

ةطقنل ةيرهاظلا ةصاخلا ةباحسلا تيبتت اهنيوكتو ةنمآلا ةياهنلا

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[VPC رشن](#)

[يرهاظلا زاهجل بيكرت](#)

[ةيلوآلا لوؤسملا ةهجاو دادعا](#)

[بيولا ربع \(GUI\) ةيموسرلا مدختسملا ةهجاو لالخ نم VPC رتوي بمكل ةيلوآلا ةيهةتلا](#)

[نيوكتلا](#)

[تامدخلا](#)

[AirGap شيدحت ةمزح](#)

[تانايابلا نزخم يف ةدفنتسم ةحاسم - 1 مقرر ةلكشملا](#)

[ميدقلا شيدحتلا - 2 مقرر ةلكشملا](#)

[يساسألا لكشب اهخالص او اعطخال افاشك تسأ](#)

[DNS و FQDN مداخ - #1 ةلكشملا](#)

[رذخلاق دصملا عجرملا عم ةلكشم - 2 مقرر ةلكشملا](#)

ةمدقملا

ESXi ةئيبي في مداوخاليلع (VPC) Virtual Private Cloud رشن ةيفيكي دننتسملا اذه فصبي عيرسلا ادبلا ليلد لثم يرخال قئاثولل ةبسنلاب .كلذ ةيفيكي ليلع زكري و حاجنب يجرى ، لوؤسملل مدختسملا ليلدو مكنحتلا ةدحوو قاقحتسالا ليلدو رشنلا ةيجيتارتساو عقوقملا اذه [قئاثو](#) ةرايز

Cisco نم TAC وس دنهم ، اتنلاف نامور ةطساوب ةمهاسملا تمت

ةيساسألا تابلطتملا

تابلطتملا:

شدا رادصا و VMware ESX 5 جمانرب

- ةدحول زكارم 8 و تياباچي 128 ةعسي ئاوشع لوصولو ةركاذ : (طقف) ةكبشلا ليلكو عضو الضاف ، (امهنم لكل ابي صوم زكارم 4 عم CPU) ةيزكرم ةجلاعم اتدحو) ةيزكرملا ةجلاعمل VMware تاناياب نزخم يف يندأ دحك تياباري ت 1 غلبت ةرح صرق ةحاسم نع
- (SSD) ةبلص تانوكم نم ةعونصم ةركاذب ةدوزم صارقأ تاكرحم : صارقألا تاكرحم عون ليلكولل ابي صومو ةيئاوهلا تارغثلا عضول ةبولطم
- (ةططخم ةآرم) ةدحاو RAID 10 ةعومجم RAID: عون
- تياباري ت 2 VMware تاناياب نزخم مجحل يندألا دحلا
- RAID 10 (4 وليك) ةعومجمل تانايابلا تاططخمل ةيئاوشعلا تاءارقولل يندألا دحلا

VPC رشن

ليزنت. قاقحتسالا ةلاسروا ميسلسلل ينورتكلإلا ديربلا يف رفوتملا URL ناونع ددح تيبتتلا ةعباتم و OVA فلم

يره اظلال زاوجل بيكرت

1: ةوطخلال

ةروصللا يف حضوم وه امك، OVF بلاق رشن جلاعم حتفل OVF بلاق رشن > فلم لىلا لقتنا

New virtual machine - AMP-vPC

- 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× PrivateCloud-Latest.ova

Back Next Finish Cancel

New virtual machine

1 Select creation type

2 Select OVF and VMDK files

3 Select storage

4 License agreements

5 Deployment options

6 Additional settings

7 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file**
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

vmware

Back Next Finish Cancel

New virtual machine - AMP-vPC

1 Select creation type

2 Select OVF and VMDK files

3 Select storage

4 License agreements

5 Deployment options

6 Additional settings

7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	Supported	Single
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	Supported	Single

4 items

vmware

Back Next Finish Cancel

✎ رايخلا اذه ديحتب تمق اذ. صرق عاشن دن عحاسمب كي مسلا دادعلا ظفتحي: عطحالم دح نألا. ايمازل سيل كلذ نإف، كلذ عمو. دوزملا عي فر نم رثكأ عادألا نيسحت هنكمي ف

✎ ةروصلال ي ف حضم وه امك ،يلالال عل

New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- 5 Ready to complete

Deployment options

Select deployment options

Network mappings	VM Network	VM Network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick	

vmware

Back Next Finish Cancel

2: ةوطخال

OVA تاملعم ةظحال م كنكمي .يلالال عل دح م ث ،OVA فلم دي دحتل ..ضارعتسإ دح .يلالال ي ف دح .ةروصلال ي ف حضم وه امك ،OVF بلاق ليلصافت ةحفص ي ف ةيضارتفال


New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

vmware

Back Next Finish Cancel

ةيلوآل لوؤسملآ ةهآو دادعإ


New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6.5_signed-disk4.vmdk
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

vmware

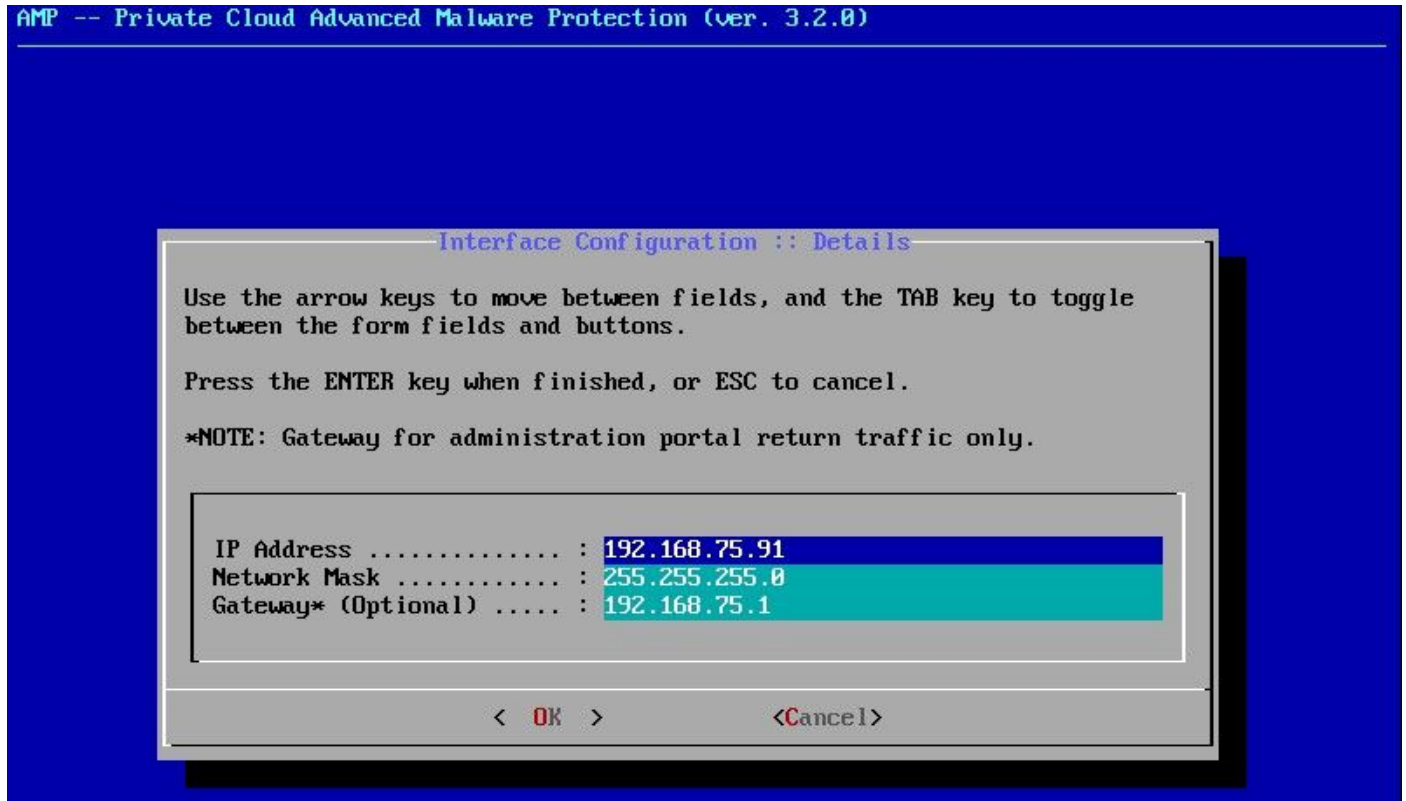
Back Next Finish Cancel

مكحتلآ ةدحو لآلآ نم يلوآلآ نيوكتلآ ءارآ ك نكمي (VM) ةيضرآرتفآلآ ةزهآلآ ديهمآ درجمب

ةيضا رتف الةزه أال ي ف (VM).

ةوطخال 1:

ءا رل ال DHCP مءا م IP ناونع ةهءاولا قللت مل اءا [نوكم ريغ] رهظي URL ناونع نأ طءالء ءق ءا نإل ةهءاو ءسيل هءه . ةراءال ةهءاو يه ةهءاولا هءه نأ ةظءال مء



ةوطخال 2:

مهس أال او Enter و Tab ءي ءافم لالء ل قنءل ال كنكم ي.

IP ناونع نيوكء ءءبل ءي ءافم ل ءءول ل ءل ء enter ءا ءافم ءءو config_network ل ل قنءنا ءءءف ، DHCP مءءءس إءيرء ال ءنك اءا . ءنم آال ءي اءنل ءطقنل ءصاءال ءبءءس ل ءراءاب صاءال ل. اءءا ءا ءافم ءءو ال

Interface Configuration :: Mode

Would you like to configure your interface with DHCP?

< Yes >

< No >

Main Menu

Your AMP Private Cloud device can be managed at:

URL : https://192.168.75.208

MAC Address ... : 00:0c:29:a6:4a:11

Password : PGBd~HbCgZ

The password shown above has been automatically generated for you. You will be required to change this password when you first login.

CONFIG_NETWORK Configure the Web administration interface.

CONSOLE Start command line console / shell.

INFO Display device status / information.

ESC

68%

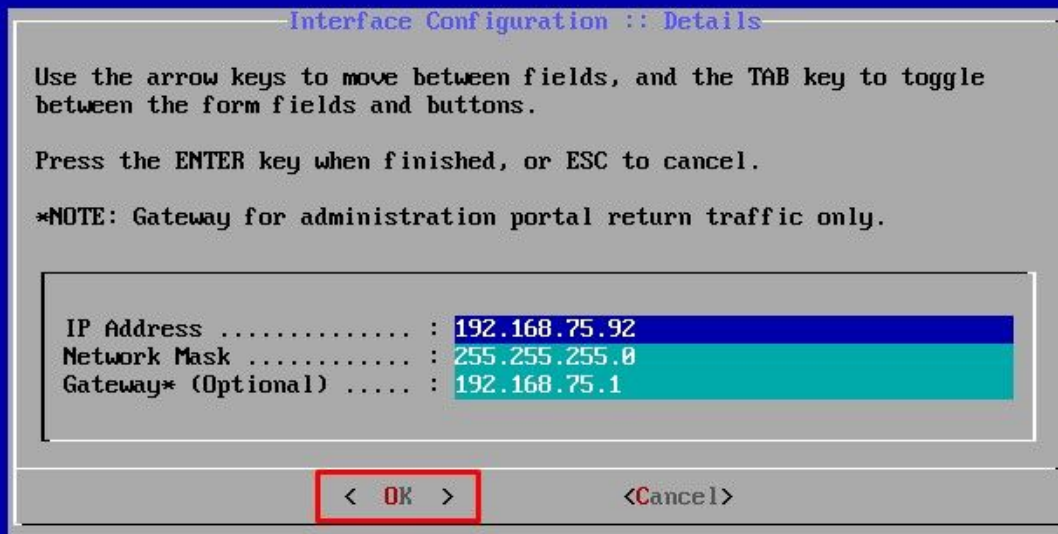
< OK >

حاجات فم لاخدا ددحو معن رتخأ، رهظت يتلا ةذفاننلا يف.



دعوة طاسبب. اذہءاطخألا ل جس عم كم لماعتلا متيسف ، لعفلاب مادختسالال دي ق IP ناك اذا
مادختسالال دي ق سيلو اديرف ائيش رتخاو.

```
Restarting eth0...  
  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) already uses address 192.168.75.91.  
=====  
ERROR: The interface failed to reconfigure.  
=====  
Press ENTER key to continue...  
-
```



اذكە ودبت تاجرخم یرتس، ماري ام یلع عيش لك راس اذإ

```

- execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
* execute[ConfigurePokedLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
* execute[ConfigureCloudLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/cloud/log(/.*)?"
* execute[ConfigureEventLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/event_log_store(/.*)?"
* execute[RestoreSELinuxFileContextData] action run
- execute restorecon -R /data
Recipe: base::ssh
* templated[etc/ssh/sshd_config] action create
- update content in file /etc/ssh/sshd_config from c85f41 to badlab
--- /etc/ssh/sshd_config      2021-04-09 13:25:01.969995024 +0000
+++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.889389544 +0000
@@ -18,7 +18,7 @@
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
-ListenAddress 192.168.75.208
+ListenAddress 192.168.75.92

# The default requires explicit activation of protocol 1
Protocol 2
- restore selinux security context
* templated[etc/ssh/ssh_config] action create (up to date)
* service[ssh_server] action enable (up to date)
* service[ssh_server] action start (up to date)
Recipe: base::grub-conf
* cookbook_file[etc/default/grub] action create (up to date)
* execute[Update grub if new kernel installed] action run (skipped due to only_if)
* execute[Ensure grub menu displays Cisco not CentOS] action run (skipped due to only_if)
Recipe: base::transparent-hugepages
* execute[disable transparent hugepage] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/enabled
* execute[disable transparent hugepage defrag] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/defrag
* execute[disable transparent hugepage for default kernel] action run

```


Restarting eth0...

