

ىلإ ةدنتسم ةقداصمب ISE SFTP نيوكت ةداهش

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[1. مداخل نيوكت CentOS](#)

[2. عدوتسم نيوكت ISE](#)

[3. مداخل ىلع حيتافم جاوزاً عاشنا ISE](#)

[3-1 ISE GUI](#)

[3-2 ISE CLI](#)

[4 - لماكللا](#)

[ةحصللا نم ققحتلا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

لقن لوكوتورب مداخلك CentOS عيزوت عم Linux مداخل نيوكت ةيفيك دننتسملا اذه حضوي
الوصو (PKI) ماعلا حاتفملا ةيساسألا ةينبالا ةقداصم مداخلتساب (SFTP) نمألا تافلما
لا (ISE) ةيوهلا تامدخ كرحم ىلا.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاللا عيضاوملاب ةفرعم كيديل نوكت نأب Cisco يصوصت:

- ISE نع ةماع تامولعم
- ISE عدوتسم نيوكت
- ةماعلا Basic Linux ةفرعم

ةمدختسملا تانوكملا

ةيلاللا ةيداملا تانوكملا وجماربالا تارادصا ىلا دننتسملا اذه يف ةدراولا تامولعملا دننتست:

- ISE 2.2
- ISE 2.4
- ISE، رادصإلا 2.6
- ISE، رادصإلا 2.7

- ISE 3.0
- CentOS Linux، رادصإلإ 8.2.2004 (Core)

ةصاخ ةي لم عم ةئيب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذ ف ةدراوللا تامولعمل عاشنإ م تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذ ف ةمدختسملا ةزهجالا عيمج تادب رما يال لم تحت حمللا ريثأتلل كمهف نم دكأتلا يجرى ف، ةرشابم كتك بش

ةيساسأ تامولعم

نم PKI تاداهش ربع ةقداصملااب ISE موقى نأ نكمي، تافلما لقن تاي لم عمل نامألا ضرفلو تاعدوتسملا تافلما لىل لوصولل انامأ رثكأ ةقيرط نامضل SFTP لال

نيوكتلا

1. CentOS مداخ نيوكت

1.1. يردج مدختسمك لىلد عاشنإ

```
mkdir -p /cisco/engineer
```

1.2. ني مدختسم ةوعومجم عاشنإ

```
groupadd tac
```

1.3. نأب مدختسملا ددحيو، (تافلما) يسيئرلا لىلدلا لىل مدختسملا رمالا اذ ف فيضي ةوعومجملا يسنهه لىل يمتنى

```
useradd -d /cisco/engineer -s /sbin/nologin engineer  
usermod -aG tac engineer
```

ليجست نم نكمتي نل مدختسملا نأ لىل رمالا نم `/sbin/nologin` عزج ريشي: **ةظالم** (SSH) نامألا ةقبط لال نم لوخدلا

1.4. تافلما لىمحتل لىلدلا عاشنإ لىل لقتنا

```
mkdir -p /cisco/engineer/repo
```

1.4.1. لىلدلا تافلما تانوذال نيغت

```
chown -R engineer:tac /cisco/engineer/repo  
find /cisco/engineer/repo -type d -exec chmod 2775 {} \+  
find /cisco/engineer/repo -type f -exec chmod 664 {} \+
```

1.5. تاداهشلا نم ققحتلاب CentOS مداخ هي ف موقى يذلا فلملاو لىلدلا عاشنإب مق

لىلدلا:

```
mkdir /cisco/engineer/.ssh
chown engineer:engineer /cisco/engineer/.ssh
chmod 700 /cisco/engineer/.ssh
```

فلمل:

```
touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
```

1.6. sshD_config. ماظن فلم ي ف لوخدلا ليجست تانوذأ عاشنإب مق

رمأ اذه عم ةادأ vim Linux ل تلمعتسا عي طتسي تنأ، فلمل ترحر in order to

```
vim /etc/ssh/sshd_config
```

هاندأ ةددحملا دونبلا ةفاضإ 1-6-1.

