

Installeren en configureren van Secure Endpoint Virtual Private Cloud

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[VPC-implementatie](#)

[VM-installatie](#)

[Eerste configuratie van beheerinterface](#)

[Eerste configuratie van de vPC via web GUI](#)

[Configuratie](#)

[Services](#)

[AirGap Update pakket](#)

[Probleem #1 - Uitgeputte ruimte in Data Store](#)

[Probleem #2 - oude update](#)

[Basis probleemoplossing](#)

[Probleemoplossing #1 - FQDN- en DNS-server](#)

[Probleem #2 - Probleem met Root CA](#)

Inleiding

In dit document wordt beschreven hoe u met succes Virtual Private Cloud (VPC) op servers in een ESXi-omgeving kunt implementeren. Voor andere documenten zoals Quick Start Guide, Implementatie Strategie, Rechten Gids, console en Beheerder Gebruikershandleiding bezoek deze site [Documentatie](#)

Bijgedragen door Roman Valenta, Cisco TAC-engineers.

Voorwaarden

Vereisten:

VMware ESX 5 of hoger

- Cloud-proxy modus (alleen): 128 GB RAM, 8 CPU cores (2 CPU's met elk 4 cores aanbevolen), 1 TB minimale vrije schijfruimte op VMware datastore
- Type aandrijving: SSD vereist voor airgap-modus en aanbevolen voor proxy
- RAID Type: Een RAID 10-groep (gestreepte spiegel)
- Minimale grootte van VMware-datastore: 2 TB
- Minimale datastore willekeurige lees voor de RAID 10-groep (4K): 60K IOPS
- Minimale datastore willekeurig schrijft voor de RAID 10-groep (4K): 30K IOPS

Cisco raadt u aan bekend te zijn met dit onderwerp:

- Basiskennis hoe te werken met certificaten.

- Basiskennis over het instellen van DNS onder DNS-server (Windows of Linux)
- Sjabloon voor installatie en open virtuele applicatie (OVA) in de VMWare ESXi

Gebruikt in dit LAB:

VMware ESX 6.5

- Cloud-proxy modus (alleen): 48 GB RAM, 8 CPU cores (2 CPU cores met elk 4 cores aanbevolen), 1 TB minimale vrije schijfruimte op VMware datastore
- Soort schijven: SATA
- RAID Type: één RAID 1
- Minimale grootte van VMware-datastore: 1 TB
- MobaXterm 20.2 (programma voor meerdere terminals vergelijkbaar met PuTTY)
- Cygwin64 (gebruikt om AirGap Update te downloaden)

Aanvullend

- Certificaat dat u maakt met openssl of XCA
- DNS-server (Linux of Windows) In mijn lab gebruikte ik Windows Server 2016 en CentOS-8
- Windows VM voor ons testendpoint
- Licentie

Als uw geheugen minder dan 48GB RAM op versie 3.2+ VPC is wordt onbruikbaar.

Opmerking: De Private Cloud OVA creëert de drive partities zodat het niet nodig is om ze in VMWare te specificeren. server die de schone interface hostname oplost.

Raadpleeg het [gegevensblad](#) van de [VPC-applicatie](#) voor meer informatie over versiespecifieke hardwarevereisten.

Opmerking: De informatie in dit document is gemaakt van de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

VPC-implementatie

Selecteer de URL in de eDelivery of de e-mail met toegangsrechten. Download het OVA-bestand en ga verder met de installatie

VM-installatie

Stap 1:

Navigeer naar **Bestand > OVF-sjabloon implementeren** om de wizard **OVF-sjabloon implementeren** te openen, zoals in de afbeelding wordt getoond.

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

Select OVF and VMDK files

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

Enter a name for the virtual machine.

AMP-vPC

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

x  PrivateCloud-Latest.ova



Back Next Finish Cancel

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

Select creation type

How would you like to create a Virtual Machine?

Create a new virtual machine

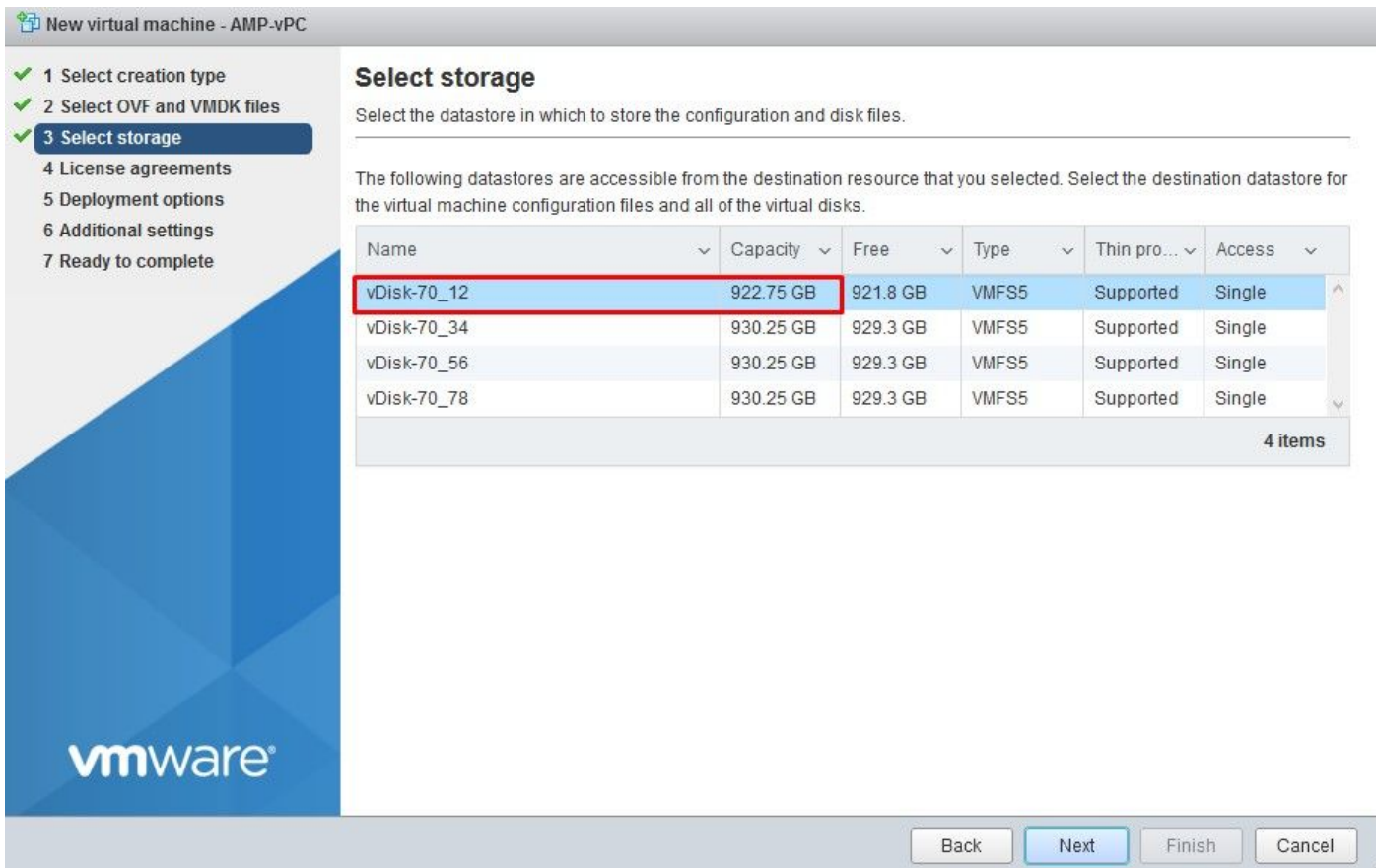
Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

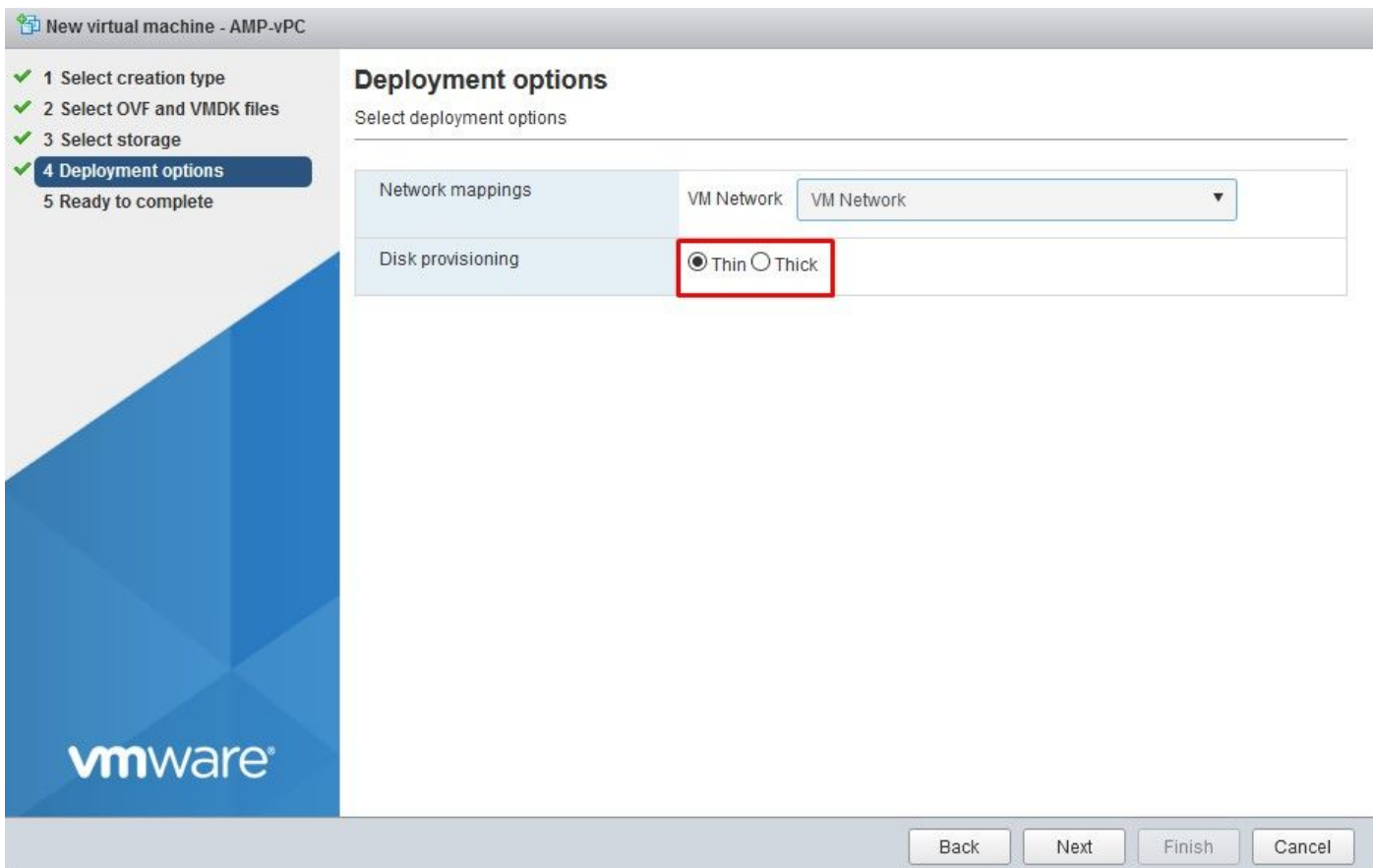
This option guides you through the process of creating a virtual machine from an OVF and VMDK files.



Back Next Finish Cancel



Opmerking: **Thick Provisioning** reserveert ruimte wanneer een schijf wordt gemaakt. Als u deze optie selecteert, kunnen de prestaties worden verbeterd via **Thin Provisioned**. Dit is echter niet verplicht. Selecteer nu op **Volgende**, zoals in de afbeelding.




Stap 2:

Selecteer **Bladeren...** om een OVA-bestand te selecteren en kies vervolgens **Volgende**. U ziet de standaard OVA parameters op de pagina **OVF Template Details**, zoals getoond in de afbeelding. selecteer **Volgende**.

The screenshot shows the 'New virtual machine - AMP-vPC' wizard in VMware vSphere. The left sidebar indicates the progress through five steps, with '5 Ready to complete' selected. The main area displays the 'Ready to complete' summary table and a warning message.

Property	Value
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.

At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

Eerste configuratie van beheerinterface


New virtual machine - AMP-vPC

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

Ready to complete

Review your settings selection before finishing the wizard

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

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

vmware

Back Next Finish Cancel

Zodra de VM is opgestart, voert u de eerste configuratie uit via VM-console.

Stap 1:

U zou kunnen opmerken dat de URL [UNCONFIGURED] toont als de interface geen IP-adres van de DHCP-server heeft ontvangen. Let op: deze interface is de **Management** interface. Dit is niet de **Production** interface.

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

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.

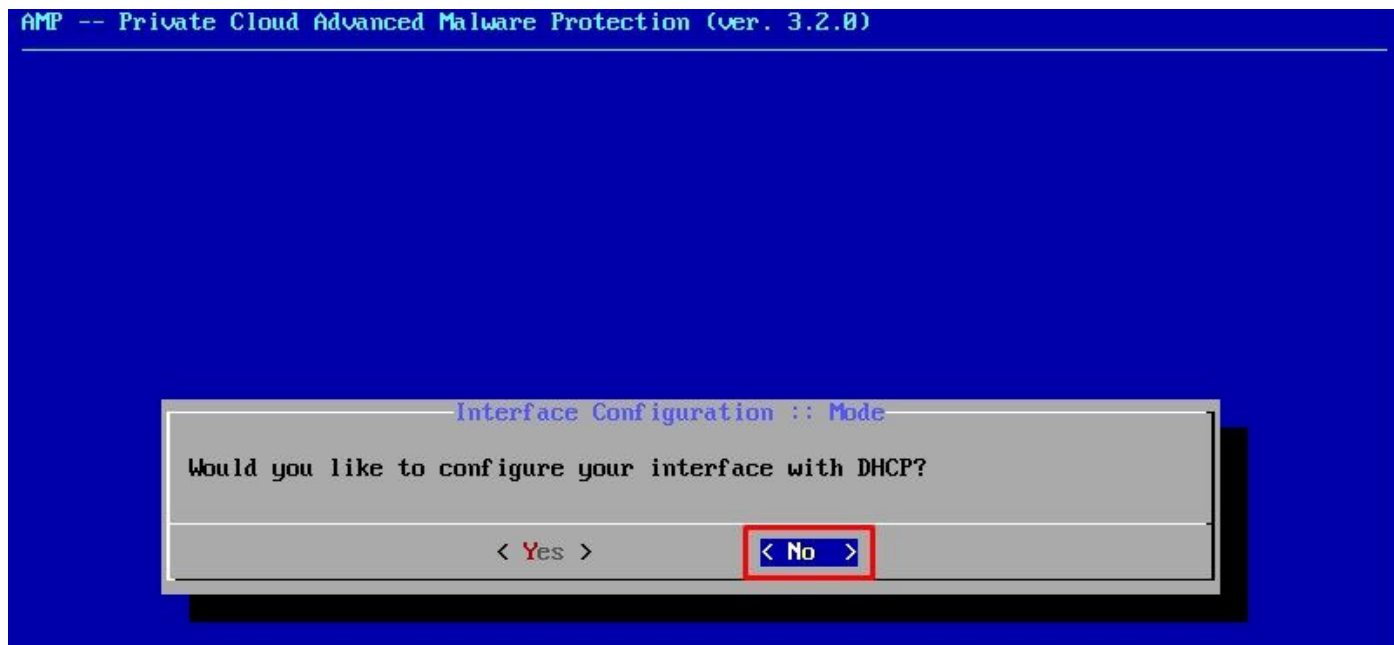
IP Address	: 192.168.75.91
Network Mask	: 255.255.255.0
Gateway* (Optional)	: 192.168.75.1

< OK > <Cancel>

Stap 2:

U kunt door de toetsen **Tab**, **Enter** en **Arrow** navigeren.

Navigeer naar **CONFIG_NETWORK** en selecteer de **ENTER**-toets op uw toetsenbord om te beginnen met de configuratie van het IP-adres voor het beheer van de Secure Endpoint Private Cloud. Als u geen DHCP wilt gebruiken, selecteert u **Nee** en selecteert u **ENTER**-toets.



Kies in het opgeroepen venster **Ja** en selecteer **ENTER**-toets.



Als het IP-adres al in gebruik is, wordt u met dit foutenlogboek behandeld. Ga gewoon terug en kies iets dat uniek en niet in gebruik is.

```
Restarting eth0...  
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 Error, some other host (00:0C:29:41:74:E3) alr  
eady uses address 192.168.75.91.  
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 Error, some other host (00:0C:29:41:74:E3) alr  
eady uses address 192.168.75.91.  
ERROR      : /etc/sysconfig/network-scripts/ifup-eth1 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>

Als alles goed gaat, zie je uitvoer die er zo uitziet

```

- 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 bad1ab
--- /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
```

Stap 3:

Wacht tot het blauwe scherm weer knalt met uw nieuwe STATISCHE IP. Let ook op het **eenmalige wachtwoord**. Neem een notitie en laten we onze browser openen.

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

Main Menu

Your AMP Private Cloud device can be managed at:

URL : <https://192.168.75.92>

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

CONSOLE

INFO

100%

Configure the Web administration interface.

Start command-line console / shell.

Display device status / information.

60%

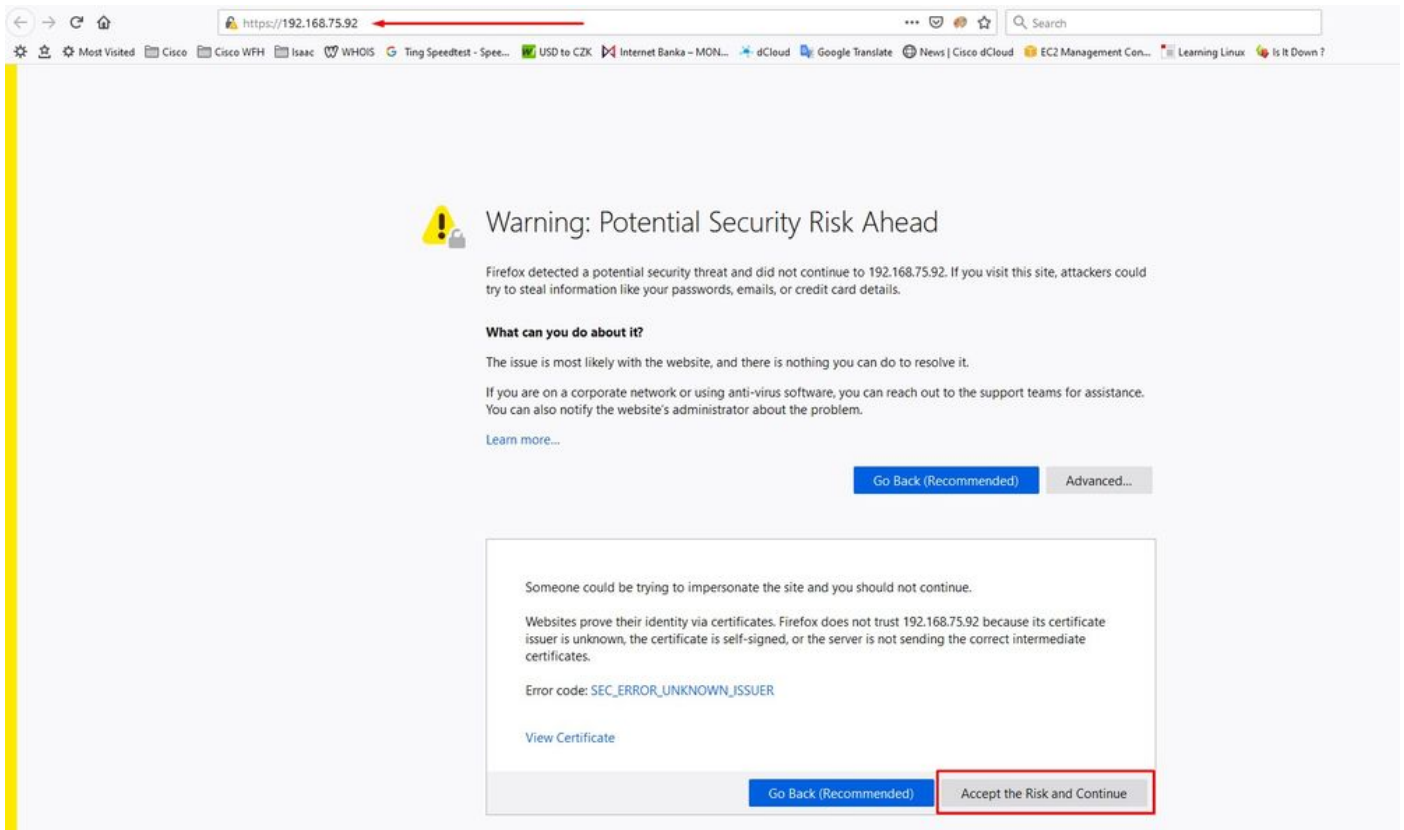
< OK >

Eerste configuratie van de vPC via web GUI

Stap 1:

Open een webbrowser en navigeer naar het IP-adres voor beheer van het apparaat. U kunt een certificaatfout ontvangen aangezien de Secure Endpoint Private Cloud aanvankelijk zijn eigen HTTPS-certificaat genereert, zoals in de afbeelding wordt getoond. Configureer uw browser om te vertrouwen op het zelfondertekende HTTPS-certificaat van Secure Endpoint Private Cloud.

Typ in uw browser het **STATISCHE IP** dat u eerder hebt ingesteld.



Stap 2:

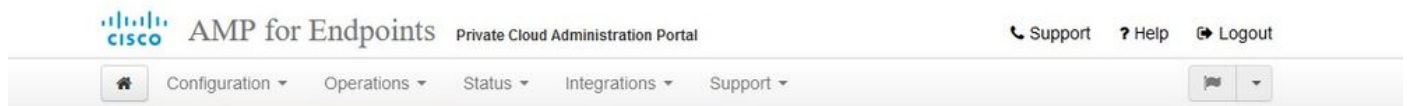
Na het inloggen moet u het wachtwoord opnieuw instellen. Gebruik het **initiële wachtwoord** van de console in het veld **Oud wachtwoord**. Gebruik uw nieuwe wachtwoord in het veld **Nieuw wachtwoord**. Voer uw nieuwe wachtwoord opnieuw in in het veld **Nieuw wachtwoord**. selecteer **Wachtwoord wijzigen**.



Stap 3:

Na het inloggen moet u het wachtwoord opnieuw instellen. Gebruik het **initiële wachtwoord** van de console in het veld **Oud wachtwoord**. Gebruik uw nieuwe wachtwoord in het veld **Nieuw wachtwoord**. Voer uw nieuwe wachtwoord opnieuw in in het veld **Nieuw wachtwoord**. selecteer

Wachtwoord wijzigen.



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.

Old one time password

Change Password

Stap 4:

Blader op de volgende pagina naar beneden om de licentieovereenkomst te aanvaarden. selecteer op **Ik heb gelezen en ga akkoord**.



Stap 5:

Nadat u de overeenkomst aanvaardt, krijgt u het installatiescherm, zoals in het beeld wordt getoond. Als u wilt herstellen van een back-up, kunt u dat hier doen, maar deze gids gaat verder met de optie **Clean Installation**. Selecteer deze optie bij **Start** in het gedeelte **Installatie reinigen**.



Installation Options

Only the License section can be altered after installation.

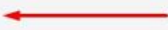
- Install or Restore
- License

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 >

Stap 6:

Het allereerste wat je nodig hebt is een vergunning om zelfs maar verder te gaan. U ontvangt een licentie en een wachtwoord wanneer u het product koopt. Selecteer de optie **+Licentiebestand uploaden**. Kies het licentiebestand en voer het wachtwoord in. Selecteer dit onder **Licentie uploaden**. Als het uploaden niet succesvol is, controleer dan of het wachtwoord juist is. Als het uploaden is geslaagd, wordt een scherm met geldige licentieinformatie weergegeven. Selecteer op **Volgende**. Als u de licentie nog steeds niet kunt installeren, neemt u contact op met Cisco Technical Support.



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 >

Stap 7:

U ontvangt de welkomspagina, zoals in de afbeelding. Deze pagina toont u de informatie die u moet hebben vóór de configuratie van de Private Cloud. Lees aandachtig de requirements Selecteer op **Volgende** om de voorinstallatie configuratie te starten.

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 >](#)

Configuratie

Stap 1:

Opmerking: Houd er rekening mee dat in de volgende sets dia enkele exclusieve items zijn opgenomen, zoals in de afbeelding, die alleen uniek zijn voor de **AIR GAP**-modus, die zijn omsloten en gemarkeerd als **ALLEEN AIRGAP**



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

Standalone

- 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.

- 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 ✓

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

Standalone

- 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.

- 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.



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

ALLEEN ≡ ≡ AIRGAP ≡ ≡

Stap 2:

Ga naar de pagina Secure Endpoint Console-account. Een beheergebruiker wordt voor de console gebruikt om beleid, computergroepen en extra gebruikers te maken. Voer naam, e-mailadres en wachtwoord in voor de console-account. Selecteer op **Volgende**.

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	
Password	[redacted]	

Next >

Als u bij het implementeren vanuit het OVA-bestand op dit probleem ingaat, hebt u twee keuzes: ga verder en los dit probleem later op of sluit het daarna af om uw geïmplementeerde VM aan te passen en aan te passen. Na het opnieuw opstarten ga je verder waar je bent vertrokken.

Opmerking: dit is vastgelegd in OVA-bestand voor versie 3.5.2 die correct wordt geladen met 128GB RAM en 8CPU kernen



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Hardware Requirements

Hardware Requirements Not Met

Your current configuration does not meet the hardware requirements.

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

Hardware Configuration

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

Shutdown

I understand the risks

Opmerking: gebruik alleen aanbevolen waarden, tenzij dit voor laboratoriumdoeleinden is

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		Connect
Network Adapter 2	VM Network		Connect
CD/DVD Drive 1	Host device		Connect
Video Card	Specify custom settings		

Save Cancel

Na de herstart gaan we verder waar we gebleven zijn.

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 >

Zorg ervoor dat u ETH1 ook configureert met STATISCHE IP.

Opmerking: u moet uw apparaat nooit configureren om DHCP te gebruiken tenzij u MAC-adresreserveringen voor de interfaces hebt gemaakt. Als de IP-adressen van uw interfaces veranderen, kan dit ernstige problemen veroorzaken met uw geïmplementeerde Secure Endpoint Connectors. Als u uw DNS-server niet hebt geconfigureerd, kunt u openbare DNS **tijdelijk** gebruiken om uw installatie te voltooien.

Stap 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 \(Applies Configuration\) ▶](#)

Stap 4:

Je krijgt de datum en tijd pagina. Voer de adressen in van een of meer NTP-servers die u wilt gebruiken voor datum- en tijdsynchronisatie. U kunt interne of externe NTP-servers gebruiken en meer dan één via een komma of een ruimte-afgebakende lijst specificeren. Synchroniseer de tijd met uw browser of voer `amp-ctl ntpdate` uit vanaf de apparaatconsole om een onmiddellijke tijdsynchronisatie met uw NTP-servers af te dwingen. Selecteer op **Volgende**.

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

← Optional
 Verify hostname resolution

Current System Time

/ /
 : : UTC

Next >

≡ ≡ ALLEEN ≡ ≡

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 >

ALLEEN ≡ ≡ AIRGAP ≡ ≡

Step 5:

U krijgt de pagina Certificaatautoriteiten, zoals weergegeven in de afbeelding. Selecteer bij **Certificaatinstantie toevoegen** om uw basiscertificaat toe te voegen.

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 >

Step 6:

De volgende stap is de configuratie van de Cisco Cloud-pagina, zoals in de afbeelding. Selecteer de juiste Cisco Cloud-regio. Breid **Hostnames bekijken** uit als u firewalluitzonderingen moet maken voor uw Secure Endpoint Private Cloud-apparaat om met Cisco Cloud te communiceren voor het opzoeken van bestanden en apparaatupdates. Selecteer op **Volgende**.

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 ✓

Cisco Cloud

Cisco Cloud Configuration

Region

Cisco Cloud, North America

[View Hostnames \(click to expand\)](#)

Cisco Cloud Identity

Client Identity

0f476ea8 [redacted] ddbc272a6c

Next >

Stap 7:

Navigeer naar de meldingen pagina, zoals in de afbeelding. Selecteer de frequentie voor kritische en reguliere meldingen. Voer de e-mailadressen in die u wilt ontvangen met een waarschuwing voor het Secure Endpoint-apparaat. U kunt e-mailaliassen gebruiken of meerdere adressen opgeven via een komma-gescheiden lijst. U kunt ook de naam van de afzender en het e-mailadres opgeven dat door het apparaat wordt gebruikt. Deze meldingen zijn niet hetzelfde als Secure Endpoint Console-abonnementen. U kunt ook een unieke apparaatnaam opgeven als u meerdere Secure Endpoint Private Cloud-apparaten hebt. Selecteer op **Volgende**.

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 Every 5 Minutes

Notification Frequency Every Week

Notification Addresses

Notification Recipients [redacted]@om

Notification Sender Address donotreply@cisco.com

Notification Sender Name AMP for Endpoints Device

Device Name

Device Name CyberNet vPC 2

Next >

Stap 8:

Daarna navigeer je naar de pagina van SSH-toetsen, zoals in de afbeelding. Selecteer op **Add SSH Key** om openbare sleutels in te voeren die u aan het apparaat wilt toevoegen. Met SSH-toetsen hebt u toegang tot het apparaat via een afstandsbediening met rootrechten. Alleen vertrouwde gebruikers moeten toegang krijgen. Uw Private Cloud-apparaat vereist een OpenSSH geformatteerde RSA-toets. U kunt later meer SSH-toetsen toevoegen via **Configuration > SSH** in uw beheerportal. Selecteer op **Volgende**.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. Below this, there are two red status boxes: 'Maintenance Mode' and 'Sanity Check Failing'. The main content area has a heading '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.' Below the text is a button labeled 'Add SSH Key'. Underneath is a section titled 'Windows PuTTY' which contains a table of SSH keys. The table has two columns for key details and an 'Edit' button. The first key is 'ecdsa-sha2-nistp256 AAAAE2' and the second is 'I4DKhrTNBv8/77T0d/Jagx7Przxs='.

Key Name	Created / Last Update	Actions
ecdsa-sha2-nistp256 AAAAE2	2021-11-17 23:01:01 +0000 created 20 days ago	Edit
I4DKhrTNBv8/77T0d/Jagx7Przxs=	2021-11-17 23:01:01 +0000 20 days since last update	Edit

Daarna krijgt u de sectie Services. Op de volgende pagina's moet u hostnamen toewijzen en het juiste certificaat en sleutelparen uploaden voor deze apparaatservices. In de volgende dia's kunnen we de configuratie van een van de 6 certificaten zien.

Services

Stap 1:

Tijdens het configuratieproces kunt u deze fouten bekijken.

De eerste "fout" die u zou kunnen opmerken, wordt gemarkeerd met de 3 pijlen. Om dit te omzeilen, vinkt u gewoon **"Strict TLS Check uitschakelen"** af

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 >](#)

Zonder strikte TLS-controle

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.	

vPC2-Authenticatic
+ Choose Certificate
← vPC2-Authentication.cyberworld.local.crt

vPC2-Authenticatic
+ Choose Key
↑ vPC2-Authentication.cyberworld.local.pem

Next >

Stap 2:

De volgende fout die u krijgt is als u "Validate DNS Name" aangevinkt. Hier heb je twee keuzes.

#1: Schakel het vinkje voor Validate DNS uit

#2: Ga terug naar uw DNS-server en configureer de rest van uw hostrecords.

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

+ Choose Certificate

+ Choose Key

Next >

Herhaal nu hetzelfde proces nog vijf keer voor de rest van de certificaten.

Verificatie

- De verificatieservice kan worden gebruikt in toekomstige versies van Private Cloud om gebruikersverificatie te verwerken.

Secure Endpoint-console

- De console is de DNS-naam waar de Secure Endpoint-beheerder toegang heeft tot de Secure Endpoint Console en Secure Endpoint Connectors nieuwe beleidsregels en updates ontvangen.

Dispositieserver

- Disposition Server is de DNS-naam waar de Secure Endpoint Connectors verzenden en ophalen cloud lookup informatie.

Disposition Server - uitgebreid protocol

- Disposition Server - Extended Protocol is de DNS-naam waar nieuwere Secure Endpoint

Connectors informatie over cloudzoeken verzenden en ophalen.

Disposition Update Service

- De Disposition Update Service wordt gebruikt wanneer u een Cisco Threat Grid-applicatie koppelt aan uw Private Cloud-apparaat. Het Threat Grid-apparaat wordt gebruikt om bestanden ter analyse te verzenden vanaf de Secure Endpoint Console en de Disposition Update Service wordt gebruikt door Threat Grid om de verwerking (*schoon of kwaadaardig*) van bestanden bij te werken nadat ze zijn geanalyseerd.

Firepower Management Center

- met Firepower Management Center Link kunt u een Cisco Firepower Management Center (FMC) apparaat koppelen aan uw Private Cloud-apparaat. Hiermee kunt u Secure Endpoint-gegevens weergeven in uw FMC-dashboard. Voor meer informatie over de integratie van VCC met Secure Endpoint, raadpleeg uw VCC-documentatie.

Waarschuwing: hostnamen kunnen niet worden gewijzigd als het apparaat klaar is met de installatie.

Noteer de vereiste hostnamen. U moet zes unieke DNS A-records maken voor de Secure Endpoint Private Cloud. Elk record wijst naar hetzelfde IP-adres van de Virtual Private Cloud Console-interface (eth1) en moet worden opgelost door zowel de Private Cloud als het Secure Endpoint.

Stap 3:

Op de volgende pagina download en controleer vervolgens **herstelbestand**.

U krijgt de pagina Herstel, zoals weergegeven in het beeld. U moet een back-up van uw configuratie downloaden en verifiëren voordat u de installatie start. Het herstelbestand bevat alle configuratie en de servertoetsen. Als u een herstelbestand kwijtraakt, kunt u uw configuratie niet herstellen en moeten alle Secure Endpoint connectors opnieuw worden geïnstalleerd. Zonder een originele sleutel, moet u de gehele private cloud infrastructuur met nieuwe sleutels opnieuw configureren. Het herstelbestand bevat alle configuraties met betrekking tot het opadmin portal. Het back-upbestand bevat de inhoud van het herstelbestand evenals alle dashboard portal gegevens zoals gebeurtenissen, connector geschiedenis enzovoort. Als u alleen de opadmin zonder de gebeurtenisgegevens en alles wilt herstellen, kunt u het herstelbestand gebruiken. Als u vanuit het back-upbestand terugzet, worden de opadmin- en dashboardportaalgegevens hersteld.

Selecteer op **Downloaden** om de back-up op de lokale computer op te slaan. Nadat het bestand is gedownload, selecteert u op **Kies bestand** om het reservebestand te uploaden en controleert u of het niet beschadigd is. Selecteer op **Next** om het bestand te verifiëren en ga verder.

- > 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](#)

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 ✓
- > 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

ALLEEN ≡ ≡ AIRGAP ≡ ≡

Je ziet soortgelijke invoer als deze...

Waarschuwing: wanneer u zich op deze pagina bevindt, verfris u niet omdat dit problemen kan veroorzaken.

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

Druk op de herstartknop als de installatie is voltooid

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

≡ ≡ ALLEEN ≡ ≡

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!
=====
```

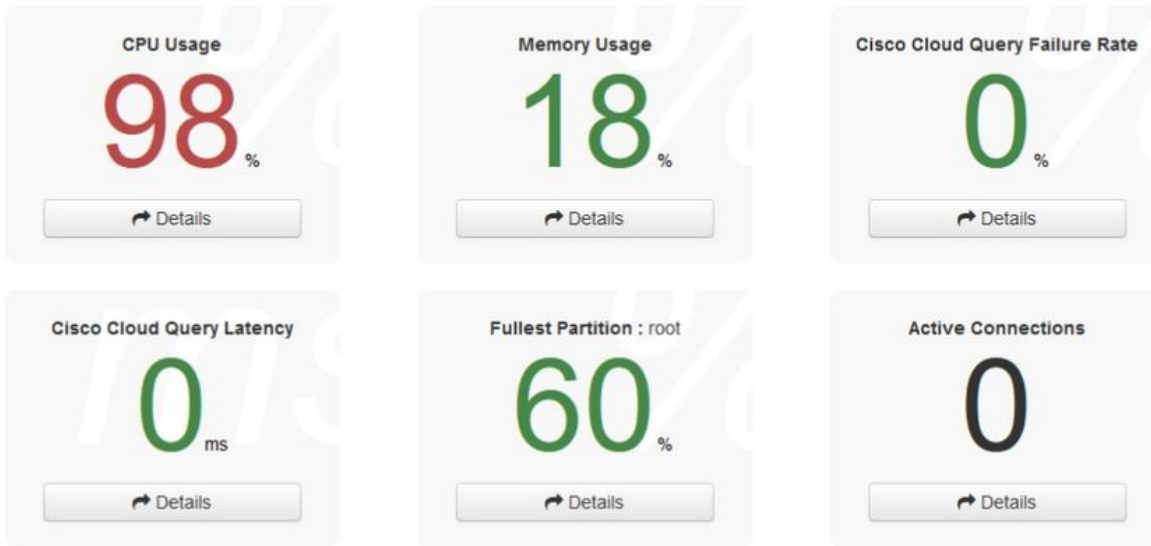
Download Output

ALLEEN AIRGAP

Wanneer het apparaat volledig opgestart is, wordt u de volgende keer dat u inlogt met uw beheerdersinterface met dit dashboard gepresenteerd. Je zou kunnen merken hoge CPU aan het begin, maar als je enkele minuten geeft wordt het vereffend.



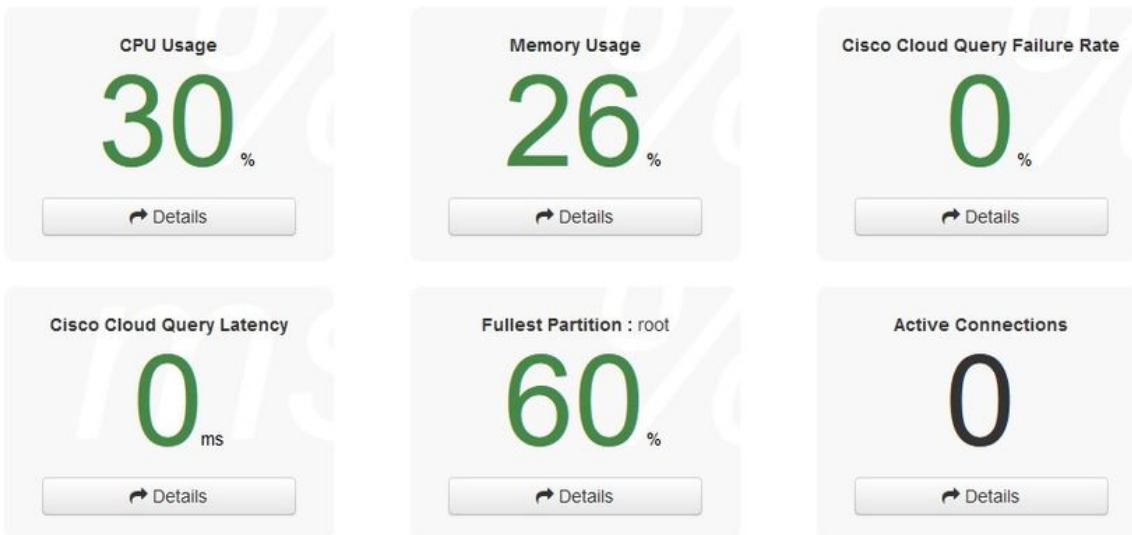
Key Metrics



Na een paar minuten...



Key Metrics



Van hieruit navigeer je naar Secure Endpoint console. Klik op het icoon dat eruit ziet als vuur in de rechterhoek naast de vlag.

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 options: Configuration, Operations, Status, Integrations, and Support. On the right side of the navigation menu, there is a red arrow pointing to a small icon that looks like a flame or a warning symbol. Below the navigation menu is a section titled "Key Metrics" which contains 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)

∨ ∨ ALLEEN ∨ ∨

Zoals u kunt zien, hebben we gefaald op de 'sanity check' door **DB Protect Snapshot**, ook Client Definitions, DFC en Tetra. Dit moet worden gedaan door offline update via gedownload ISO-bestand dat eerder is voorbereid via **amp-sync** en geüpload naar de VM of opgeslagen op NFS-locatie.



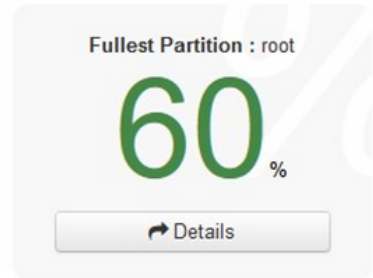
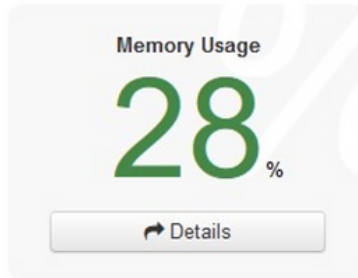
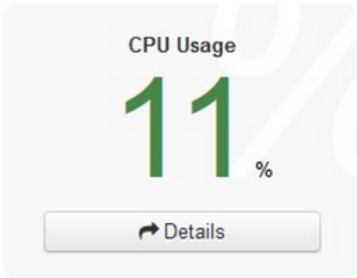
Sanity Check Failing

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

Details

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

Key Metrics





✖ Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

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

Content

✖ 3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

! ABSENT
Protect DB Version

! Import a Protect DB snapshot to your standalone device.

Checked 1 minute ago; the update check failed.

Software

✖ 3.2.0_202010082118
Private Cloud Software Version

Update Software

Checked 1 minute ago; the update check failed.

AirGap Update pakket

Voor het eerst moeten we deze opdracht gebruiken om de Protect DB te ontvangen

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

Opmerking: Download alle pakketten via deze opdracht en controleer vervolgens of het **meer dan 24 uur** kan duren. Afhankelijk van de snelheid en koppelingskwaliteit. In mijn geval met 1Gig fiber duurt het nog steeds bijna 25 uur om te voltooien. Dit is deels ook te wijten aan het feit dat deze download rechtstreeks van AWS is en dus is vertraagd. Ten slotte merk op dat deze download vrij groot is. In mijn geval was het gedownloade bestand **323GB**.

In dit voorbeeld gebruikten we **CygWin64**

1. Download en installeer de x64 versie van Cygwin.
2. Start setup-x86_64.exe en ga door het installatieproces om alle standaardwaarden te kiezen.
3. Kies een downloadspiegel.
4. Selecteer te installeren pakketten:
Alle -> Net -> krullen
Alle -> Utils -> Genisoimage
Alle -> Utils -> xmlstarlet
* VPC 3.8.x omhoog -> 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
% 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/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 915k 100 915k 0 0 3324k 0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-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/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 135k 100 135k 0 0 747k 0 --:~:~ --:~:~ --:~:~ 756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 54480 100 54480 0 0 383k 0 --:~:~ --:~:~ --:~:~ 385k
```

```
99.91% done, estimate finish Thu Nov 4 08:39:50 2021
99.91% done, estimate finish Thu Nov 4 08:39:51 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:51 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:51 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:52 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
100.00% done, estimate finish Thu Nov 4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)
Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso
User@VMStation-1 ~
```



Opmerking: In de nieuwste update VPC 3.8.x met CygWin64 als uw belangrijkste download tool kunt u dit probleem onderaan de lijst hieronder beschreven.

```
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.
```

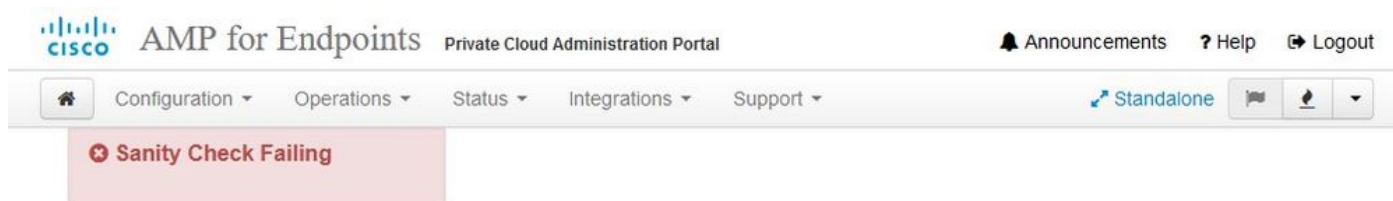
[Releaseopmerkingen](#) Pagina #58. Zoals u kunt zien is "xorriso" nu vereist. We veranderden het formaat van de ISO naar de ISO 9660 en die afhankelijkheid is wat het beeld naar het juiste formaat converteert zodat de update kan voltooien. Helaas, CygWin64 bieden geen xorriso in een van hun ingebouwde repositories. Maar voor degenen die nog steeds CygWin64 willen gebruiken is er een manier om dit probleem op te lossen.

Voer de back-up van de huidige 3.2.0 VPC (in dit geval) in Airgap Mode uit.

U kunt dit opdrachtformulier van CLI gebruiken

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

U kunt ook navigeren naar **Operations > Backups**, zoals in de afbeelding wordt getoond en daar **back-up uitvoeren**.



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](#)

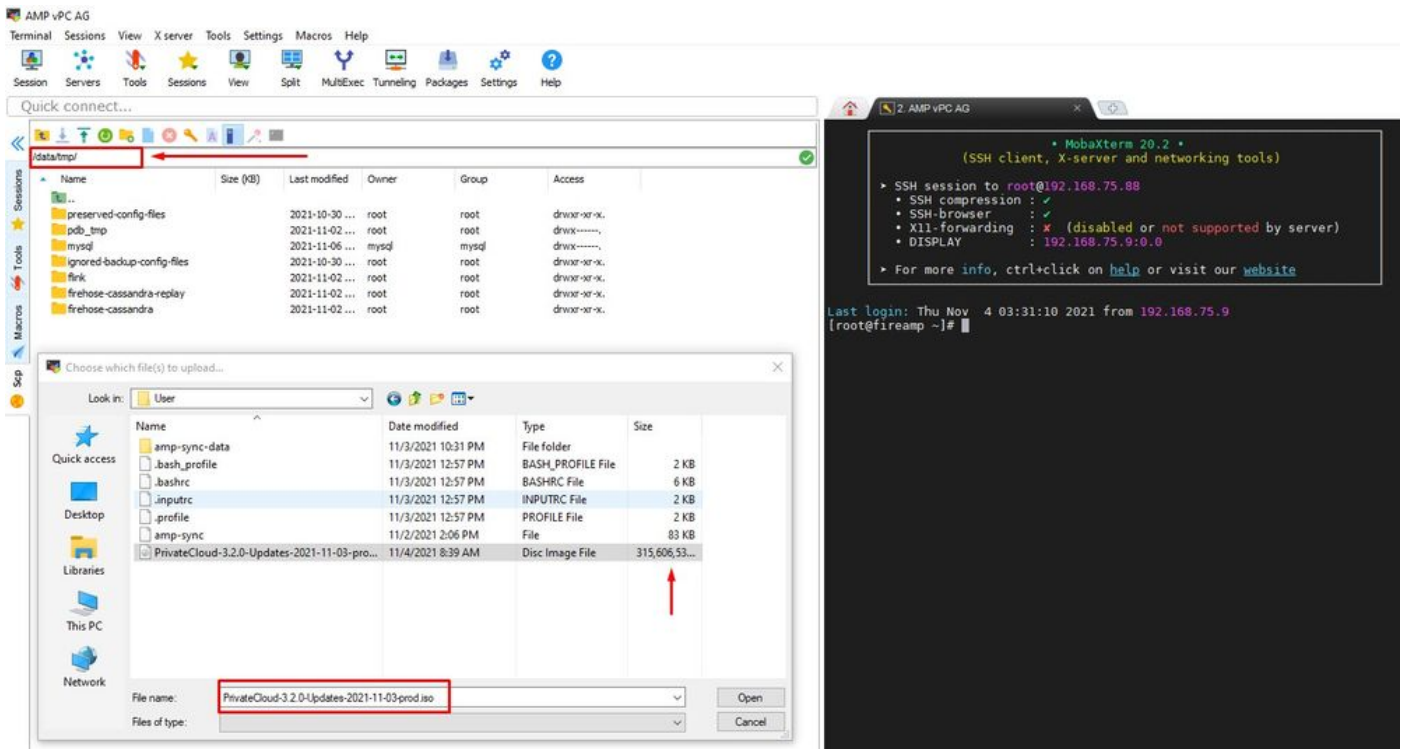
Previous Backups

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	Download Delete

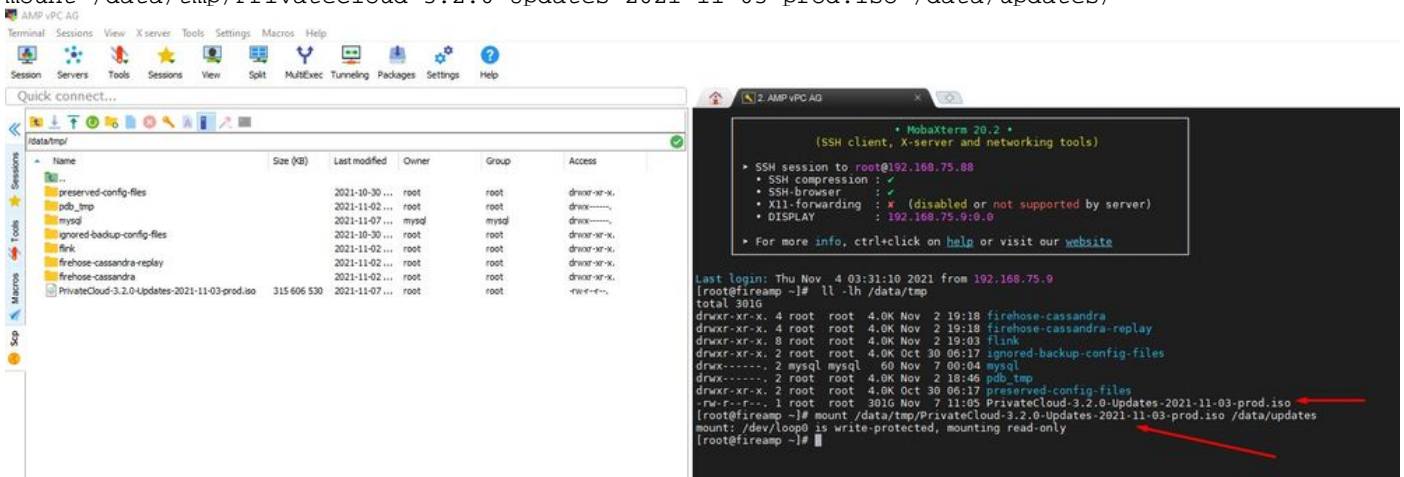
Breng de nieuwste ISO gegenereerd met amp-sync over naar de VPC. Dit kan ook tot enkele uren duren, afhankelijk van uw snelheid. In dit geval nam de overdracht 16 uur in beslag

```
/data/tmp
```



Nadat het uploaden is voltooid, koppel de ISO

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



Navigeer naar de Opdamin UI om de update uit te voeren Operations > Update apparaat > Selecteer Update ISO controleren.



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Checking ISO for updates...

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content
Import Protect DB

ABSENT
Protect DB Version

Import a Protect DB snapshot to your standalone device.

Checked 9 minutes ago; the update check failed.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

In dit voorbeeld ga ik eerst verder met Update Content



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update Content
Import Protect DB

ABSENT
Protect DB Version

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

A content update is available.

Software

3.2.0_202010082118
Private Cloud Software Version

Update Software

A software update is available.

Selecteer vervolgens Protect DB importeren.

The screenshot displays the Cisco AMP for Endpoints Private Cloud Administration Portal. At the top, there is a navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. A 'Sanity Check Failing' notification is visible. Below this, there is a section for updates with a 'Download amp-sync' button and a 'Check Update ISO' button. The 'Content' section shows a green checkmark for version '20211102210054' (Client Definitions, DFC, Tetra Content Version) and a red 'ABSENT' status for 'Protect DB Version'. A red box highlights the version number and the 'Import Protect DB' button. A red arrow points to the 'Import Protect DB' button. Below the content section, there is a 'Software' section showing version '3.2.0_202010082118' (Private Cloud Software Version) and an 'Update Software' button. A message indicates 'A software update is available'.

Zoals u ziet, is dit een ander zeer langdurig proces dat lang kan duren.

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

[Download Output](#)

⚙️ Protect DB importing

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

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

☰ Output

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

Probleem #1 - Uitgeputte ruimte in Data Store

Hier kun je op twee zaken ingaan. Aangezien vPC voor 3.5.2 geen externe NFS-opslag kan koppelen, moet u het update ISO-bestand uploaden naar de map **/data/temp**. In mijn geval, omdat mijn datastore maar 1 TB was, kwam ik de kamer uit en crashte de VM. Met andere woorden u hebt minimaal 2 TB ruimte in uw Data Store nodig om AirGap VPC succesvol te implementeren die onder versie 3.5.2 valt

Dit beeld hieronder is afkomstig van de ESXi-server die de fout laat zien dat er geen beschikbare ruimte op de vaste schijf meer is wanneer u de VM probeert op te starten. Ik kon van deze fout herstellen door een tijdelijke switch van de 128 GB RAM naar 64GB. Toen kon ik weer opstarten. Vergeet ook niet dat als u deze VM als Thin Client instelt, de negatieve kant van de Thin Client-implementatie is dat de schijfgrootte kan groeien, maar het zou niet krimpen zelfs als u wat ruimte vrijmaakt. Met andere woorden, laten we zeggen dat je je 300GB-bestand hebt geüpload naar de directory van de vPC en vervolgens hebt verwijderd. De schijf in ESXi geeft nog steeds 300 GB minder ruimte op uw vaste schijf weer

Event Details

Type: **error** User: **root** Time: **11/15/2021 12:24:43 PM** Target: **AMP-vPC AirGap**

Description:  11/15/2021 12:24:43 PM, Error message on AMP-vPC AirGap on UCS-2 in ha-datacenter: Failed to power on VM.

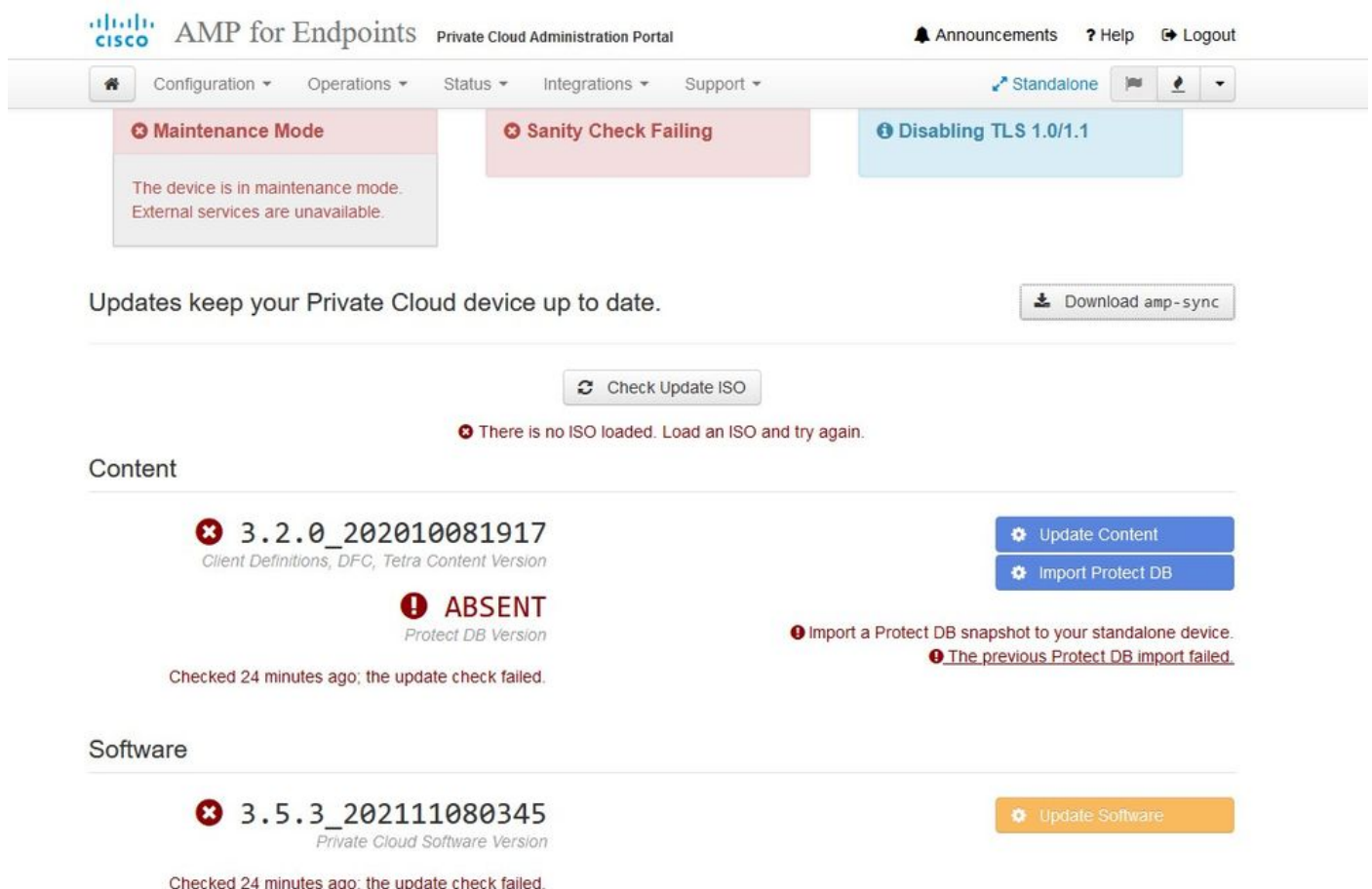
Error Stack: [Hide](#)

- ↳ Failed to power on VM.
- ↳ Could not power on virtual machine: msg.vmk.status.VMK_NO_SPACE.
- ↳ Failed to extend the virtual machine swap file
- ↳ Current swap file size is 0 KB.
- ↳ Failed to extend swap file from 0 KB to 134217728 KB.
- ↳ File system specific implementation of LookupAndOpen[file] failed
- ↳ File system specific implementation of Lookup[file] failed

Related Events: [Show](#)

Probleem #2 - oude update

Het 2^{de} probleem is als u de software-update eerst in werking stelt zoals ik in mijn 2^e proef deed en van 3.2.0 eindig ik met VPC aan verbetering aan 3.5.2 en wegens dat moest ik gloednieuwe ISO update dossier downloaden aangezien 3.2.0 ongeldig worden wegens het feit dat ik niet meer op de originele versie 3.2.0 was.



The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. At the top, there are navigation tabs for Configuration, Operations, Status, Integrations, and Support. A notification bar displays three alerts: 'Maintenance Mode' (The device is in maintenance mode. External services are unavailable.), 'Sanity Check Failing', and 'Disabling TLS 1.0/1.1'. Below the navigation, a section titled 'Updates keep your Private Cloud device up to date.' includes a 'Download amp-sync' button and a 'Check Update ISO' button. A message states: 'There is no ISO loaded. Load an ISO and try again.' The 'Content' section shows two entries: '3.2.0_202010081917' (Client Definitions, DFC, Tetra Content Version) with 'Update Content' and 'Import Protect DB' buttons, and 'ABSENT' (Protect DB Version) with a message: 'Import a Protect DB snapshot to your standalone device. The previous Protect DB import failed.' The 'Software' section shows '3.5.3_202111080345' (Private Cloud Software Version) with an 'Update Software' button. Both software entries indicate they were checked 24 minutes ago and the update check failed.

Dit is de fout die u ziet als u het ISO update bestand opnieuw probeert te koppelen.



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

Dit beeld laat zien hoe u het updatebeeld op een andere manier kunt monteren op uw VPC. In versie 3.5.x kunt u externe locatie, zoals NFS-opslag, gebruiken om het updatebestand met uw VPC te delen.



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.

Sanity Check Failing is gerelateerd aan Protect DB niet beschikbaar op de VPC



AMP for Endpoints

Private Cloud Administration Portal

Announcements

Help

Logout



Configuration

Operations

Status

Integrations

Support

Standalone



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download amp-sync

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

Update Content

Import Protect DB

ABSENT

Protect DB Version

ISO contains Protect DB snapshot version 20210531-0613.

Import a Protect DB snapshot to your standalone device.

A content update is available.

Software

3.5.2_202110130433

Private Cloud Software Version

Update Software

A software update is available.

⚙️ Protect DB importing

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

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

☰ Output

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

⬇️ Download Output



✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

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

☰ Output

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

Download Output

Volgende update automatisch starten



⚙ 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



Protect DB

20211116-2135

Queued Protect DB Update Version

20210531-0613

0.80%

Update Progress

Na dit zeer langdurige proces van het importeren Protect DB Database kunt u verplaatsen en bijwerken van de Clientdefinitie en -software die ongeveer 3+ uur extra kan nemen.

✔ 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!
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
--> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
--> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
--> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
--> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
--> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
--> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be updated
```

Download Output

Tot slot, let op, dit proces zal heel lang duren.

Ga voor VPC-applicatie naar deze TZ die andere methoden bevat om HW-applicatie te updaten, ISO-bestand te monteren en op te starten vanaf USB.

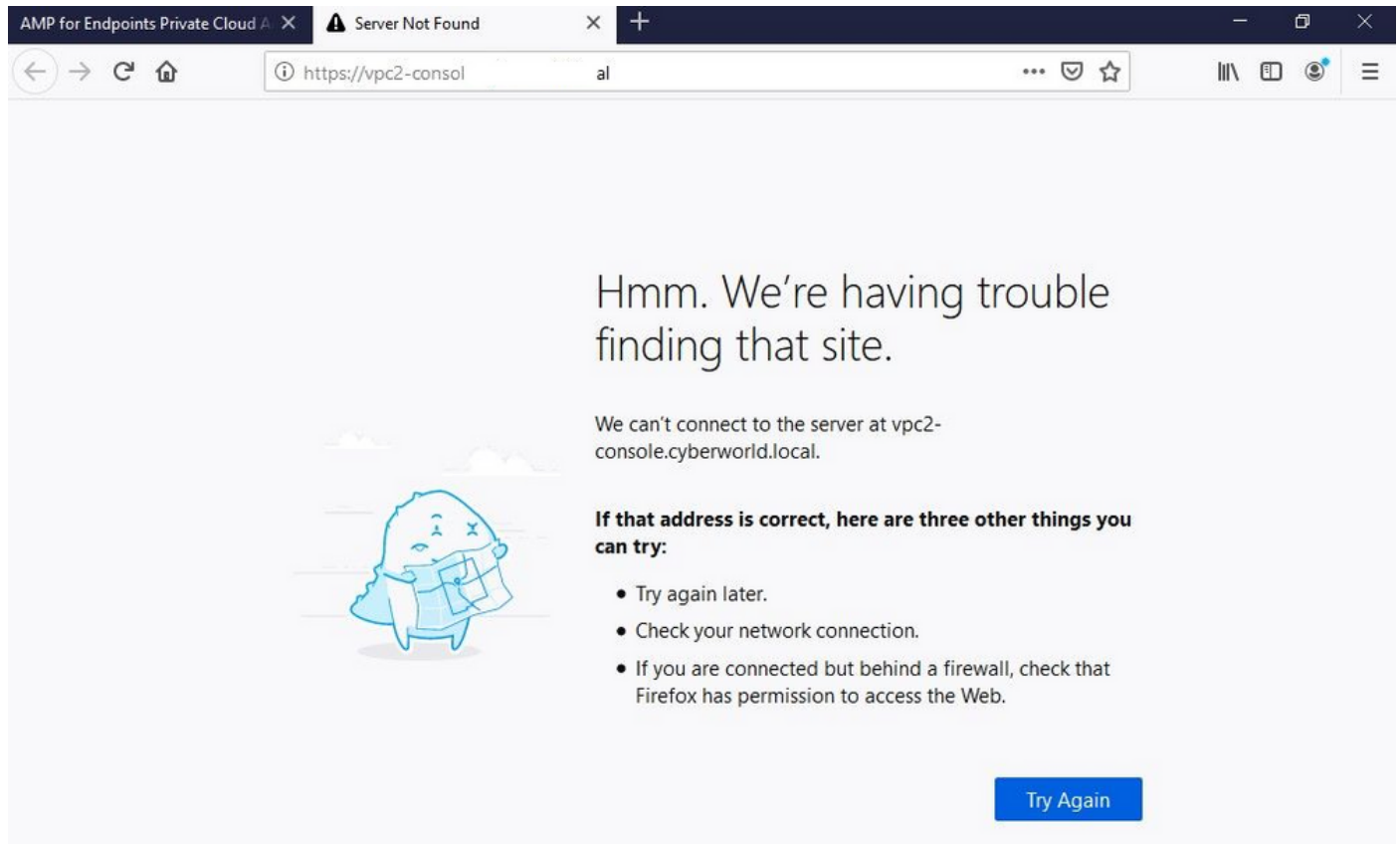
<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5>

ALLEEN ≡ ≡ AIRGAP ≡ ≡

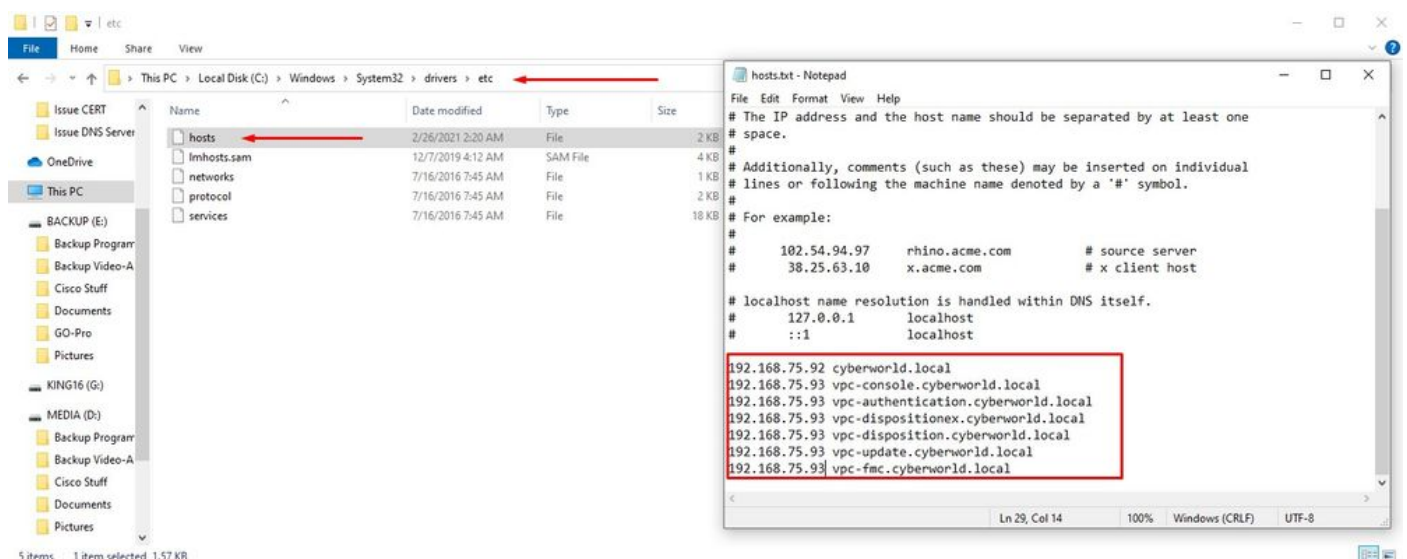
Basis probleemoplossing

Probleemoplossing #1 - FQDN- en DNS-server

Het eerste probleem dat u kunt tegenkomen is als uw DNS-server niet is ingesteld en alle FQDN niet correct zijn opgenomen en opgelost. Het probleem kan er zo uitzien wanneer u probeert te navigeren naar Secure Endpoint console via Secure Endpoint "fire" pictogram. Als u alleen IP-adres gebruikt, werkt het, maar kunt u de connector niet downloaden. Zoals je kunt zien op 3^e foto hieronder.



Als u HOSTS-bestand op uw lokale machine wijzigt zoals in de afbeelding, lost u het probleem op en krijgt u fouten.



U ontvangt deze fout terwijl u probeert om het installatieprogramma voor de Secure Endpoint-connector te downloaden.

A failure has occurred downloading an installer. Please contact support.

Download Connector

Group Protect

Na wat probleemoplossing was de enige juiste oplossing de installatie van DNS-server.

```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0000, finish 2021-03-02 15:43:00 +0000, duration 0.047382799
===== Server: 8.8.8.x
Address: 8.8.8.x#53 ** server can't find vPC-Console.cyberworld.local: NXDOMAIN
```

Zodra u alle FQDN's in uw DNS-server hebt opgenomen en de record in Virtual Private Cloud van openbare DNS naar uw DNS-server hebt gewijzigd, begint alles te werken zoals het had moeten doen.

Configuration network settings.

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

eth0 / 00:0C:29:A6:4A:11	IP Assignment 192.168.75.92	More details
eth1 / 00:0C:29:A6:4A:1B	IP Assignment 192.168.75.93	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

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 192.168.75.4



Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

Reconfigure Now

Reconfiguration

Configuration saved.



Home / Operations - Apply Configuration / Details

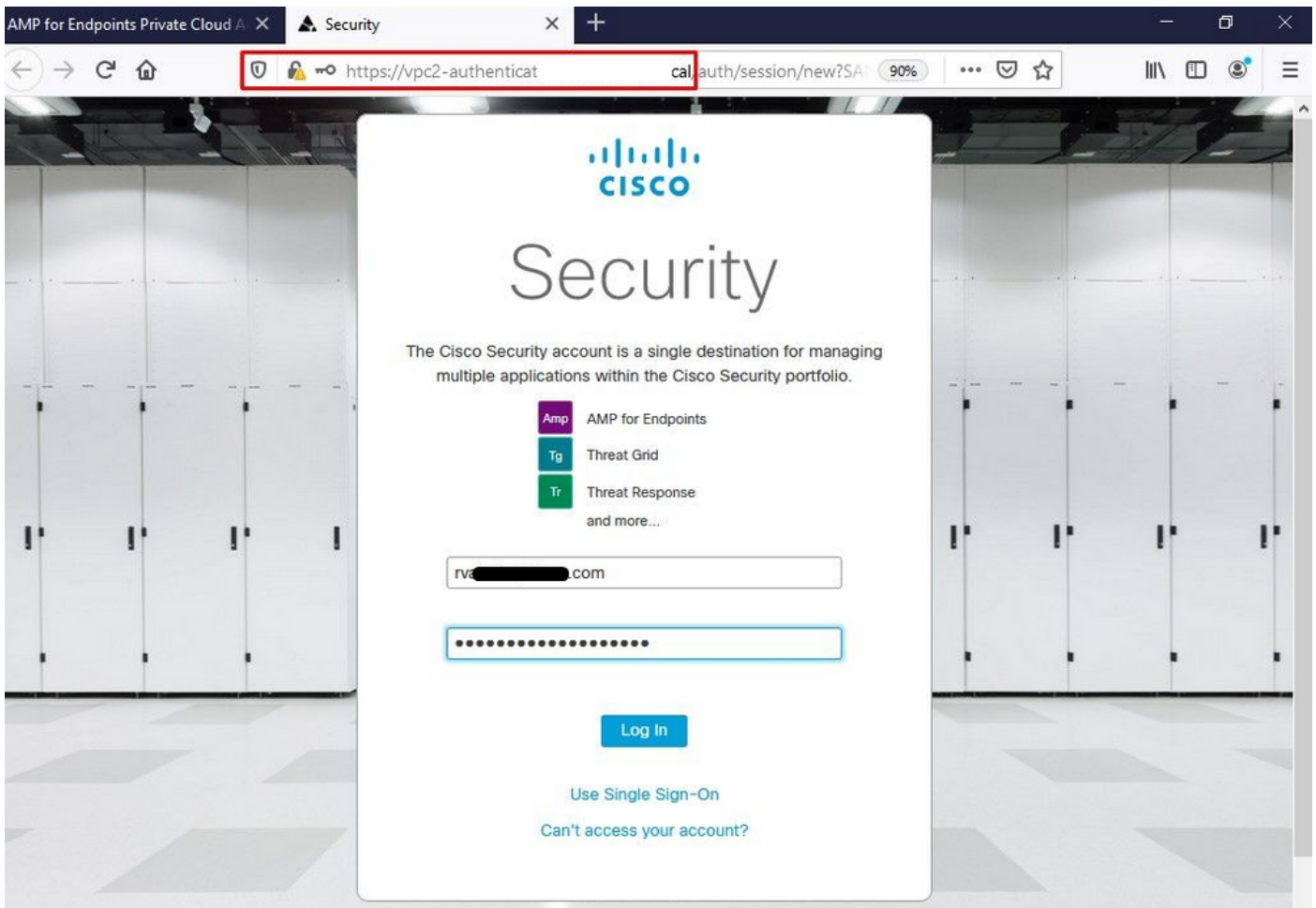
State	Started	Finished	Duration
Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...	Please wait...

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_password.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/run/cookbooks/cassandra/providers/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::Provider::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::Provider::Execute
```

Download Output

Op dit punt kunt u inloggen en de connector downloaden



U krijgt de eerste Secure Endpoint-beleids wizard voor uw omgeving. Het leidt u door de selectie van anti-virus product u gebruikt, als om het even welk, evenals volmacht, en de types van beleid u wilt opstellen. Selecteer een geschikte knop voor de configuratie... afhankelijk van het besturingssysteem van de -aansluiting.

U krijgt de pagina Bestaande beveiligingsproducten, zoals in de afbeelding. Kies de beveiligingsproducten die u gebruikt. Het genereert automatisch toepasselijke uitsluitingen om prestatiekwesties op uw endpoints te voorkomen. Selecteer op **Volgende**.

AMP for Endpoints Private Cloud | Dashboard | <https://vpc2-consol> | dashboard/fresh

AMP for Endpoints | Roman Valenta

Dashboard | Analysis | Outbreak Control | Management | Accounts

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.

Download de connector.

AMP for Endpoints | Roman Valenta

Dashboard | Analysis | Outbreak Control | Management | Accounts

Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

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

[Back](#) [Next](#)

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

You have chosen to open:

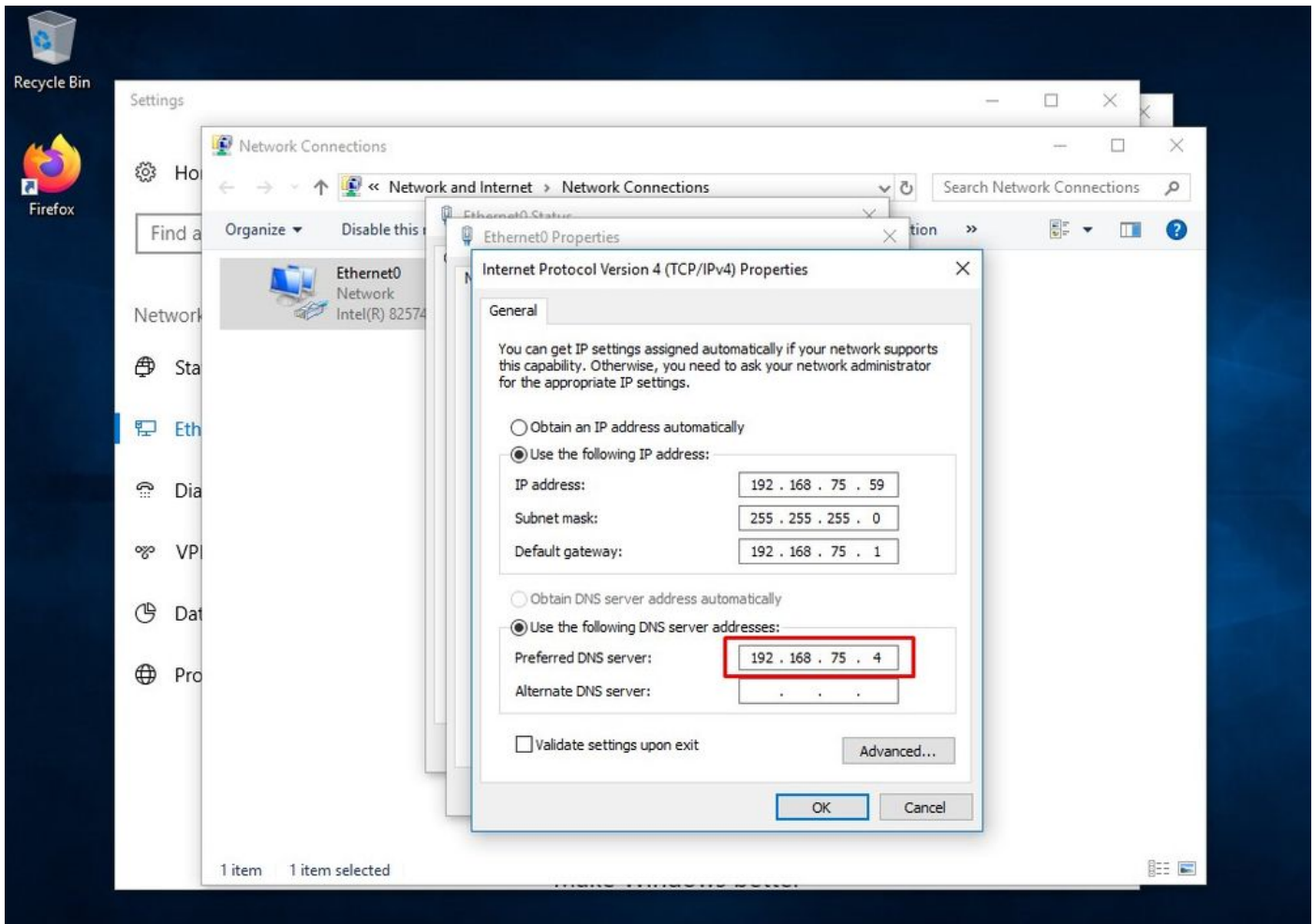
amp_Protect.exe
which is: exe File
from: https://vpc-console.cyberworld.local

Would you like to save this file?

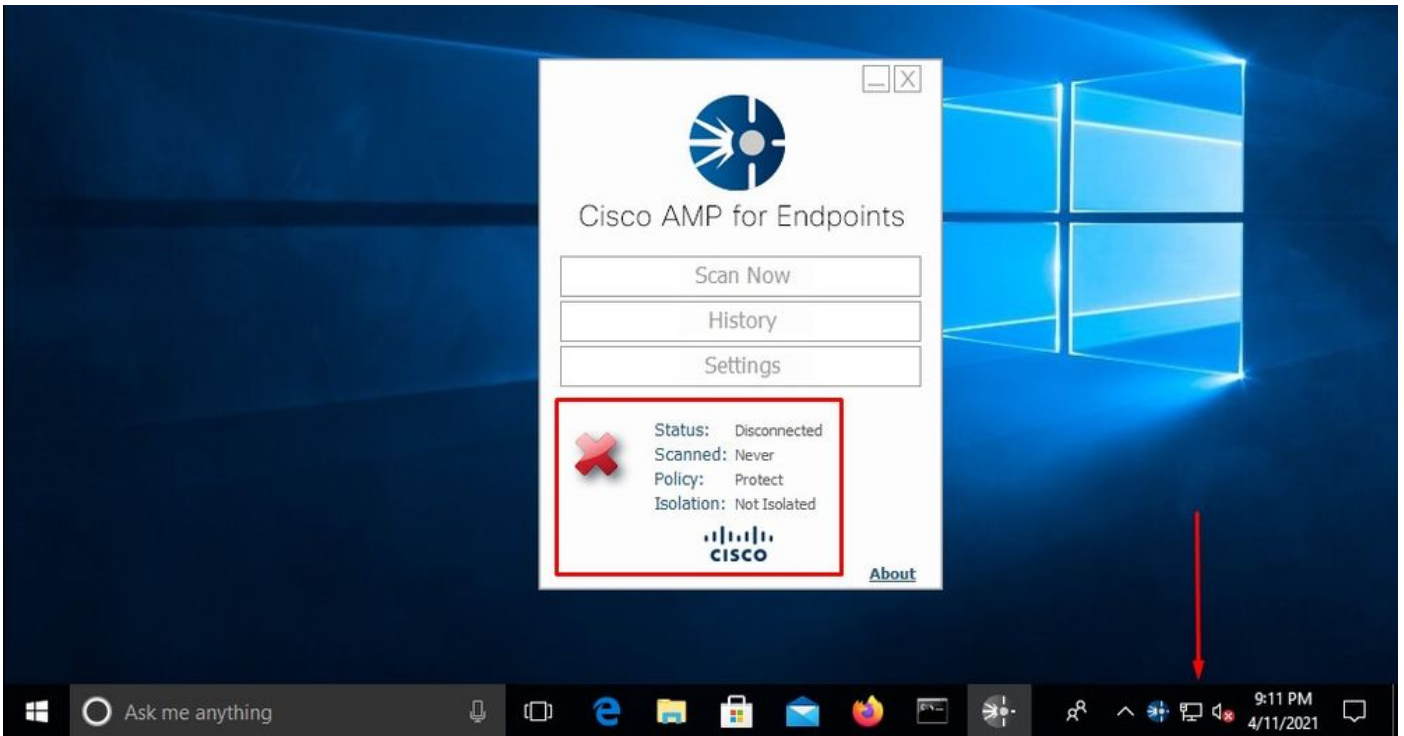
[Save File](#) [Cancel](#)

Probleem #2 - Probleem met Root CA

Het volgende probleem dat u kunt tegenkomen is als u uw eigen interne certificaten gebruikt is dat na de eerste installatie, connector kan tonen als losgekoppeld.



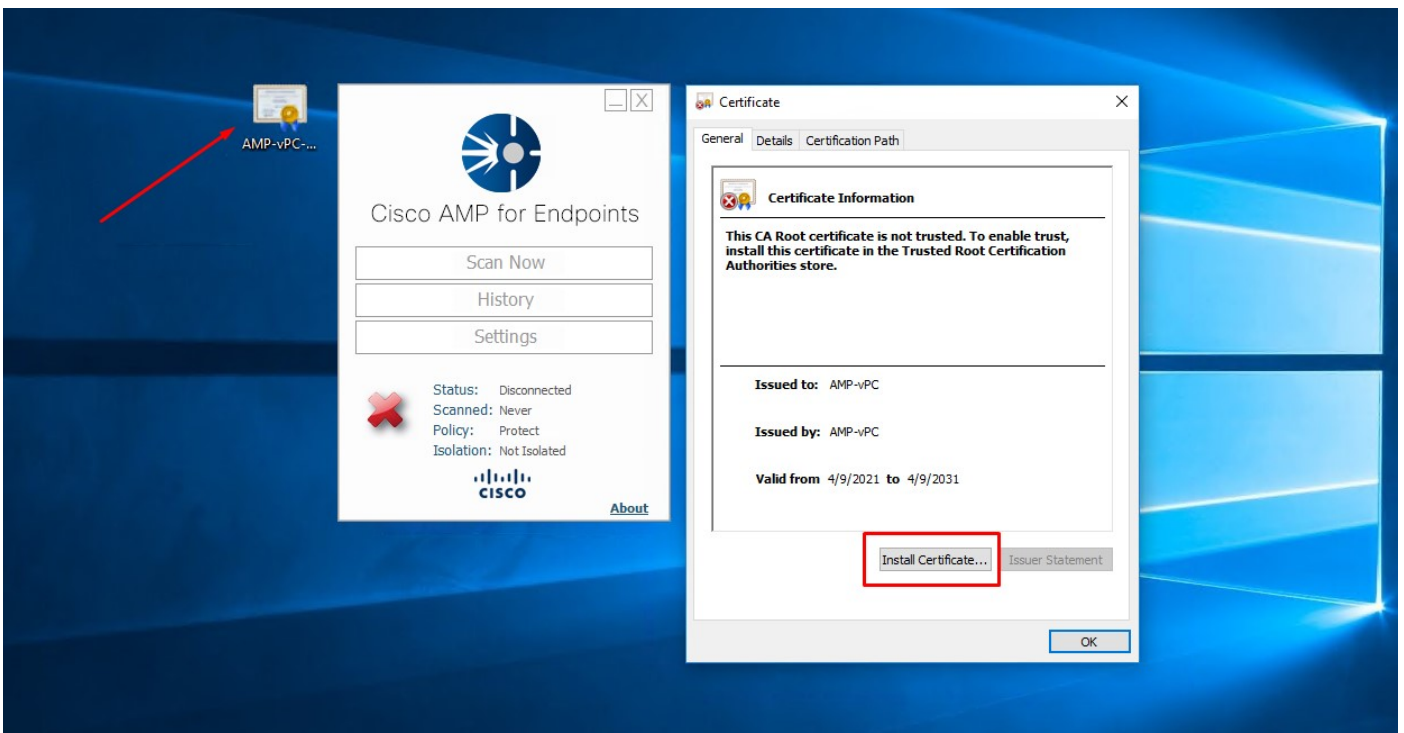
Zodra u de connector hebt geïnstalleerd, kan Secure Endpoint worden gezien als losgekoppeld. Voer diagnostische bundel uit en kijk door de logbestanden, kunt u de kwestie bepalen.

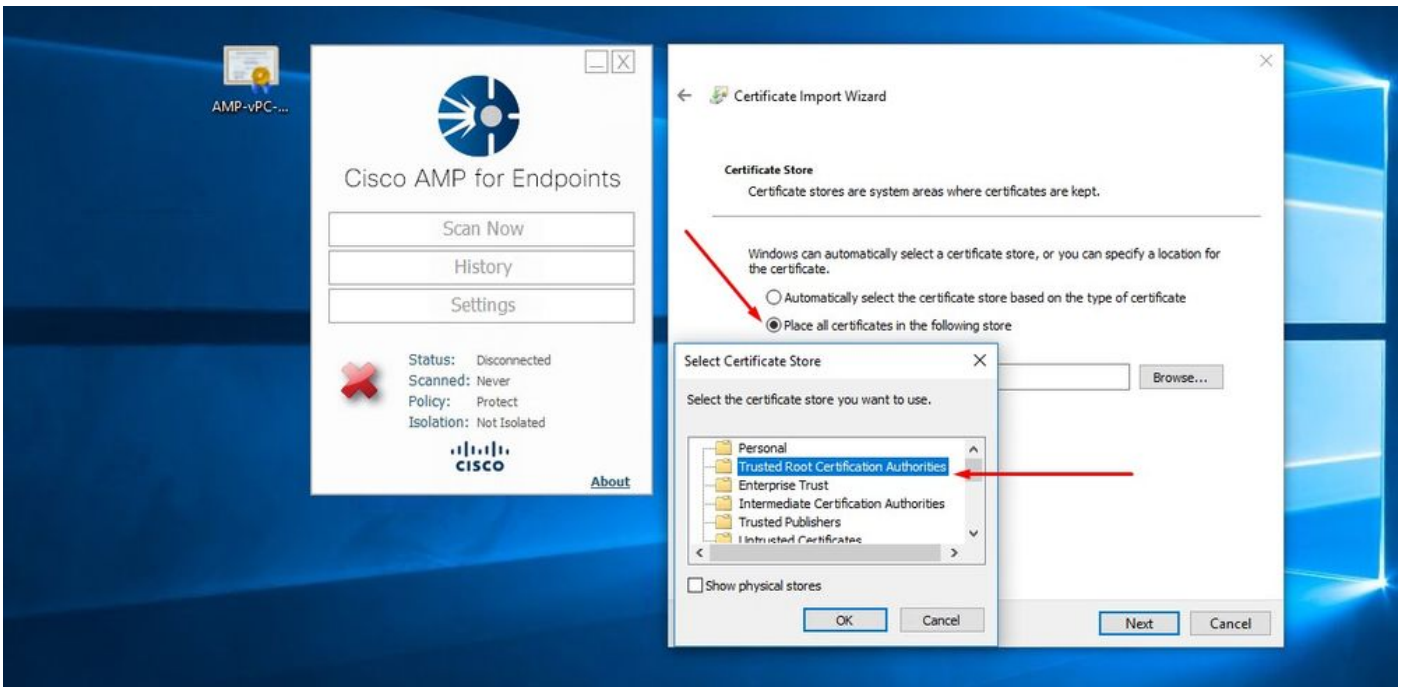
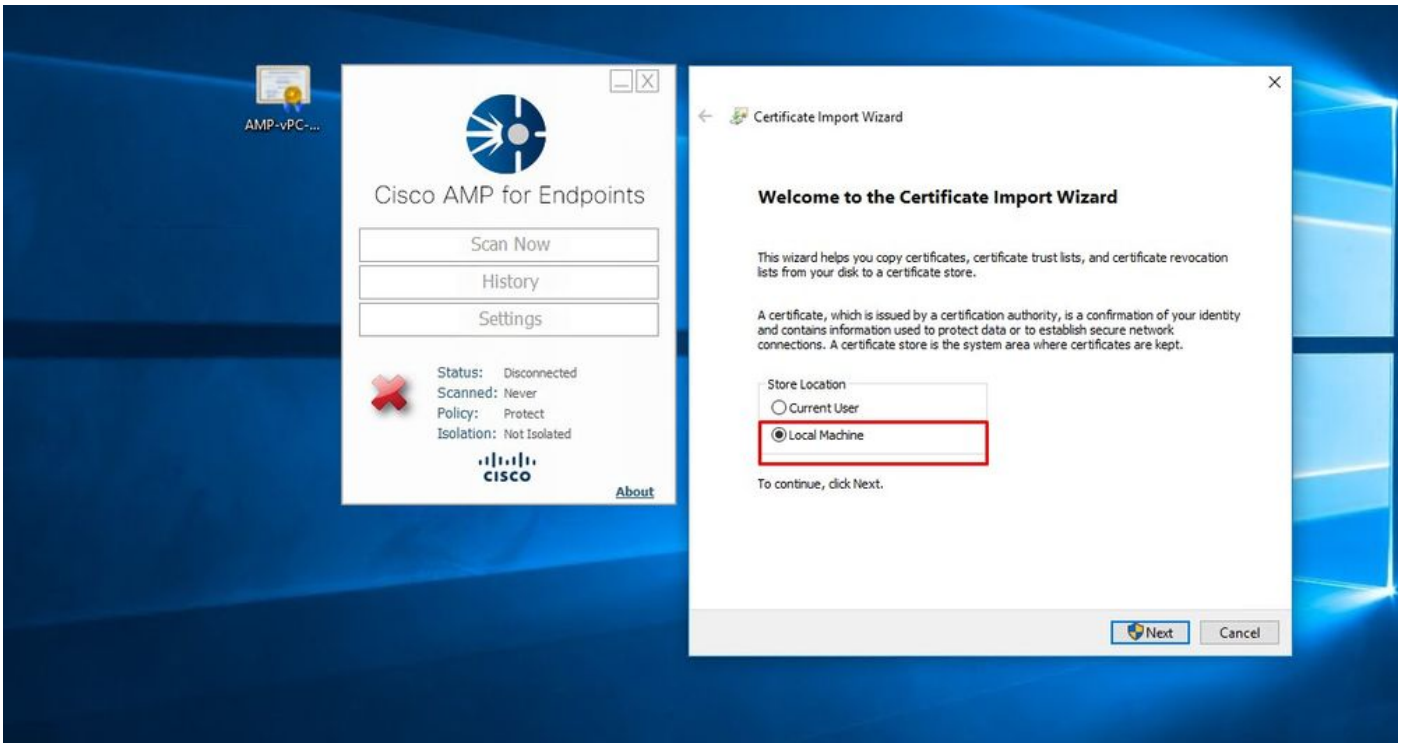


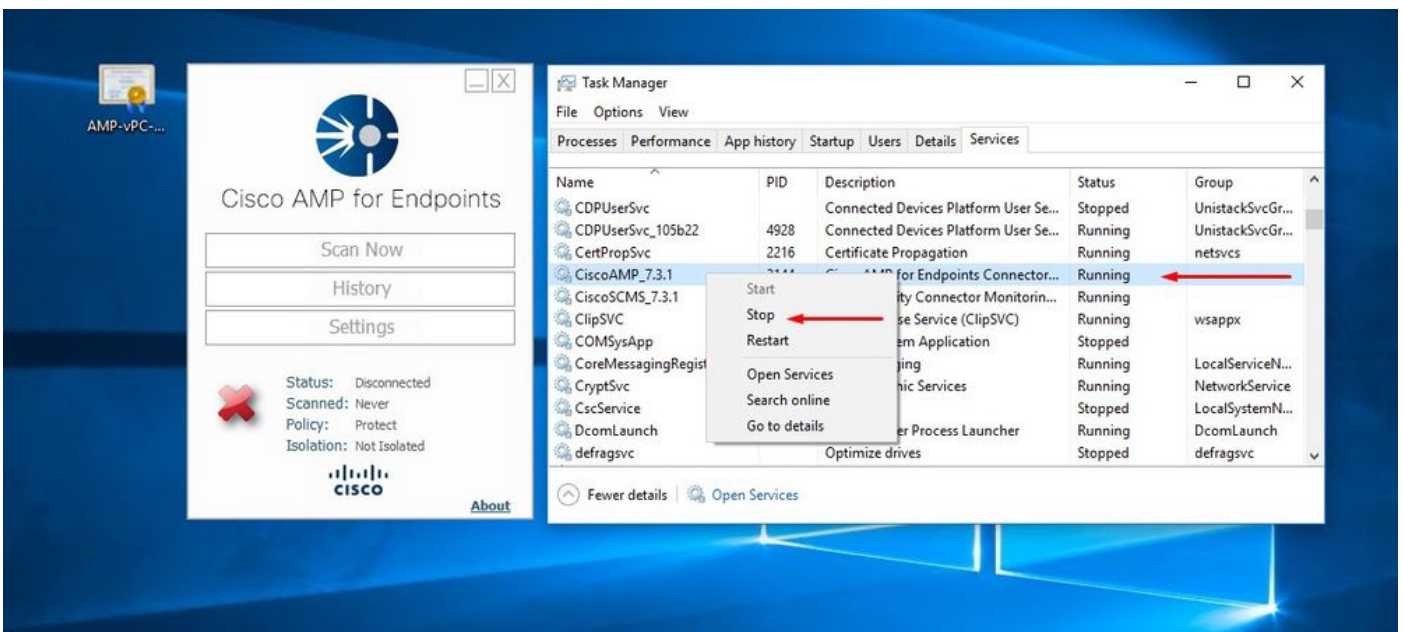
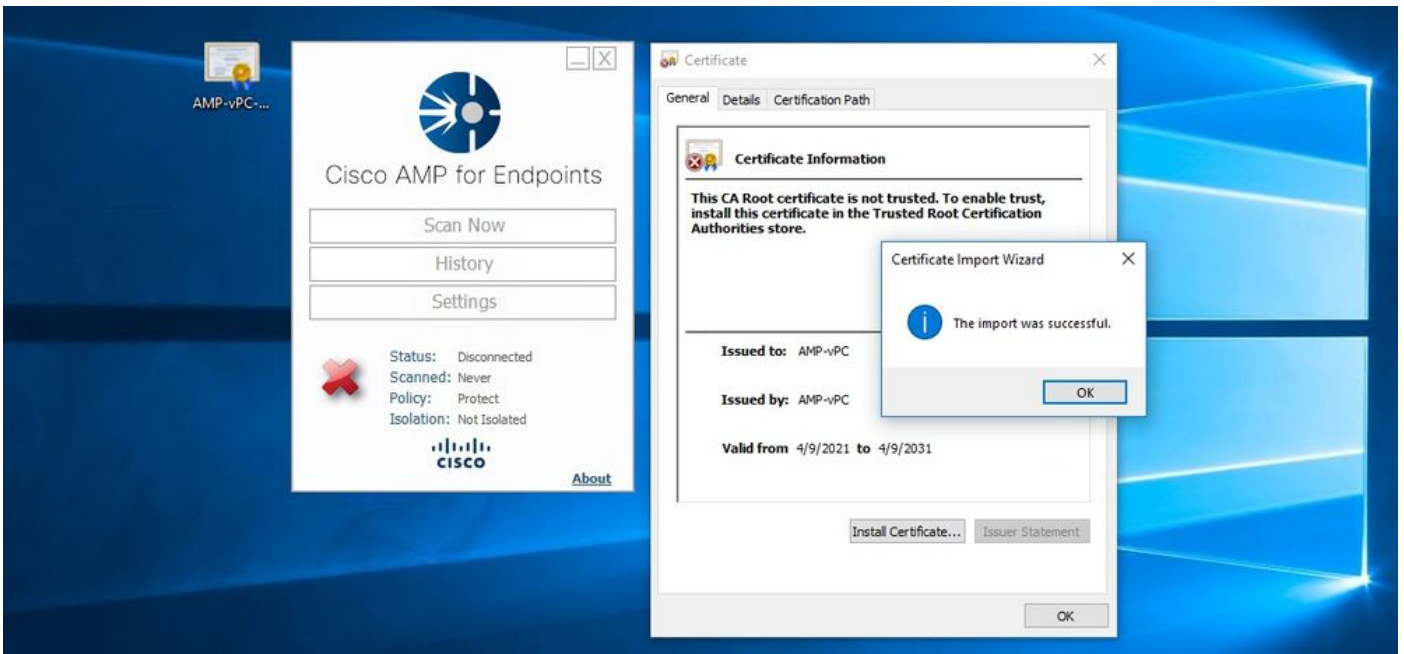
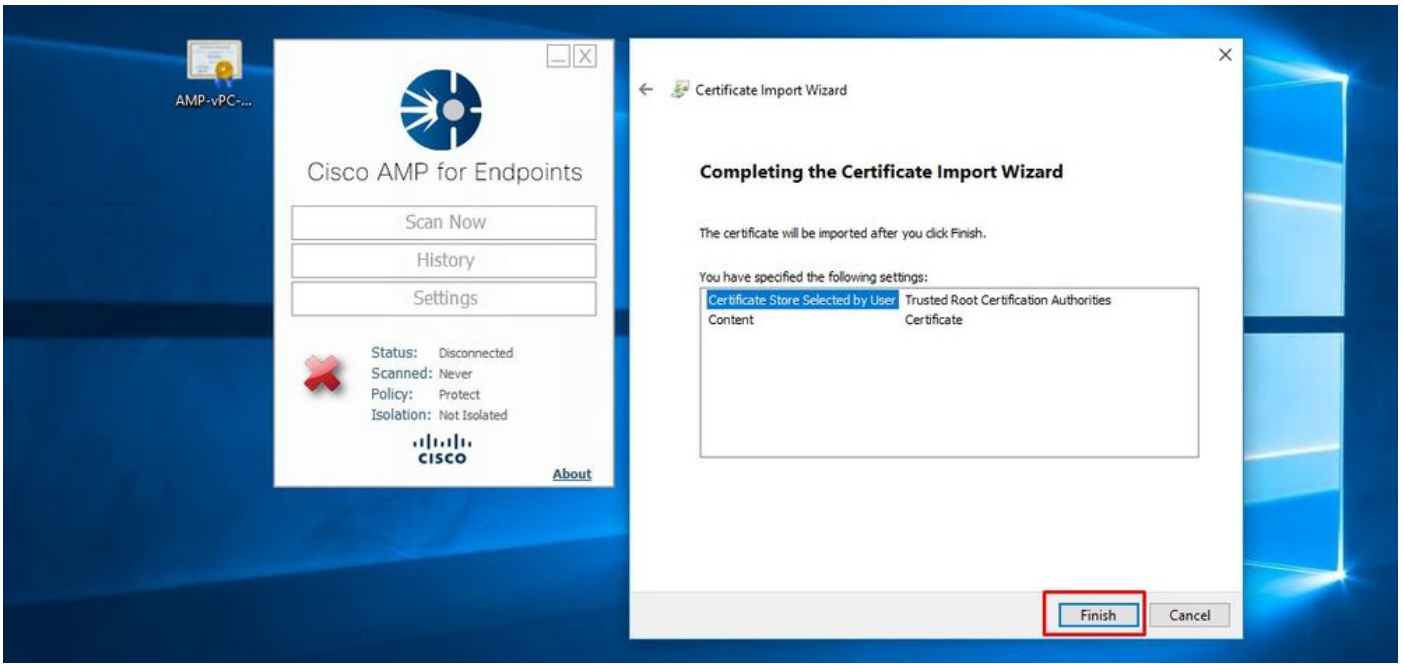
Gebaseerd op deze output die van diagnostische bundel wordt verzameld kunt u de fout van CA van de Wortel zien

```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworld.local/health failed (60): SSL peer certificate or SSH remote key was not OK (SSL certificate problem: unable to get local issuer certificate) (804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificate or SSH remote key was not OK) to https://vPC-Console.cyberworld.local/health (804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

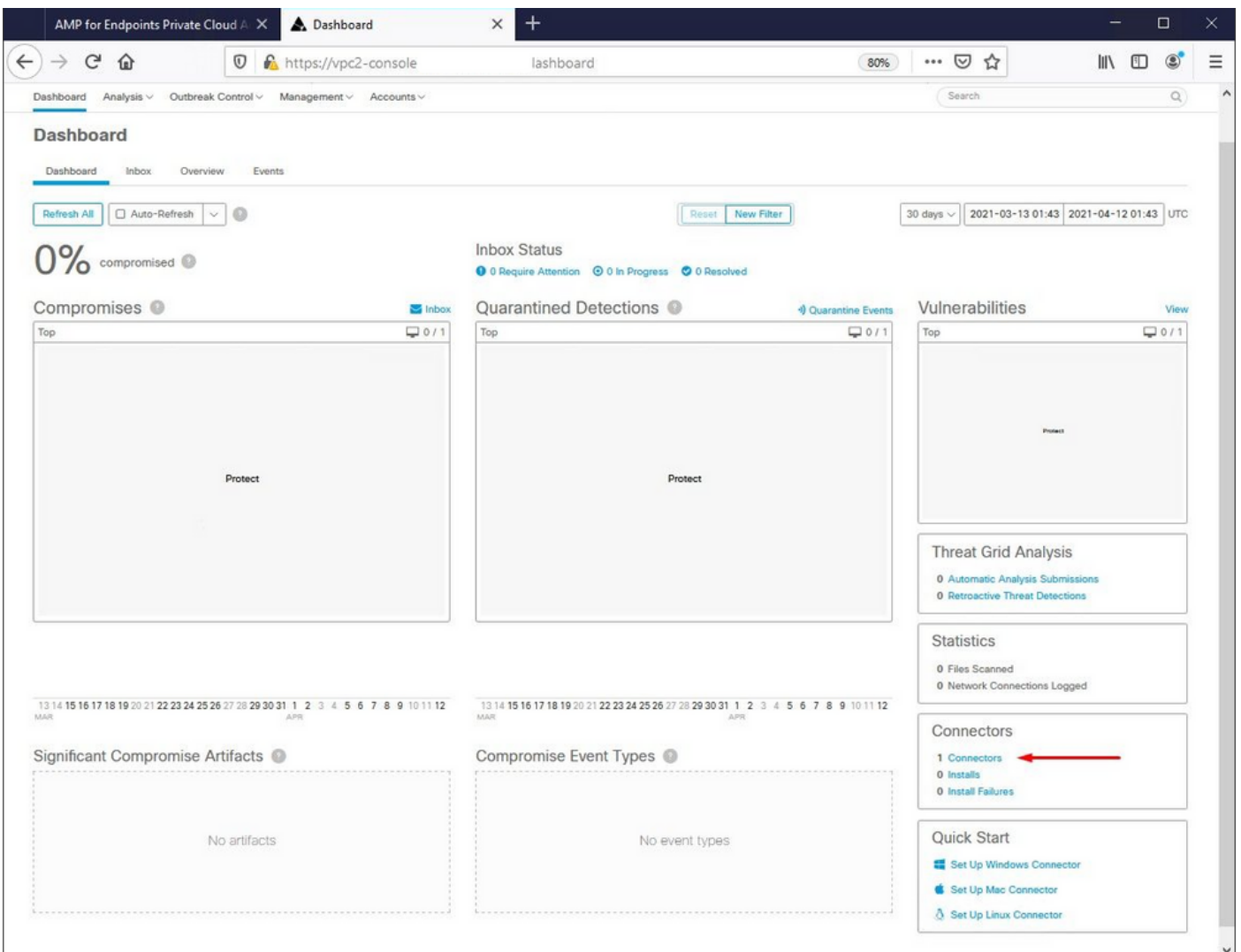
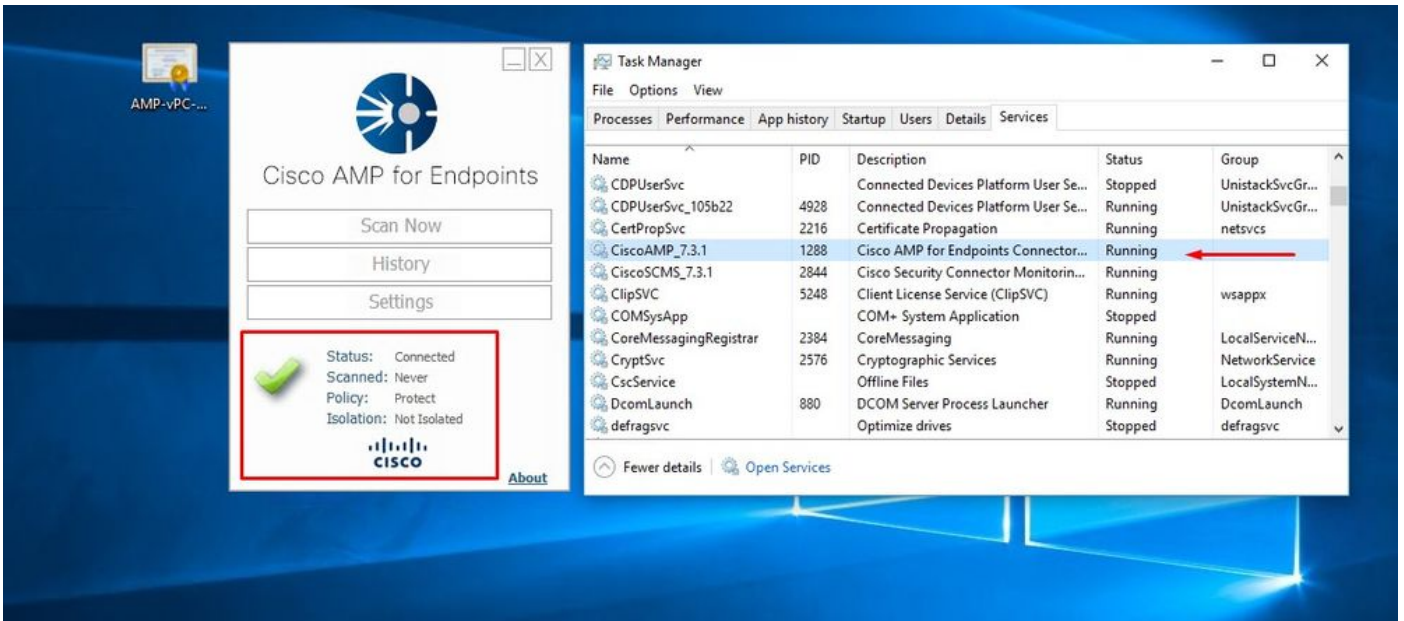
Nadat u de Root CA hebt geüpload naar de vertrouwde Root CA-winkel, start u de Secure Endpoint-service opnieuw. Alles begint te werken zoals verwacht.







Zodra we de Secure Endpoint-serviceconnector weer online krijgen zoals verwacht.



Geteste kwaadaardige activiteit

AMP for Endpoints Private Cloud A X Dashboard X Download Anti Malware Testfil X +

https://vpc2- /dashboard 80%

AMP for Endpoints Private Cloud A Dashboard

AMP for Endpoints

Dashboard Analysis Outbreak Control Management Accounts Search

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

Compromises

Inbox 0 / 1

Protect

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Quarantined Detections

Quarantine Events 1 / 1

Protect

Vulnerabilities

View 0 / 1

Protect

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

Significant Compromise Artifacts

No artifacts

Compromise Event Types

No event types

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.