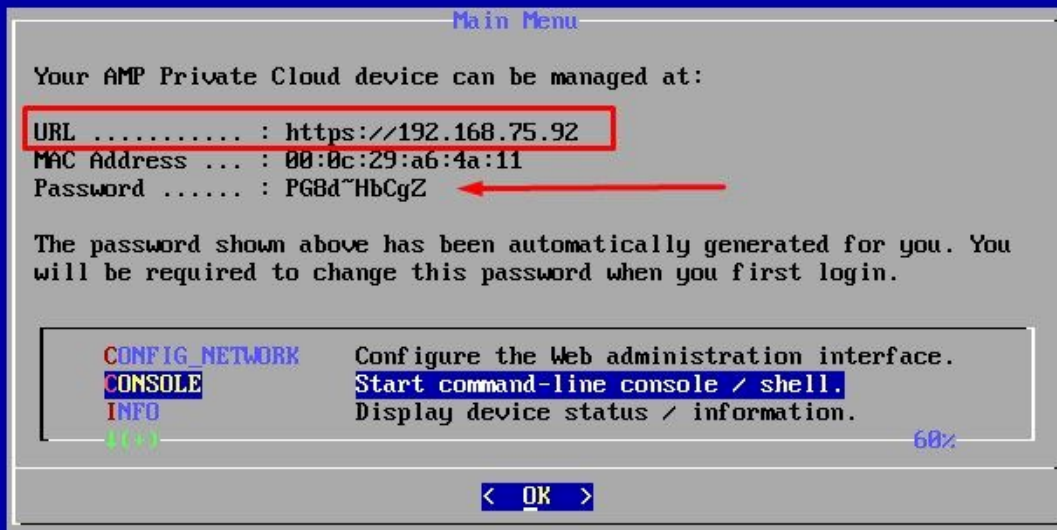
Reconfiguring...

```
[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in your configuration file to configure :disabled_plugins for ohai.  
[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in your configuration file to configure :disabled_plugins for ohai.  
Starting Chef Client, version 12.14.89
```

3: ةوطخل

ةظحال ماضي أءارلا. كيدل ديدجل تباثل ال IP عم ىرخأ ةرم ءاقرزلا ةشاشل رهظت ىتح رظتنا انيدل ضرعتسمل حتفن انوعدو ةظحال م نود. ةءاولا ةرمل رورم ةملك

AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

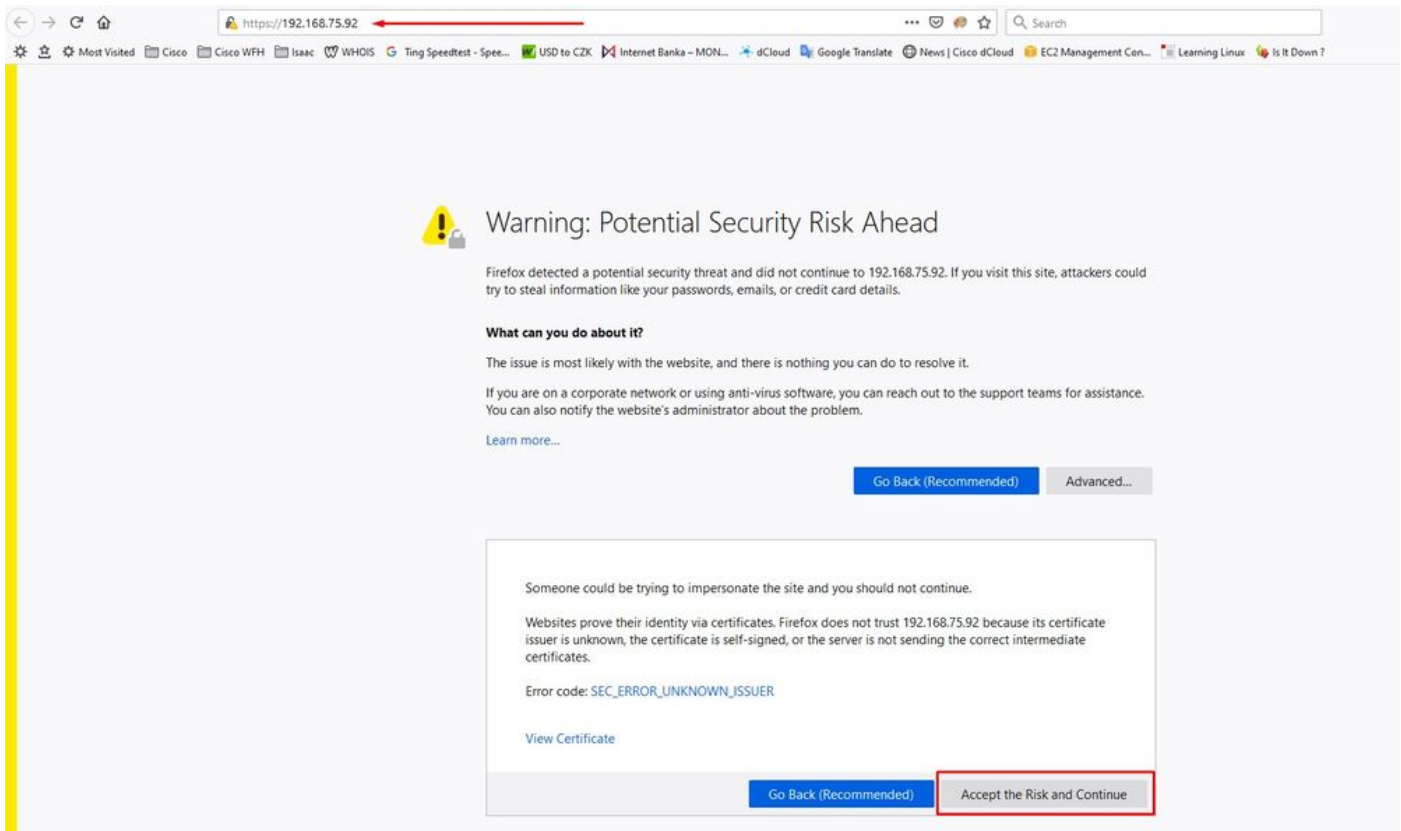


ربع (GUI) ةيموسرل مدختسمل ةءاو ربع vPC رتوي بمك لل لوال نيوكتل بيولا

1: ةوطخل

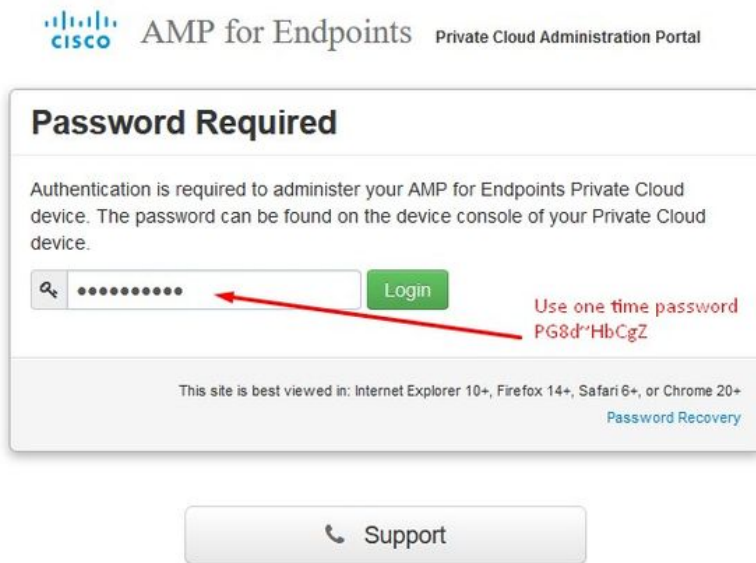
يف أطخ ىقلت كنكمي. زاهجال ةراداب صاخ ال IP ناو نع ىل لقت ناو بيو ضرعتسمل حتفا هب ةصاخ ال HTTPS ةءاش ءاشناب Secure Endpoint Private ةءاش ةءاش ال HTTPS ةءاش ىف قثيل ضرعتسمل نيوكتل مق. ةروصل ىف حضوم وه امك، ائىءبم ةنمآل ةءاهنل طاقن ةءاشب ةصاخ ال اءاذ ةءومل

اقبس مهن يوك تب تمق يذلا تب اثل ال IP ،كب صاخ ال ضرعت سمل ا عون يف



2: ةوطخ ال

نم ةي لوالا رورم ال ةم لك مدخت س أ. رورم ال ةم لك ني عت ةداع ا كي لع بجي ،لوخدلا لي ج ست دع ب ةم لك لقح يف ةدي دجال ك رورم ةم لك مدخت س أ. ةم يدق ال رورم ال ةم لك لقح يف مكحت ال ةدحو ريغت يلع دح . ةدي دجال رورم ال ةم لك لقح يف ةدي دجال رورم ال ةم لك لاخذ ا دع . ةدي دجال رورم ال رورم ال ةم لك



3: ةوطخال

نم ةيولوال رورملا ةملك مدختسأ. رورملا ةملك نييعة ةداعإ كيلع بجي، لوخدلا ليحست دعب ةملك لقح يف ةديدل رورم ةملك مدختسأ. ةميدقلا رورملا ةملك لقح يف مكحتلا ةدحو ريغت ىلع دح. ةديدل رورملا ةملك لقح يف ةديدل رورملا ةملك لاخدإ دعأ. ةديدل رورملا رورملا ةملك.

The screenshot shows the AMP for Endpoints Private Cloud Administration Portal interface. At the top, there is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. A yellow warning box at the top left contains the text 'Password Expired' with a red arrow pointing to it. Below this, a message instructs the user to change the password used to access the portal and the device console, noting that it is also the root password. A 'Warning' box below states that the device password is used for authentication and that complex passwords may not be pasted into the console. The password change form consists of three input fields: the first is labeled 'Old one time password', the second is for the new password, and the third is for the confirmation password. A 'Change Password' button is located at the bottom of the form.

4: ةوطخال

دح. صيخرتلا ةيقافاتإ لوبقول لفسألا ىلإ لفسأل ريرمتلاب مق ةيولاتلا ةحفصلا يف هيلع ةقفاوملاو هتءارقب تمق يذلا ىلع.

The screenshot shows a consent form with two buttons: a green button labeled 'I HAVE READ AND AGREE' and a red button labeled 'DECLINE'. A red arrow points to the 'I HAVE READ AND AGREE' button.

5: ةوطخال

ديرت تنك اذا. ةروصلا يف حضوم وه امك تيبتتلا ةشاش ىلع لصحت، ةيقافاتالا لوبق دعب عم ليلدلا اذه رمتسي، كذعمو، انه كذلم مايقلا كنكمي، ةيطايتحإ ةخسن نم ةداعتسالا فيظنلا تيبتتلا مسق يف ءدبلا يف دح. فيظنلا تيبتتلا راخي.



Installation Options

Only the License section can be altered after installation.

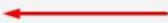
- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >



Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

/data

Start >

6: ةوطخ لا

دح .جت نمل اارش دن ع رورم ةرابع و اصيخرت ي ق ل ت . امدق ي ضم ل ل ة صخر وه هجاتحت ايش لوأ صيخرت يلع دح . رورم ل ةرابع ل خ دا و صيخرت ل فل م رت خ . ل . لي محت ل صيخرت فل م + يلع م تي ، لي محت ل حجن اذ . رورم ل ةرابع ة حص نم ق قحت ل اءا ر ل اف ، لي محت ل حجن ي مل اذ . ل . لي محت ل نم دع ب ن ك م ت ت مل اذ . ي ل ل ا ل ي ف دي دح ت . ة ح ل اص صيخرت ت ا م و ل عم يلع ي و ت ح ت ة ش اش ضرع ي ن ق ت ل Cisco م دع ب ل ص ت اف ، ك ب ص ا خ ل ص ي خ ر ت ل ت ي ب ت



Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

License

Device ID

EG.....V5

License

No license has been installed.

Install New License

license + Upload License File

.....

Upload License

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome
- > Deployment Mode
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Welcome to Private Cloud

Before you begin

AMP for Endpoints Private Cloud needs certain network and infrastructure resources in place.



You will be asked to provide this information as you proceed through the installation. For more information and examples, please refer to the Private Cloud Deployment Strategy guide.



Two Static IP Addresses

One for administrative use, and the other for enterprise-facing services.



DNS Server

Provides hostname resolution to the Private Cloud device.



Hostnames and Trusted Certificates

One hostname and trusted certificate for each of the following services:

- Authentication.
- AMP for Endpoints Console.
- Disposition Server.
- Disposition Server - Extended Protocol.
- Disposition Update Service.
- Firepower Management Center Link.

Note: Hostnames can not be changed once the device has finished installation.



SMTP Server

Used for emails, alerts, and notifications.



NTP Server

Provides time synchronization across your Private Cloud device and endpoints.



External Internet connection (Proxy Mode only)

Proxy Mode devices perform anonymized disposition queries against the Cisco Cloud.

Next >

نيوكالتا

1: ةوطخال

✎ ةيرصحل رصانعلا ضعب جردن، ةحيرشلا نم ةيلالتا تاعومجما يف هنا طحلن: ةطحالما اهقافرا متي يتلاو، ةاول ةوجف عوضوب طقف درفنت يتلاو ةروصل يف حضوم وه امك طقف ةاول ةوجف انا يلع اهيلع ةمالع عوضوو



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require an Internet connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

طوق Airgap



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode
- > Standalone Operation
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require an Internet connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately or automatically on this device.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Standalone Operation

Air Gap mode requires updates to be downloaded separately from this Private Cloud device, and applied via an ISO file attached to the device.

Air Gap

- Does not require an Internet Connection
- Updates must be downloaded separately and applied to this Private Cloud device.

طرق Airgap

2: ةوطخل

يراد إدخال مديتسم مادختسإ م تي. ةنمآلا ةياهنلا ةطقن مكحت ةدحو باسح ةحفص ىلإ لقتنا لخدأ. نييفاضا ني مديتسم ةفاضإ ورتوي بمكلا تاعومجمو تاسايسلا عاشنإل مكحتلا ةدحول ىلاتلا يف دح. مكحتلا ةدحو باسحل رورملا ةم لك و ينورتكلإل دي ربلاناونعو مسالا

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

AMP for Endpoints Console Account

Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

Name	Roman	Valenta
Business Name	Cisco - rvalenta	
Email Address	rval[REDACTED].com	
	rval[REDACTED].com	
Password	
	

Next >

نانثإ ىقلتت تنأ كلذ دعب دربم OVA ل نم تنأ رشنني ام دنع رادصإ اذه ىلإ تنأ ضكري نإ ترشن in order to كلذ دعب لمع فاقيا وأ دعب اميف رادصإ اذه تححصو تعباتو، ام راخ هيف ترداغ يذلا ناكملا يف رمتسا، ليغشتلا ةداعإ دعب. كلذل اقفو تقبوطو

✎ حيص لكشب هليمت متي يذلا 3.5.2 رادصالل OVA فلم يف كلذ حالصا مت: عظامالم (CPU) ةيزكرملا ةجالعالم ةدحو زكارموتيا باجيج 128 ةعس يئوشع لوصو ةركاذ عم 8. ةعرب

CISCO AMP for Endpoints Private Cloud Administration Portal Support Help Logout

Configuration Operations Status Integrations Support

Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- AMP for Endpoints Console ✓
- Account ✓
- Hardware Requirements

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Cisco Cloud
- Email ✓
- Notifications ✓
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Hardware Requirements

Hardware Requirements Not Met

Your current configuration does not meet the hardware requirements.

It is recommended that you shutdown this device and adjust its hardware allocation to meet or exceed the minimum requirements. If you proceed, you may experience system instability.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	4	8
Memory	125 GB	128 GB

[Shutdown](#) [I understand the risks >](#)

✎ ةي لمعم ضارغأل كلذ ناك اذا اإل طقف ةن سحت سمل ميقلا مدختسا: عظامالم

Edit settings - AMP-vPC (ESXi 5.0 virtual machine)

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8		
Memory	131072	MB	It will work with 48Gb as well
Hard disk 1	376.52343	MB	
Hard disk 2	17.272949	GB	
Hard disk 3	1.7216082	TB	
Hard disk 4	4.765625	GB	
SCSI Controller 0	LSI Logic Parallel		
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect	
Network Adapter 2	VM Network	<input checked="" type="checkbox"/> Connect	
CD/DVD Drive 1	Host device	<input type="checkbox"/> Connect	
Video Card	Specify custom settings		

Save Cancel

انرداغ شيح عباتن ىتح ليغشلتال اداعإ مت إن ام

AMP for Endpoints Private Cloud Administration Portal

Support Help Logout

Configuration Operations Status Integrations Support

Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- AMP for Endpoints Console Account ✓
- Hardware Requirements ✓

Configuration

- Network
- Date and Time
- Certificate Authorities
- Upstream Proxy Server ✓
- Cisco Cloud
- Email ✓
- Notifications
- Backup ✓
- SSH ✓
- Syslog ✓
- Updates ✓

Hardware Requirements

✓ Hardware Requirements Met

Your current configuration meets or exceeds the hardware requirements.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	8	8
Memory	125 GB	128 GB

Next >

اضيا تباثلل IP مادختساب ETH1 نيوكت نم دكأت

تازوجح عاشنإب مقت مل ام DHCP مادختسال كزاهج نيوكتب ادبأ موقت ال بجي: ةطخال م كلذ يدؤي دقف، لاصتال تاهجاوب ةصاخلل IP نيوانع ريغت مت اذا. تاهجاولل MAC ناوع متي مل اذا. اهرشن مت يتللة نم الة ةطقن تالصوم يف ةريطخ لكاشم ثودح ىلإ تيبثتال اهانإل تقؤملا ماعلل DNS مادختسإ كنكمي، DNS مادخ نيوكت

3: ةوطخال

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Network Configuration

Clicking Next will apply your interface configuration before validating your settings. If using DHCP, a release/renew will be performed to obtain the reserved DHCP lease.