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
Match Group tac
ChrootDirectory %h
X11Forwarding no
AllowTCPForwarding no
ForceCommand internal-sftp
```

1.7. ssh_config. ماظن فلم ةنمازم نم ققحتلل رملال ليجشتب مق

```
sshd -t
```

ةجحص فلملا ةغايص نأ ينع ي جارخا دجوي ال: ةظالم

1.8. SSH. ةمدخ ليجشت ةداعإل ةعباتملاب مق

```
systemctl restart sshd
```

كنكمي، ةملعمل هذه ديكأتل، Selinux قيبطت لىع Linux مداوخ ضعب يوتحت: ةظالم
لىل اهرغت اهنإف، ذافنإل اعضوي فننك اذا، ةيصوتك و. getenforce رملال مادختسا
ةلهاستم.

1.9. حمسي لىع ذافنإل ةيلمع نييعتل semanage.conf فلم ريرحتب مق (يرايخا).

```
vim /etc/selinux/semanage.conf
```

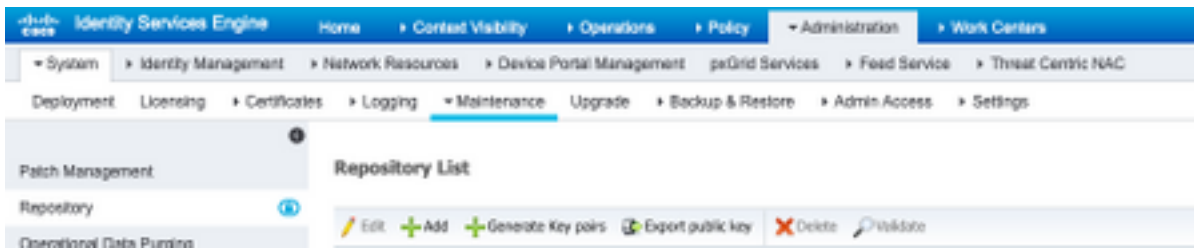
setenforce0 رملال ةفاضإب مق

