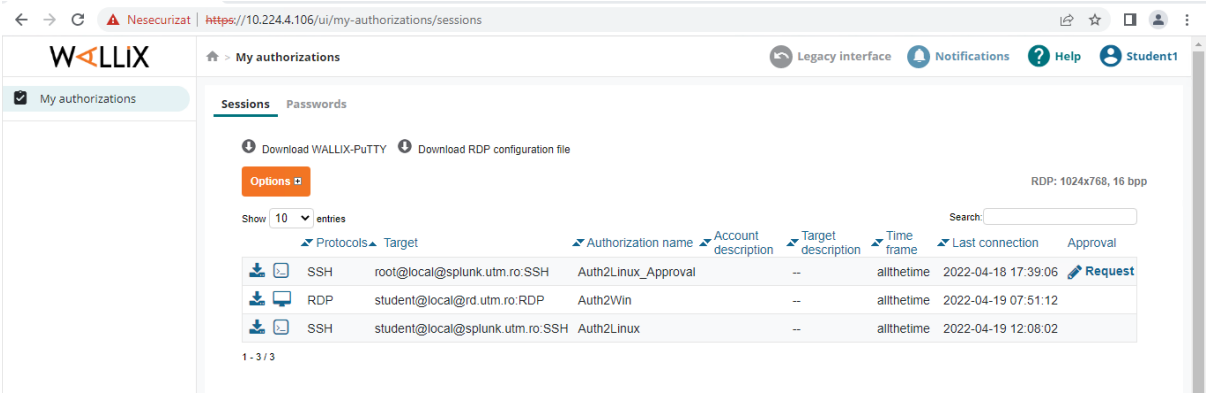
- Se da Authorization

Add Authorization

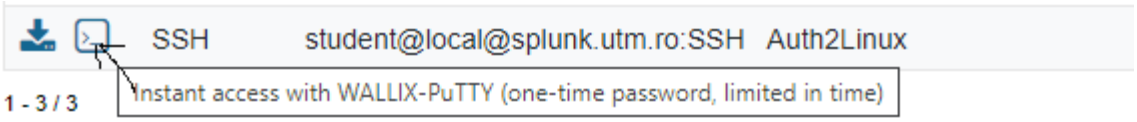