Administration Portal eth0 / 00:0C:29:A6:4A:11

IP Assignment 192.168.75.92 [More details](#)

Interface Configuration eth1 / 00:0C:29:A6:4A:1B

IP Assignment 192.168.75.209 [More details](#)

IP Assignment Static

IP Address 192.168.75.93

Check for IP Address conflicts

Subnet Mask 255.255.255.0

Gateway 192.168.75.1

DNS

Primary DNS Server 8.8.8.8 [Use public DNS temporary.](#)

Secondary DNS Server

Next (Applies Configuration) ▶

4: ةوطخال

ديرت يذلا رثكأ وأ دحاو NTP مداخ نيوانع لخدأ. تقول اوخي راتاللا ةحفص ىلع لوصح لال كنكم ي تنيعو لدان NTP يجراخ وأ يلخاد تلمعتسا عي طتسي تنأ. تقول اوخي راتاللا ةنمازمل هم ادختسا عم تقولا ةنمازمل مق. بناج ىلا ناليم ةمئاق غارف وأ ةلصاف لال خ نم دحاو نم رثكأ ةيروف ةنمازمل ضرفل زاوجلل مكحت ةدحو نم AMP-CTL NTPDATE لي غشتب مق وأ ضرعتسم لال يلاتال ي ف ديدحت. NTP مداوخ عم

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓

Date and Time

NTP Servers

192.168.75.254 ← Optional Verify hostname resolution

Current System Time

2021 / 4 / 10
 8 : 17 : 24 UTC
 Set by NTP

Next >

طوق Airgap

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Prepare amp-sync ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Prepare amp-sync

You will need to load a snapshot of the Protect DB and retrieve the latest AMP updates from Cisco after your device has finished installing in air gap mode. Cisco provides a shell script called amp-sync that will retrieve the updates and build an ISO file that you can then mount on your AMP device.

It is suggested that you begin the download process now since the initial update is very large.

[Download amp-sync](#)

Next >

طوق Airgap

5: ةوطخال

عجرم ةفاضل ةل ددح. ةروصلال ةف حضم وه امك، ةقدصملا عجارملا ةحفص ةل لصحت رذل ك تدهاش ةفاضل تادهاش.

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Certificate Authorities

Add Certificate Authority

No certificate authorities have been uploaded to this device.

Next >

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓

Add Certificate Authority

Certificate Root (PEM .crt) Disable Strict TLS Check

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate end date is later than 20 months from today.
- Certificate file only contains one certificate.
- Certificate does not use sha-1 signature algorithm.
- Certificate using RSA keys must use a key size of 2048 or more.

AMP-vPC-Root-CA.pem + Add Certificate Root

Cancel

Upload

Installation Options

- Only the License section can be altered after installation.
- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓

Certificate Authorities

Add Certificate Authority

Certificate		(click to collapse)
Issuer	AMP-vPC	Download
Subject	AMP-vPC	
Validity	2021-04-09 16:28:00 UTC - 2031-04-09 16:28:00 UTC	Delete

Next >

6: ةوطخل

دج ةروصلال في حضوم وه امك، Cisco Cloud ةحفص نيوكت في ةيلاتال ةوطخلال لثمتت ل ةجاحب تنك اذ فيضمال امامسأ ضرع عيسوتب مق. ةبسانمال Cisco ةباحس ةقطنم

لاصتال كيديل ةنمآلا ةياهنلا ةطقنل صاخلا ةباحسلا زاهل ةيامل راج تاءانثتسإ عاشنإ يلاتل يف دح. ةزهجل تاتيحتو تافللمل نع شحبل تايلمع ءارجل Cisco ةباحسب.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes 'Support', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. The main content area is titled 'Cisco Cloud' and contains the following sections:

- Installation Options:** Only the License section can be altered after installation. This section includes links for 'Install or Restore', 'License', 'Welcome', 'Deployment Mode', 'AMP for Endpoints Console', 'Account', and 'Hardware Requirements', all of which are checked.
- Configuration:** This section includes links for 'Network', 'Date and Time', 'Certificate Authorities', 'Upstream Proxy Server', 'Cisco Cloud', 'Email', 'Notifications', 'Backup', 'SSH', 'Syslog', and 'Updates', all of which are checked.
- Cisco Cloud Configuration:** This section includes a 'Region' dropdown menu set to 'Cisco Cloud, North America' and a 'View Hostnames (click to expand)' button.
- Cisco Cloud Identity:** This section includes a 'Client Identity' field with the value '0f476ea8[REDACTED]dbbc272a6c'.

A 'Next' button is located at the bottom right of the page, highlighted with a red box.

7: ةوطخل

ةماهال تامالعلل ددرتلل دح. ةروصلل يف حضوم وه امك، تامالعلل ةحفصلل لقتنا ةطقن زاهل هيبنتل تامالعلل يقلت ديرت يتلل ينورتكللإل ديربلل نيوانع لخدأ. ةمظتنملاو نيوانع ديحت وأ ينورتكللإل ديربلل ةراع تسم ءامسأ مادختسإ كنكمي. ةنمآلا ةياهنلا ديربلل ناوعولسرملل مسا ديحت اضيأ كنكمي. ةلصافب ةلوصفم ةمئاق لالخنم ةددعتم مكحت ةدحو تاكلارثشا سفن تسيلا تامالعلل هذه. زاهل ةطساوب مدختسملل ينورتكللإل ةزهجل نم ديدعلل كيدل ناك اذل ديرف زاهل مسا ديحت اضيأ كنكمي. ةنمآلا ةياهنلا ةطقن يلاتل يف ديحت. ةنمآلا ةياهنلا ةطقنل صاخلا ةباحسلا

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol

Notifications

Notification Frequency

Critical Notification Frequency	HELP	Every 5 Minutes
Notification Frequency	HELP	Every Week

Notification Addresses

Notification Recipients	HELP	rv@...om
Notification Sender Address	HELP	donotreply@cisco.com
Notification Sender Name	HELP	AMP for Endpoints Device

Device Name

Device Name	HELP	CyberNet vPC 2
-------------	------	----------------

Next >

8: ةوطخال

ىل ع ددح . ةروصلال ي ف حضوم وه امك ، SSH حيتافم ةحفص ىل ل قننلاب موقت كلذ دعب SSH حيتافم كل حيتت . زاهالال ىل اهتفاضل ديرت ةماع حيتافم ي ل اخلال SSH حاتفم ةفاضل نيمدختسملل لوصولال قح حنم بچي . رذللال تازايتمما تاذ ةديعب ةقبط ربع زاهالال ىل لوصولال كنكمي . OpenSSH ل قسنم RSA حاتفم صاخلال ةباحسال زاهج بلطتي . طقف مهب قوئومال ي ف ددح . كيدل ةرادلال لخدم ي SSH > نيوكتلال لال خ نم اقحال SSH حيتافم نم ديزملا ةفاضل ىللال.

Maintenance Mode

Sanity Check Failing

This page allows you to add and remove SSH keys on your Cisco AMP for Endpoints Private Cloud device. SSH keys allow administrators remote root authentication to the device. Only trusted users should be granted access.

Add SSH Key

Windows PuTTY

2021-11-17 23:01:01 +0000 created 20 days ago	2021-11-17 23:01:01 +0000 20 days since last update	Edit Delete
<pre>ecdsa-sha2-nistp256 AAAAE2K...oeCAvfEzyIea9Pbgwn1B9DjTeJgFXtR7QGfd0g4vT9eD5XOXZd I4DKhrTNBv8/77T0d/Jagx7Przxs=</pre>		

ليحتو فيضم الامسا نبيعت بجي، ةليلات الاحفصلا في تامدخل مسق ىلع لصحت م ث ةليلات ةليلق الحارشل في . هذه ةزهجال تامدخل ةبسانملا حاتفملا و تاداهشلا جاوزا ، تسلا تاداهشلا يدح ةئيهت ةيؤر انكمي .

تامدخل

1: ةوطخل

ءاطخال هذه ليغشت متي دق ، نيوكتلا ةيلمع ءانثأ

ليطعت ديدحت ءاغل ةطاسبب اذه زواجتل . ةثالثل مهسلاب هزاربإ متي هظحالت دق "أطخ" لوأ TLS" نم مراصل ققحتلا

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > **Authentication**
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
<input checked="" type="checkbox"/> Certificate issued after 07/01/2019 must have a validity period of 825 days or less.	
<input checked="" type="checkbox"/> Certificate issued after 09/01/2020 must have a validity period of 398 days or less.	
<input checked="" type="checkbox"/> Certificate does not use sha-1 signature algorithm.	
<input checked="" type="checkbox"/> Certificate using RSA keys must use a key size of 2048 or more.	
<input checked="" type="checkbox"/> Certificate must specify server certificate in Extended Key Usage extension.	

vPC2-Authenticator + Choose Key

vPC2-Authenticator + Choose Certificate

[Next >](#)

مراحل TLS صحف نودب

An error occurred while processing your request.

• Hostname does not resolve

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname HELP

vPC2-Authentication.cyberworld.local Validate DNS Name

Authentication Certificate Disable Strict TLS Check Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	<input type="text"/> + Choose Key
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
<input type="text"/> + Choose Certificate	

Next >

تاداهشال ةيقبل ىرخأ تارم سمخ ةيلمعال سفن ررك نأل.

ةقداصملا

ةجلاعمل Private Cloud نم ةيلبقتسملا تارادصلإل يف ةقداصملا ةمدخ مادختسا متي -
مدختسملا ةقداصم

ةنمآل ةياهنلا ةطقن يف مكحتلا ةدحو

ةدحو لوصول ةنمآل ةياهنلا ةطقن لوؤسمل نكمي شي DNS مسا يه مكحتلا ةدحو -
تاثير دحتو تاسايس ةنمآل ةياهنلا ةطقن تالصوصم يقلتي و ةنمآل ةياهنلا ةطقن مكحت
ةديج.

يئاهنلا ريصملا مداخ

تامولعم لاسراب ةنمآل ةياهنلا ةطقن تالصوصم موقت شي DNS مسا وه Disposition Server -
اهدادرتساو ةباحسلا نع شحبال

- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓
- Services**
- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

1. Download Recovery File

Please keep a copy of this file in a safe place.

[Download](#)

2. Verify Recovery File

After downloading your backup, upload it to the device to verify that you have a matching copy.

[Browse...](#) pre-install-backup.bak

Recovery File Ready for Download
created less than a minute ago

[Next >](#)



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

[▶ Start Installation](#)

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type

[Edit](#)

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

AMP for Endpoints Console Account

[Edit](#)

Name	Roman Valenta
Email Address	rva[REDACTED].com
Business Name	Cisco - rvalenta

Recovery

[Edit](#)

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

≡ ≡ Airgap ≡ ≡ طوقف

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Prepare amp-sync ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type ✎ Edit

Standalone Air Gap ←

- Does not require an Internet Connection
- Communication with AMP for Endpoints Connectors managed by this device are needed.
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates must be downloaded separately and applied to this Private Cloud device.

AMP for Endpoints Console Account ✎ Edit

Name	Roman Valenta
Email Address	rvalenta@...m
Business Name	Cisco vamrodia PC v2

Recovery ✎ Edit

Uploaded Recovery File Matches Current Settings

▶ Start Installation

طوق Airgap

هذه لثم ةلثامم تالخدم ىرت

⚠ شودح يف ببستى دق هنأل شىدحتلاب مقت ال ةحفصلا هذه يف كدوجو دنع :رىذحت لكاشم.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```
le_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP::StreamHandler calling Chef::HTTP::Decompressor::NoopInflater#handle_chunk
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: HTTP server did not include a Content-Length header in response, cannot identify truncated downloads.
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::CookieManager#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONOutput#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONInput#handle_stream_complete
[2021-04-10T17:36:20+00:00] INFO: Storing updated cookbooks/rabbitmq/recipes/default.rb in the cache.
[2021-04-10T17:36:20+00:00] DEBUG: Creating directory /var/run/cookbooks/rabbitmq/recipes
```

Download Output

ليغش التال ةداع | رزى لى طغضا تيبت التال نم ءاهت التال درجب

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 24 minutes, 14 seconds ago	Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 3 minutes, 17 seconds ago	0 day, 0 hour, 20 minutes, 57 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration against the AMP for Endpoints Disposition Server has previously succeeded.

=====
Installation has finished successfully! Please reboot!
=====
```

Download Output

≈ ≈ Airgap ≈ ≈ طوف

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Tue Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 21 minutes, 21 seconds ago	Tue Nov 02 2021 15:07:02 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 49 seconds ago	0 day, 0 hour, 20 minutes, 32 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-11-02T19:07:01+00:00] INFO: Running report handlers
[2021-11-02T19:07:01+00:00] INFO: Report handlers complete
[2021-11-02T19:07:01+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-11-02T19:07:01+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-11-02T19:07:01+00:00] DEBUG: Forked instance successfully reaped (pid: 29292)
[2021-11-02T19:07:01+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration is not possible in air gap mode.
=====
Installation has finished successfully! Please reboot!
=====
```

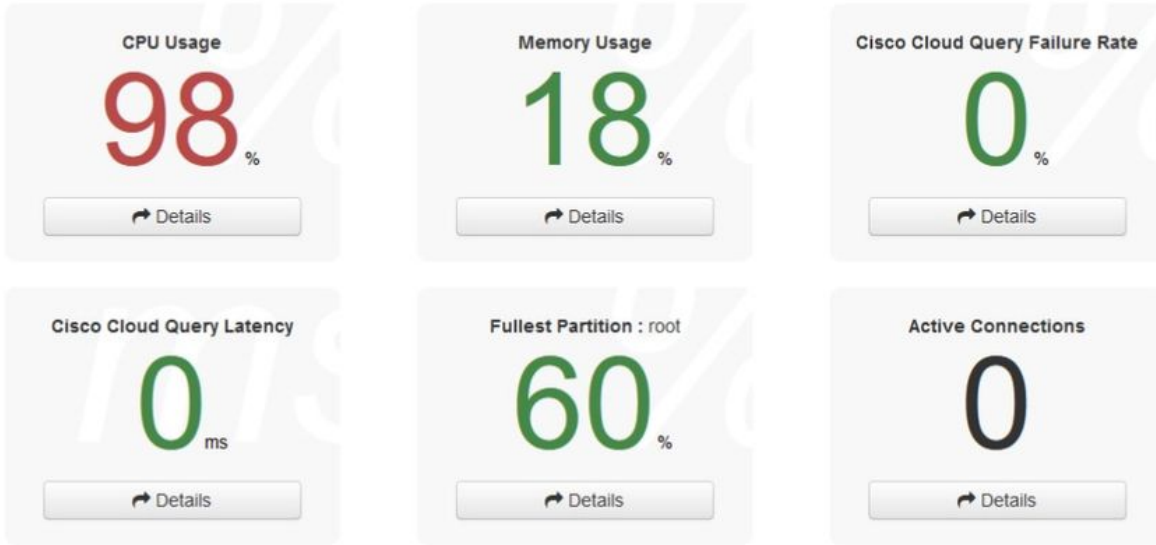
Download Output

طرق Airgap

موقت يتل اة لالتا لة رمال في هذه تامول عمل اة حول مي دقت متي ، لم الكلاب زاهج ل دي هم ت درج م ج ل ا عمل ا في ع ا ف ت ر ا ط ح ا ل ت د ق . ك ب ا ص ا خ ل ل و و س م ل ا ا ه ج ا و م ا د خ ت س ا ب ل و خ د ل ل ل ج س ت ب ا ه ي ف ر ق ت س ي ه ن ا ف ، ق ئ ا ق د ع ض ب ت ي ط ع ا ا ذ ا ن ك ل ، ا ي ا د ب ل ل ي ف



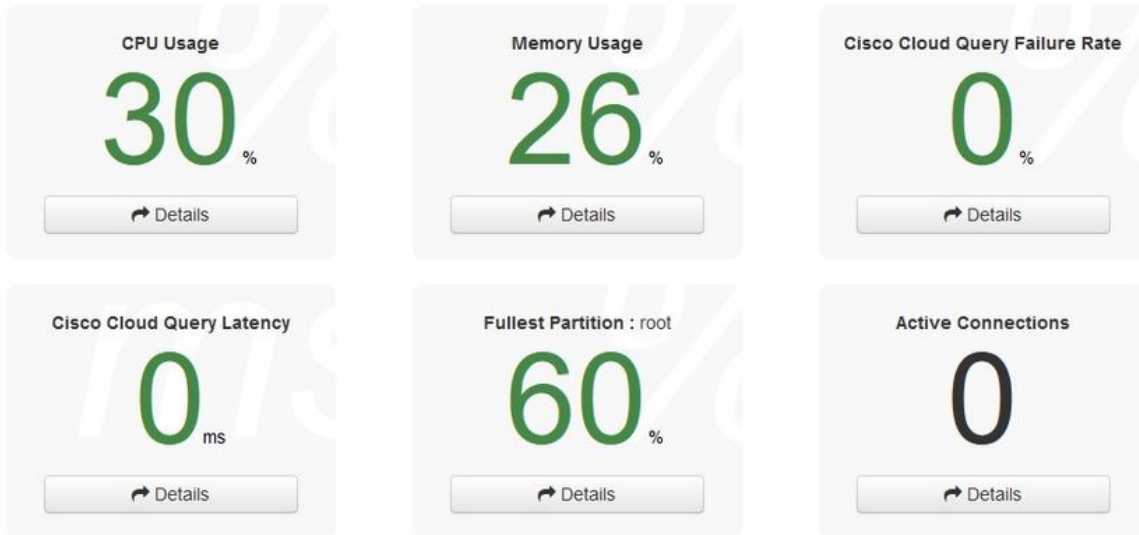
Key Metrics



...ة ليلق قئاق دعب



Key Metrics



ةريغصلا ةنوقيألا ىلع رقنا .ةنمألا ةياهنلا ةطقن مكحت ةدحو ىلإ لقننتلاب موقت انه نم ملعل راوجب ينمىلا ةيوازلا يف رانلا لثم ودبت يتلا

AMP for Endpoints Private Cloud Administration Portal

Support Announcements Help Logout

Configuration Operations Status Integrations Support

Key Metrics

Metric	Value
CPU Usage	11%
Memory Usage	36%
Cisco Cloud Query Failure Rate	0%

طقف Airgap

تافيرت ببسب اضي أو، DB ةطقلة يامح ببسب ةحصلا نم ققحتلا يف انلشف، ىرت امك فلم ربع تنرتن إلاب لاصتا نود شيدحتلا قيرط نع كلدب مايقلا بجي. Tetra و DFC و ليمعلا (VM) يرهاظلا زاھجلا ىلإ هليمحتو AMP-Sync لالخ نم اقبس م هدادعإ متو هليزنت مت يذلا ISO NFS عقوم يف هنيخت وأ



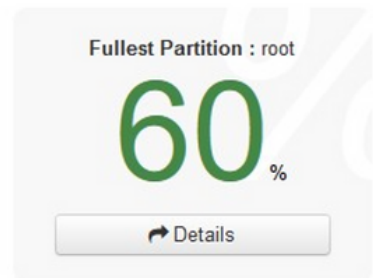
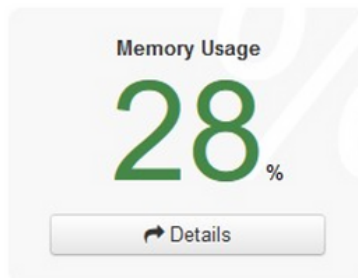
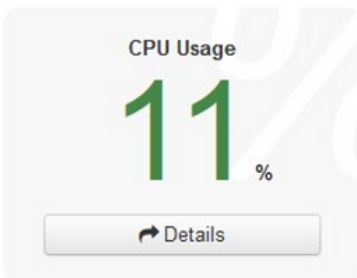
Sanity Check Failing

The device `sanity_check` is failing; your device might not function properly until corrective measures are taken.

Details

FAIL: A Protect DB snapshot has not been loaded. Devices configured in standalone mode should have a Protect DB snapshot loaded. Protect DB snapshots contain threat intelligence about known clean and known malicious files.

Key Metrics





✖ Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

✖ There is no ISO loaded. Load an ISO and try again.

Content

✖ 3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

! ABSENT

Protect DB Version

! Import a Protect DB snapshot to your standalone device.

Checked 1 minute ago; the update check failed.

Software

✖ 3.2.0_202010082118

Private Cloud Software Version

Update Software

Checked 1 minute ago; the update check failed.

AirGap شيدحت ةمزم

ةيامحلل تانايب ةدعاق مالتسال رمالا اذه مادختسا انيلع يلوالا ةرملل

```
./amp-sync all
```

رثكأ قرغتسي نأ نكمي هنا نم ققحت مث رمالا اذه ربع مزحلا عيمج ليزنتب مق: ةظحالم رمالا لازي ال 1Gig فايلا عم يتلاح في. طابترالا ةدوجو ةعرسال ليلع دمتعت. ةعاس 24 نم ليزنتلا اذه نأ ةقيقح ليلع ايئزج اضيا اذه عجرىو. لامتكال ل ابي رقت ةعاس 25 قرغتسي ناك. ريبك ليحمتلا اذه نأ ظحال اريخأ. هببرخت متي يلاتلابو AWS نم ةرشابم متي رقص. تياباحيج 323 هتعتس غلبت يتلاح في هليزنت مت يذلا فلملا

CygWin64 انمدختسا لاثملا اذه في

1. هتبتتو Cygwin نم x64 رادصلا ليزنت.
2. تادادعلا عيمج رتخأ تبتتال ةيلمع لالخال لقتناو setup-x86_64.exe ليغشتب مق. ةيضارتفالا.
3. ليزنتلل ةأرم رتخأ.
4. اهتبتتل مزح ددح:

all -> Net -> Curl

All -> Utils -> Genisoimage

all -> utils -> xmlstarlet

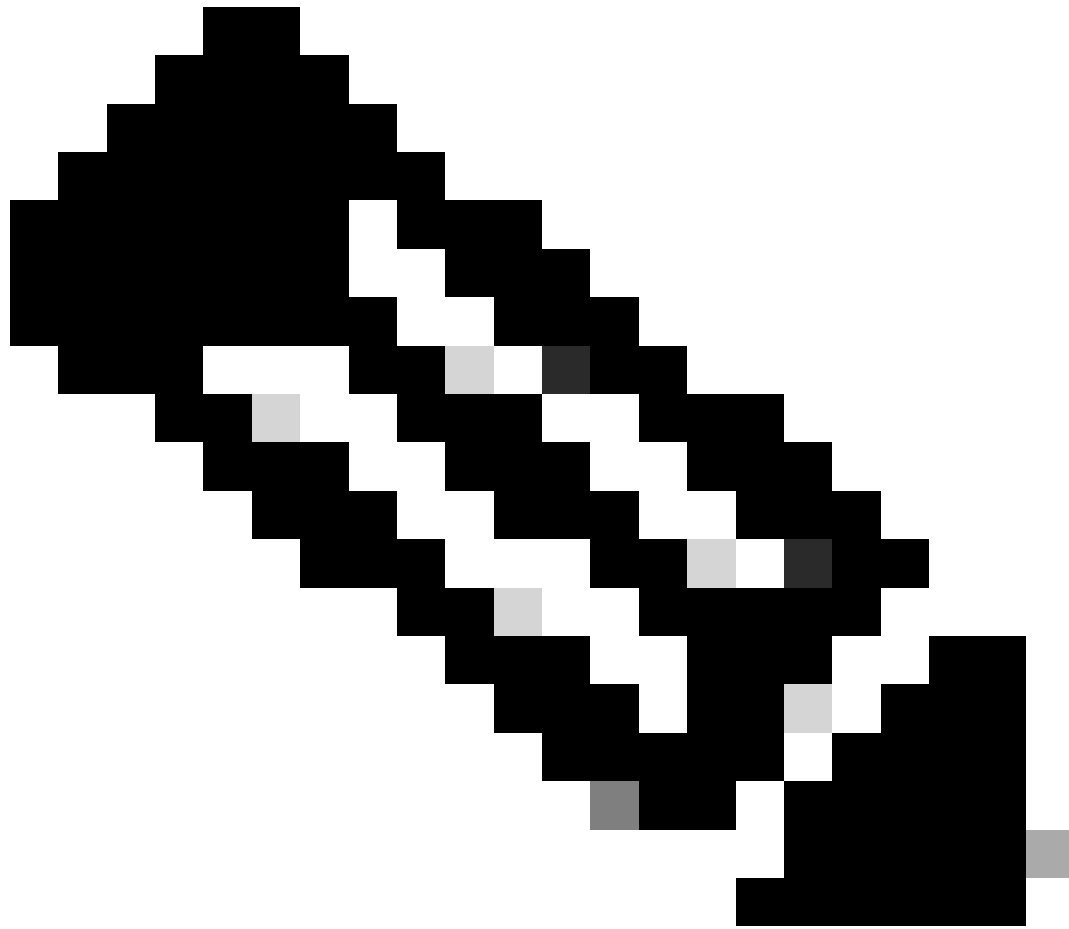
* VPC 3.8.x up -> xorriso

```
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing...
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2991 100 2991 0 0 15991 0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 11331 100 11331 0 0 98544 0 --:--:-- --:--:-- --:--:-- 97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdf10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 915k 100 915k 0 0 3324k 0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1094k 100 1094k 0 0 3302k 0 --:--:-- --:--:-- --:--:-- 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb547309376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 135k 100 135k 0 0 747k 0 --:--:~ --:~:~ --:~:~ 756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 54480 100 54480 0 0 383k 0 --:~:~ --:~:~ --:~:~ 385k
```

```
99.91% done, estimate finish Thu Nov 4 08:39:50 2021
99.91% done, estimate finish Thu Nov 4 08:39:51 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:51 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:51 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:52 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
100.00% done, estimate finish Thu Nov 4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)

Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso

User@VMStation-1 ~
$
```



كُنْ مِي ةِ سِي ئِر ل ل لِي ز ن ت ل ل ة ا د ا ك C y g W i n 6 4 ع م V P C 3 . 8 . x ث ي د ح ت ث د ح ا ي ف : ة ظ ا ل م
ه ا ن د ا ة ح ص و م ل ا ة ل ك ش م ل ا ه ذ ه ة ه ج ا و م .

```
User@VMStation-1 ~
$ ./amp-sync all

=====
Prerequisite Program(s) Missing
=====

A prerequisite tool was not found in your PATH, or is not an appropriate
version. You must have the following tools installed in order for the AMP for En
dpoints
Air-Gap Update Tool to function:

    awk
    base64
    basename
    cat
    comm
    curl
    dirname
    mv
MISSING -> xorriso
            sha256 / sha256sum / shasum
            sort
            tr
            xmlstarlet

These tools should be available in both Windows Subsystem for Linux and most
Unix-like operating systems.
```

قيسنت انريغ. ةبولطم "وسيرروسكنا نإف نآلا نورت امكو. 58 مقر ةحفصلال [رادصلال ةظحال](#)م نكمي ىتح بسانملا قيسنتلال ىل ةروصلال لوحي ام يه ةيعبتلال نأو ISO 9660 ىل ISO ةجمدملا تاعدوتسملا نم يا في CygWin64 xorriso مدقي ال، ظحلل ءوسلو. شيحتلال لامكإ، CygWin64 مادختسا في نوبغري اولاز ام نذللا كئلوال ةبسنلابف، كلذ عمو. هب ةصاخلا ةلأسملا هذه ىلع بلغتلل ةقيرط كانه.

Installing dependencies

CentOS

To run amp-sync you will first have to install EPEL, xorriso, and xmlstarlet.

1. Enable the EPEL repo.
 - > `sudo yum install epel-release`
2. Install dependencies via yum.
 - > `sudo yum install xorriso`
 - > `sudo yum install xmlstarlet`

Ubuntu

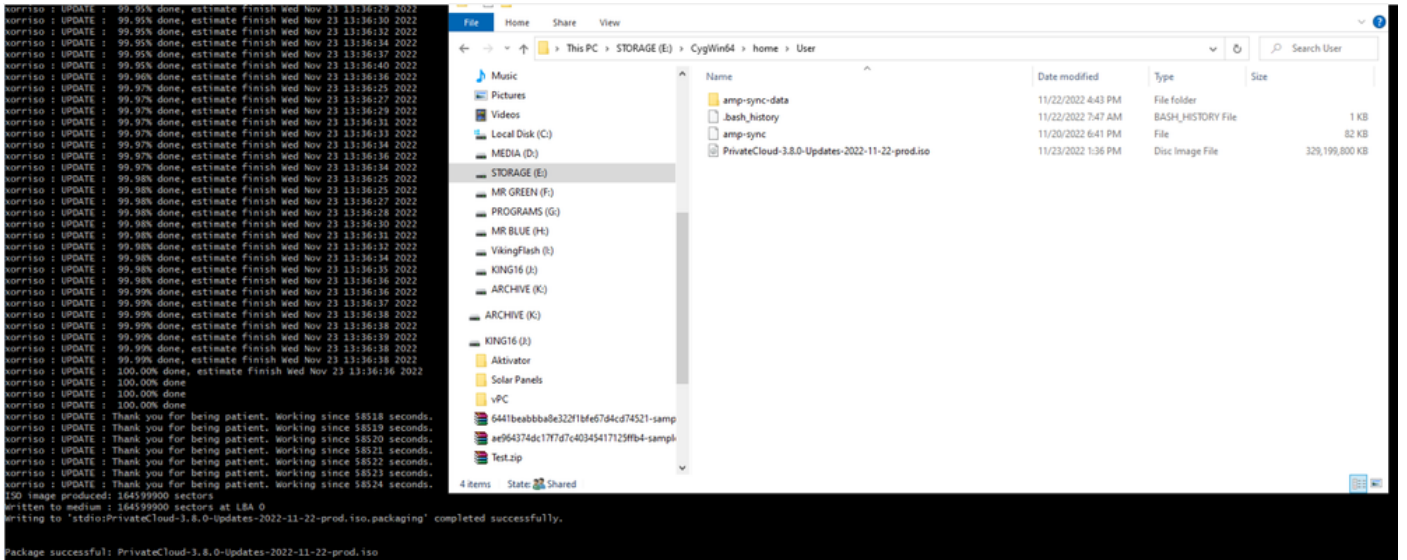
To run amp-sync you will first have to install xorriso and xmlstarlet.

- Install dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

Windows

1. Set up Windows Subsystem for Linux (WSL) with the Ubuntu distribution. See the [Microsoft documentation](#) for details.
2. Expand the WSL virtual hard disk size to comply with minimum free disk space. See the [Microsoft documentation](#) for details.
3. Install xorriso and xmlstarlet dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

حت فا GitHub عدوتسم نم ايودي xorriso ليزنت بجي، رخأ قرم CygWin مادختسإ نم نكمتتل لوأك رهظي نأ بجي <Windows ل ق بسم ءانب 1.5.2 Latest xorriso.exe> بتكاو ضرعتسملا مقو هذه GitHub ءحفص ىلإ لقتنا <PeyTy/xorriso-exe-for-windows - GitHub> ىمسي طاابترا رخأ تافل نمي ب هجت يذلا zip فلم لخاد <xorriso-exe-for-windows-master.zip> فلم ليزنت ب Cyg تيبتت راسم <CygWin64\bin> ىلإ هقصلو فلملا اذخسننا <xorriso.exe> ىمست ءللق نأل دعب أطخلا ءلاسرىرت ال نأ بجي. <amp-sync> رمأل لىغشت رخأ قرم لواح. يلحمل ءروصلال يف حضوم وه امك ءاهتناوالا وءبال ليزنتو.



قروض و Airgap في VPC 3.2.0 (الاحال هذه في) رايت لل يطاي تحال خسن ال اراجاب مق

CLI نم رم اذه تلمعتسا عيطتسي تنأ

`rpm -qa | grep Pri`

ارجا و ةروصل في حضوم وه امك ، ةيطاي تحال خسن ال > تاي لمعل ال ال ل قنن ال اضيأ كنكمي و ا
 لكانه يطاي تحال خسن ال



Sanity Check Failing

Backups create a copy of your configuration and databases.

Manual Backup

Perform Backup

Last Backup Successful

Transferring Backups To External Storage Is Recommended

To facilitate disaster recovery, you are strongly encouraged to transfer backup archives to a secure external backup location. Transfer of backup archives can be performed via download, sftp, or rsync.

Backup Job Details

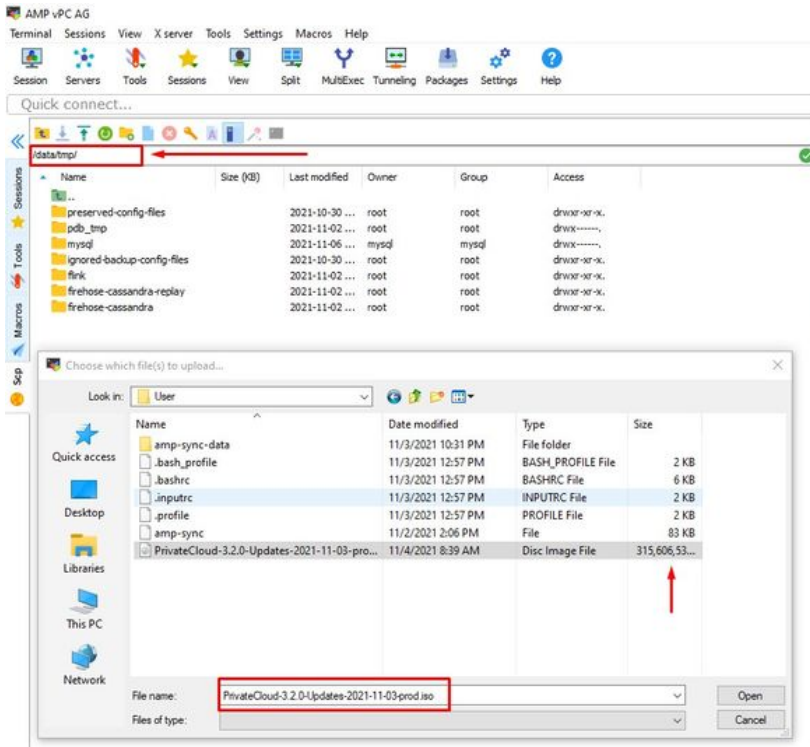
Previous Backups

The number of backups that will be stored on disk is: 1.

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20211106-0000.18.bak	738 MB	2021-11-06 00:03:43 +0000 about 17 hours ago	 

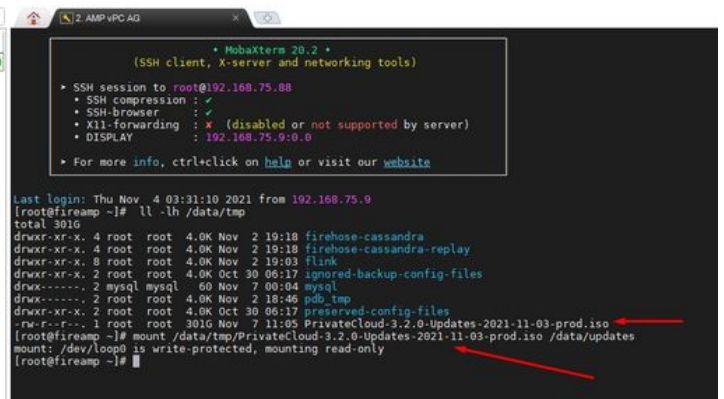
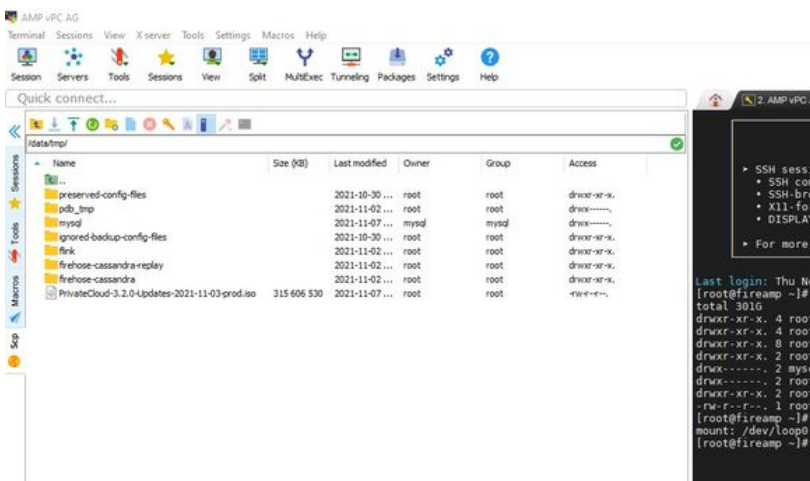
ةدع رمألا اذه قرغتسي دق. VPC ىلإ AMP-sync مادختساب هؤاشنإ مت يذلا ISO ثدحأ لقن ب مق
ةعاس 16 نم رثكأ لقنلا قرغتسا، ةلجال هذه يف. كتعرس ىلإ ادانتسا اضيأ تاعاس

/data/tmp



ISO لي محتب مق ، لي محت التا نم عاهت التا ل دعب

mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/



ققحت التا دي دحت > زا هج التا شي دحت > تا ي لم عم شي دحت التا اراج ال Opdamin م دخت سم ة هج او ي ل ل ق ت ن ا

ISO شيدحت نم

CISCO AMP for Endpoints Private Cloud Administration Portal

Announcements ? Help Logout

Configuration Operations Status Integrations Support Standalone

Sanity Check Failing

Updates keep your Private Cloud device up to date. [Download amp-sync](#)

[Check Update ISO](#) ←

[Checking ISO for updates...](#)

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

ABSENT
Protect DB Version

Checked 9 minutes ago; the update check failed.

[Update Content](#)

[Import Protect DB](#)

Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

[A software update is available.](#)

[Update Software](#)

الواى وتحملا شيدحت عباتا، لاثملا اذه يف

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

A content update is available.

ISO contains Protect DB snapshot version 20210531-0613.
Import a Protect DB snapshot to your standalone device.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

داري ت سالا ةي امح تانايب ةدعاق ددح م ث



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

20211102210054
Client Definitions, DFC, Tetra Content Version

Update Content
Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked less than a minute ago; content is up to date.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

لمتكت ىتح الیوط اتقو قرغتست دق ادج ةلیوط ةیلمع هذه نإف نورت امك و

Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

Table with 4 columns: State, Started, Finished, Duration. Row 1: Running, 2021-11-07 18:48:44 +0000, Please wait..., Please wait...

Output

Attempting to mount an ISO, if one is present.
mount: special device /dev/cdrom does not exist
Starting update.
Stopping apply-cloud-deltas...
Stopping authentication_web...
Stopping authentication_worker...

Download Output

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-07 18:48:44 +0000 42 minutes ago	⌚ Please wait...	⌚ Please wait...

☰ Output

```

Extraction 14.9GB at 6.6MB/s eta: 9:28:03 0% [---]
Extraction 14.9GB at 6.6MB/s eta: 9:28:21 6% [==]
Extraction 14.9GB at 6.6MB/s eta: 9:28:27 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:40 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:46 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:28:58 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:29:12 6% [==]
Extraction 14.9GB at 6.5MB/s eta: 9:29:26 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [==]
Extraction 15.0GB at 6.6MB/s eta: 9:28:20 6% [==]
Extraction 15.0GB at 6.6MB/s eta: 9:28:28 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:44 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:51 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:48 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:28:56 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:29:10 6% [==]
Extraction 15.0GB at 6.5MB/s eta: 9:29:23 6% [==]
                    
```

[Download Output](#)

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌚ Please wait...	⌚ Please wait...

☰ Output

```

Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
                    
```




Maintenance Mode

The device is in maintenance mode.
External services are unavailable.

Sanity Check Failing

Disabling TLS 1.0/1.1

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

The previous Protect DB import failed.

Checked 24 minutes ago; the update check failed.

Software

3.5.3_202111080345
Private Cloud Software Version

Update Software

Checked 24 minutes ago; the update check failed.

يُرجى تحميل ISO ثيديجت فلم ليحمحت تلواح اذا ىرت يذلا اطلخال وه اذه.



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Home / Operations - Update Device / Update Check Details

The update check failed

Something went wrong while checking for updates.

State	Started	Finished	Duration
Failed	2021-11-16 16:29:23 +0000 less than a minute ago	2021-11-16 16:29:30 +0000 less than a minute ago	less than a minute

Output

```
Attempting to mount an ISO, if one is present.
Starting update check.
http://127.0.0.1:8080/PrivateCloud/3.5.3/prod/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below wiki article

https://wiki.centos.org/yum-errors

If above article doesn't help to resolve this issue please use https://bugs.centos.org/.

One of the configured repositories failed (FireAMP PrivateCloud Repository),
and yum doesn't have enough cached data to continue. At this point the only
safe thing yum can do is fail. There are a few ways to work "fix" this:

1. Contact the upstream for the repository and get them to fix the problem
```

Download Output

رإدص إإا ف .كب صإخإل VPC إىل شىء حتال ةروص لىءم حتال ةلءىءب ةقءرط ةروصلإا هءه رهظت VPC زاهء عم شىء حتال ةرإشمل NFS نىءء لثم ءىءب ةقووم ماءءءس إك نكمى 3.5.x .كب صإخإل



Maintenance Mode

Sanity Check Failing

Disabling TLS 1.0/1.1

Mount an Update ISO

ISO Configuration

HELP

Mount Type

- ISO
- ISO
- NFS4
- NFS3

Mount Status

No ISO mounted



Sanity Check Failing

Disabling TLS 1.0/1.1

Configuration saved.

Mount an Update ISO

ISO Configuration

HELP

Mount Type

NFS3

Remote Share

192.168.75.4:/AMPAG

Remote ISO File

PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Mount

Mount Status

Mounted ISO

nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Unmount

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

ايلاج رفوتم ريغ (DB) لوحمل تانايب دعاق ةيامحب طبترم ماظنلا ةمالس نم ققحتلا لشف (VPC) ي صخشلا رتوي بمكلا لىع



AMP for Endpoints

Private Cloud Administration Portal

Announcements

Help

Logout

Configuration Operations Status Integrations Support

Standalone

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433


Private Cloud Software Version

Update Software

A software update is available.

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

🗄️ State	📅 Started	📅 Finished	🕒 Duration
 ▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌛ Please wait...	⌛ Please wait...

☰ Output

```
Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

[Download Output](#)

✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

State	Started	Finished	Duration
✔ Successful	2021-11-19 17:04:05 +0000 about 1 month ago	2021-12-21 01:08:11 +0000 less than a minute ago	about 1 month

Output

```
Starting firehose_cassandra...
Starting firehose_cassandra_replay...
Starting firehose_publisher...
Starting firehose_publisher_replay...
Starting install-token-api...
Starting mgmt_unicorn...
Starting mongo_event_consumer...
Starting portal_unicorn...
Starting redis...
Starting retro-dipper...
Starting retrohose...
Starting retrohose-replay...
Starting tevent_listener...
Starting crond...
Starting flight...
Starting docker...
Sending notification (this may take some time).
```

Download Output

ايئاقولت يلاتلا شيدحتلا ادبي



⚙ Importing Protect DB deltas.

Your Protect DB is being updated with threat intelligence that was queued during a previous content update. Each delta can take several hours to import, and system performance might be impacted during this time.

You should run content updates at the end of the business day or week to ensure updates are applied outside of peak use.

Queued Updates

20211116-2135

Queued Protect DB Update Version



Protect DB

20210531-0613

0.80%

Update Progress

لقن ك نكمي ،داريتسالا ةيامح تانايب ةدعاق تانايب ةدعاق ل ادج ةليوطالا ةيلمعلا هذه دعب
تاعاس 3 نم رثكأ بلطت نأ ابيرقت اهنكمي يتلا جماربلال او لي معلا فيرعت شي دحت و
ةفياضإ .

✔ Content updated successfully

The device successfully performed a content update.

State	Started	Finished	Duration
✔ Successful	2021-12-21 03:10:11 +0000 28 minutes ago	2021-12-21 03:37:53 +0000 less than a minute ago	28 minutes

Output

```
Attempting to mount an ISO, if one is present.
PASS: The mount point / has sufficient space available: 23273033728 >= 1000000000
PASS: The mount point / has sufficient inodes available: 2018323 >= 100000
All checks succeeded!
Repdata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
--> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
--> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
--> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
--> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be updated
```

Download Output

ادج اليوط اتقو قرغتستس ةي لمعلا هذه نأ اوطحال مك لصف نم ،مت اريخأ و

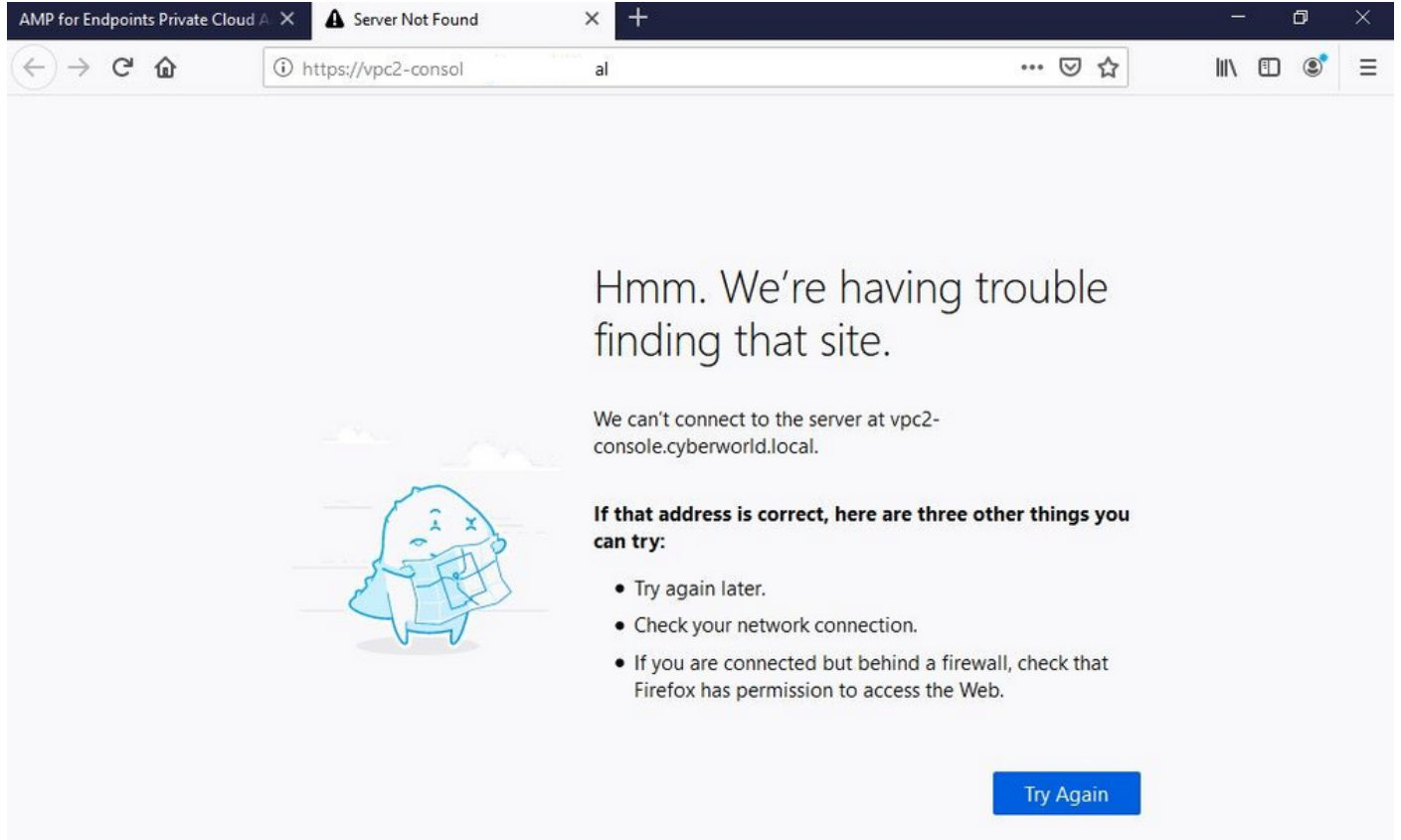
زاهج شي دحتل ىرخأ قرط ىلع يوتحي يذلا زاهجال اذه ةرايزب لصف ، VPC زاهج ةبس نلاب USB. زاهج نم ديهم تلالو ISO فلم تيبتت و ةزهجال

<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5>

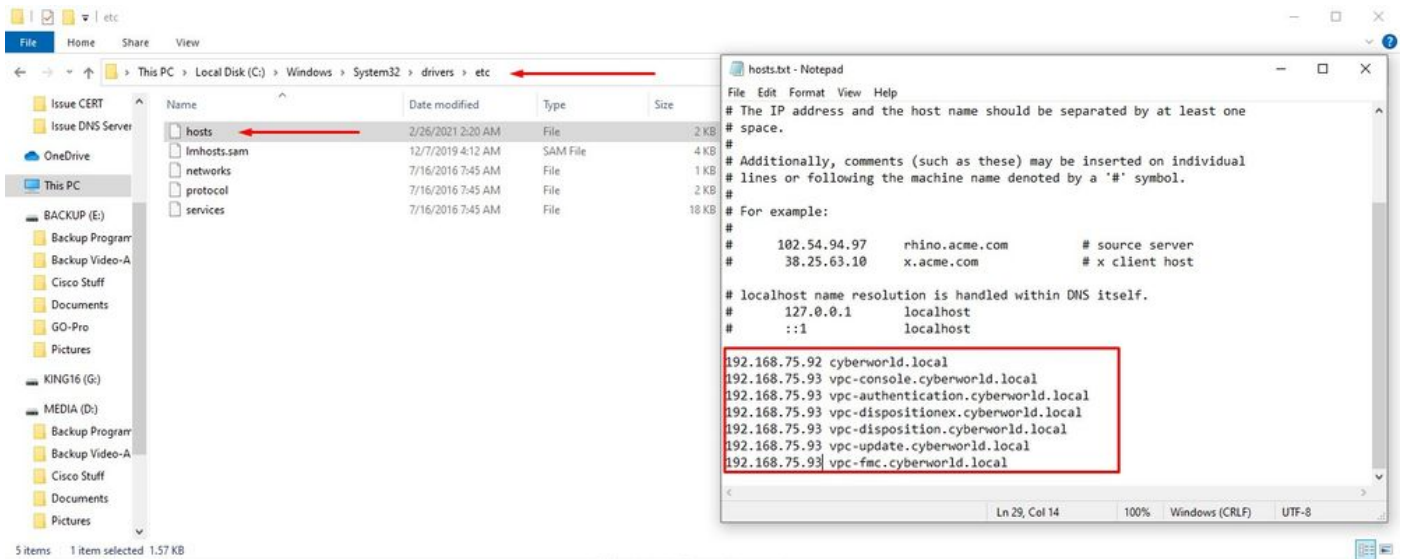
يساساً لكش ب اه حال صا و ااطخ ال ا فاش ك تساً

DNS و FQDN م داخ - #1 ة لكش م ل

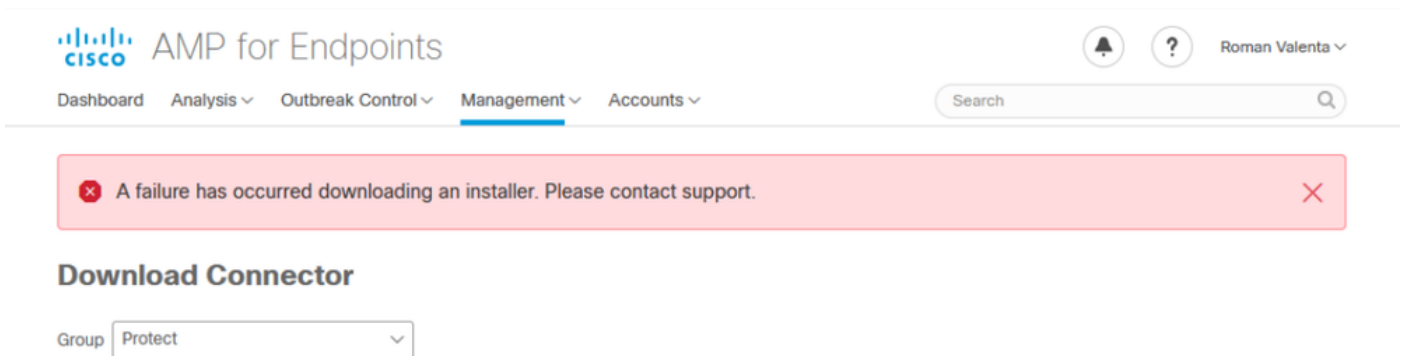
م تي م لو ك ب صا ل DNS م داخ ااش ن ا م تي م ل اذا يه اه ج اوت ن ا ن ك مي ي ت ل ا ي ل و ال ا ة لكش م ل ل و ا ح ت ا م د ن ع ل ك ش ل ا ا ذ ه ب ة لكش م ل و د ب ت د ق . ج ي ح ص ل ك ش ب ا ه ل ح و FQDN ع ي م ج ل ي ج س ت ا ذ ا . ة ن م ال ا ة ي ا ه ن ل ا ة ط ق ن ل "fire" ز م ر ل ل ا خ ن م ة ن م ال ا ة ي ا ه ن ل ا ة ط ق ن م ك ح ت ة د ح و ي ل ل ا ق ت ن ا ل ا ي ف ي ر ت ا م ك . ل ص و م ل ل ي ز ن ت ك ن ك م ي ا ل ن ك ل و ، ل م ع ي ا ذ ه ف ، ط ق ف IP ن ا و ن ع م د خ ت س ت ت ن ك ل³ ل ر و ص ل ا خ ا ف ن م .



ل ح ب م ق ة ر و ص ل ا ي ف ح و م و ه ا م ك ي ل ح م ل ا ك ز ا ه ج ي ل ع (ف ي ض م) Host File ل ي د ع ت ب ت م ق ا ذ ا . ا ا ط خ ا ب ي ه ت ن ت و ة لكش م ل



ةنمآلا ةياهنلا ةطقن لصوم تيبتت ةادأ ليزنت ةلواحم ءانثأ هذه أطخلال ةلاسري قلت



DNS مداخل دا دع| وه حي حصلا دي حولا ل حل ناك ، اء حال صا و لك اش م لا ضعب فاشك تسأ دع

DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0

```
=====
Server:      8.8.8.x
Address:     8.8.8.x#53
```

```
** server can't find vPC-Console.cyberworld.local: NXDOMAIN
```

نم Virtual Private Cloud في لءسلال ريغ و لكي دل DNS مءا في ف QDN ةفاك لءءسء ءرءم ب
ضءرء فم وه امك لمءءال ب ءي ش لك أءبي ، DNS مءا في لء مءال DNS.



Configuration network settings.

- Device Summary
- Change Password
- Cisco Cloud
- Network**
- Date and Time
- Certificate Authorities
- Proxy
- Notifications
- License
- Email
- Backup
- SSH
- Syslog
- Updates
- Services

Admin	eth0 / 00:0C:29:A6:4A:11
	IP Assignment 192.168.75.92 More details
Interface	eth1 / 00:0C:29:A6:4A:1B
	IP Assignment 192.168.75.93 More details
	IP Assignment <input type="text" value="Static"/>
	IP Address <input type="text" value="192.168.75.93"/>
	<input checked="" type="checkbox"/> Check for IP Address conflicts
	Subnet Mask <input type="text" value="255.255.255.0"/>
	Gateway <input type="text" value="192.168.75.1"/>

Warning: Address and Hostname Changes

If you change the IP address of the interface you must also update the DNS records for each of your configured hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.

[View the Configuration help page for a list of affected services.](#)

DNS
Primary DNS Server <input type="text" value="192.168.75.4"/>



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

[Reconfigure Now](#)

[Reconfiguration](#)

Configuration saved.



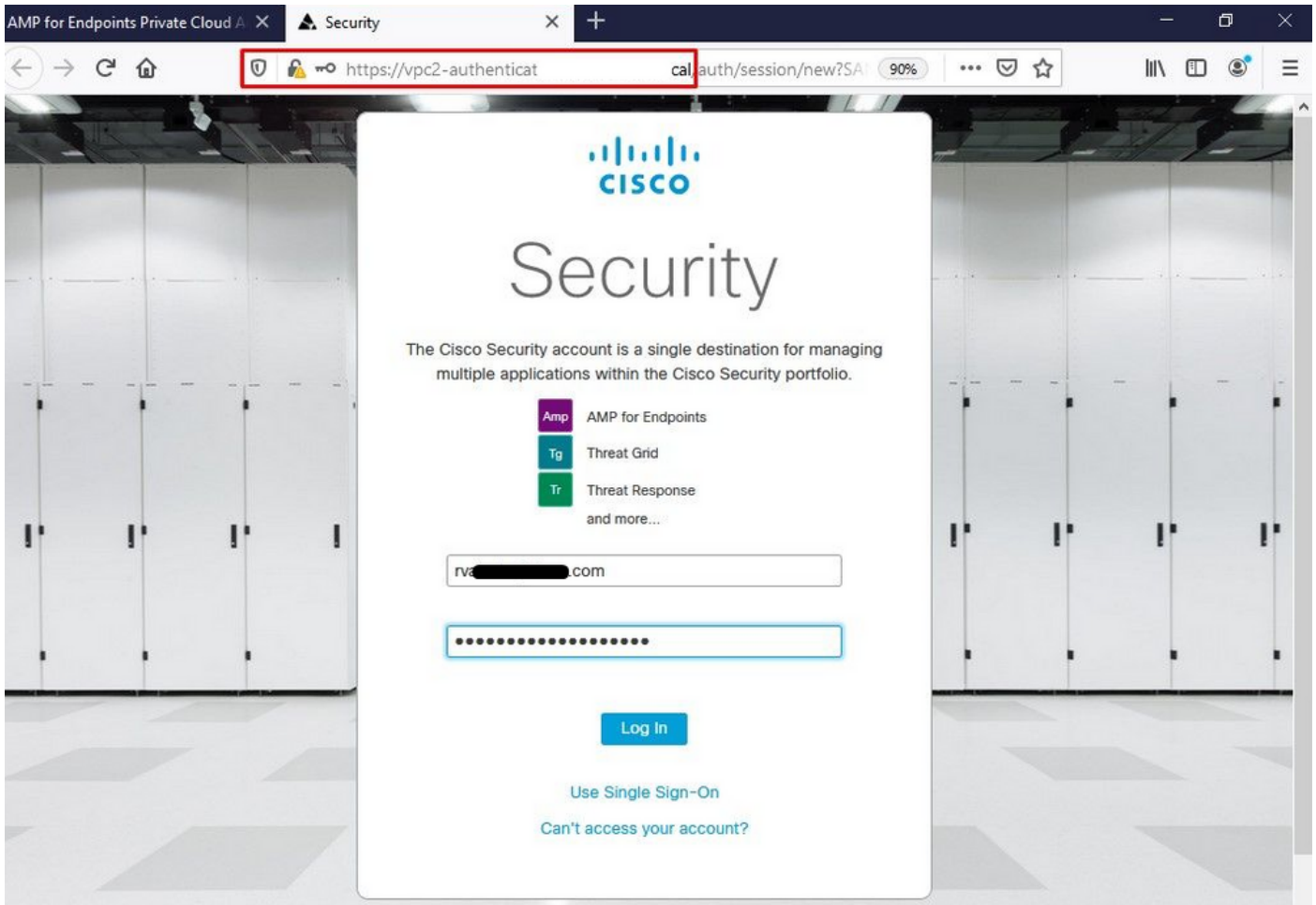
State	Started	Finished	Duration
▶ Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	⌚ Please wait...	⌚ Please wait...

Output

```
[2021-04-12T00:20:43+00:00] DEBUG: Found current_uid == nil, so we are creating a new file, updating owner
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] owner changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_gid == nil, so we are creating a new file, updating group
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] group changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_mode == nil, so we are creating a new file, updating mode
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] mode changed to 600
[2021-04-12T00:20:43+00:00] DEBUG: Restoring selinux security content with /sbin/restorecon -R "/tmp/cqlsh_check_superuser_passwo
rd.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/run/cookbooks/cassandra/pro
viders/cqlsh.rb line 16)
[2021-04-12T00:20:43+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:43+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
[2021-04-12T00:20:43+00:00] INFO: Retrying execution of execute[cqlsh_check_superuser_password], 19 attempt(s) left
[2021-04-12T00:20:45+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Chef::Provider::Execute]
[2021-04-12T00:20:45+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_password] is Chef::Provide
r::Execute
```

Download Output

لصوملا لي زنتو لوخذلا لي جست كنكمي ةلحرمللا هذه يف



چمانربال كدعاسي .كتئيبل يلوألا "نمآلا ةياهنلا ةطقن" جهن چلاعم يلعل لوصحلل كنكمي لامعتلا لىلة فاضلاب ،دوجو هل ناك نإ ،همدختست يذلا تاسوري فلا ةحفاكم چتتم رايخا يف دمتهي ... "بسانم دادعإ" رزلا ديدحت .اهرشن يف بغرت يتلا تاسايسلا عاونأو ،يسكوربال عم لوصولل ليغشت ماظن يلعل .

تاجتتم رتخأ .ةروصلل يف حضوم وه امك ،ةدوجومل نامألا تاجتتم ةحفص يلعل لوصحلل كنكمي عنمل قيبطتلل ةلباق تاداعبتسا عاشنإب ايئاقلت موقوي وهف .اهمدختست يتلا نامألا يلاتلا يف ديدحت .كب ةصاخلا ةياهنلا طاقن يلعل ءادألا يف لكاشم ثودح .

AMP for Endpoints Private Cloud X Dashboard X +

← → ↻ 🏠 🔒 https://vpc2-consol dashboard/fresh 📄 ⋮ 📌 ⚙️

CISCO AMP for Endpoints 🔔 ? Roman Valenta ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾ 🔍 Search

Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

Getting Started

- [View Online Help](#)
- [Download Cisco AMP for Endpoints User Guide](#)
- [Download Cisco AMP for Endpoints Deployment Strategy](#)

Deploy AMP for Endpoints Connectors

- [Set Up Windows Connector](#)
- [Set Up Mac Connector](#)
- [Set Up Linux Connector](#)

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by populating your Console with replayed data from actual malware infections. Enabling Demo Data will add computers and events to your Cisco AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, and Detections and Events displays behave when malware is detected. Demo Data can coexist with live data from your Cisco AMP for Endpoints deployment, however, because of the severity of some of the Demo Data

Demo Computers

WannaCry [Click here to view PDF](#)
The WannaCry attack involves a remote compromise through the Windows SMB (Server Message Block) service using the ETERNALBLUE exploit. Upon system compromise, the attacker drops the WannaCry ransomware variant that is initially identified by AMP for Endpoints using ransomware indicators of compromise, and later by AMP Cloud signatures.

SFEicar [Click here to view PDF](#)
Learn how Indications of Compromise can alert you to potential malware problems and how to determine their effects in Device Trajectory.

ZAccess [Click here to view PDF](#)
Use Device Trajectory to watch a rootkit exploit privilege escalation on a computer, and use File Trajectory to discover which other endpoints have been compromised.

ZBot [Click here to view PDF](#)
See how a vulnerable version of Internet Explorer can expose you to malware. Use Device Trajectory to learn what happened and use application blocking lists to stop the future execution of vulnerable programs.

CozyDuke [Click here to view PDF](#)
Trace a detection back to an abused DLL search path, block any communications to its upstream CnC, and deploy an Endpoint IOC to contain further attacks.