```
setenforce0
```

2. ISE عدوتسم نيوكت

2.1. ISE (GUI) ةيموسرلا مدختسمل اةجاو لالخنم عدوتسمل ةفاضإ لىل لقتنا.

Add > عدوتسم ةفاضإ > ماظنلا ةنايص > رادإل لىل لقتنا



2.2. إعداد مستعمل نوي وكالت لخدأ.

[Repository List](#) > [Add Repository](#)

Repository Configuration

* Repository Name

* Protocol

Location

* Server Name

* Path

Credentials

* Enable PKI authentication

* User Name

* Password

رذجل ليلدل نم الدب عارشلل ةداع ليلد لى لوصولا لى ةجأب تنك اذا: **ةظحالم** /repo/ فدهل راسمل نوئي نا بجي، سدنهملل

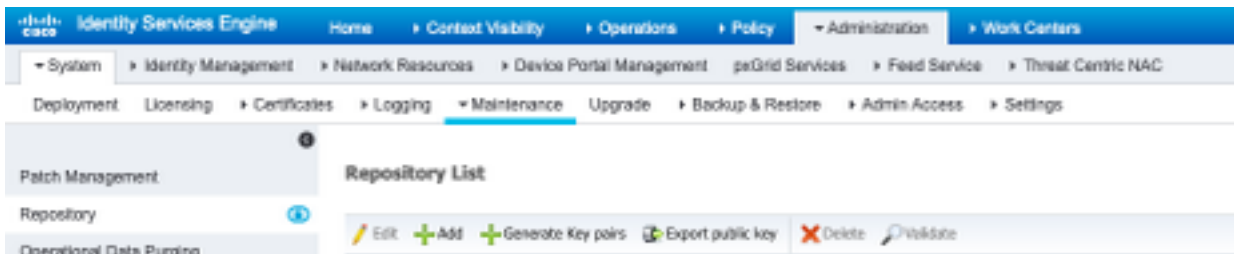


3. مداخل حيتافم جاوزا عاشن إ ISE

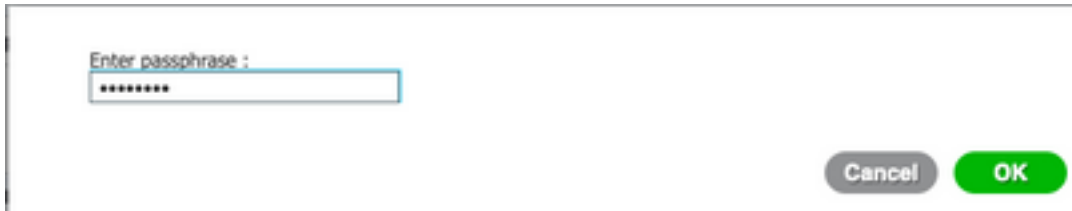
3-1 ISE GUI

في حضورم وه امك، حيتافم جاوزا عاشن إ مق > عدوت سمل > ماطنللا ةنايص > رادا لى لقتنلا ةروصللا.

ةهجاوو (ISE) ةيموسرللا مدخت سمللا ةهجاو نم حيتافم جاوزا عاشن إ كيلع بجي: **ةظحالم** عدوت سمللا لى لى لك هاجتاللا يئانث لوصولو لى لوصولل (CLI)، رماوالا رطس.



3.1.1. حيت افم ل جوز ةي ام حل بولطم اذو، رورم ةراب ع لخدأ.

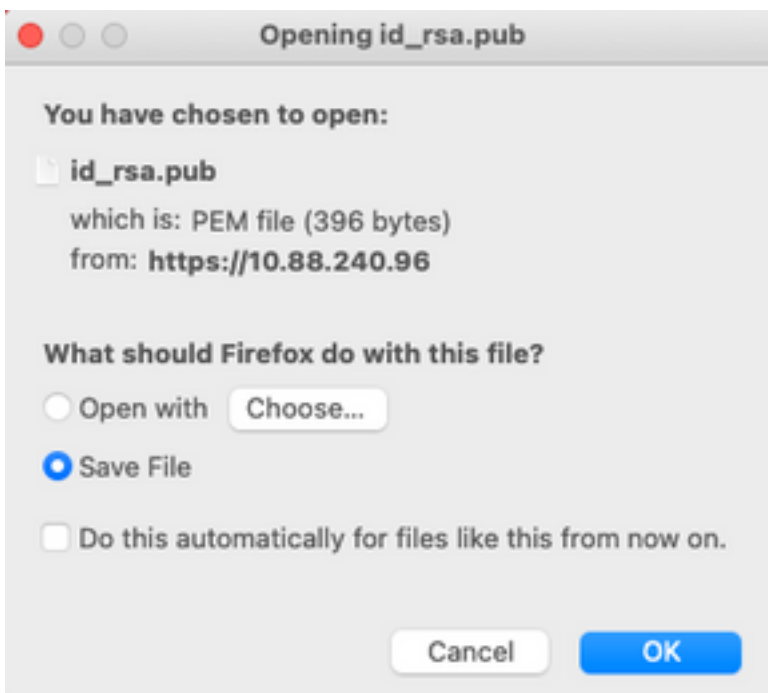


ةم اع ل حيت افم ل ري دصت ل بق حيت افم ل اوزأ عاشن اب الوأ مق :ةظ حالم

3-1-2- م اع ل حات فم ل ري دصت ي ف ام دق ي ضم ل.

م اع ل حات فم ل ري دصت > عدوت س م ل > م اظن ل ةناي ص > ةراد ل ل ل ل ل ق ت ن ا

ع جارم ل ل رم ال اذو ظف ح نم دكأت) id_rsa.pub م ساب فلم عاشن ل متي . م اع ل حات فم ل ري دصت دح (ةي ل بق ت س م ل).



3-2 ISE CLI

3.2.1. اهي ف عدوت س م ل ني وكت ءاهن ل دي رت ي ت ل ةدق ع ل اب صا خ ل ال CLI ل ل ل ق ت ن ا.

ي ف ب غرت ةدق ع ل ل ةي ل ل ل ل ا و ط خ ل ل ا ذ خ ت ل م ز ل ي ، ا د ع ا ص ف ة ط ق ن ل ل ه ذه نم :ةظ حالم
PKI ة ق د ا ص م م ا ذ خ ت س اب SFTP عدوت س م ل ل ل ل و ص و ل اب ح ا م س ل ل

3.2.2. ماطن فلم ىل Linux مداخ ب صاخ ال IP ناو نع ةفاض لجا نم رمأل اذه ليغشت ب مق `host_key`.

```
crypto host key add host <Linux server IP>
ise24https/admin# crypto host_key add host 10.88.240.102
host key fingerprint added
# Host 10.88.240.102 found: line 2
10.88.240.102 RSA_SHA256:sFA1b+NujB8NxIx4zhS/7Fj1hyHRkJLKyLhJCLteSpE
```

3.2.3. ماع CLl حات فم ءاشن ا.

```
crypto key generate rsa passphrase <passphrase>
ise24https/admin# crypto key generate rsa passphrase admin123
```

3.2.4. رمأل اذه مادختساب ISE ب صاخ ال CLI نم ةماع ال حيات فم ال تافلم ري دصت .