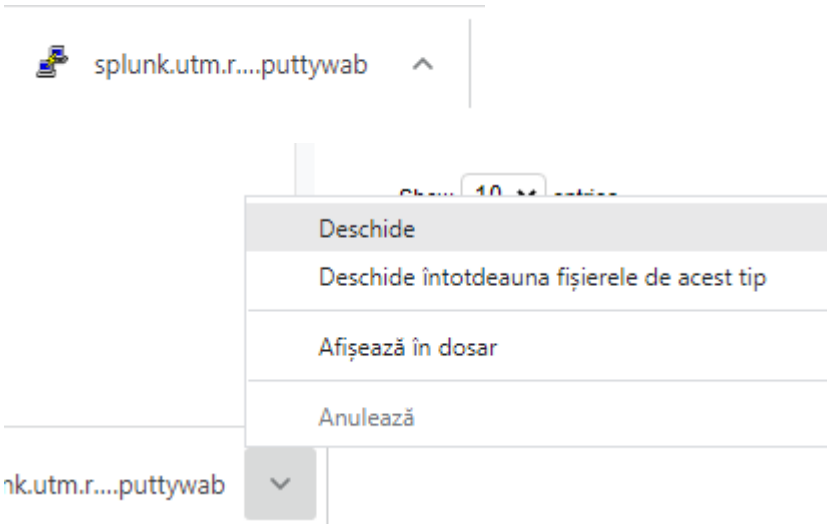
Studentul

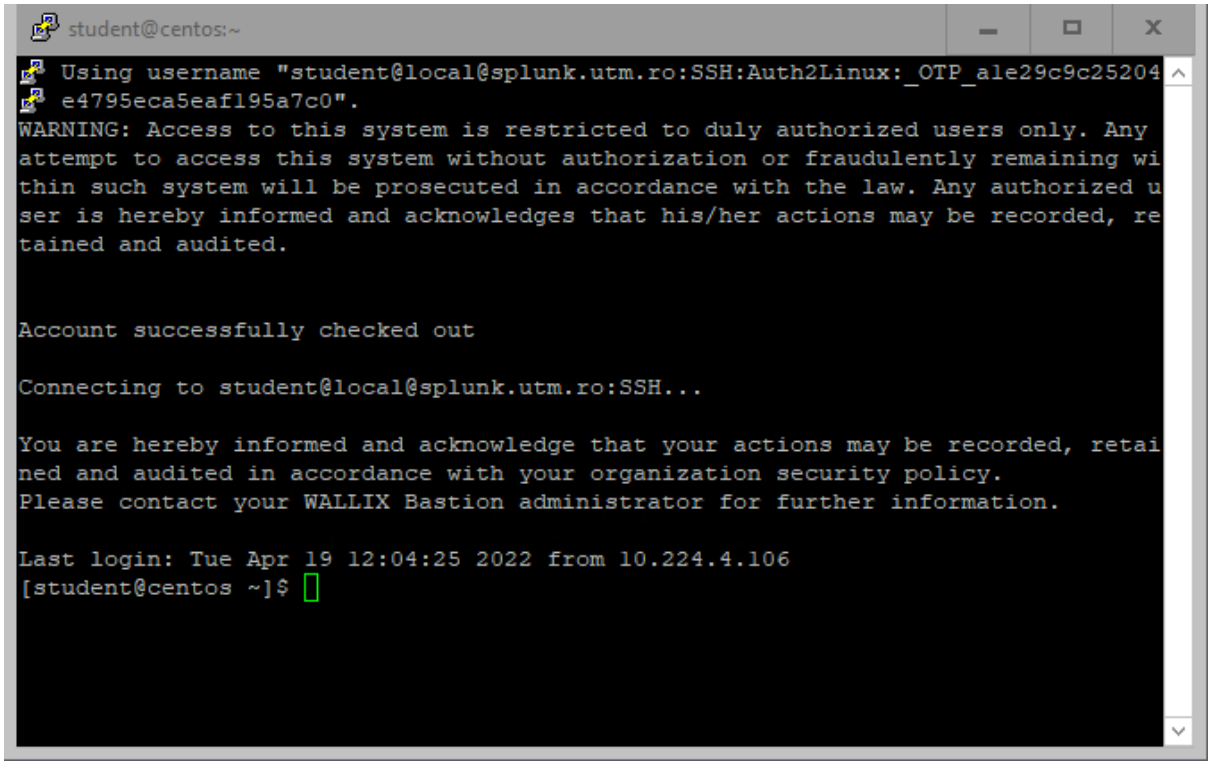
1 . Se conecteaza si vede autorizarile la care are acces



2. Se conecteaza la userul student de pe serverul de splunk→fara parola



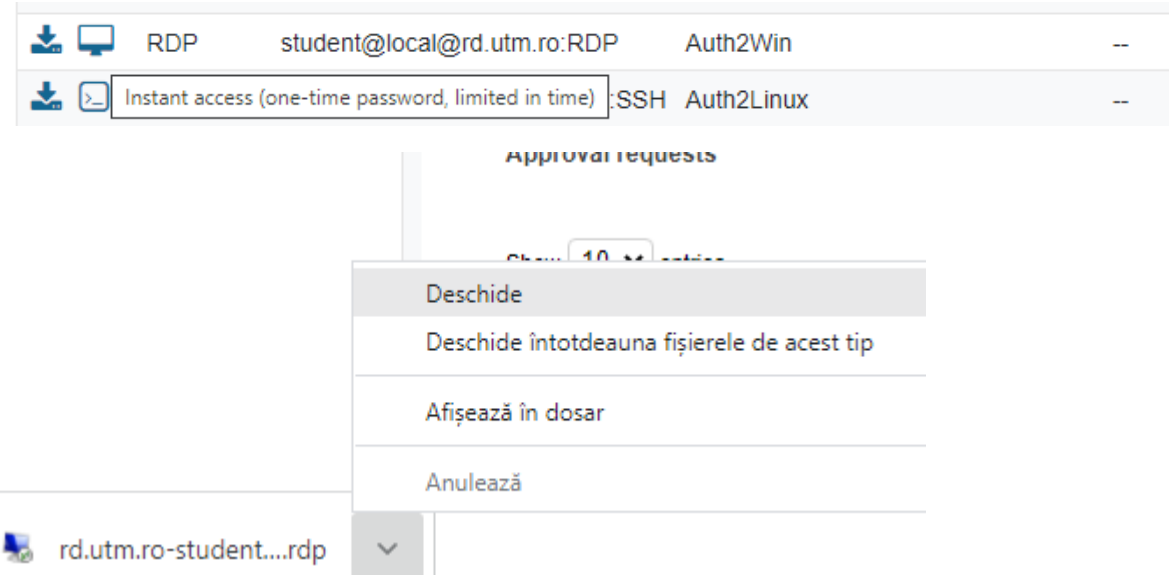


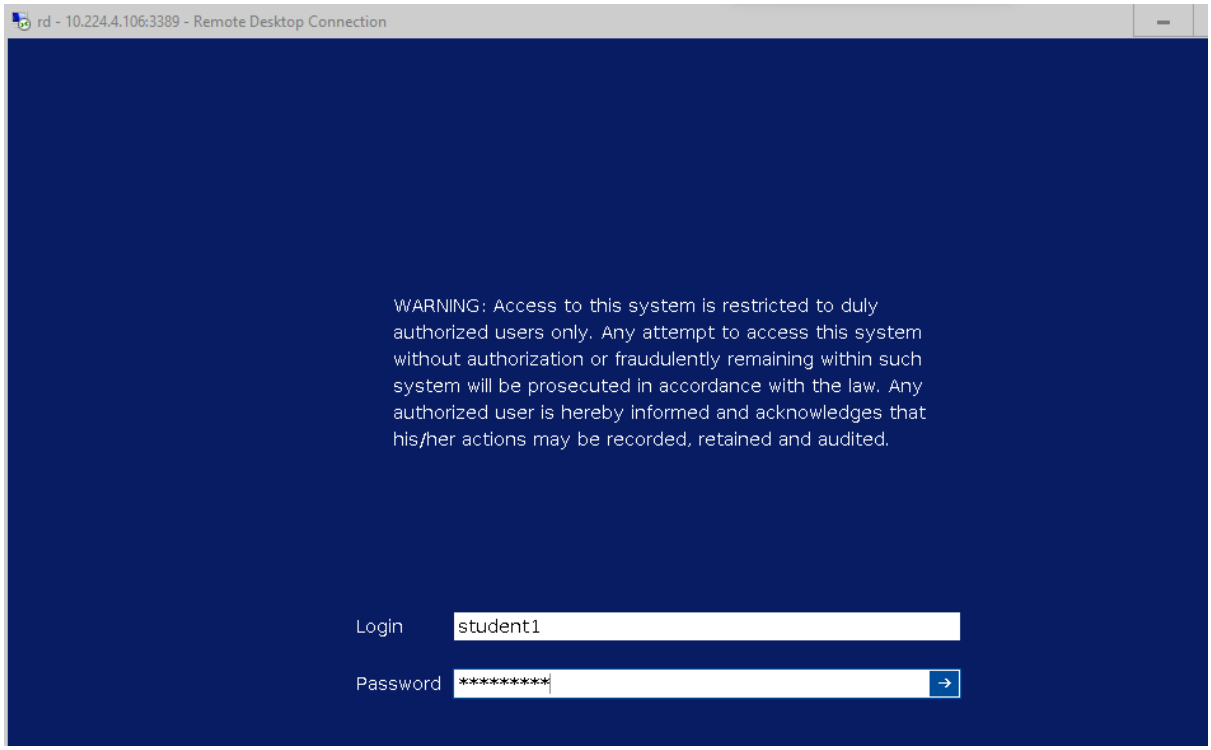


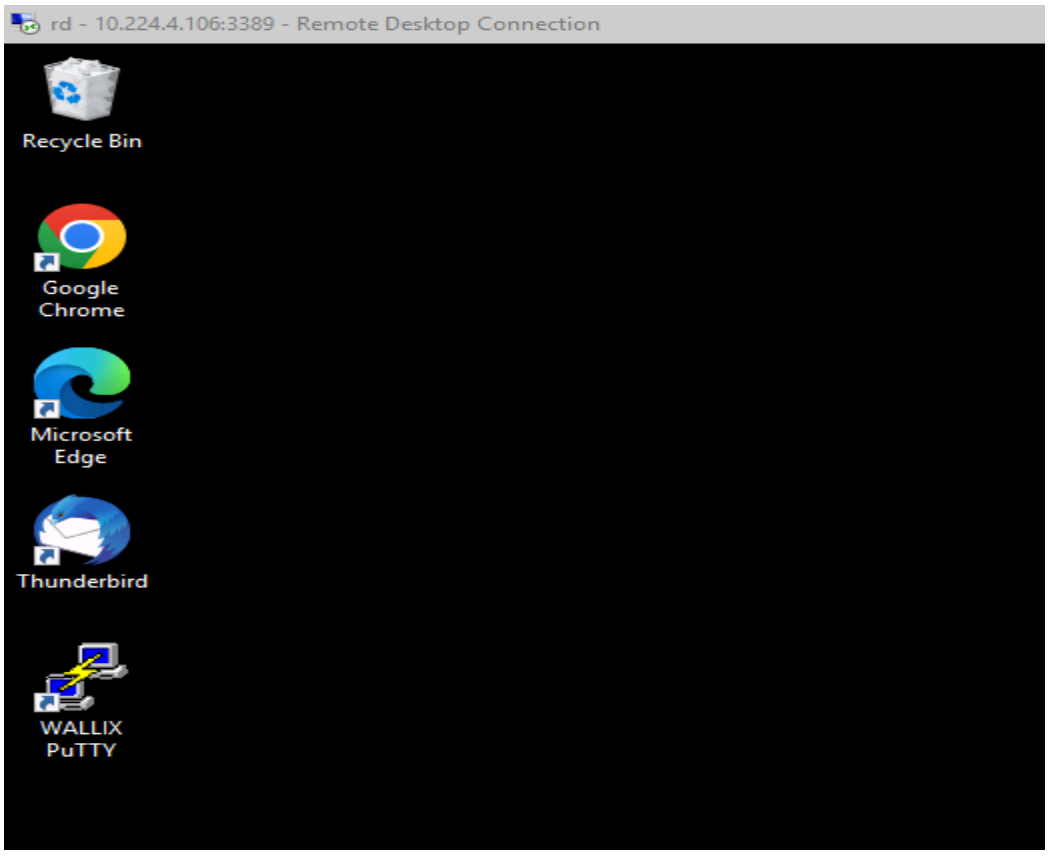
Studentul executa apoi comezile: ls -l / echo / df -h / ifconfig / users / netstat -at

si inchide conexiunea. Studentul nu trebuie modifice parola userului.

3. Studentul se conecteaza la serverul RP tot fara parola

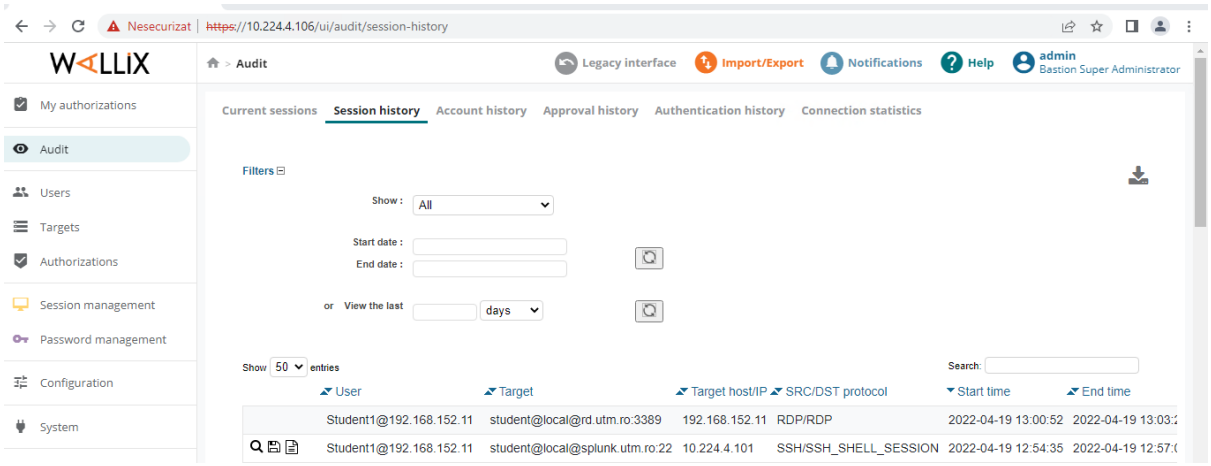


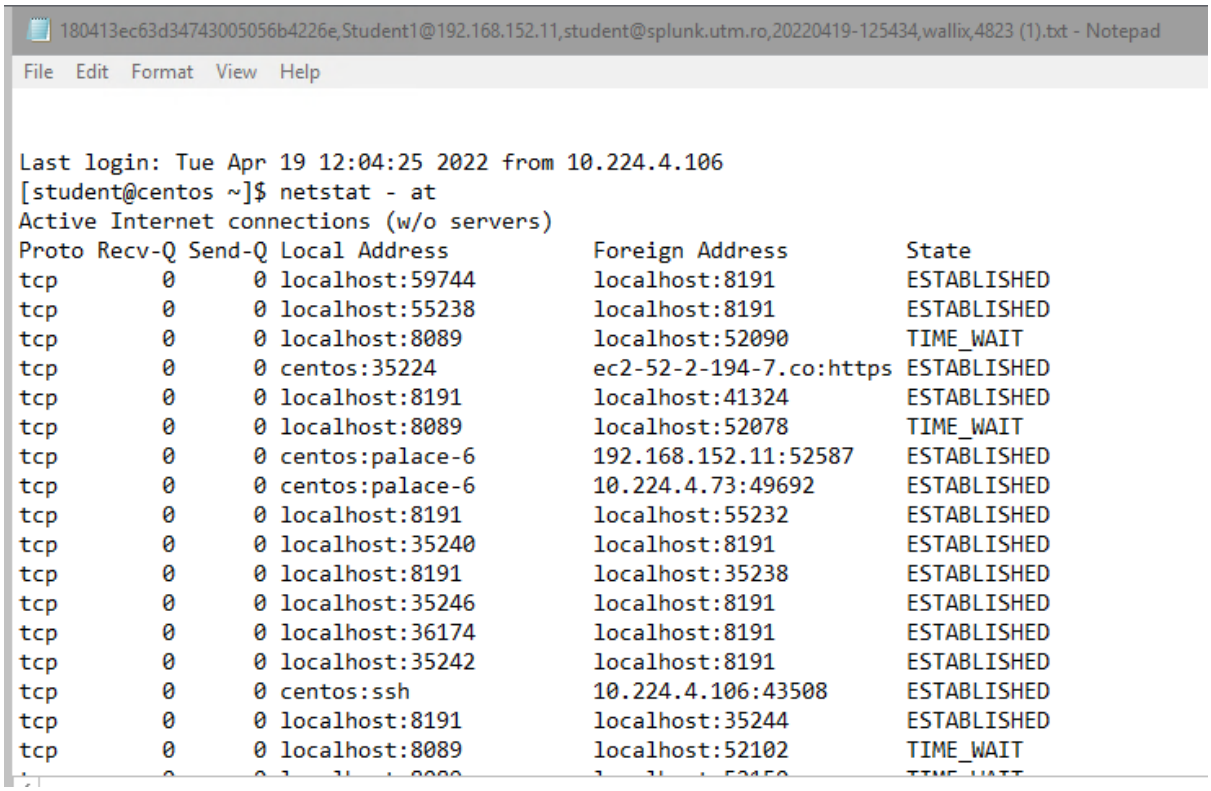


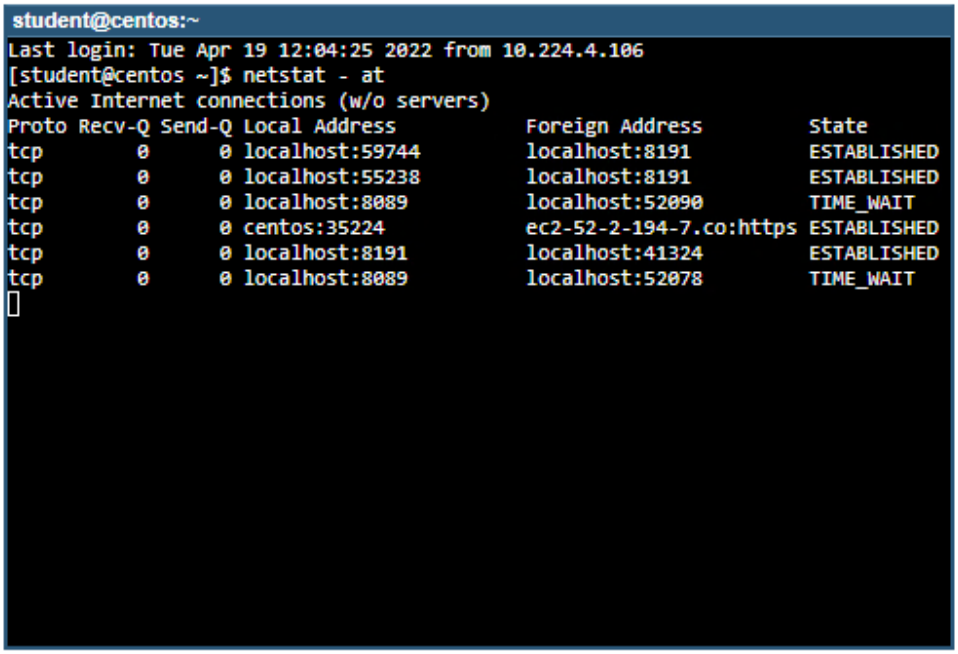


Studentul are access la Putty, Thunderbird etc.

Profesorul→arata studentilor monitorizarea conexiunilor in timp real inclusive comenzile effectuate de student la serverul splunk.


Nesecurizat | https://10.224.4.106/ui/audit/session-history
WALLIX
Audit
Legacy interface
Import/Export
Notifications
Help
admin
Bastion Super Administrator
My authorizations
Audit
Users
Targets
Authorizations
Session management
Password management
Configuration
System
Current sessions
Session history
Account history
Approval history
Authentication history
Connection statistics
Filters
Show : All
Start date :
End date :
or View the last days
Show 50 entries
Search:
User
Target
Target host/IP
SRC/DST protocol
Start time
End time
Student1@192.168.152.11 student@local@rd.utm.ro:3389 192.168.152.11 RDP/RDP 2022-04-19 13:00:52 2022-04-19 13:03:
Student1@192.168.152.11 student@local@splunk.utm.ro:22 10.224.4.101 SSH/SSH_SHELL_SESSION 2022-04-19 12:54:35 2022-04-19 12:57:


180413ec63d34743005056b4226e,Student1@192.168.152.11,student@splunk.utm.ro,20220419-125434,wallix,4823 (1).txt - Notepad
File Edit Format View Help
Last login: Tue Apr 19 12:04:25 2022 from 10.224.4.106
[student@centos ~]$ netstat - at
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 localhost:59744 localhost:8191 ESTABLISHED
tcp 0 0 localhost:55238 localhost:8191 ESTABLISHED
tcp 0 0 localhost:8089 localhost:52090 TIME_WAIT
tcp 0 0 centos:35224 ec2-52-2-194-7.co:https ESTABLISHED
tcp 0 0 localhost:8191 localhost:41324 ESTABLISHED
tcp 0 0 localhost:8089 localhost:52078 TIME_WAIT
tcp 0 0 centos:palace-6 192.168.152.11:52587 ESTABLISHED
tcp 0 0 centos:palace-6 10.224.4.73:49692 ESTABLISHED
tcp 0 0 localhost:8191 localhost:55232 ESTABLISHED
tcp 0 0 localhost:35240 localhost:8191 ESTABLISHED
tcp 0 0 localhost:8191 localhost:35238 ESTABLISHED
tcp 0 0 localhost:35246 localhost:8191 ESTABLISHED
tcp 0 0 localhost:36174 localhost:8191 ESTABLISHED
tcp 0 0 localhost:35242 localhost:8191 ESTABLISHED
tcp 0 0 centos:ssh 10.224.4.106:43508 ESTABLISHED
tcp 0 0 localhost:8191 localhost:35244 ESTABLISHED
tcp 0 0 localhost:8089 localhost:52102 TIME_WAIT



Transcription

```
Last login: Tue Apr 19 12:04:25 2022 from 10.224.4.106
[student@centos ~]$ netstat - at
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:59744         localhost:8191          ESTABLISHED
tcp        0      0 localhost:55238         localhost:8191          ESTABLISHED
tcp        0      0 localhost:8089          localhost:52090         TIME_WAIT
tcp        0      0 centos:35224            ec2-52-2-194-7.co:https ESTABLISHED
tcp        0      0 localhost:8191          localhost:41324         ESTABLISHED
tcp        0      0 localhost:8089          localhost:52078         TIME_WAIT
```