لصوملا ليزنت

🟢 Step 1: Existing Security Products

🟢 Step 2: Set Up Proxy

🟢 Step 3: Download Connector

Audit Only	Protect	Triage	Server	installing a connector on Windows Domain Controllers.
Used when you're still learning about the product and want to install it without any impact to your existing systems.	Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.	Used when you have a known or suspected infected machine.	Used when you're installing a connector on standard Windows servers.	
Policy Details	Policy Details	Policy Details	Requirements	Requirements
Files Audited Network Blocked Offline Engine TETRA	Files Quarantined Network Blocked Offline Engine TETRA	Files Quarantined Network Blocked Offline Engine TETRA	Files Audited Network Off Offline Engine TETRA	Files Audited Network Off Offline Engine TETRA
Download	Download	Download	Download	Download

[< Back](#)
[Next >](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

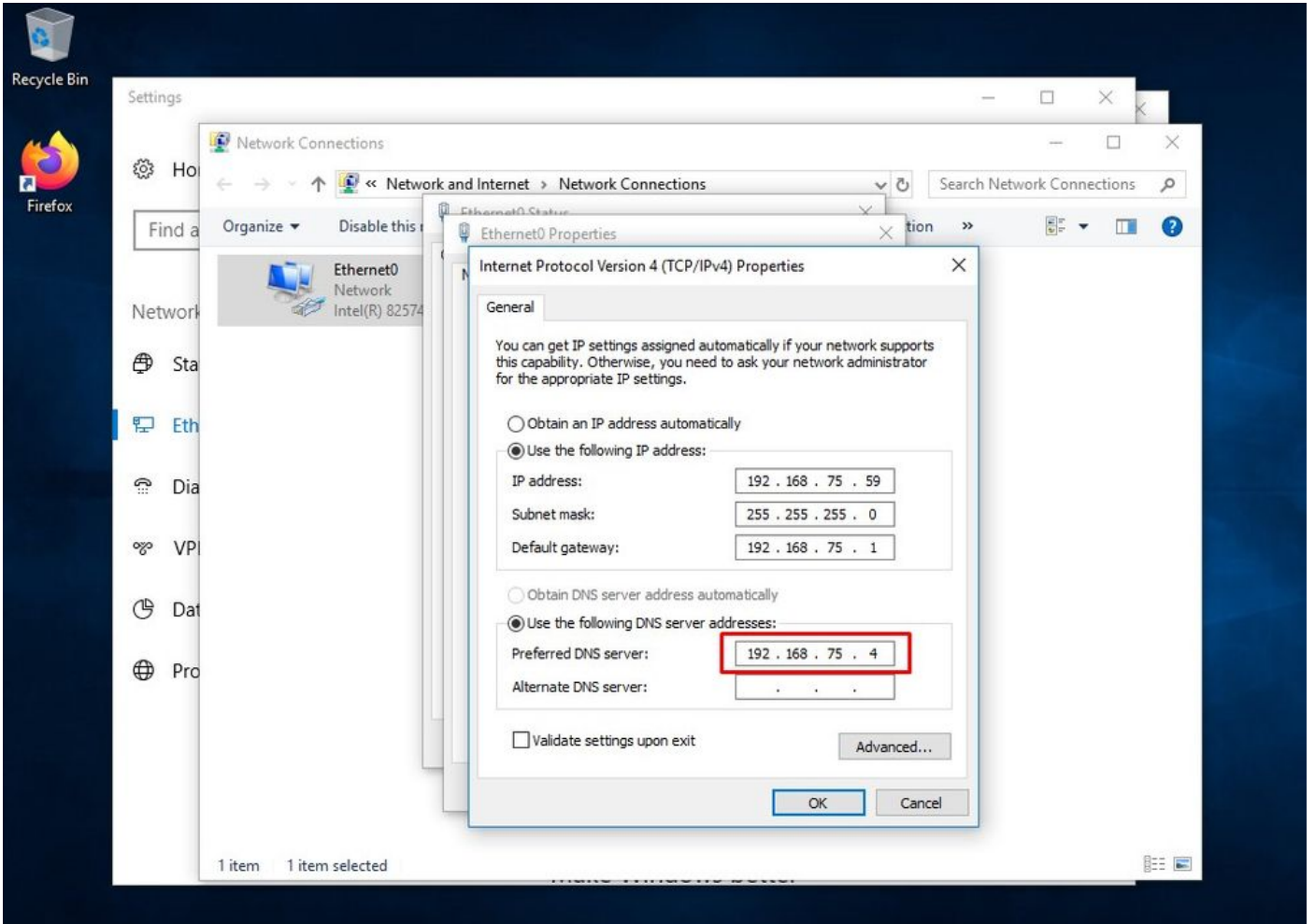
You have chosen to open:

amp_Protect.exe
 which is: exe File
 from: https://vpc-console.cyberworld.local

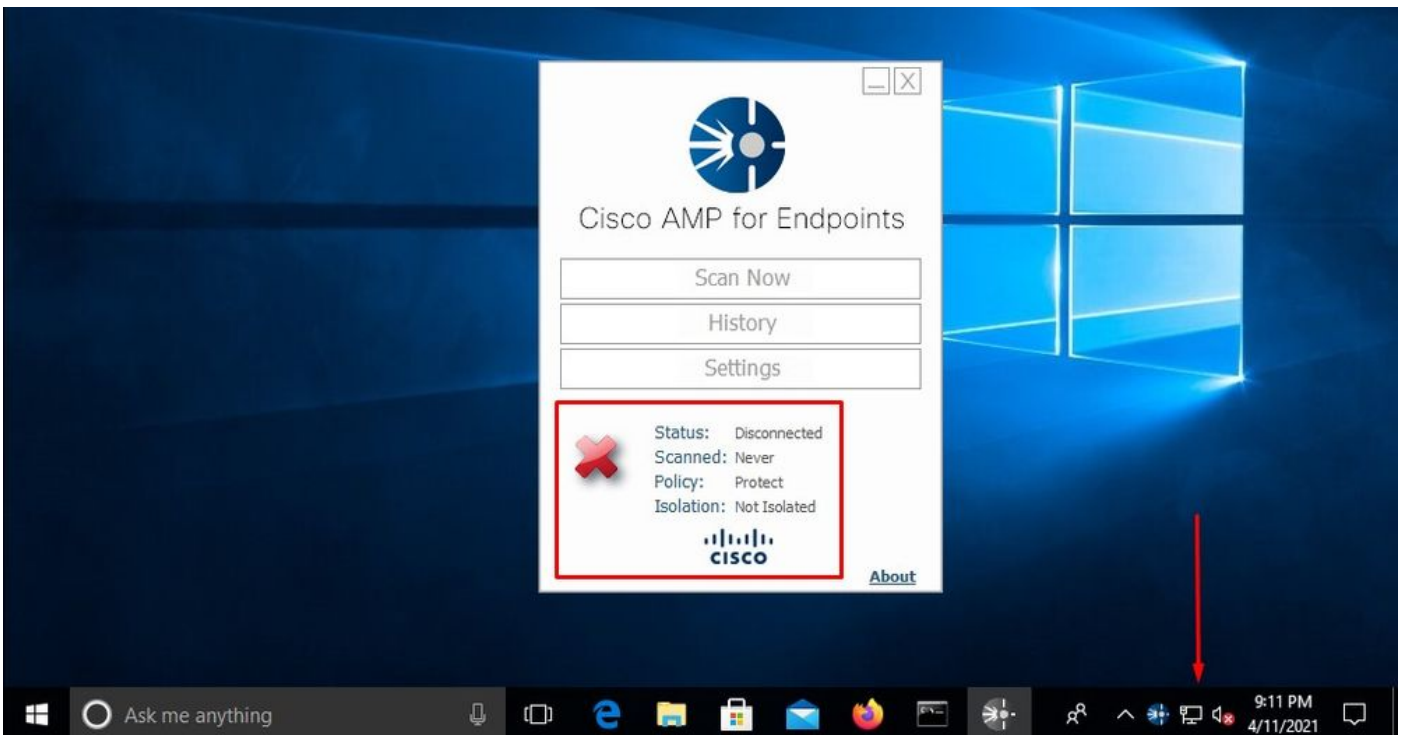
Would you like to save this file?

رذجال قدصملا عجرملا عم ةلكشم - 2 مقرة لكشملا

كب ةصاخلا ةيلخادلا تاداهشلا مدختست تنك اذا يه اههجاوت نأ نكمي يتلا ةيلاتلا ةلكشملا لصلتم ريغ هنا لعل لصلوملا رهظي نأ نكمي، لوالا تيبتتلا دعب هنا يه.



طوش. قةلصتم ريغ اهنأ لىلع اهتيرؤن كمى لىصوم لل ةنمآلا ةياهنلا ةطقن تيبتت درجمب رادصإلا تدح عيطتسي تنأ، log لال لال رظناو ةمزح صيخش



عجرملا أطخ ةيرؤن كمى، ةصيخشلا ةمزحلا نم هعيجت مت يذلا جارحإلا اذه لىلإ ادانتسا

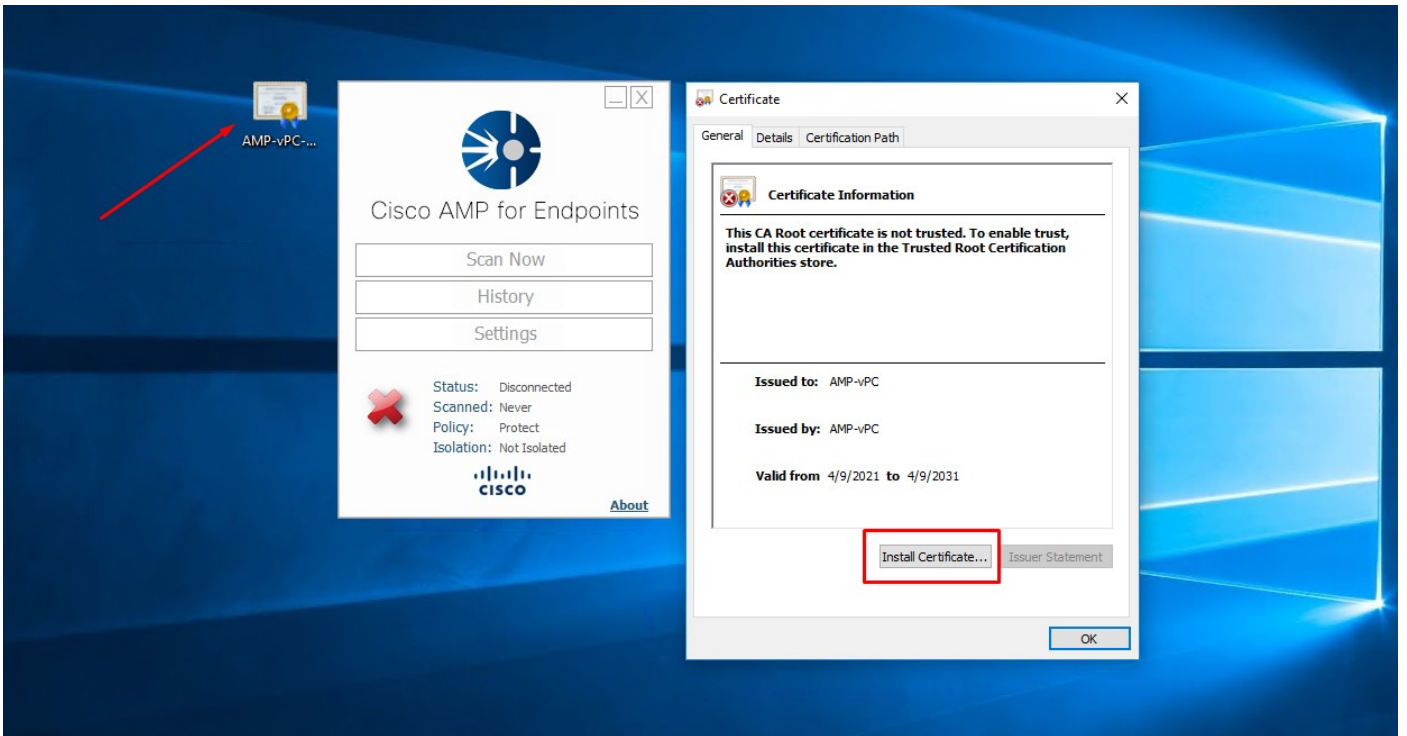
رذجل ا قءصم ل

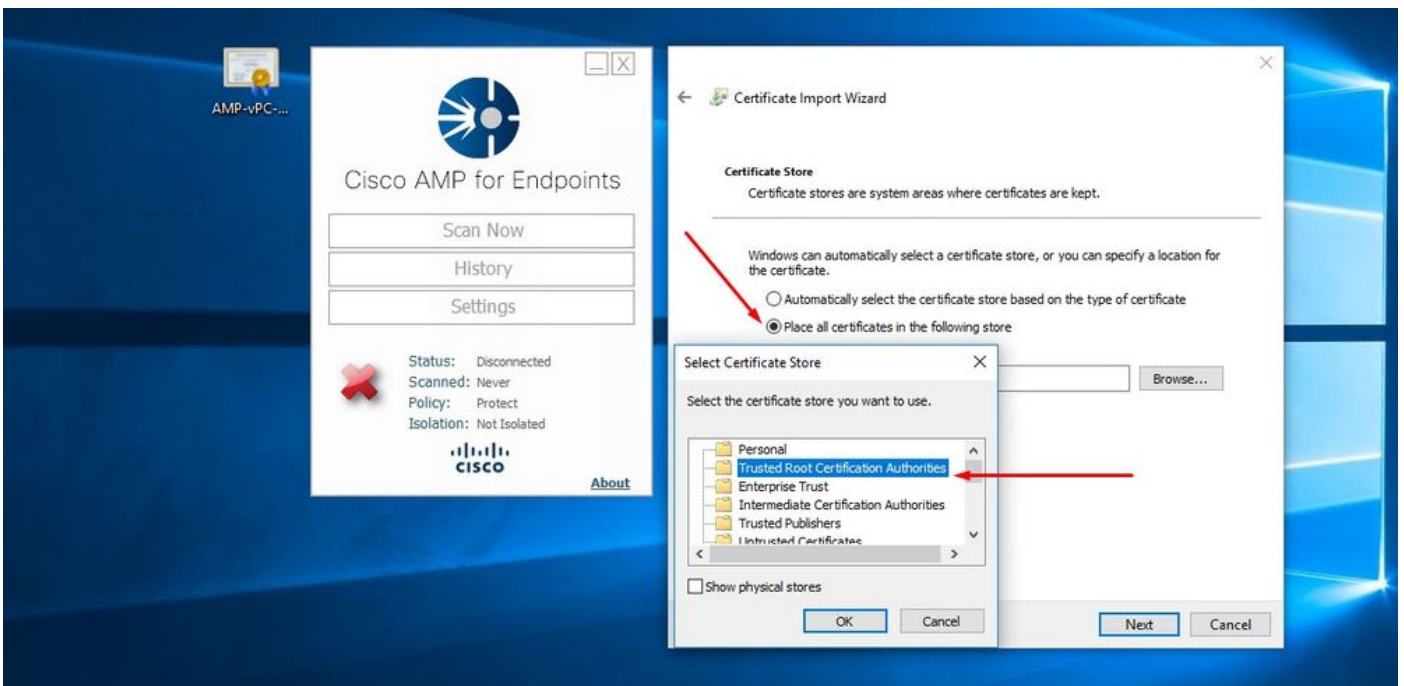
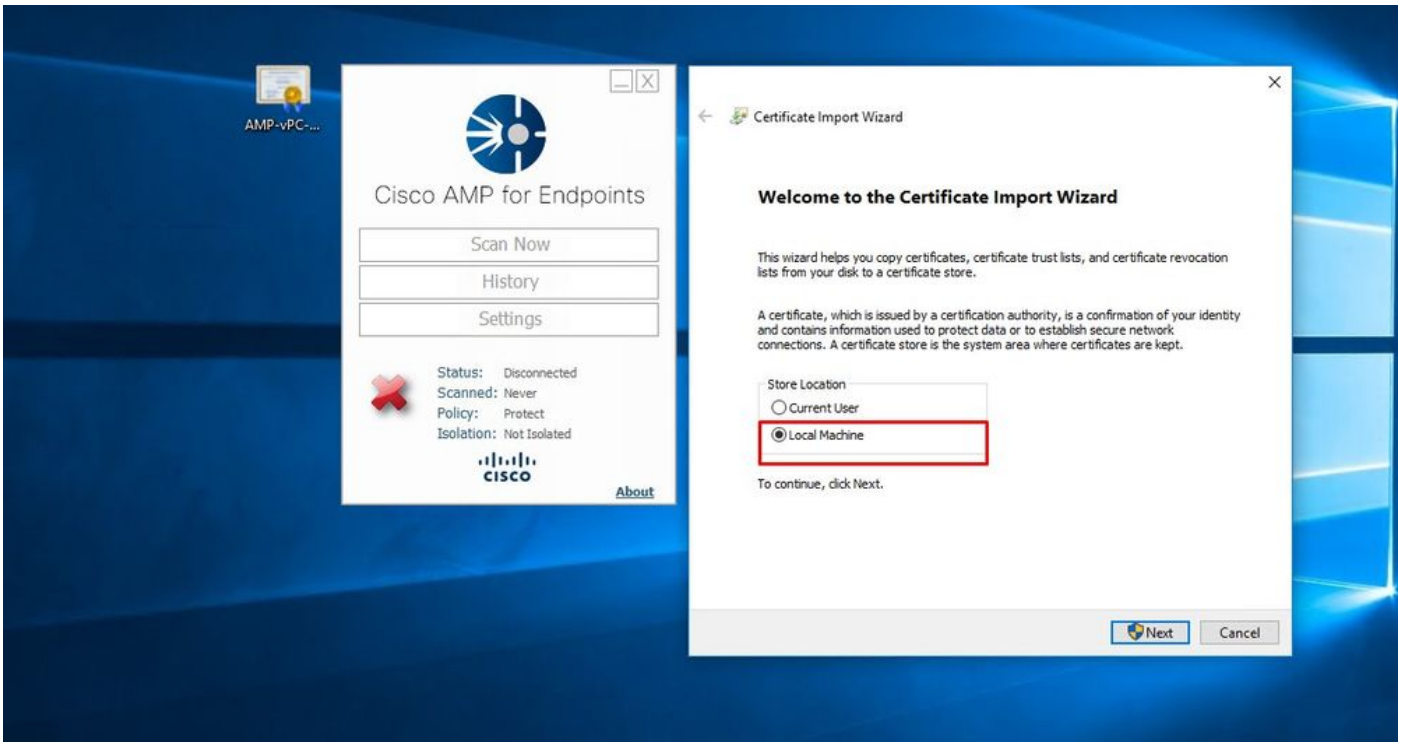
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworld

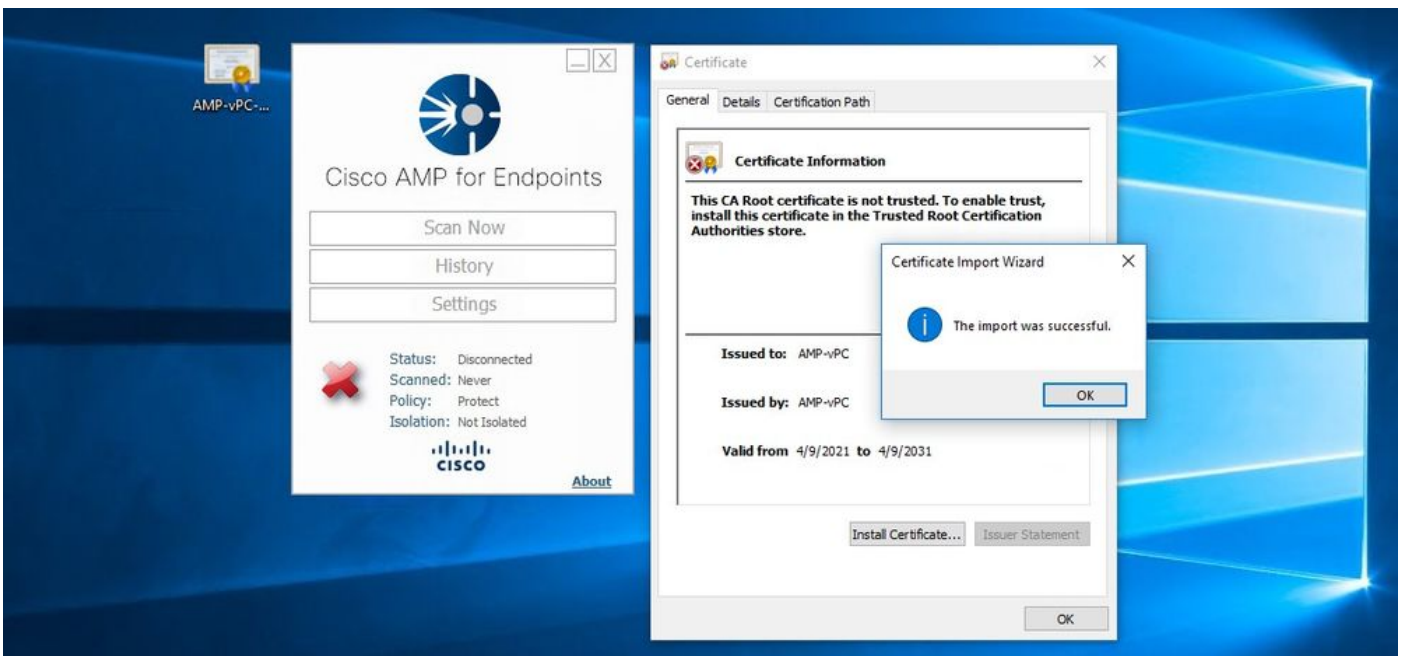
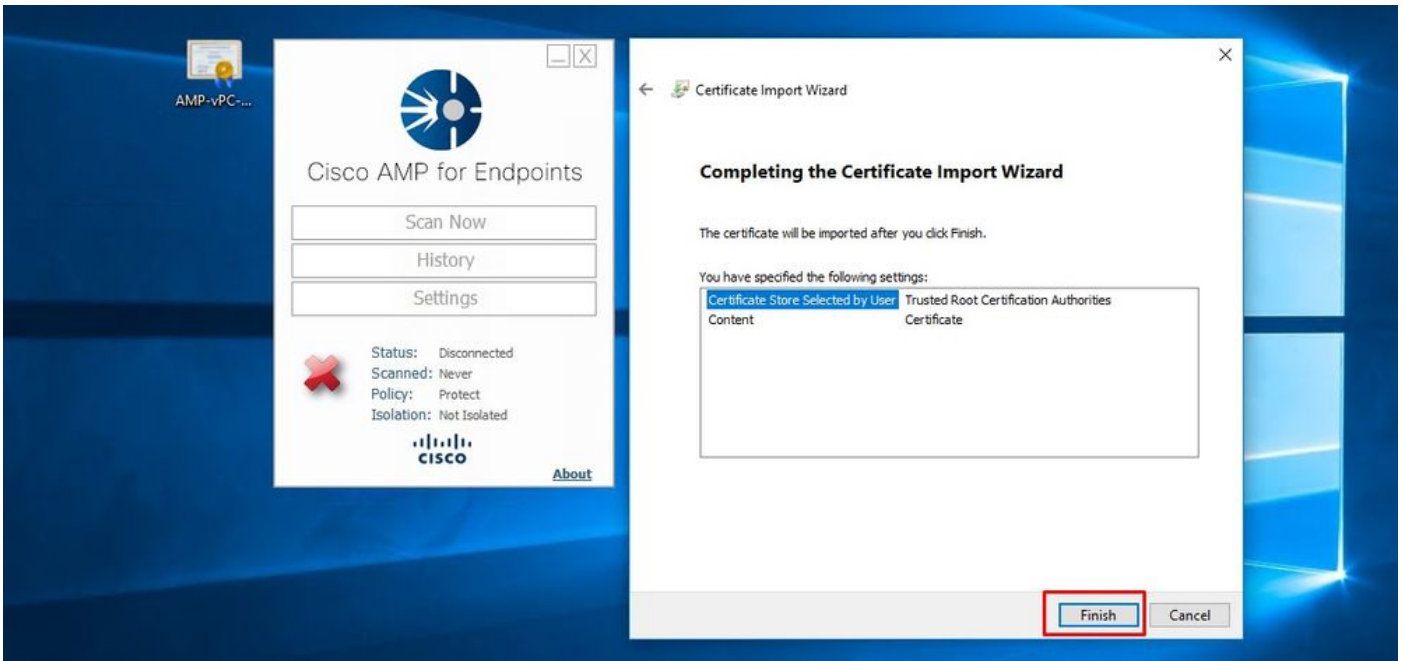
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat

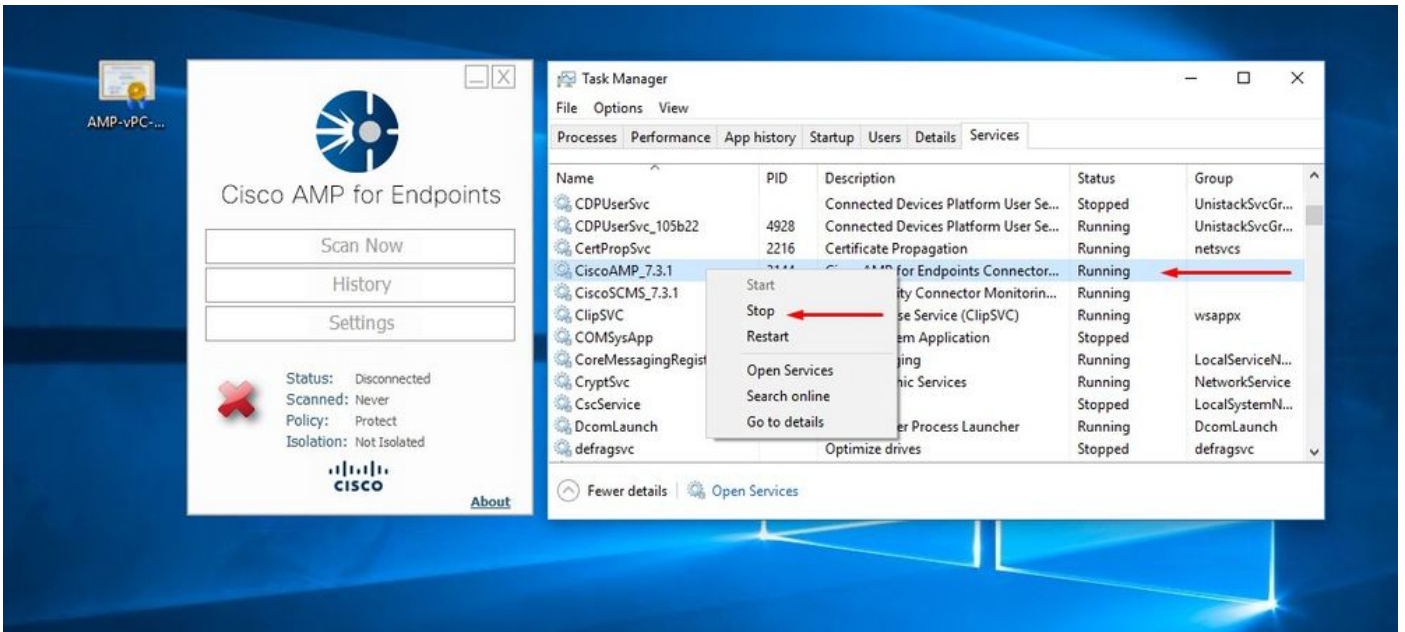
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60

ءءاع ءو هب قوؤوم ل رذجل ا قءصم ل اءرمل ن زخم ي ف رذجل ا قءصم ل اءرمل ل ي مءء ءرءم ب
عقوؤم وه امك لمع ل اب اءب ي عي ش لك . ءنم آل ءه ان ل ءطقن ءم ءخ ل ي ءشء

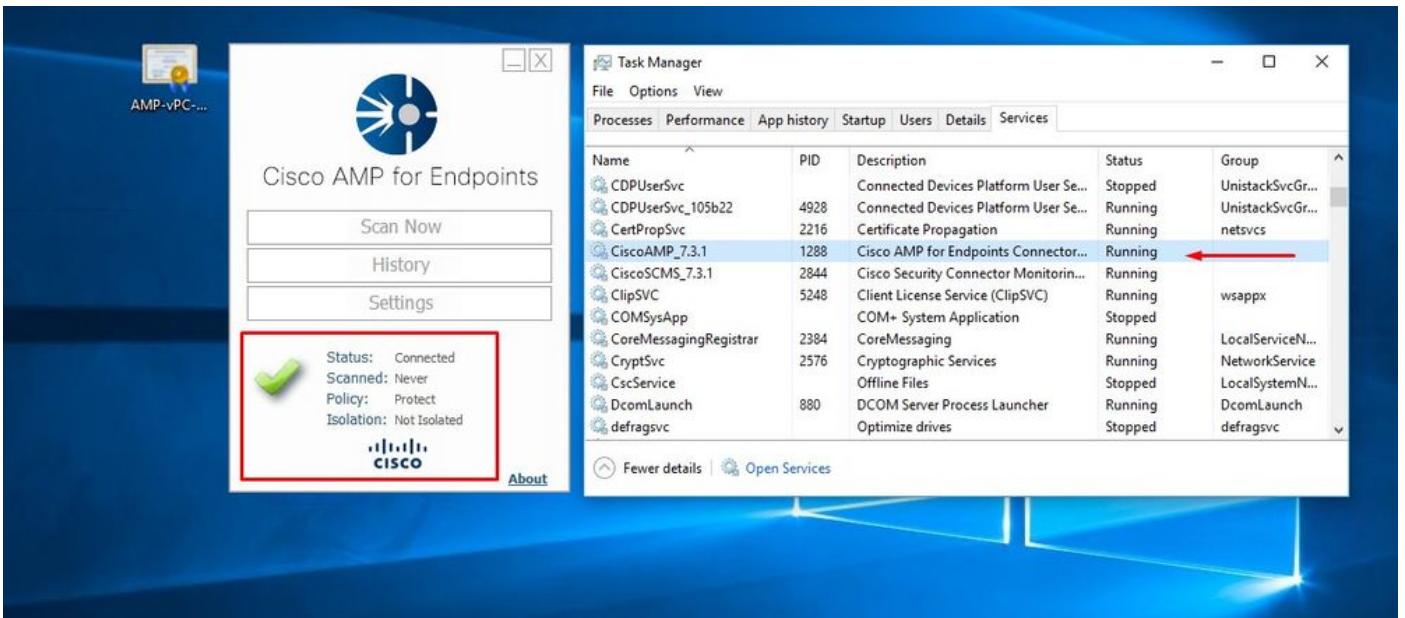








عقوتم وه امك الصتم حبصي ةنمآلا ةياهنلا ةطقن ةمدخ لصوم دادترا درجمب.



The screenshot displays the AMP for Endpoints Private Cloud console dashboard. At the top, the browser address bar shows the URL `https://vpc2-console`. The dashboard header includes navigation tabs for Dashboard, Analysis, Outbreak Control, Management, and Accounts, along with a search bar. The main content area is divided into several sections:

- Dashboard Summary:** Shows a 0% compromise rate. Includes controls for Refresh All, Auto-Refresh, and a date range filter (30 days, 2021-03-13 01:43 to 2021-04-12 01:43 UTC).
- Inbox Status:** Displays 0 Require Attention, 0 In Progress, and 0 Resolved items.
- Compromises:** A large empty box with a "Protect" button.
- Quarantined Detections:** A large empty box with a "Protect" button.
- Vulnerabilities:** A large empty box with a "Protect" button.
- Threat Grid Analysis:** Shows 0 Automatic Analysis Submissions and 0 Retroactive Threat Detections.
- Statistics:** Shows 0 Files Scanned and 0 Network Connections Logged.
- Connectors:** Shows 1 Connectors (highlighted with a red arrow), 0 Installs, and 0 Install Failures.
- Quick Start:** Provides links to Set Up Windows Connector, Set Up Mac Connector, and Set Up Linux Connector.
- Significant Compromise Artifacts:** Shows "No artifacts".
- Compromise Event Types:** Shows "No event types".

هرابتخا مت راض طاشن

Dashboard

Dashboard **Inbox** Overview Events

Refresh All Auto-Refresh

Reset New Filter

30 days 2021-03-13 01:56 2021-04-12 01:56 UTC

0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

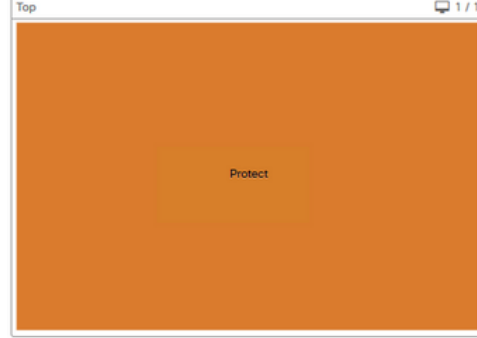
Compromises

Inbox 0 / 1



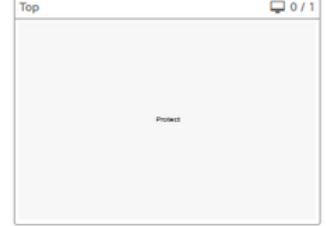
Quarantined Detections

Quarantine Events 1 / 1



Vulnerabilities

View 0 / 1



Threat Grid Analysis

0 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

0 Files Scanned
0 Network Connections Logged

Connectors

1 Connectors
0 Installs
0 Install Failures

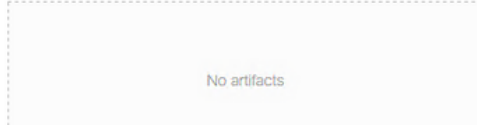
Quick Start

Set Up Windows Connector

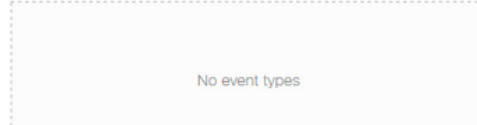
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Significant Compromise Artifacts



Compromise Event Types



ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل