

Installazione e configurazione di Secure Endpoint Virtual Private Cloud

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Installazione di VPC](#)

[Installazione VM](#)

[Configurazione iniziale dell'interfaccia di amministrazione](#)

[Configurazione iniziale del vPC tramite GUI Web](#)

[Configurazione](#)

[Servizi](#)

[Pacchetto di aggiornamento di AirGap](#)

[Problema 1 - Spazio esaurito nell'archivio dati](#)

[Problema 2 - Aggiornamento precedente](#)

[Risoluzione dei problemi di base](#)

[Problema 1 - FQDN e server DNS](#)

[Problema n. 2 - Problema con la CA radice](#)

Introduzione

In questo documento viene descritto come implementare correttamente Virtual Private Cloud (VPC) sui server in ambiente ESXi. Per altri documenti, quali Guida introduttiva, Strategia di distribuzione, Guida ai diritti, Console e Guida per l'amministratore, visitare il sito [Documentazione](#)

Contributo di Roman Valenta, Cisco TAC Engineers.

Prerequisiti

Requisiti:

VMware ESX 5 o successivo

- Modalità cloud-proxy (solo): 128 GB di RAM, 8 core CPU (2 CPU con 4 core ciascuno consigliato), 1 TB di spazio minimo disponibile su disco nell'archivio dati VMware
- Tipo di unità: SSD necessaria per la modalità air gap e consigliata per il proxy
- Tipo RAID: un gruppo RAID 10 (mirroring con striping)
- Dimensioni minime archivio dati VMware: 2 TB
- Numero minimo di letture casuali di datastore per il gruppo RAID 10 (4K): 60K IOPS
- Numero minimo di scritture casuali dell'archivio dati per il gruppo RAID 10 (4K): 30K IOPS

Cisco raccomanda la conoscenza di questo argomento:

- Conoscenze base di utilizzo dei certificati.
- Informazioni di base sulla configurazione del DNS nel server DNS (Windows o Linux)
- Installazione di un modello di Open Virtual Appliance (OVA) in VMWare ESXi

Utilizzato in questo laboratorio:

VMware ESX 6.5

- Modalità cloud-proxy (solo): 48 GB di RAM, 8 core CPU (2 CPU con 4 core ciascuno consigliato), 1 TB di spazio minimo disponibile su disco nell'archivio dati VMware
- Tipo di unità: SATA
- Tipo RAID: un RAID 1
- Dimensioni minime archivio dati VMware: 1 TB
- MobaXterm 20.2 (programma multi-terminale simile a PuTTY)
- Cygwin64 (utilizzato per scaricare l'aggiornamento di AirGap)

Inoltre

- Certificato creato con openssl o XCA
- Server DNS (Linux o Windows) Nel mio laboratorio ho utilizzato Windows Server 2016 e CentOS-8
- VM Windows per l'endpoint di test
- Licenza

Se la memoria è inferiore a 48 GB di RAM sulla versione 3.2+ VPC, non è più possibile utilizzarla.



Nota: il cloud privato OAV crea le partizioni dell'unità in modo che non sia necessario specificarle in VMWare. server che risolve il nome host dell'interfaccia pulita.

Per ulteriori informazioni sui requisiti hardware specifici della versione, consultare la [scheda tecnica dell'accessorio VPC](#).



Nota: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

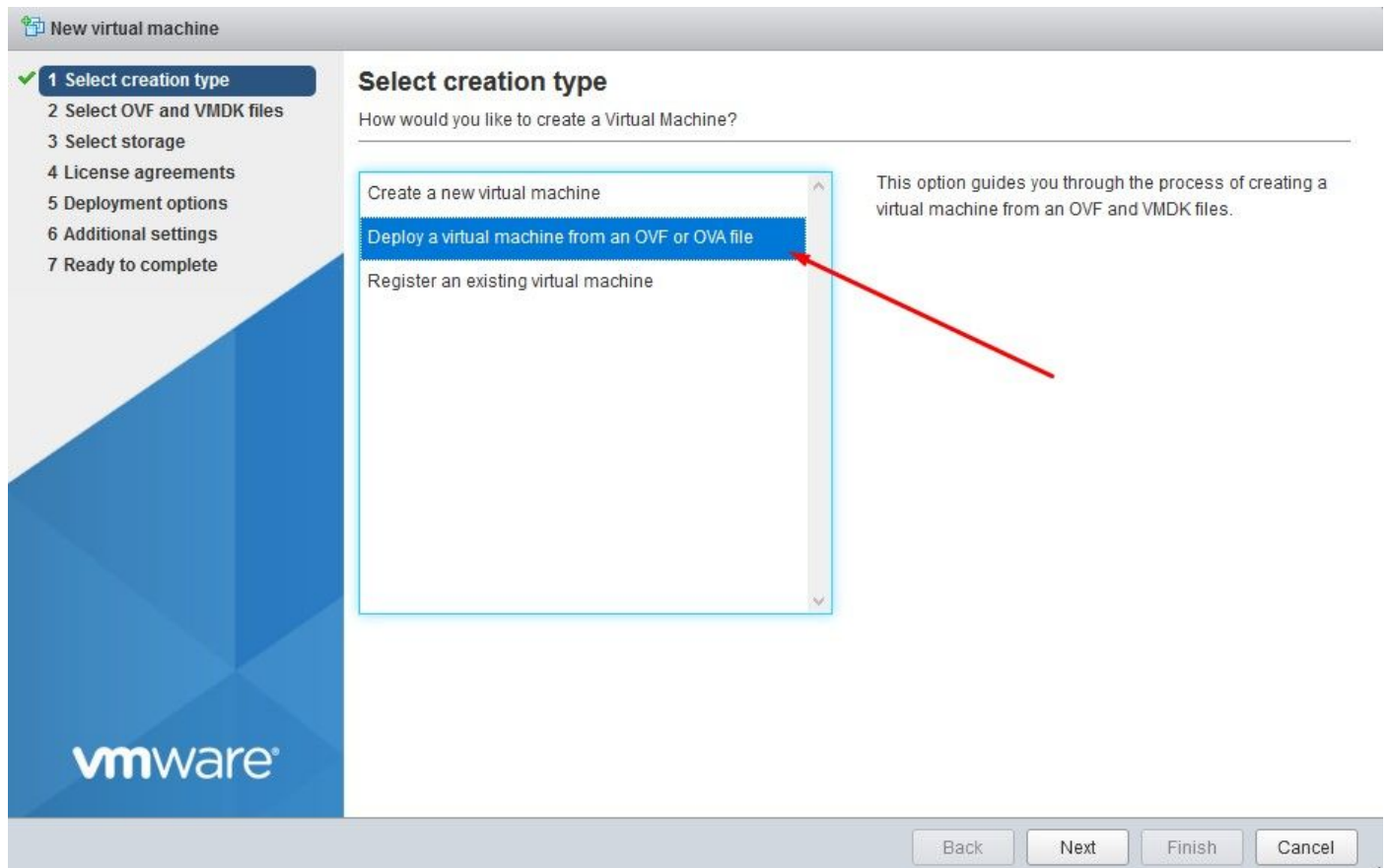
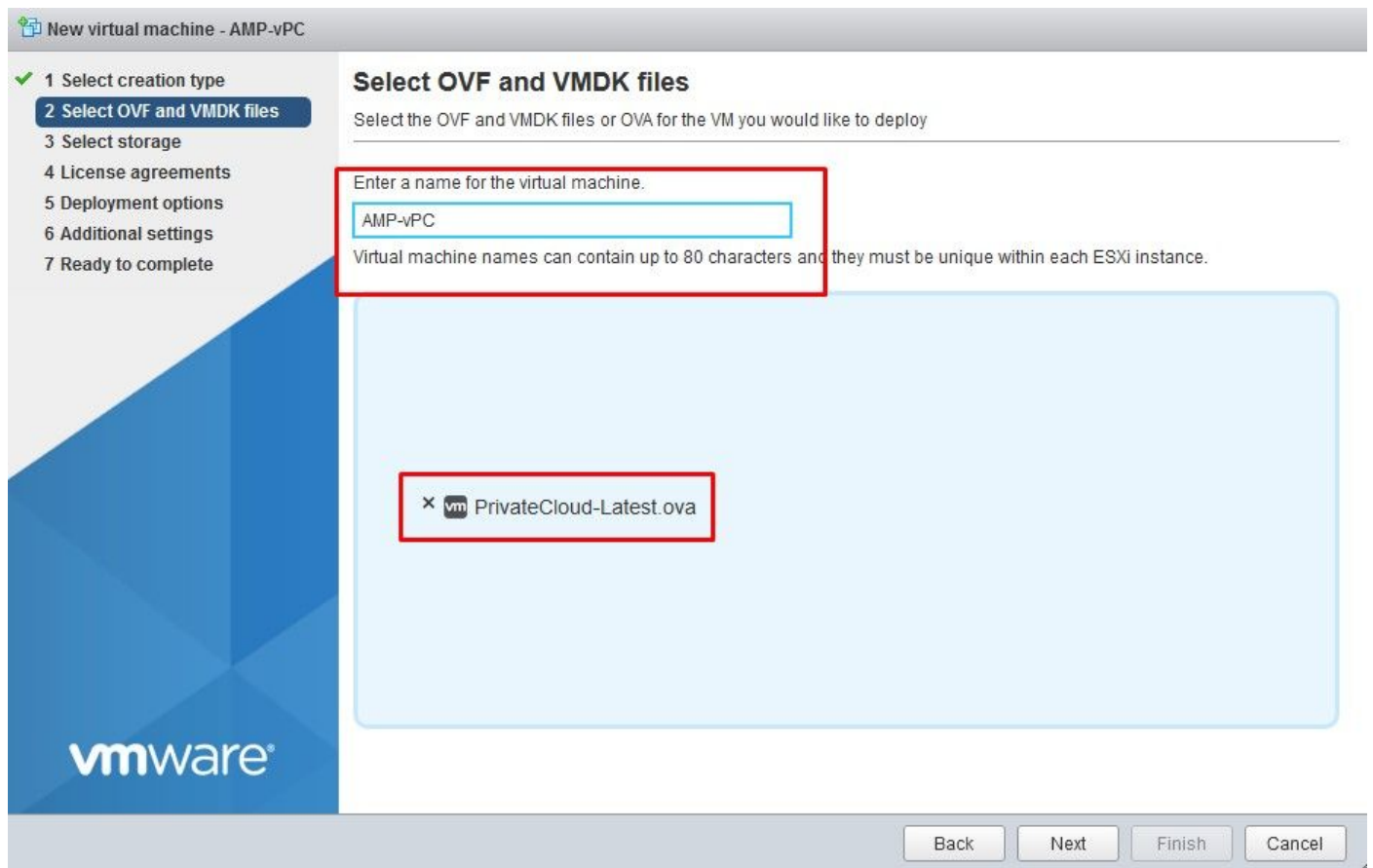
Installazione di VPC

Selezionare l'URL fornito nell'e-mail di eDelivery o di adesione. Scaricare il file OVA e procedere con l'installazione

Installazione VM

Fase 1:

Passare a File > Distribuisci modello OVF per aprire la procedura guidata Distribuisci modello OVF, come mostrato nell'immagine.



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.

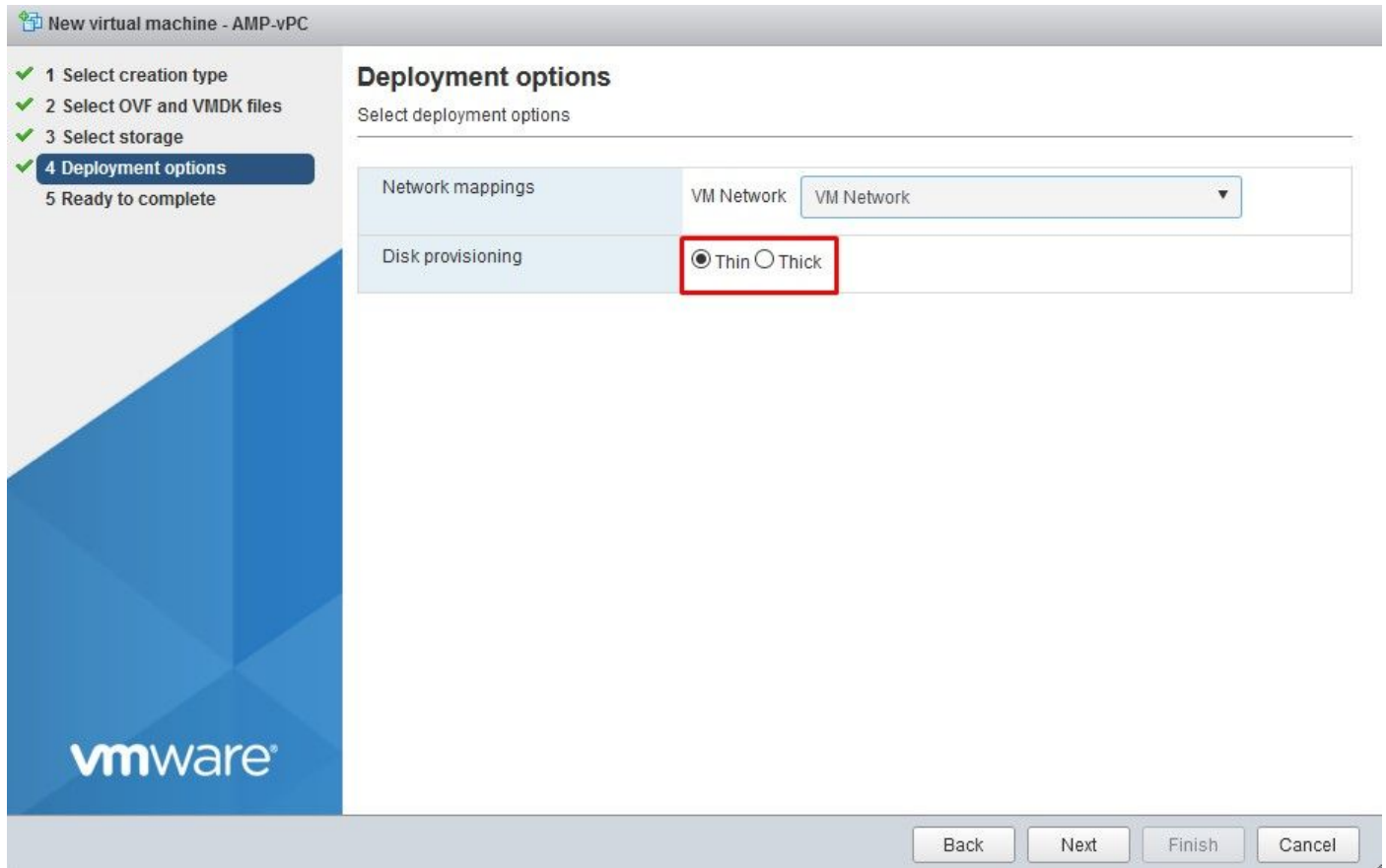
Name	Capacity	Free	Type	Thin pro...	Access
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	Supported	Single
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	Supported	Single
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	Supported	Single

4 items

vmware

Back Next Finish Cancel

 Nota: Thick Provisioning riserva spazio quando viene creato un disco. Se si seleziona questa opzione, è possibile migliorare le prestazioni rispetto al thin provisioning. Tuttavia, non è obbligatorio. Selezionare Avanti, come mostrato nell'immagine.



Passaggio 2:

Selezionare Sfoglia... per selezionare un file OVA, quindi scegliere Avanti. Nella pagina Dettagli modello OVF si notano i parametri OAV predefiniti, come mostrato nell'immagine. Selezionare Avanti.


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.

Back Next Finish Cancel



Configurazione iniziale dell'interfaccia di amministrazione


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.

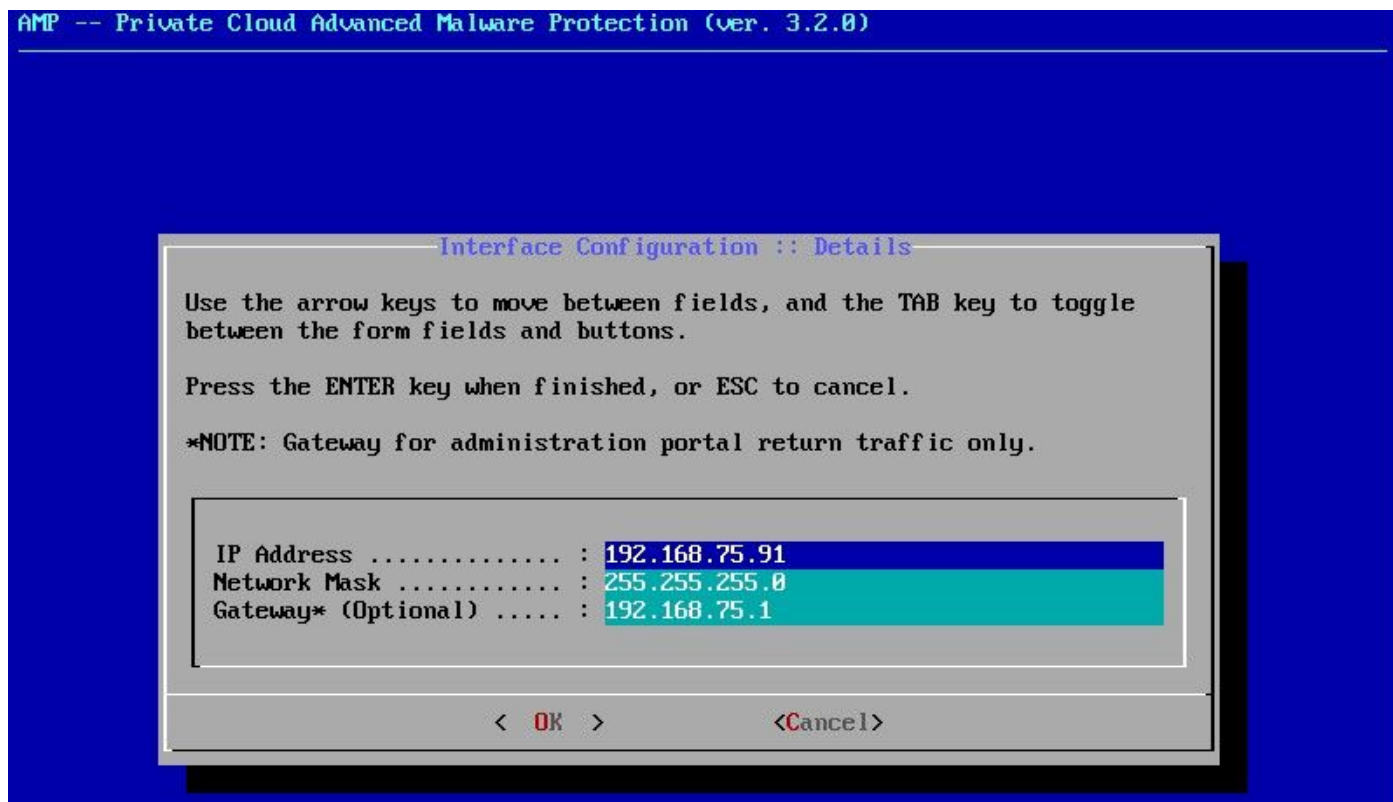
Back Next Finish Cancel



Una volta avviata la VM, è possibile eseguire la configurazione iniziale tramite VM Console.

Passaggio 1:

È possibile notare che l'URL indica [UNCONFIGURED] (NON CONFIGURATO) se l'interfaccia non ha ricevuto un indirizzo IP dal server DHCP. Questa interfaccia è l'interfaccia di gestione. Questa non è l'interfaccia di produzione.



Passaggio 2:

È possibile spostarsi tra i tasti Tab, Enter e Arrow.

Passare a CONFIG_NETWORK e selezionare il tasto Invio sulla tastiera per iniziare la configurazione dell'indirizzo IP di gestione per il cloud privato dell'endpoint protetto. Se non si desidera utilizzare DHCP, selezionare No, quindi Enter key.

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.

60%

< OK >

Nella finestra visualizzata, scegliere Sì e selezionare Invio tasto.



Se l'indirizzo IP è già in uso, verrà visualizzato questo log degli errori. Tornate indietro e scegliete qualcosa di unico non in uso.

```
Restarting eth0...  
  
ERROR      : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr  
eady uses address 192.168.75.91.  
ERROR      : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr  
eady uses address 192.168.75.91.  
ERROR      : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr  
eady uses address 192.168.75.91.  
=====
```

```
ERROR: The interface failed to reconfigure.
```

```
=====
```

```
Press ENTER key to continue...  
-
```

Interface Configuration :: Details

Use the arrow keys to move between fields, and the TAB key to toggle between the form fields and buttons.

Press the ENTER key when finished, or ESC to cancel.

*NOTE: Gateway for administration portal return traffic only.

IP Address	: 192.168.75.92
Network Mask	: 255.255.255.0
Gateway* (Optional)	: 192.168.75.1

< OK > <Cancel>

Se tutto va bene, vedrete un output simile a questo

```

- 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
* template[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
* template[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

```

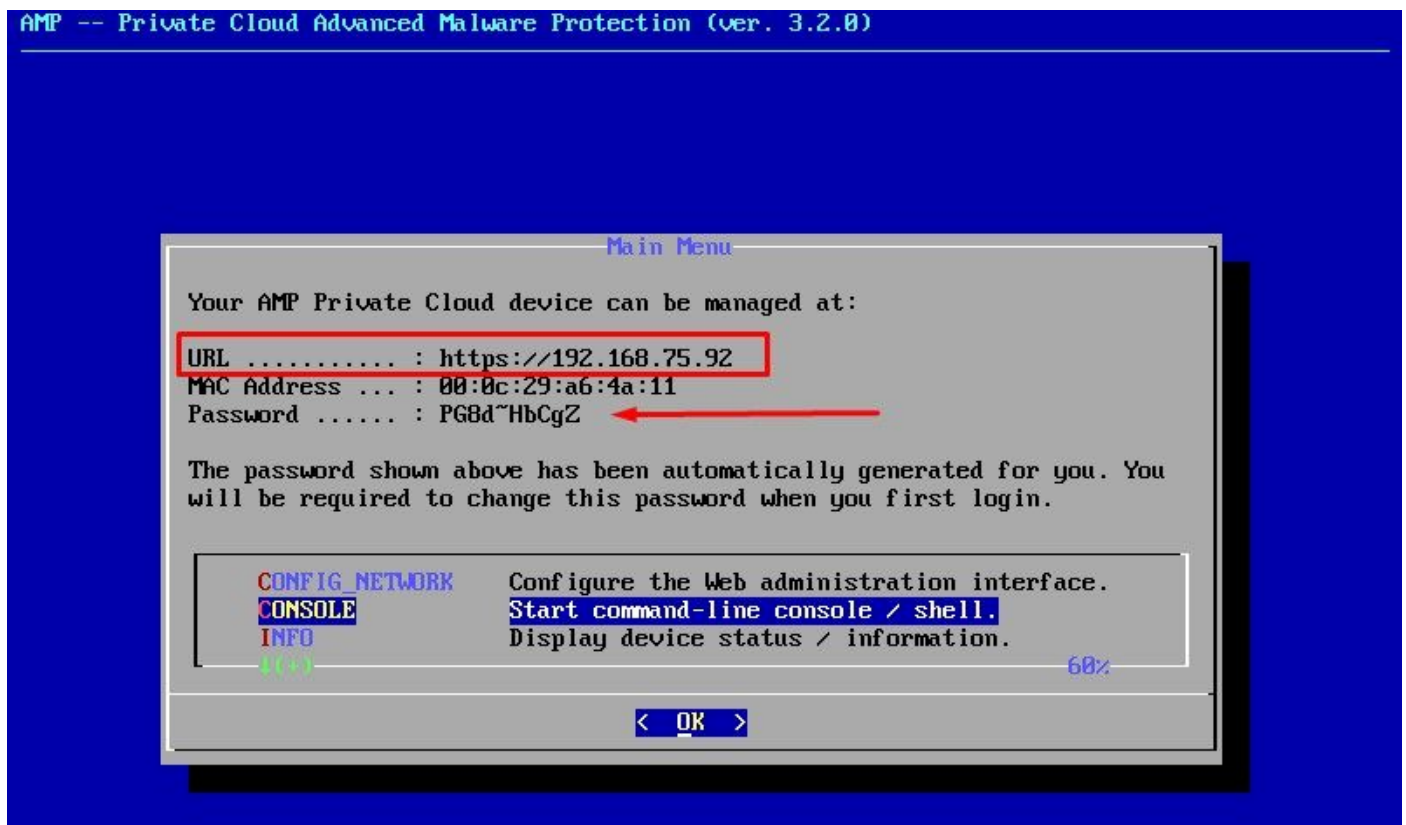
```
Restarting eth0...
```

```
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
```

Passaggio 3:

Attendere che la schermata blu venga visualizzata di nuovo con il nuovo indirizzo IP STATICO. Notare anche la password monouso. Prendi una nota e apriamo il nostro browser.

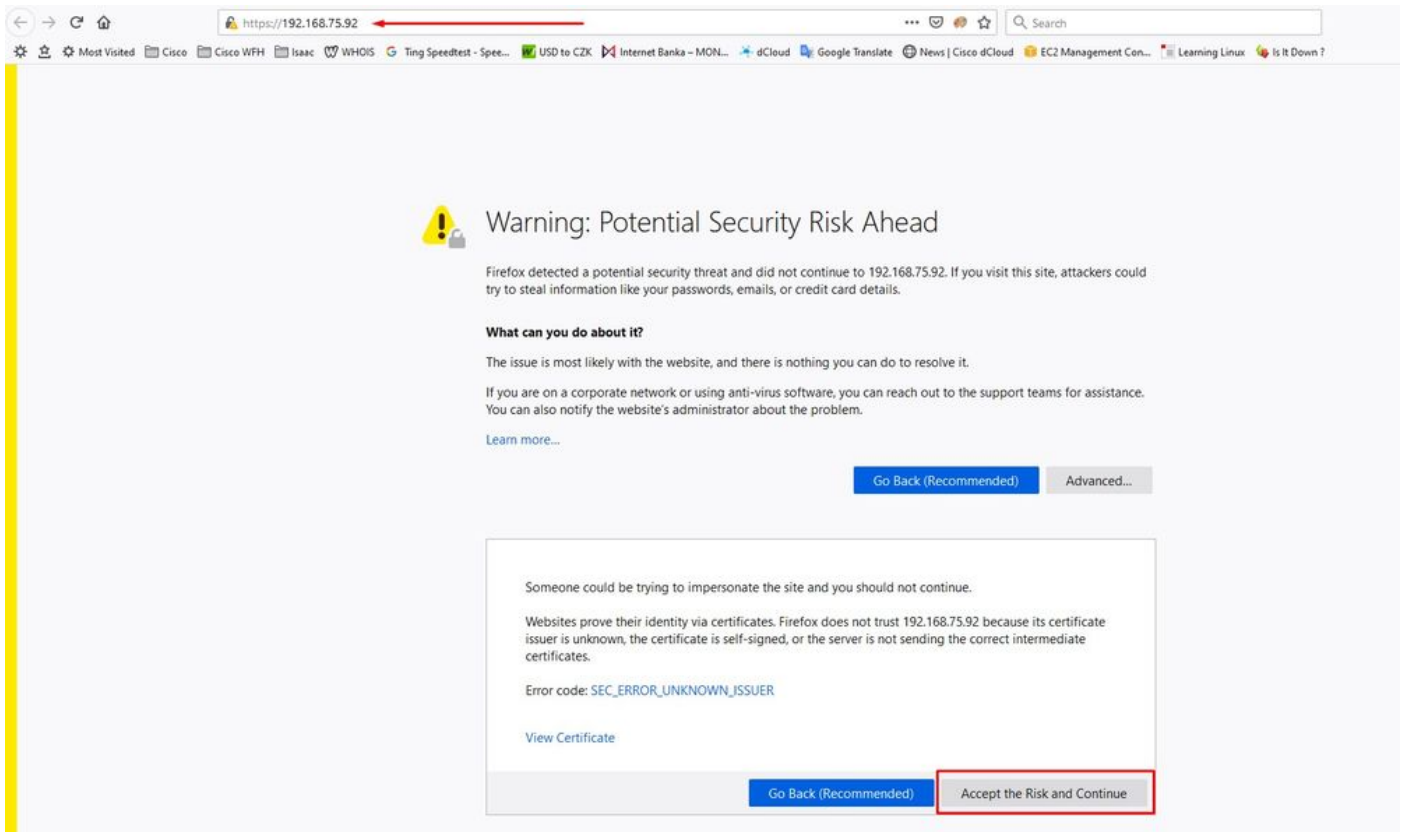


Configurazione iniziale del vPC tramite GUI Web

Passaggio 1:

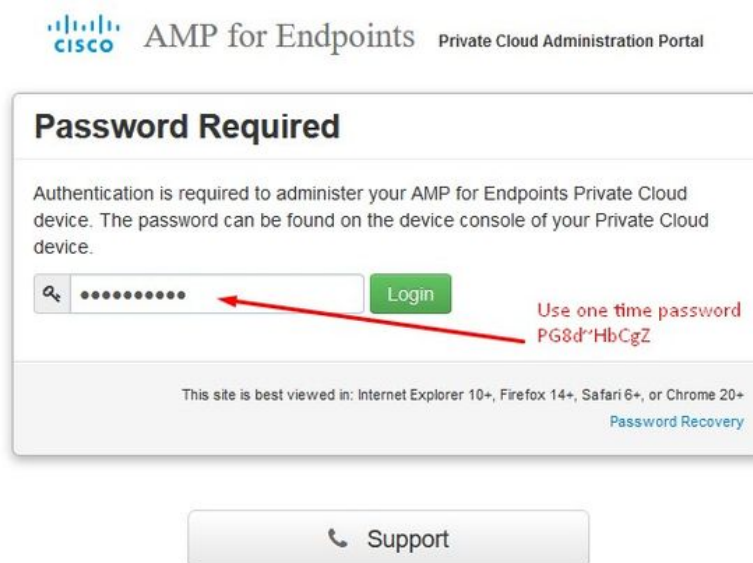
Aprire un browser Web e selezionare l'indirizzo IP di gestione dell'accessorio. È possibile ricevere un errore di certificato poiché il cloud privato dell'endpoint sicuro genera inizialmente il proprio certificato HTTPS, come mostrato nell'immagine. Configurare il browser per considerare attendibile il certificato HTTPS autofirmato di Secure Endpoint Private Cloud.

Nel browser digitare l'indirizzo IP STATICO configurato in precedenza.



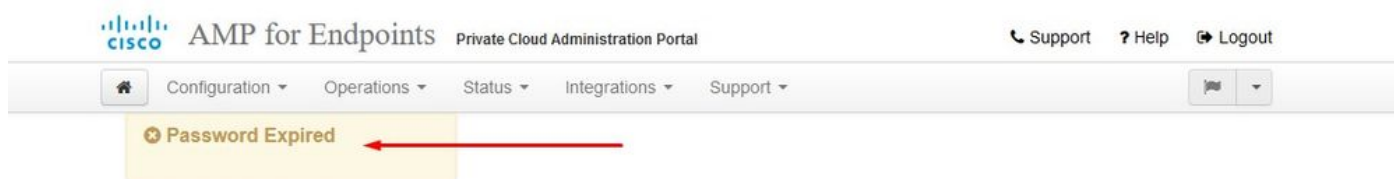
Passaggio 2:

Dopo aver eseguito l'accesso, è necessario reimpostare la password. Utilizzare la password iniziale della console nel campo Vecchia password. Utilizzare la nuova password nel campo Nuova password. Immettere nuovamente la nuova password nel campo Nuova password. selezionare Cambia password.



Passaggio 3:

Dopo aver eseguito l'accesso, è necessario reimpostare la password. Utilizzare la password iniziale della console nel campo Vecchia password. Utilizzare la nuova password nel campo Nuova password. Immettere nuovamente la nuova password nel campo Nuova password. selezionare Cambia password.



Change the password used to access the AMP for Endpoints Private Cloud Administration Portal and the device console. Note that this is also the root password for your device. ?

Warning
Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the device console.

The image shows a password change form with three input fields. The first field is labeled 'Old one time password' and has a red arrow pointing to it. The second and third fields are for the new password. A green 'Change Password' button is located below the fields.

Passaggio 4:

Nella pagina successiva scorrere verso il basso per accettare il contratto di licenza. selezionare Ho letto e accetto.



Passaggio 5:

Dopo aver accettato il contratto, viene visualizzata la schermata di installazione, come illustrato nell'immagine. Se si desidera eseguire il ripristino da un backup, è possibile eseguire questa operazione in questa pagina. Tuttavia, la presente guida prosegue con l'opzione Pulizia installazione. Selezionare Start nella sezione Clean Installation.



Installation Options

Only the License section can be altered after installation.

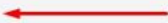
- Install or Restore
- License

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 >

Passaggio 6:

La prima cosa di cui avete bisogno è la licenza per andare avanti. Quando si acquista il prodotto, si riceve una licenza e una passphrase. Selezionare +Upload License File. Scegliere il file di licenza e immettere la passphrase. Selezionare Upload License (Carica licenza). Se il caricamento non riesce, verificare che la passphrase sia corretta. Se il caricamento ha esito positivo, viene visualizzata una schermata con le informazioni sulla licenza valide. Selezionare Avanti. Se non è ancora possibile installare la licenza, contattare il supporto tecnico Cisco.



Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License

License

Device ID
EG[REDACTED]V5

License
No license has been installed.

Install New License

license + Upload License File

.....

Upload License



License was successfully uploaded



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

License

Device ID
E60[REDACTED]5

License	
Licensee	Roman Valenta rva[REDACTED].com
Business	Cisco - rvalenta 395a6444[REDACTED]-7a86fb49b7a5
Validity	2021-04-01 - 2025-12-31
Product SKU	FP-AMP-CLOUD=
Seats	50

Replace License [\(click to expand\)](#)

Next >

Passaggio 7:

Viene visualizzata la pagina di benvenuto, come illustrato nell'immagine. In questa pagina vengono visualizzate le informazioni necessarie prima della configurazione del cloud privato. Leggere attentamente i requisiti. Selezionare Avanti per avviare la configurazione di preinstallazione.



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 >

Configurazione

Passaggio 1:

 Nota: nella prossima serie di diapositive ne includeremo alcune esclusive, come mostrato nell'immagine, che sono esclusive solo per la modalità AIR GAP , che devono essere racchiuse e contrassegnate come AIRGAP ONLY



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.

≡ ≡ AIRGAP ONLY ≡ ≡



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.

⌘ ⌘ AIRGAP ONLY ⌘ ⌘

Passaggio 2:

Passare alla pagina Account di Secure Endpoint Console. Un utente con privilegi amministrativi viene utilizzato per la console per creare criteri, gruppi di computer e aggiungere altri utenti. Immettere il nome, l'indirizzo e-mail e la password per l'account console. Selezionare Avanti.

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

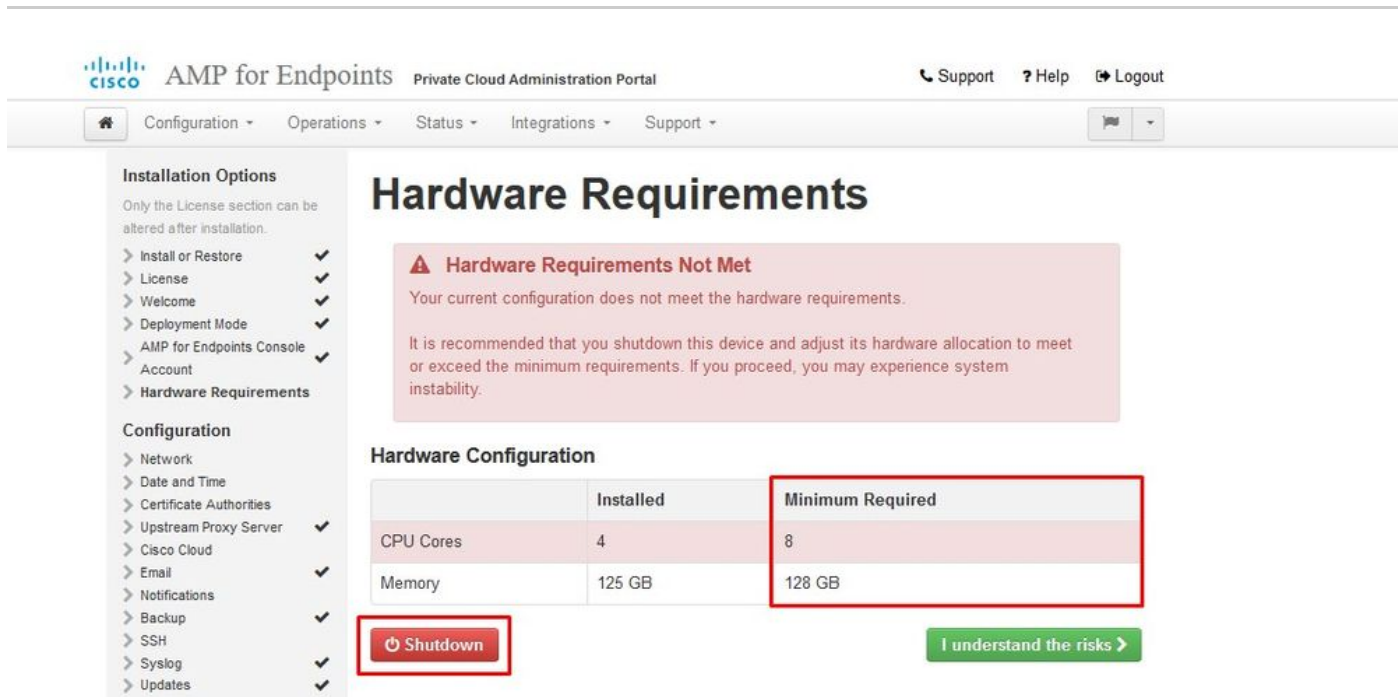
Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

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

Next >

Se si esegue in questo caso quando si esegue la distribuzione dal file OVA, è possibile scegliere tra due opzioni: continuare e risolvere il problema in un secondo momento oppure arrestare il sistema per eseguire la distribuzione della VM e apportare le modifiche necessarie. Dopo il riavvio, si continua dal punto in cui si è partiti.

 Nota: questo problema è stato risolto nel file OVA per la versione 3.5.2 che viene caricata correttamente con 128 GB di RAM e 8 core CPU



Hardware Requirements

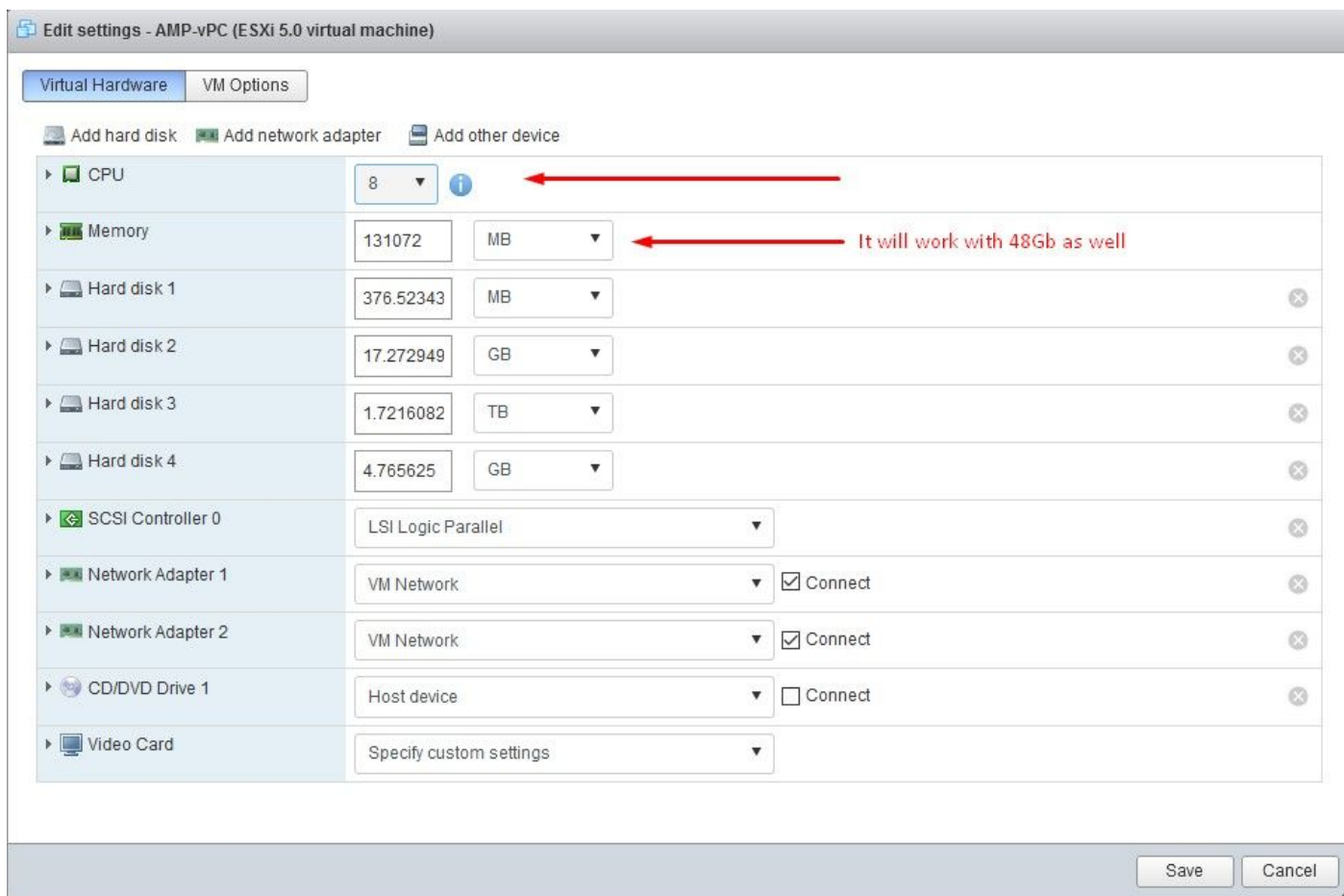
Hardware Requirements Not Met
Your current configuration does not meet the hardware requirements.

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.

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

Shutdown [I understand the risks >](#)

 Nota: utilizzare solo i valori consigliati a meno che non siano utilizzati per scopi di laboratorio



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

Una volta riavviati, continuiamo da dove siamo partiti.



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 >

Accertarsi di configurare ETH1 anche con IP STATICO.

 Nota: non configurare mai il dispositivo per l'utilizzo di DHCP a meno che non siano state create prenotazioni di indirizzi MAC per le interfacce. La modifica degli indirizzi IP delle interfacce può causare gravi problemi con i connettori di endpoint sicuri distribuiti. Se il server DNS non è configurato, è possibile utilizzare il DNS pubblico temporaneo per completare l'installazione.

Passaggio 3:



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)

Passaggio 4:

Viene visualizzata la pagina Data e ora. Immettere gli indirizzi di uno o più server NTP che si desidera utilizzare per la sincronizzazione di data e ora. È possibile utilizzare server NTP interni o esterni e specificarne più di uno tramite una virgola o un elenco delimitato da spazi. Sincronizzare l'ora con il browser o eseguire `amp-ctl ntpdate` dalla console del dispositivo per forzare una sincronizzazione immediata con i server NTP. Selezionare Avanti.



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 >

≡ ≡ AIRGAP ONLY ≡ ≡



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 >

≡ ≡ AIRGAP ONLY ≡ ≡

Passaggio 5:

Viene visualizzata la pagina Autorità di certificazione, come illustrato nell'immagine. Selezionare Aggiungi autorità di certificazione per aggiungere il certificato radice.

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 >

Passaggio 6:

Il passaggio successivo è configurare la pagina Cisco Cloud, come mostrato nell'immagine. Selezionare l'area Cisco Cloud appropriata. Espandere Visualizza nomi host se è necessario

creare eccezioni del firewall per il dispositivo Secure Endpoint Private Cloud per comunicare con Cisco Cloud per le ricerche di file e gli aggiornamenti dei dispositivi. Selezionare Avanti.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The main header includes the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. There are links for 'Support', 'Help', and 'Logout'. Below the header is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. On the left is a sidebar menu with 'Installation Options' and 'Configuration' sections. The main content area is titled 'Cisco Cloud' and contains 'Cisco Cloud Configuration' and 'Cisco Cloud Identity' sections. The 'Region' section has a dropdown menu set to 'Cisco Cloud, North America' and a 'View Hostnames (click to expand)' link. The 'Client Identity' section shows a client ID '0f476ea8[redacted]dbbc272a6c'. A green 'Next' button with a right arrow is highlighted with a red box at the bottom right of the configuration area.

Passaggio 7:

Passare alla pagina delle notifiche, come illustrato nell'immagine. Selezionare la frequenza per le notifiche critiche e regolari. Immettere gli indirizzi di posta elettronica a cui si desidera inviare le notifiche di avviso per il dispositivo Secure Endpoint. È possibile utilizzare alias di posta elettronica o specificare più indirizzi tramite un elenco separato da virgole. È inoltre possibile specificare il nome del mittente e l'indirizzo di posta elettronica utilizzati dal dispositivo. Queste notifiche non corrispondono alle sottoscrizioni di Secure Endpoint Console. È inoltre possibile specificare un nome di dispositivo univoco se si dispone di più dispositivi cloud privati di endpoint sicuri. Selezionare Avanti.

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	rvd[REDACTED]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 >

Passaggio 8:

Passare quindi alla pagina Chiavi SSH, come mostrato nell'immagine. Selezionare Add SSH Key per immettere le chiavi pubbliche che si desidera aggiungere al dispositivo. Le chiavi SSH consentono di accedere al dispositivo tramite una shell remota con privilegi root. L'accesso deve essere concesso solo agli utenti attendibili. Il dispositivo cloud privato richiede una chiave RSA in formato OpenSSH. Altre chiavi SSH possono essere aggiunte anche in un secondo momento usando Configuration > SSH nel portale di amministrazione. Selezionare Avanti.

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...oeCAvfEzyIea9PbgwnlB9DjTeJgFXtR7QGfd0g4vT9eD5X0XZd I4DKhrTNBv8/77T0d/Jagx7Przxs=</pre>		

Viene visualizzata la sezione Servizi. Nelle pagine successive è necessario assegnare i nomi host e caricare le coppie di certificati e chiavi appropriate per questi servizi dei dispositivi. Nelle diapositive successive è illustrata la configurazione di uno dei 6 certificati.

Servizi

Passaggio 1:

Durante il processo di configurazione è possibile che questi errori vengano eseguiti.

Il primo "errore" che potreste notare è evidenziato con le 3 frecce. Per evitare questo problema, è sufficiente deselezionare "Disabilita controllo TLS rigoroso"

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 >](#)

Senza controllo TLS rigoroso

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

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.	vPC2-Authenticat + Choose Key
<input checked="" type="checkbox"/> Certificate matches hostname.	vPC2-Authentication.cyberworld.local.pem
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	
vPC2-Authenticat + Choose Certificate	vPC2-Authentication.cyberworld.local.crt

Next >

Passaggio 2:

L'errore successivo si verifica se si lascia selezionata l'opzione "Convalida nome DNS". Qui avete due scelte.

1: deselezionare il segno di spunta Convalida DNS

N. 2: Tornare al server DNS e configurare i record host rimanenti.

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 checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	

+ Choose Certificate

+ Choose Key

Next >

Ripetere la stessa procedura altre cinque volte per gli altri certificati.

Autenticazione

- Il servizio di autenticazione potrà essere utilizzato nelle versioni future di Private Cloud per gestire l'autenticazione degli utenti.

Secure Endpoint Console

- Console è il nome DNS con il quale l'amministratore di Secure Endpoint può accedere a Secure Endpoint Console e Secure Endpoint Connectors riceve nuovi criteri e aggiornamenti.

Server di disposizione

- Server di disposizione è il nome DNS utilizzato dai connettori di endpoint sicuri per inviare e recuperare le informazioni di ricerca nel cloud.

Server di disposizione - Protocollo esteso


- Server di disposizione - Protocollo esteso è il nome DNS utilizzato dai nuovi connettori di endpoint sicuri per inviare e recuperare le informazioni di ricerca nel cloud.

Servizio di aggiornamento della disposizione

- Il servizio di aggiornamento delle disposizioni viene utilizzato quando si collega un'appliance Cisco Threat Grid al dispositivo cloud privato. L'accessorio Threat Grid viene utilizzato per inviare i file per l'analisi da Secure Endpoint Console e il servizio di aggiornamento dell'eliminazione viene utilizzato da Threat Grid per aggiornare l'eliminazione (pulita o dannosa) dei file dopo l'analisi.

Firepower Management Center

-Firepower Management Center Link consente di collegare un dispositivo Cisco Firepower Management Center (FMC) al dispositivo Cloud privato. In questo modo è possibile visualizzare i dati dell'endpoint protetto nel dashboard di FMC. Per ulteriori informazioni sull'integrazione di FMC con Secure Endpoint, vedere la documentazione di FMC.

 Attenzione: non è possibile modificare i nomi host al termine dell'installazione del dispositivo.

Prendere nota dei nomi host richiesti. È necessario creare sei record A DNS univoci per il cloud privato dell'endpoint sicuro. Ogni record punta allo stesso indirizzo IP dell'interfaccia della console cloud privata virtuale (eth1) e deve essere risolto sia dal cloud privato che dall'endpoint protetto.

Passaggio 3:

Nella pagina successiva scaricare e verificare il file di ripristino.

Viene visualizzata la pagina Recupero, come illustrato nell'immagine. È necessario scaricare e verificare un backup della configurazione prima di iniziare l'installazione. Il file di ripristino contiene tutta la configurazione e le chiavi del server. Se si perde un file di ripristino, non sarà possibile ripristinare la configurazione e sarà necessario reinstallare tutti i connettori dell'endpoint sicuro. Senza una chiave originale, è necessario riconfigurare l'intera infrastruttura cloud privata con nuove chiavi. Il file di recupero contiene tutte le configurazioni correlate al portale opadmin. Il file di backup contiene il contenuto del file di ripristino e tutti i dati del portale del dashboard, ad esempio gli eventi, la cronologia dei connettori e così via. Se si desidera ripristinare solo l'opadmin senza i dati dell'evento e tutto, è possibile utilizzare il file di ripristino. Se si esegue il ripristino dal file di backup, verranno ripristinati i dati del portale di opadmin e del dashboard.

Selezionare Download per salvare il backup nel computer locale. Una volta scaricato il file, selezionare Scegli file per caricare il file di backup e verificare che non sia danneggiato. Selezionare Avanti per verificare il file e procedere.

- > 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 ONLY ≡ ≡

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@xxxxxxxxx.com
Business Name	Cisco vamrodia PC v2


Recovery [Edit](#)

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

⌘ ⌘ AIRGAP ONLY ⌘ ⌘

Vedi input simili come questo...

 **Attenzione:** quando ci si trova in questa pagina, non aggiornare in quanto può causare problemi.

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

Al termine dell'installazione, fare clic sul pulsante di riavvio

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 ONLY ≡ ≡

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!
=====
```

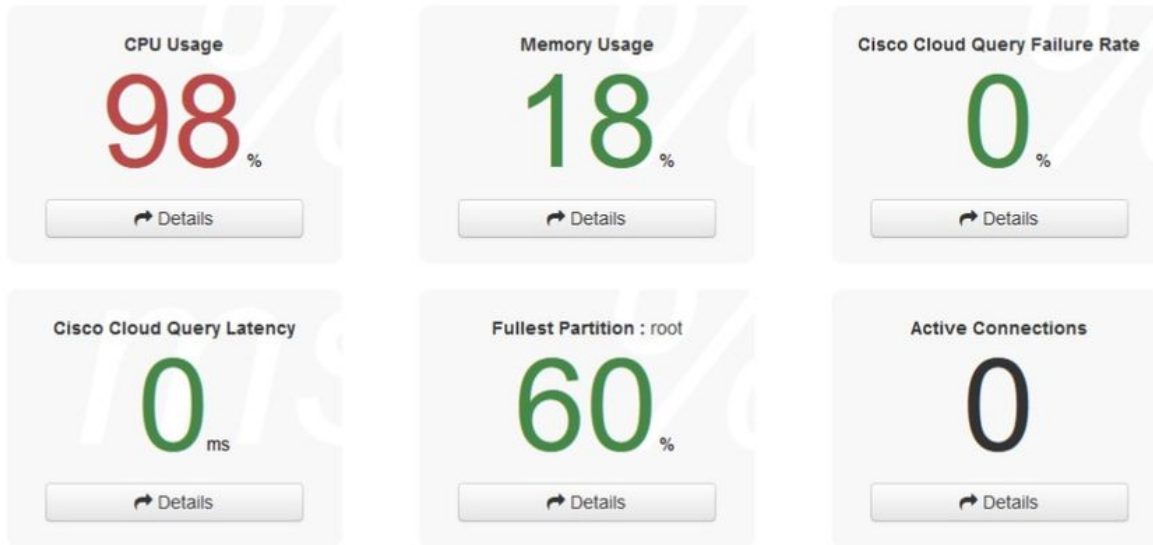
Download Output

⌘ ⌘ AIRGAP ONLY ⌘ ⌘

Una volta che l'accessorio è stato completamente avviato, al successivo accesso con l'interfaccia di amministrazione verrà visualizzato questo dashboard. All'inizio si nota un'elevata CPU, ma se si danno alcuni minuti la CPU si stabilizza.



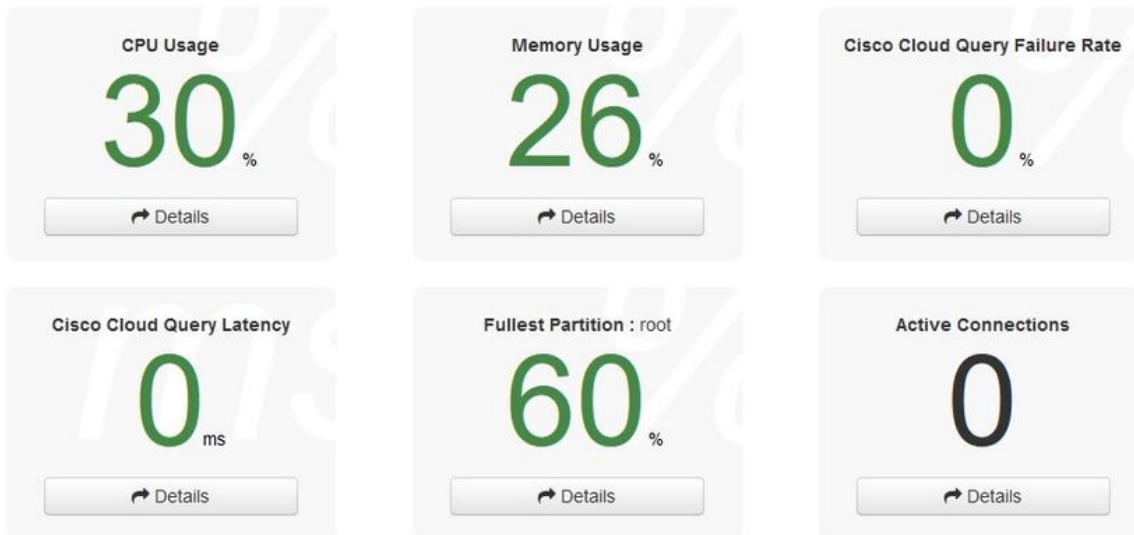
Key Metrics



Dopo pochi minuti...



Key Metrics



Da qui si passa alla console Secure Endpoint. Fare clic sulla piccola icona che appare come il fuoco nell'angolo a destra accanto alla bandiera.

The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. The browser address bar displays `https://192.168.75.92`. The page header includes the Cisco logo, the title "AMP for Endpoints Private Cloud Administration Portal", and navigation links for Support, Announcements, Help, and Logout. Below the header is a navigation menu with "Configuration", "Operations", "Status", "Integrations", and "Support". A red arrow points to a small icon in the top right corner of the navigation menu. The main content area is titled "Key Metrics" and features three cards:

- CPU Usage:** 11% (with a "Details" button)
- Memory Usage:** 36% (with a "Details" button)
- Cisco Cloud Query Failure Rate:** 0% (with a "Details" button)

≡ ≡ AIRGAP ONLY ≡ ≡

Come si può vedere, non abbiamo superato il controllo di integrità a causa di DB Protect Snapshot, anche le definizioni dei client, DFC e Tetra. A tale scopo, è necessario eseguire l'aggiornamento offline tramite il file ISO scaricato preparato in precedenza tramite amp-sync e caricato nella macchina virtuale o archiviato in posizione NFS.



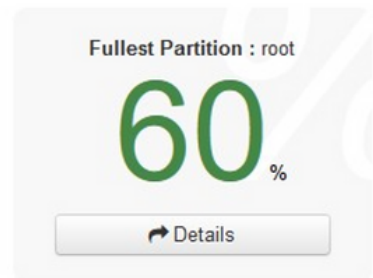
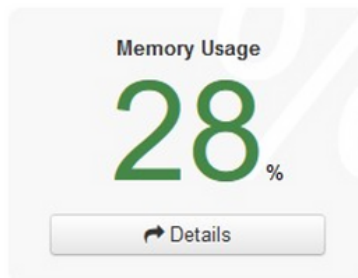
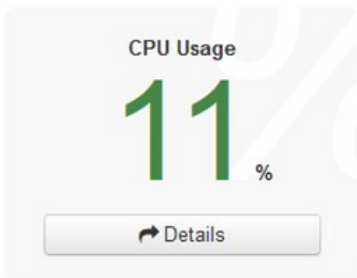
Sanity Check Failing

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.

Pacchetto di aggiornamento di AirGap

Per ricevere il comando Protect DB, è necessario utilizzarlo per la prima volta

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

 Nota: scarica tutti i pacchetti con questo comando e la verifica potrebbe richiedere più di 24 ore. Dipende dalla velocità e dalla qualità del collegamento. Nel mio caso, con la fibra da 1 Gb, il completamento richiede ancora quasi 25 ore. In parte ciò è dovuto anche al fatto che questo download è direttamente da AWS e quindi è limitato. Si noti, infine, che questo download è piuttosto grande. Nel mio caso il file scaricato era 323 GB.

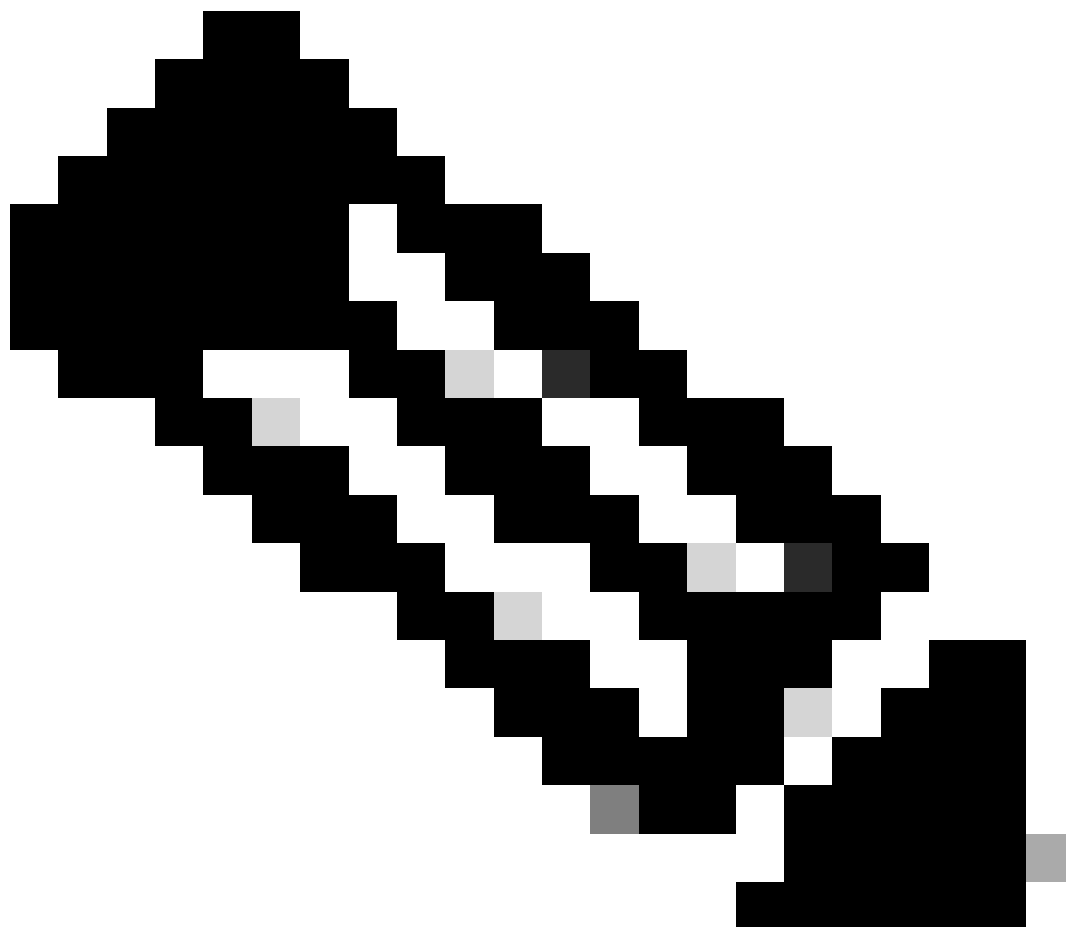
In questo esempio viene utilizzato CygWin64

1. Scaricare e installare la versione x64 di Cygwin.
2. Eseguire setup-x86_64.exe e passare attraverso il processo di installazione scegliere tutti i valori predefiniti.
3. Scegliere un mirror di download.
4. Selezionare i pacchetti da installare:

Tutto -> Netto -> ricciolo
Tutto -> Utilità -> genisoimage
Tutto -> Utilità -> 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/22f49a7fe81b71ee153be870c7f6d20c9238a89c7de277956bbccb2c2f41d8-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/22f49a7fe81b71ee153be870c7f6d20c9238a89c7de277956bbccb2c2f41d8-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/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdeb47ff069-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
```

```
User@VMStation-1 ~  
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 08:39:50 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  
99.98% 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 ~  
$
```

Nota: nel più recente aggiornamento VPC 3.8.x con CygWin64 come principale strumento di download si può incontrare questo problema descritto di seguito.

```
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.
```

[Note release](#) Pagina n. 58. Come si può vedere "xorriso" è ora necessario. È stato modificato il formato ISO in ISO 9660 e questa dipendenza è ciò che converte l'immagine nel formato corretto in modo che l'aggiornamento possa essere completato. Purtroppo, CygWin64 non offre xorriso in nessuno dei loro repository incorporati. Tuttavia, per coloro che vorrebbero ancora utilizzare CygWin64 c'è un modo per superare questo problema.

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

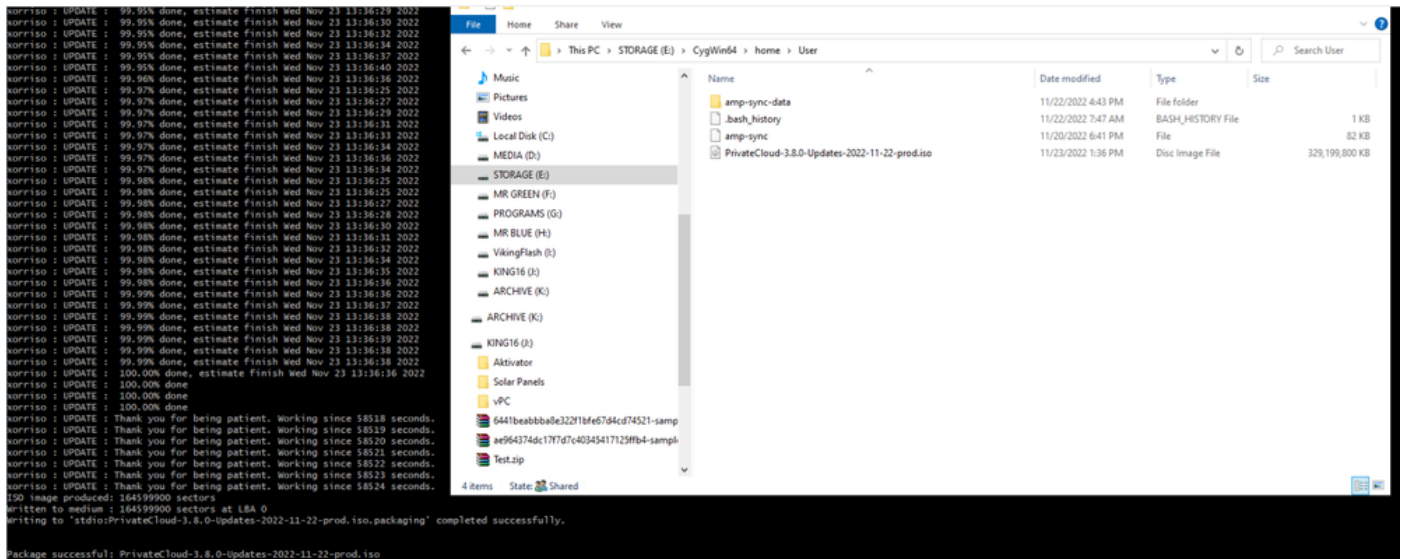
To run amp-sync you will first have to install xorriso and xmlstarlet.

- 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`

Per poter utilizzare di nuovo CygWin è necessario scaricare manualmente xorriso dal repository GitHub. Aprire il browser e digitare <Latest xorriso.exe 1.5.2 pre-build for Windows> dovrebbe apparire come primo collegamento denominato come <PeyTy/xorriso-exe-for-windows - GitHub> passare a quella pagina GitHub e scaricare <xorriso-exe-for-windows-master.zip> il file all'interno del file zip che si trova tra pochi altri file denominati <xorriso.exe> copiare e incollare questo file in <CygWin64\bin> percorso del file Cyg installazione. Riprovare eseguendo il comando <amp-sync>. Il messaggio di errore e l'inizio e la fine del download non dovrebbero più essere visualizzati, come mostrato nell'immagine.



Eseguire il backup del VPC 3.2.0 corrente (in questo caso) in modalità Airgap.

È possibile utilizzare questo comando dalla CLI

```
rpm -qa | grep Pri
```

In alternativa, è possibile passare a Operazioni > Backup, come illustrato nell'immagine, ed eseguire il backup qui.



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

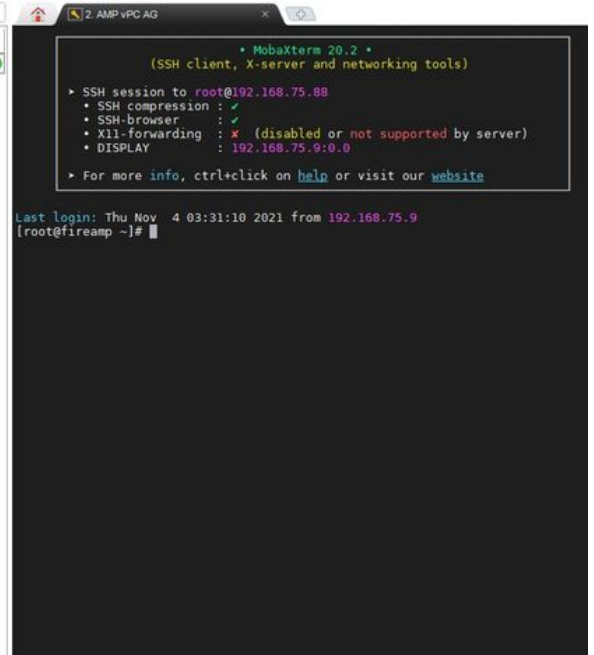
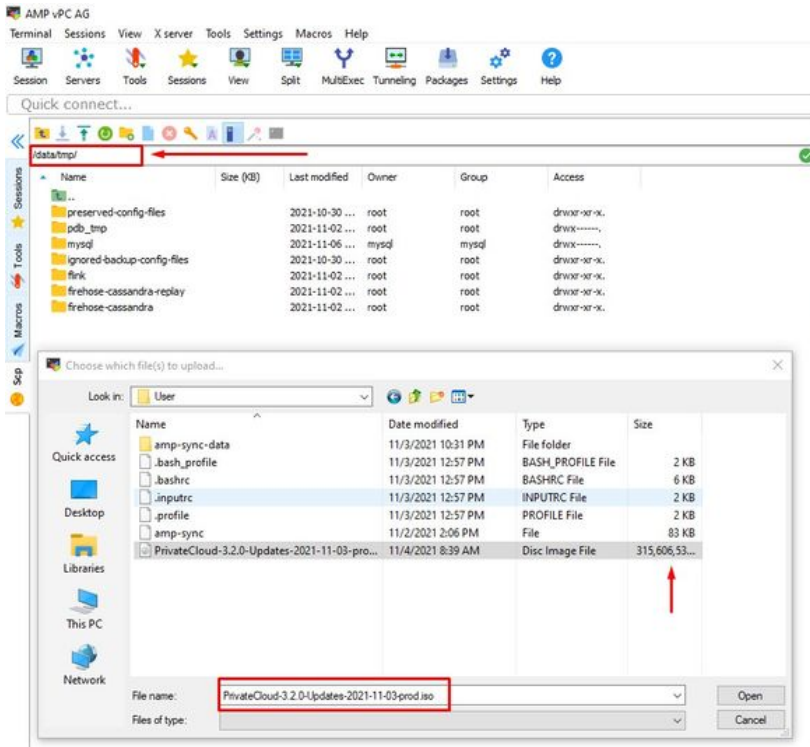
Previous Backups

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	 

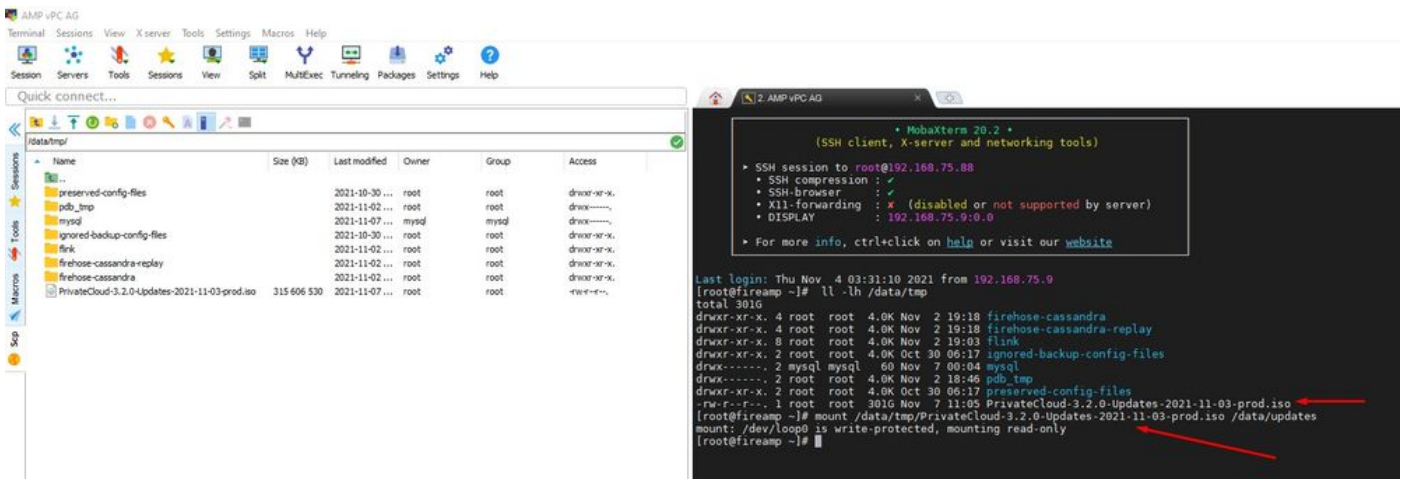
Trasferire l'ultimo ISO generato con amp-sync al VPC. Questa operazione può richiedere anche diverse ore in base alla velocità. In questo caso il trasferimento ha richiesto più di 16 ore

/data/tmp



Al termine del caricamento, montare l'ISO

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



Passare all'interfaccia utente di opdamin per eseguire l'aggiornamento Operazioni (Operations) >

Aggiorna periferica (Update Device) > Seleziona (Select) Aggiorna ISO (Update ISO).

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with the Cisco logo, 'AMP for Endpoints', and 'Private Cloud Administration Portal'. On the right, there are links for 'Announcements', 'Help', and 'Logout'. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. A 'Sanity Check Failing' alert is visible in a red box. The main content area has a heading 'Updates keep your Private Cloud device up to date.' with a 'Download amp-sync' button. A 'Check Update ISO' button is highlighted with a red arrow, and a status indicator shows 'Checking ISO for updates...'. The 'Content' section displays version '3.2.0_202010081917' for 'Client Definitions, DFC, Tetra Content Version' with an 'ABSENT' status for 'Protect DB Version'. It includes buttons for 'Update Content' and 'Import Protect DB', and a message: 'Import a Protect DB snapshot to your standalone device.' The 'Software' section displays version '3.2.0_202010082118' for 'Private Cloud Software Version' with a message: 'A software update is available.' and an 'Update Software' button.

In questo esempio prima si procede con l'aggiornamento del contenuto

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

ABSENT
Protect DB Version

A content update is available.

Update Content

Import Protect DB

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

A software update is available.

Update Software

Quindi selezionare Importa protezione DB.



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.

Come potete vedere, questo è un altro processo molto lungo che può richiedere molto tempo per essere completato.

Home / Operations - Update Device / Protect DB Import Details

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 less than a minute ago	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: 0:00:00 100% [=====]
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).
```

Problema 1 - Spazio esaurito nell'archivio dati

In questa schermata è possibile esaminare due problemi. Poiché vPC precedente alla versione 3.5.2 non è in grado di installare lo storage NFS esterno, è necessario caricare il file ISO di aggiornamento nella directory /data/temp. Nel mio caso, poiché il datastore era solo di 1 TB, sono uscito dalla stanza e la VM si è bloccata. In altre parole, sono necessari almeno 2 TB di spazio sul data store per installare correttamente il VPC AirGap versione inferiore alla 3.5.2

L'immagine seguente è tratta dal server ESXi, che mostra l'errore che non c'è più spazio disponibile sul disco rigido quando si tenta di avviare la VM. Sono riuscito a correggere l'errore commutando temporaneamente la RAM da 128 GB a 64 GB. Poi sono riuscito a riavviarmi. Inoltre, se si esegue il provisioning di questa VM come Thin Client, il lato negativo dell'implementazione di Thin Client è che le dimensioni del disco possono aumentare, ma non diminuirebbero anche se si liberasse spazio. In altre parole, supponiamo che il file da 300 GB sia stato caricato nella directory del vPC e quindi eliminato. Il disco in ESXi mostra ancora 300 GB di spazio in meno sul disco rigido



Problema 2 - Aggiornamento precedente

Il secondo problema è che se si esegue prima l'aggiornamento software come ho fatto nella mia 2nd prova e dalla 3.2.0 finisco con VPC per aggiornare alla 3.5.2 e per questo ho dovuto scaricare il nuovo file di aggiornamento ISO dal 3.2.0 diventato non valido a causa del fatto che non ero più sulla versione 3.2.0 originale.

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.

Questo è l'errore che viene visualizzato se si tenta di montare di nuovo il file di aggiornamento ISO.



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

In questa immagine è illustrato un metodo alternativo per montare l'immagine di aggiornamento sul PC. Nella versione 3.5.x è possibile utilizzare una postazione remota come lo storage NFS per condividere il file di aggiornamento con il computer virtuale.



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.

L'errore del controllo di integrità è correlato al database di protezione attualmente non disponibile nel VPC



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

Avvio automatico del prossimo aggiornamento



⚙ 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

Dopo questo lungo processo di importazione del database Protect DB, è possibile spostare e aggiornare la definizione client e il software, operazione che può richiedere più di 3 ore.

✔ 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 0:1634076372-7 will be updated
    
```

Download Output

E alla fine, vi prego di notare che questo processo richiederà molto tempo.

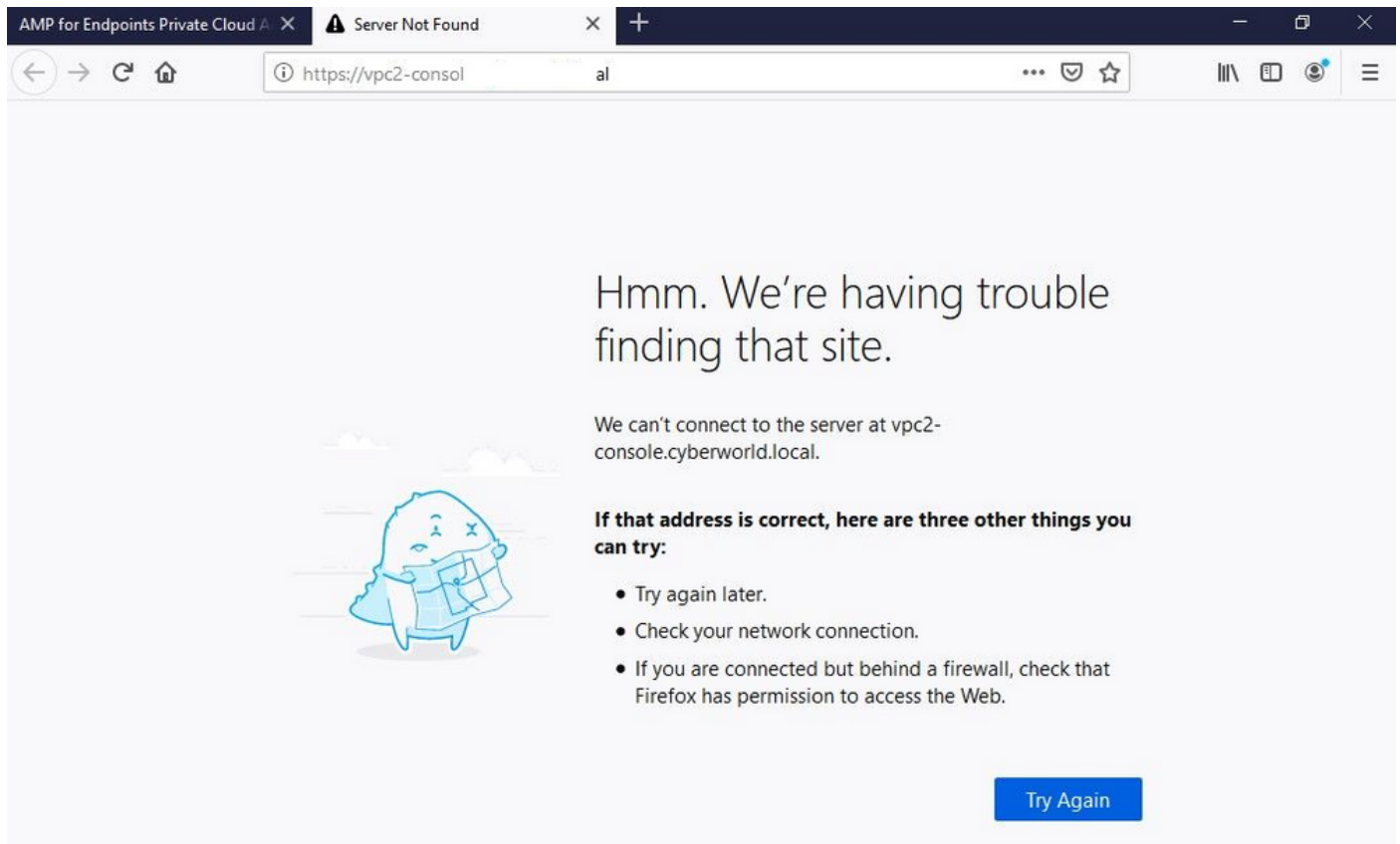
Per l'accessorio VPC visitare questa TZ che contiene altri metodi per aggiornare l'accessorio hardware, il file ISO e l'avvio da USB.

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

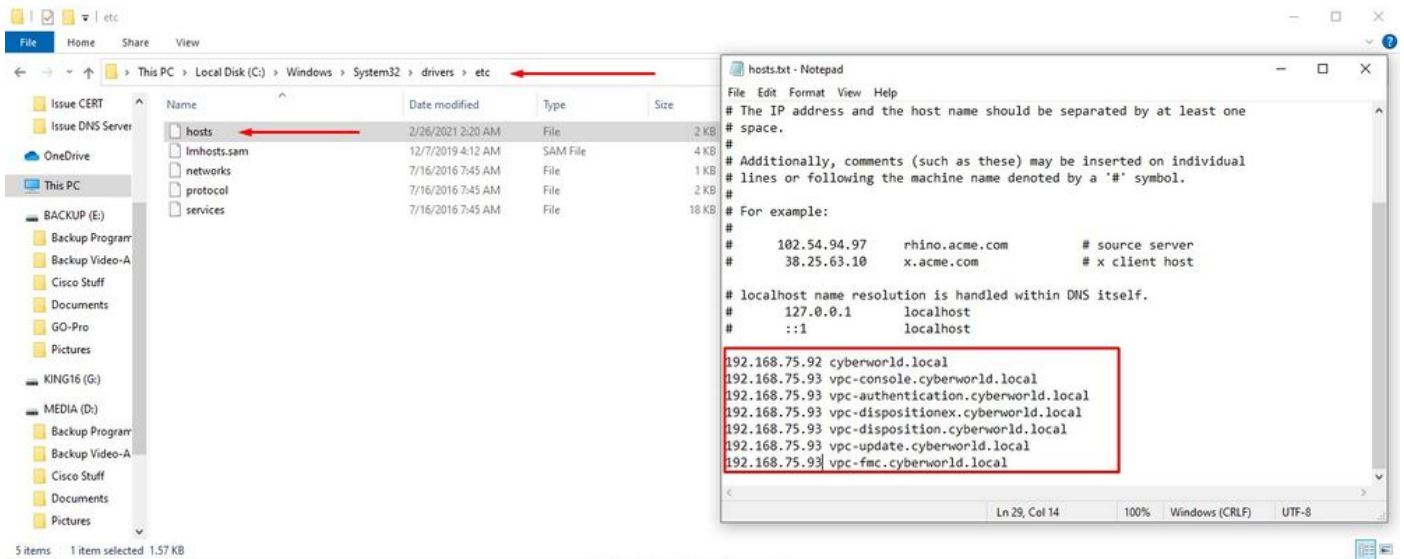
Risoluzione dei problemi di base

Problema 1 - FQDN e server DNS

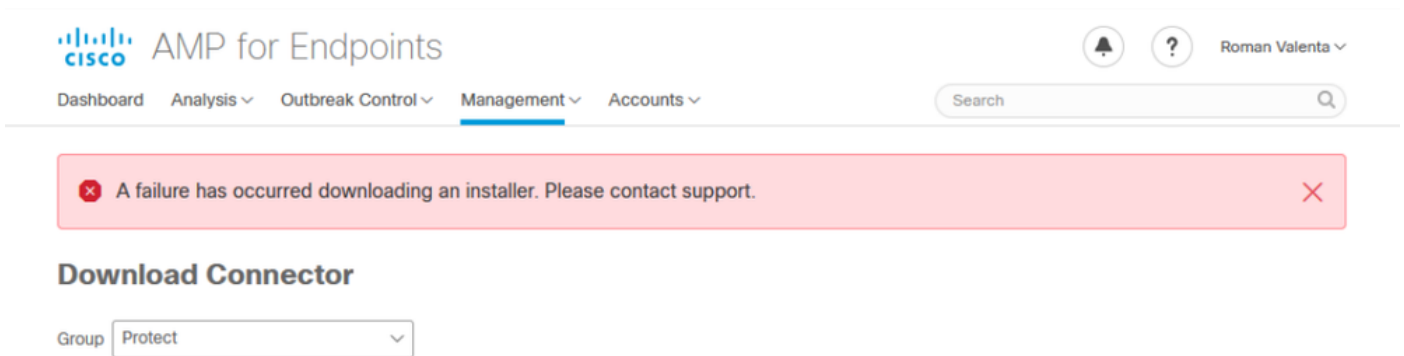
Il primo problema che si può verificare è se il server DNS non è stato stabilito e tutti i nomi di dominio completo (FQDN) non sono stati registrati e risolti correttamente. Il problema potrebbe essere simile a questo quando si tenta di passare alla console Secure Endpoint tramite l'icona "fire" di Secure Endpoint. Se si utilizza solo l'indirizzo IP funziona, ma non è possibile scaricare il connettore. Come si può vedere nella 3^{esima} immagine qui sotto.



Se si modifica il file HOSTS sul computer locale come mostrato nell'immagine, il problema viene risolto e si verificano degli errori.



Questo errore si verifica quando si tenta di scaricare il programma di installazione del connettore Secure Endpoint.



Dopo alcune operazioni di risoluzione dei problemi, l'unica soluzione corretta è stata la configurazione del server DNS.

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

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

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

Dopo aver registrato tutti i nomi di dominio completo (FQDN) nel server DNS e aver modificato il record nel cloud privato virtuale dal DNS pubblico al server DNS, tutto inizia a funzionare come previsto.



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.



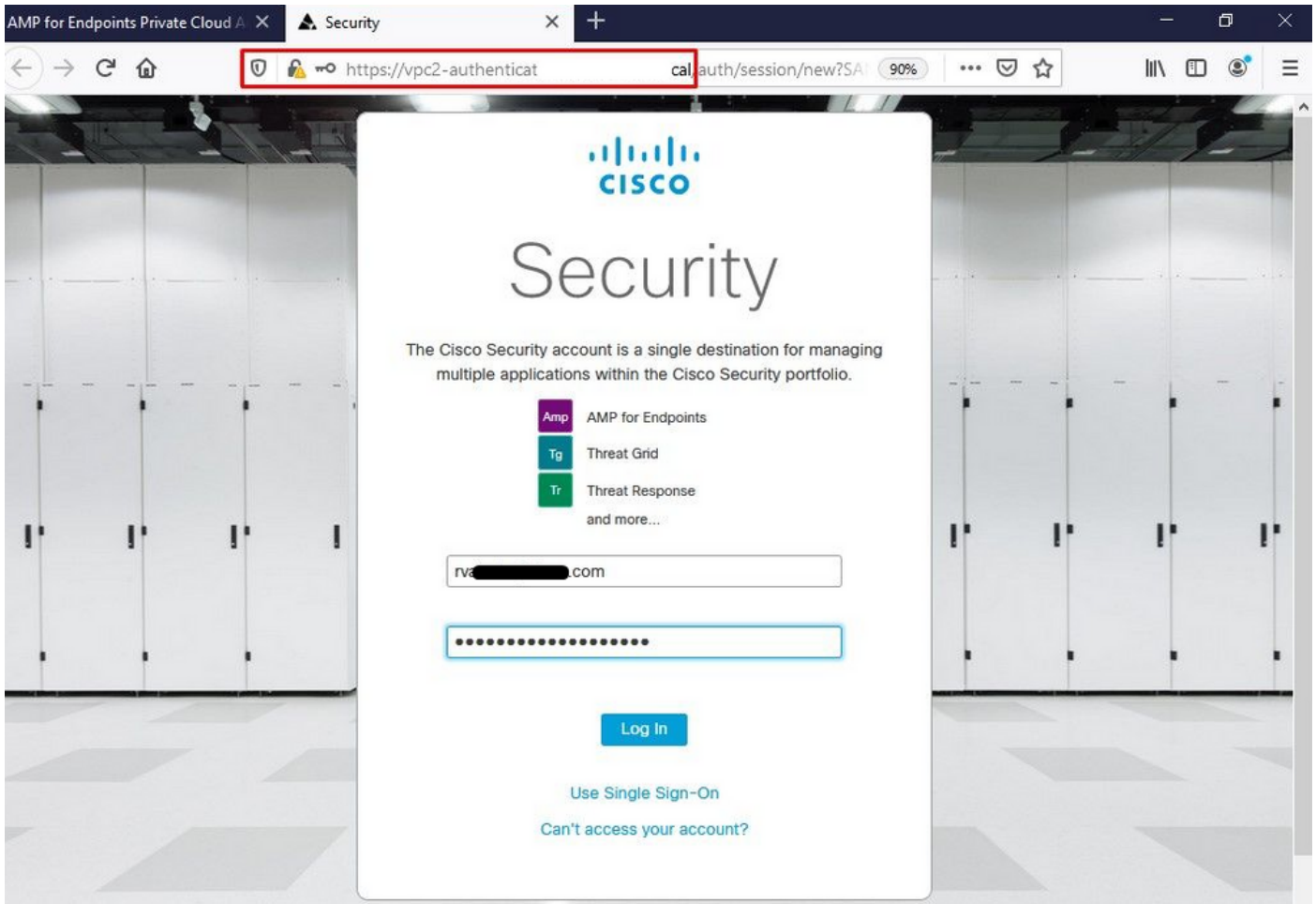
State	Started	Finished	Duration
▶ Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	⌚ Please wait...	⌚ Please wait...

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](#)

A questo punto è possibile accedere e scaricare il connettore



Viene visualizzata la procedura guidata iniziale per il criterio Endpoint sicuro per l'ambiente. La guida fornisce una selezione di prodotti antivirus utilizzati, se presenti, nonché di proxy e dei tipi di criteri che si desidera implementare. Selezionare il pulsante di configurazione appropriato in base al sistema operativo del connettore.

Viene visualizzata la pagina Prodotti di sicurezza esistenti, come illustrato nell'immagine. Scegli i prodotti di sicurezza che utilizzi. Genera automaticamente esclusioni applicabili per impedire problemi di prestazioni sugli endpoint. Selezionare Avanti.

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.

Connettore download.

🟢 Step 1: Existing Security Products

🟢 Step 2: Set Up Proxy

🟢 Step 3: Download Connector

<p style="text-align: center;">Audit Only</p> <p>Used when you're still learning about the product and want to install it without any impact to your existing systems.</p> <p style="text-align: center;">Policy Details</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Files</p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Network</p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Offline Engine</p> <p>TETRA</p> </div> <p style="text-align: center;">Download</p>	<p style="text-align: center;">Protect</p> <p>Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.</p> <p style="text-align: center;">Policy Details</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Files</p> <p> Quarantined</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Network</p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Offline Engine</p> <p>TETRA</p> </div> <p style="text-align: center;">Download</p>	<p style="text-align: center;">Triage</p> <p>Used when you have a known or suspected infected machine.</p> <p style="text-align: center;">Policy Details</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Files</p> <p> Quarantined</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Network</p> <p> Blocked</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Offline Engine</p> <p>TETRA</p> </div> <p style="text-align: center;">Download</p>	<p style="text-align: center;">Server</p> <p>Used when you're installing a connector on standard Windows servers.</p> <p style="text-align: center;">Requirements</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Files</p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Network</p> <p> Off</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Offline Engine</p> <p>TETRA</p> </div> <p style="text-align: center;">Download</p>	<p style="text-align: center;">installing a connector on Windows Domain Controllers.</p> <p style="text-align: center;">Requirements</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Files</p> <p> Audited</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Network</p> <p> Off</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Offline Engine</p> <p>TETRA</p> </div> <p style="text-align: center;">Download</p>
--	--	--	---	---

[Back](#)

[Next](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

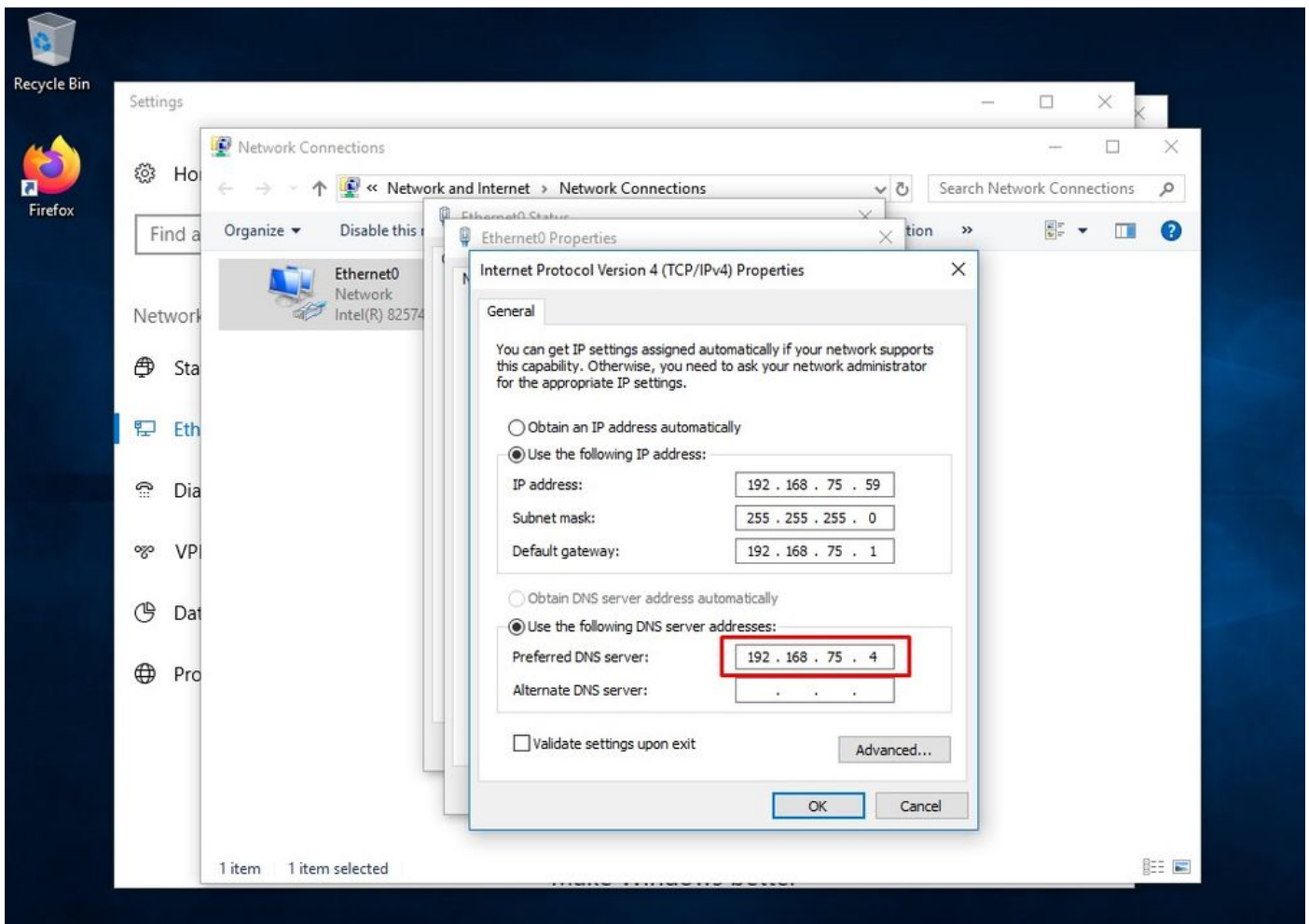
You have chosen to open:

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

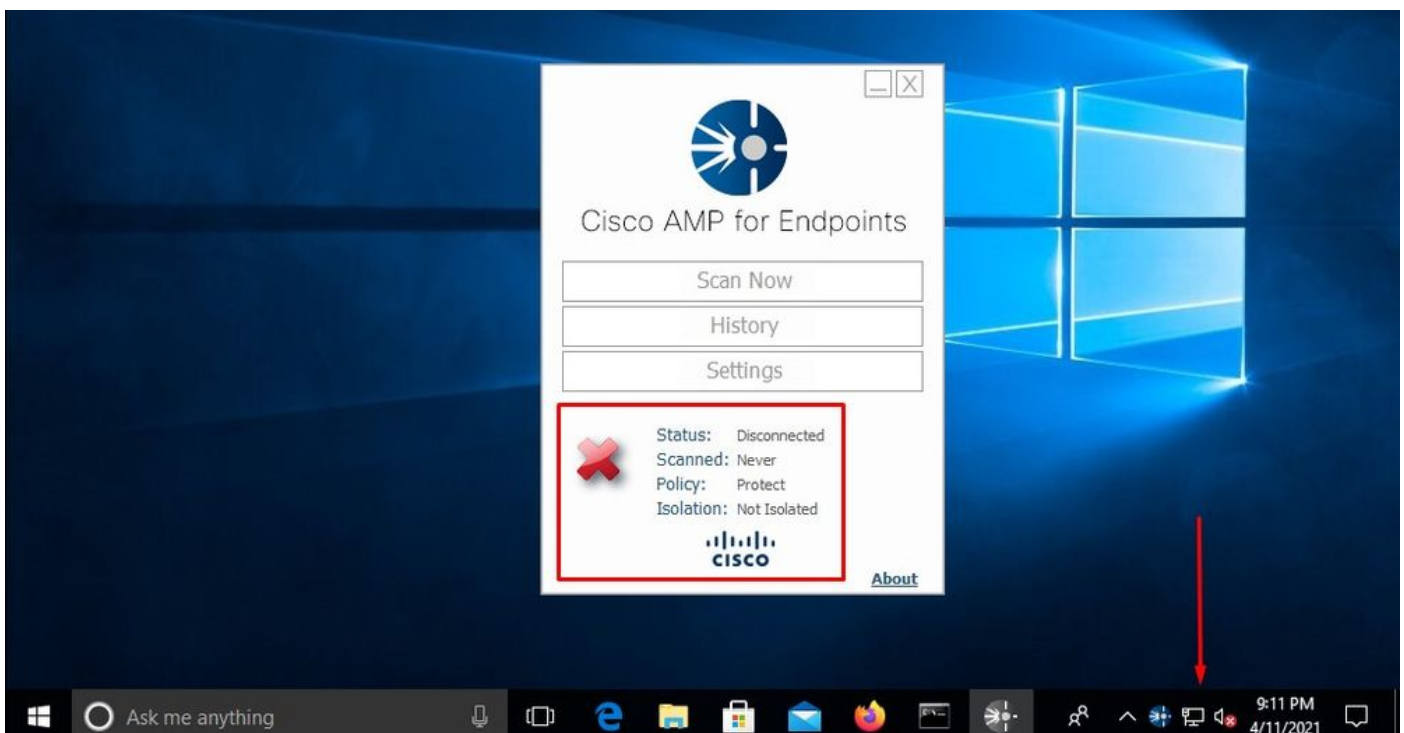
Would you like to save this file?

Problema n. 2 - Problema con la CA radice

Il problema successivo che si può affrontare è che se si utilizzano i propri certificati interni è che dopo l'installazione iniziale, il connettore può essere visualizzato come disconnesso.



Una volta installato, il connettore Secure Endpoint può essere visualizzato come Disconnesso. Eseguire il pacchetto di diagnostica ed esaminare i registri, in modo da poter determinare il problema.



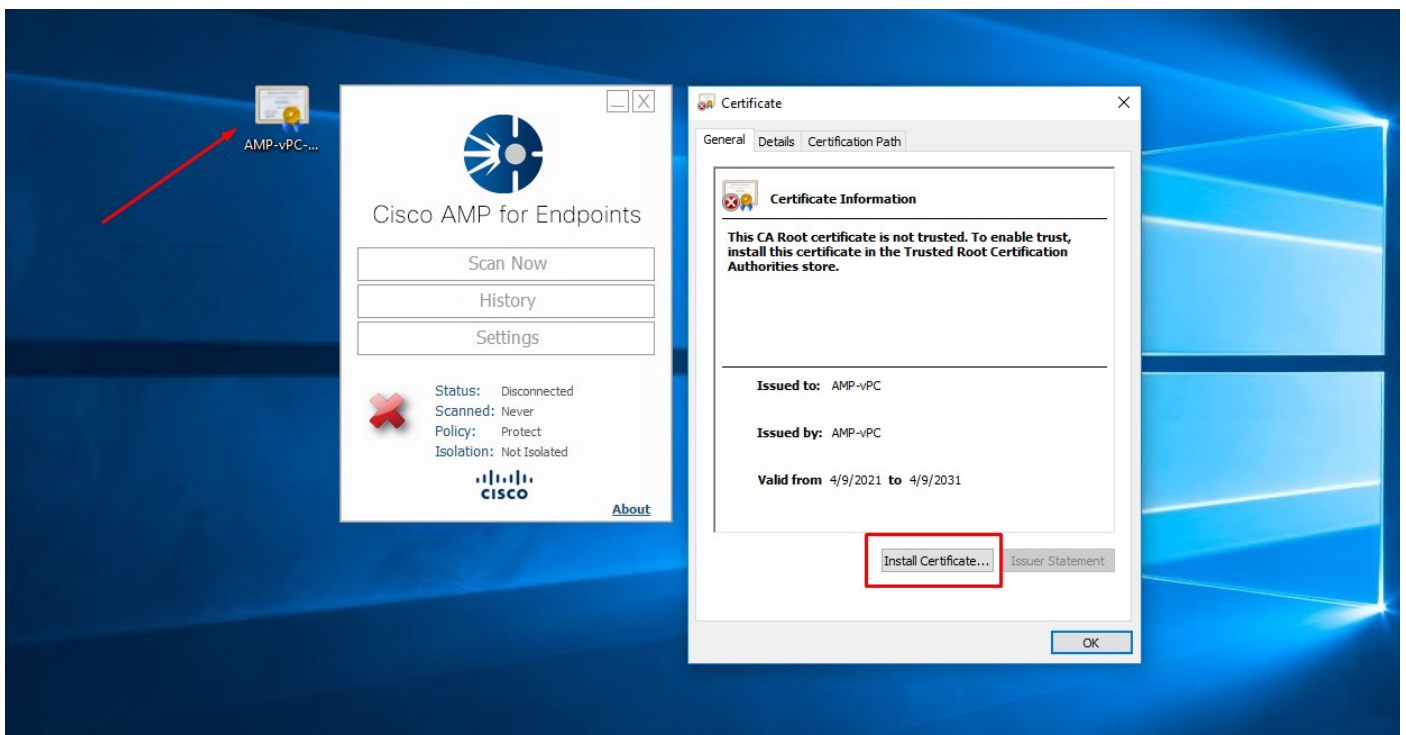
In base all'output raccolto dal bundle diagnostico è possibile visualizzare l'errore CA radice

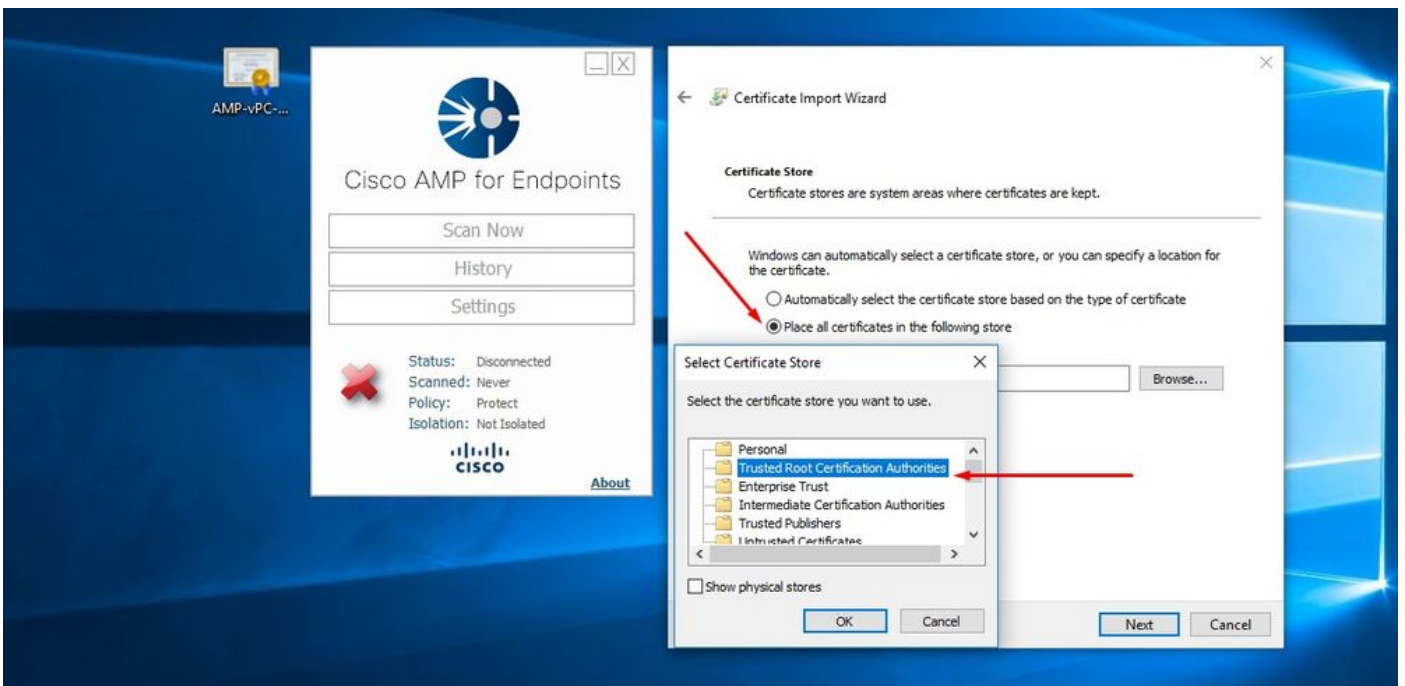
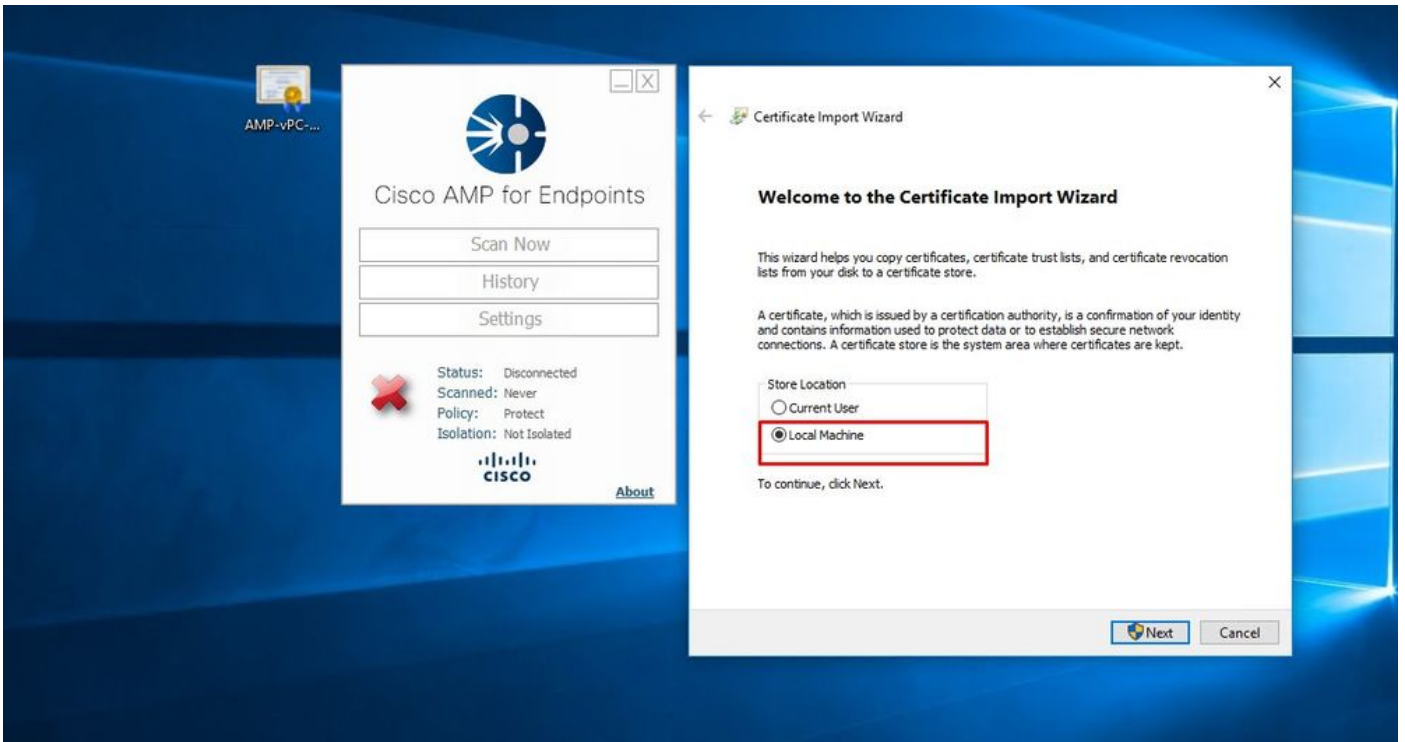
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl

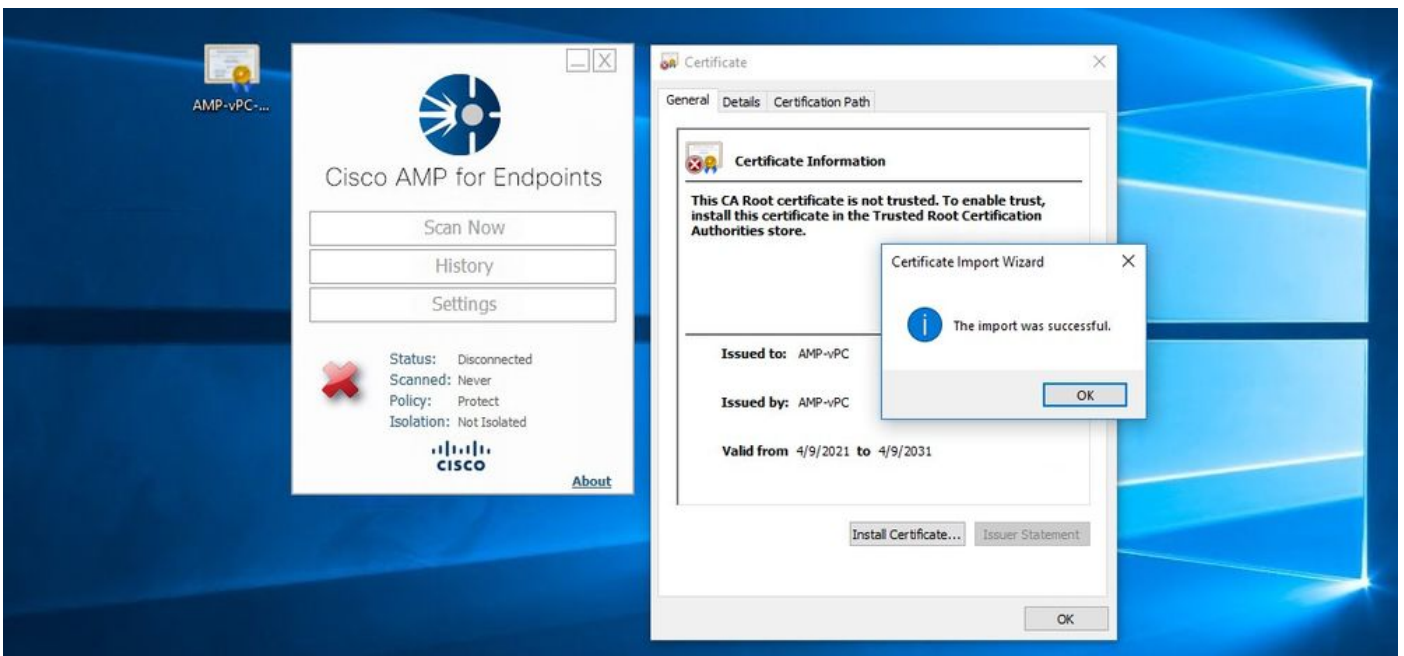
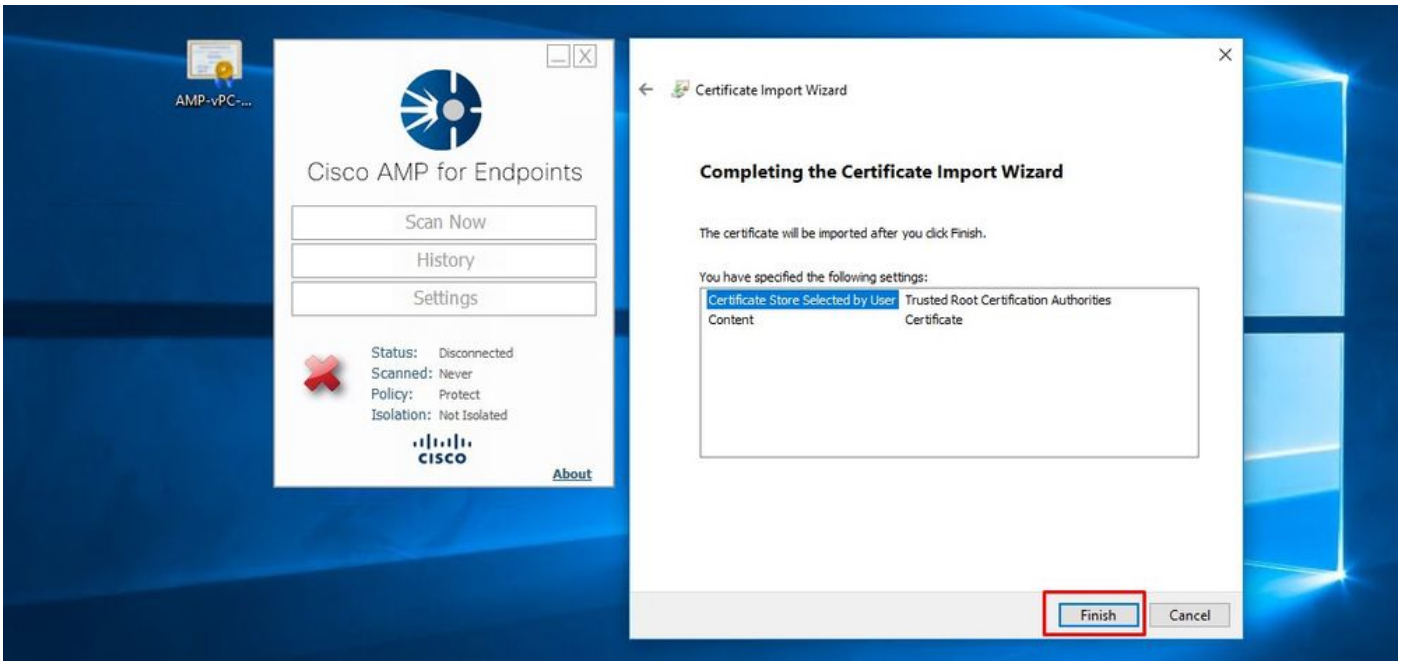
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat

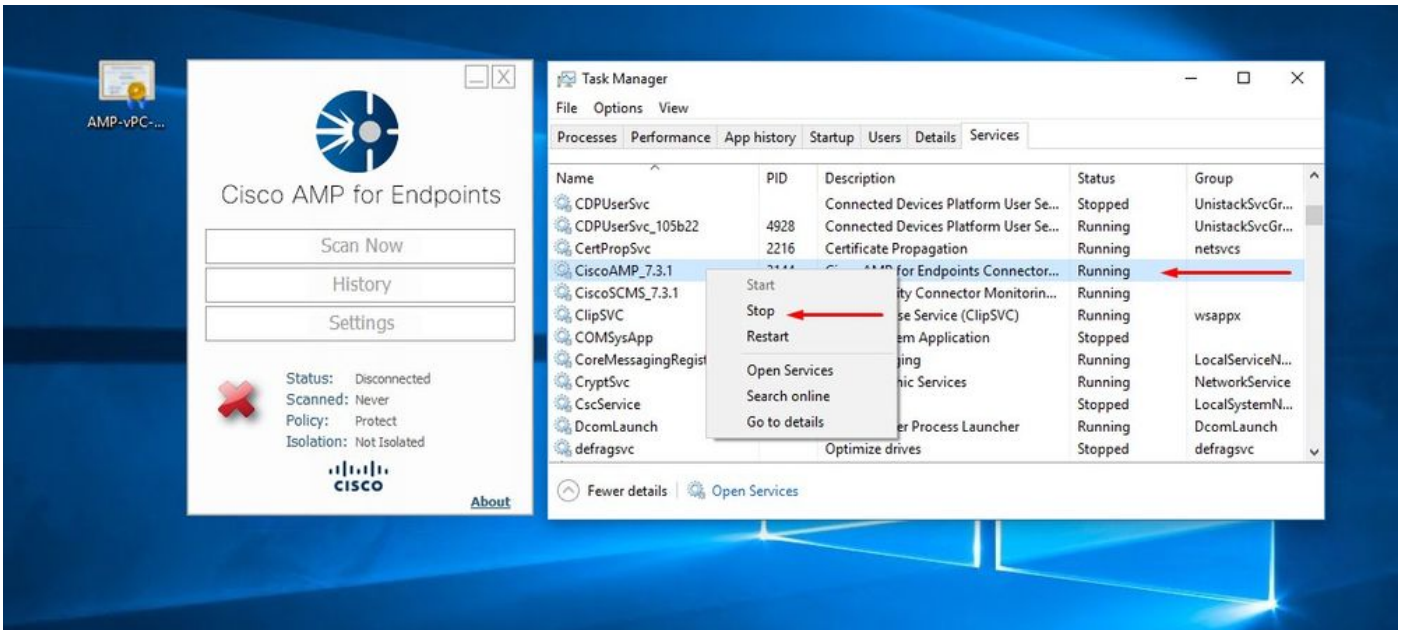
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60

Dopo aver caricato la CA radice nell'archivio delle CA radice attendibili e aver riavviato il servizio Endpoint sicuro. Tutto inizia a funzionare come previsto.

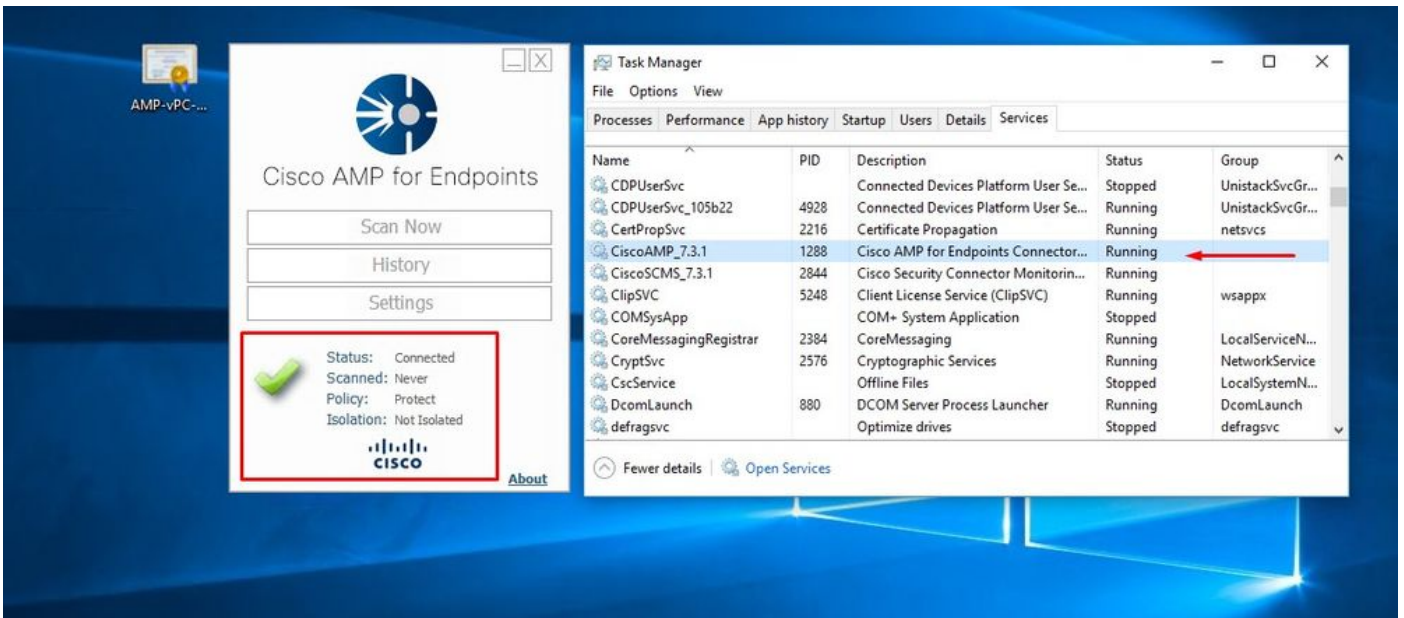








Una volta avviato, il connettore del servizio Secure Endpoint diventa online come previsto.



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".

Attività dannosa testata

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

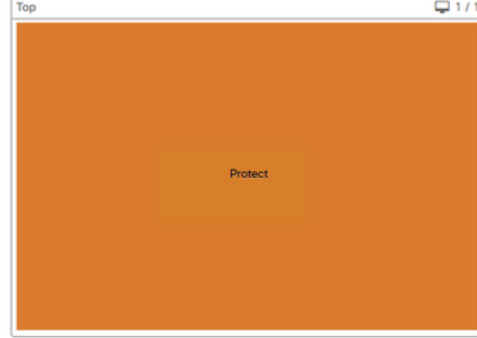
Compromises

Inbox 0 / 1



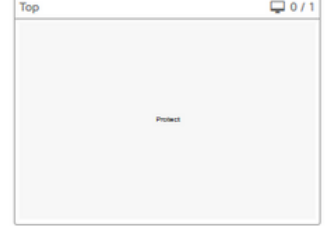
Quarantined Detections

Quarantine Events 1 / 1



Vulnerabilities

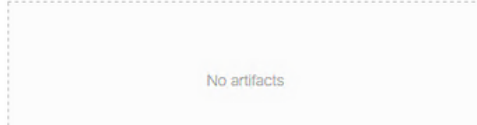
View 0 / 1



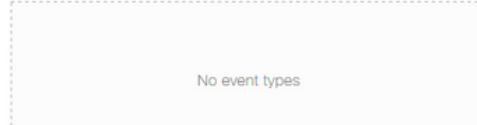
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

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



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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).