```
crypto key export <name of the file> repository <repository name>
```

كنكمي يذلا واقبسم هي لوصول نكمي عدوتسم كي دل نوكي نأ بجي :ةظحال م
هي لماع ال حات فم ال فلم ري دصت .

```
ise24https/admin# crypto key export public repository FTP
```

4 - لم اكلال

4.1. م داخ ىل ل وخذل ل جس CentOS.

`authorized_key` فلم ال ني وكت ب اق بسم هي ف تم مق يذلا دل جم ال ىل لقتنا

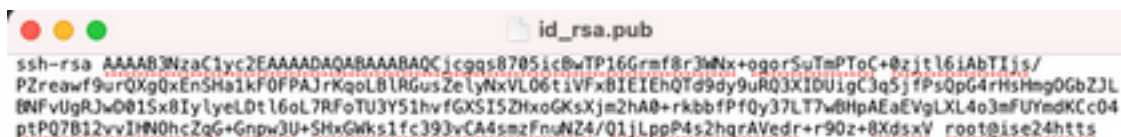
دمت عم ال حات فم ال فلم ري حت -2-4

فلم ال لي دع تل vim رمأل ليغشت ب مق

```
vim /cisco/engineer/.ssh/authorized_keys
```

حيات فم ال جاوزأ ءاشن ا مسق نم هقصلو و6 و4 تا واطخال نع جتان ال ىوت حمل ا خسنا .3-4

ISE: ب ةصاخ ال (GUI) ةي م و سرل ا مدختس م ال ةه جاو نم ماع ال حات فم ال ءاشن ا مت



```
id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcjc9gs8705ic8wTP16Grmf8r3Mnx+ogorSuTmPToC+0zjt16iAbTIjs/
PZreawf9urQXg0xEnSHa1kF0FPAJrKqoLBlRGusZelyNxVL06t1VFx8IEIEhQTd9dy9uRQ3XIDUigC3q5jFPs0pG4rHsHmg0GbZJL
BNFvUgRjw0015x8IylyeLdt16oL7RFoTU3Y51hvfGXSI5ZhxGKsXjm2hA0+rkbffPfqy37LT7w8HpAEaEVgLXL4o3mFUrdKCc04
ptPQ7B12vvIHnQhcZqG+Gnpw3U+SHxGwks1fc393vCA4smzFnuNZ4/Q1jLppP4s2hqrAVedr+r90z+8XdsxV root@ise24https
```

ISE: رمأل ال رطس ةه جاو نم ءاشن ا مت يذلا ماع ال حات فم ال

```
public
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCAH+5ANAYb47+NXFyuz06s0+gSykTRrGfdMryIiitCwBs0bGs5yc9S8VKpLyyocsIvco4/
vF/pSHoTE1R3wrZTL1vCIUrGnnqdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQB886tkno40cmT/
HAYXQ/a9YRZ1l29D6pjK5WyuTkbUxwVn9hx/
5E5zp34pFr9opq+UaTNX0yYuuJ328FGFEfDKuFBSuJAokP0nJTLN8GdLAQ6x4kkkcXWxkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm
D0Cj6vMaV0L7GZdDI4NZHn7llpptqJFYAb65QB admin@ise24https
```

Authorized_key file سكونيل مداخل لىع:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAH+5ANAYb47+NXFyuz06s0+gSykTRrGfdMryIiitCwBs0bGs5yc9S8VKpLyyocsIvco4/vF/pSHoTE1R3wrZTL1vCIUrGnnqdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQB886tkno40cmT/HAYXQ/a9YRZ1l29D6pjK5WyuTkbUxwVn9hx/5E5zp34pFr9opq+UaTNX0yYuuJ328FGFEfDKuFBSuJAokP0nJTLN8GdLAQ6x4kkkcXWxkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zmD0Cj6vMaV0L7GZdDI4NZHn7llpptqJFYAb65QB admin@ise24https
:~$ cat /etc/ssh/authorized_keys
:~$ tail -f /var/log/secure
:~$
```

4.4. رمأل لىغشت لى لىقتنا، ESC حاتفم طغضا، فلمل لىف حىتافم لى قصلب موقت نأ دعب. فلمل لىظفح wq!

ةحصلال نم ققحتال

1. رىچك رمأل اذذ ذىفنتب مق سكونيل مداخل نم.

```
tail -f /var/log/secure
```

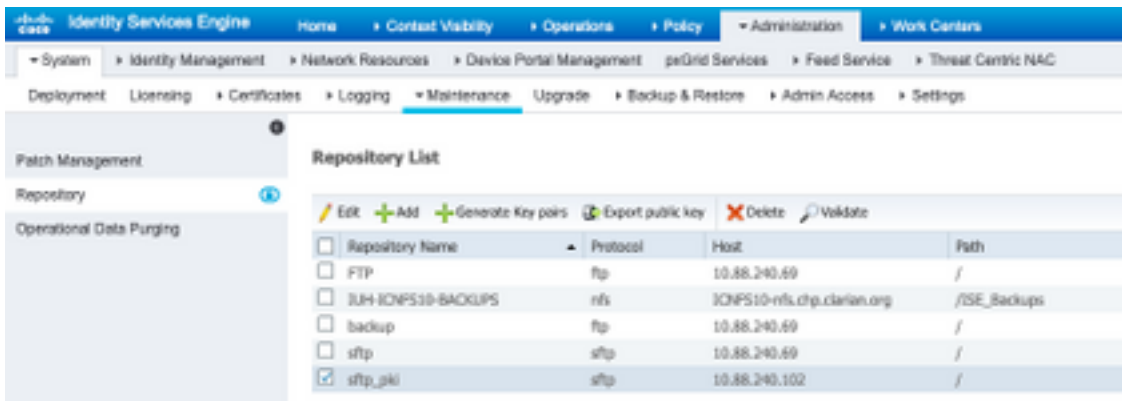
ةروصلال لىف حضوم وه امك، جارخال لىضرع بىچى.

```
[[root@localhost ~]# tail -f /var/log/secure
Apr 12 21:37:53 localhost sshd[668112]: Accepted publickey for root from 10.24.140.234 port 61159 ssh2: RSA SHA256:MNHNp2AtvX080bTswgPLK0G8awFUue
GbKEWIEkcaeXU
Apr 12 21:37:53 localhost systemd[668117]: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668112]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtvX080bTswgPLK0G8aw
FUueGbKEWIEkcaeXU
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
```

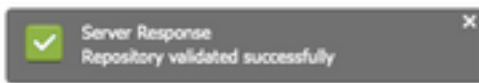
2. ةىوهال تامدخ كرحم تاصاصتخا نم ققحتال لى.

ةىموسرل ملىدختس ملة هجاو لىع عدوتسم Administration>System>Maintenance لى لىقتنا

ةحصلال نم ققحتال لىدحو عدوتسم لىملىق نم هىف بوغرمل عدوتسم لىدحو.



ةشاشلا نم ىنم يلا ةيوازلا لفسأ يف مداخللا ةباجتسا حضوت ةقثب نم ىرت نأ بجي.



ةحص نم ققحتلل `show repo sftp_pki` رمأل ليغشتب مق، (CLI) رمأوالا رطس ةهجاو نم حيتافملا.

```
ise24https/admin# show repo sftp_pki
repo
```

in order to ىلج رمأ اذه تذفن ISE، تححص يف اضا:

debug transfer 7

ةروصلا يف حضوم وه امك، جارخال اضرع بجي:

```
ise24https/admin# debug transfer 7
ise24https/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] [admin]: sftp dir of repository sftp_pki requested
6 [16745]:[info] transfer: cars_xfer_util.c[2298] [admin]: resolved server to 10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[1027] [admin]: Running sftp command: 10.88.240.102 engineer *** /repo/ ls -l /repo/
6 [16745]:[info] transfer: sftp_handler.c[554] [admin]: DEBUG: local user: admin UID: 0 sftp_run_parent FD: 5 remote host: 10.88.240.102 remote user: engineer comm
nd: ls -l /repo/
7 [16747]:[debug] transfer: sftp_handler.c[268] [admin]: Executing SFTP command: 0 admin /usr/bin/sftp -oIdentityFile=/home/admin/.ssh/id_rsa -oUserKnownHostsFile=/
home/admin/.ssh/known_hosts -oPasswordAuthenticationno engineer@10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[586] [admin]: fd is 5
7 [16745]:[debug] transfer: sftp_handler.c[461] [admin]: Found sftp prompt; No more data to read
7 [16745]:[debug] transfer: sftp_handler.c[917] [admin]: sftp parent status 0
7 [16745]:[debug] transfer: cars_xfer_util.c[2315] [admin]: ssh_list xfer succeeded
% Repository is empty
```

ةلص تاذا تامولعم

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin/guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01011.html

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ل ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة يرش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا