

# Distribuisci CSDAC per oggetti O365 dinamici su FMC locale

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Distribuzione CSDAC su Ubuntu 20.04](#)

[Crea un connettore di Office 365](#)

[Crea connettore vCenter](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come distribuire e integrare CSDAC per oggetti Microsoft 365 dinamici su FMC locale con Ansible su Ubuntu 20.04.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comandi Linux di base.
- Python, Docker e Ansible Knowledge di base.
- Conoscenze base di Office 365.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firewall Management Center Virtual (FMCv) VMware con versione 7.2.5.
- Cisco Secure Dynamic Attributes Connector (CSDAC) versione 2.2.
- Ubuntu 4vCPU/8GB release 20.04.

- Docker release 24.0.6.
- Python 3.8.10.
- Ansible 2.12.10.

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

## Premesse

Cisco Secure Dynamic Attributes (CSDAC) consente di raccogliere dati quali reti e indirizzi IP dai provider del cloud e di inviarli al Centro gestione Cisco Secure Firewall in modo che possano essere utilizzati nelle regole dei criteri di controllo dell'accesso.

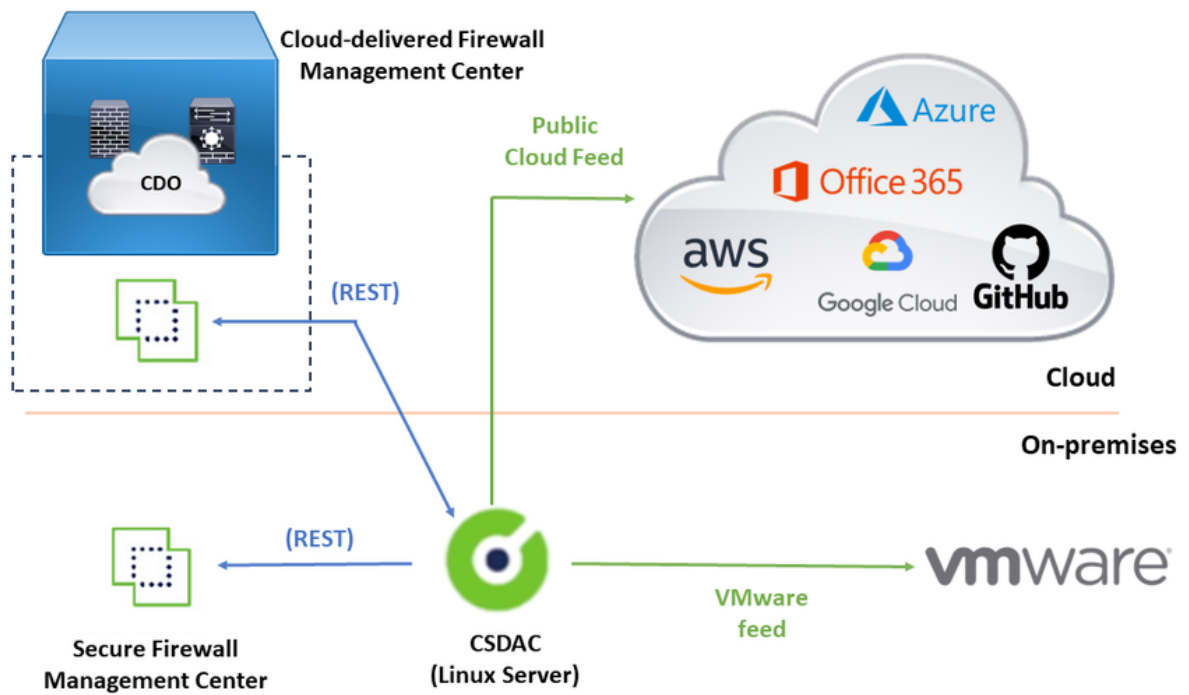
Cisco Secure Dynamic Attributes Connector consente di utilizzare codici di matricola e categorie di diverse piattaforme di servizi cloud quali AWS, Github, Google Cloud, Azure, codici di matricola di Azure, Microsoft Office 365 e vCenter.

I costrutti di rete, ad esempio gli indirizzi IP, non sono affidabili negli ambienti virtuali, cloud e contenitori a causa della natura dinamica dei carichi di lavoro e dell'inevitabilità della sovrapposizione degli indirizzi IP. Talvolta è necessario definire le regole dei criteri in costrutti non di rete, ad esempio il nome della macchina virtuale o il gruppo di sicurezza. Pertanto, le policy del firewall continuano a essere applicate anche quando l'indirizzo IP o la VLAN cambia. Tali tag e attributi possono essere raccolti utilizzando gli attributi dinamici contenitori Docker del connettore in esecuzione su macchine virtuali Ubuntu, CentOS o Red Hat Enterprise Linux. Se si desidera installare CSDAC su CentOS o Red Hat, consultare la [guida ufficiale](#) alla [documentazione](#).

Il connettore degli attributi dinamici sull'host Ubuntu viene installato utilizzando Ansible Collection. Cisco Secure Dynamic Attributes supporta due tipi di schede.

- Centro gestione firewall protetto locale.
- Centro gestione firewall distribuito tramite cloud.

Questo articolo è incentrato sulla distribuzione di Cisco Secure Dynamic Attributes Connect sull'host Ubuntu per il servizio cloud Microsoft Office 365 con Centro gestione firewall sicuro locale.

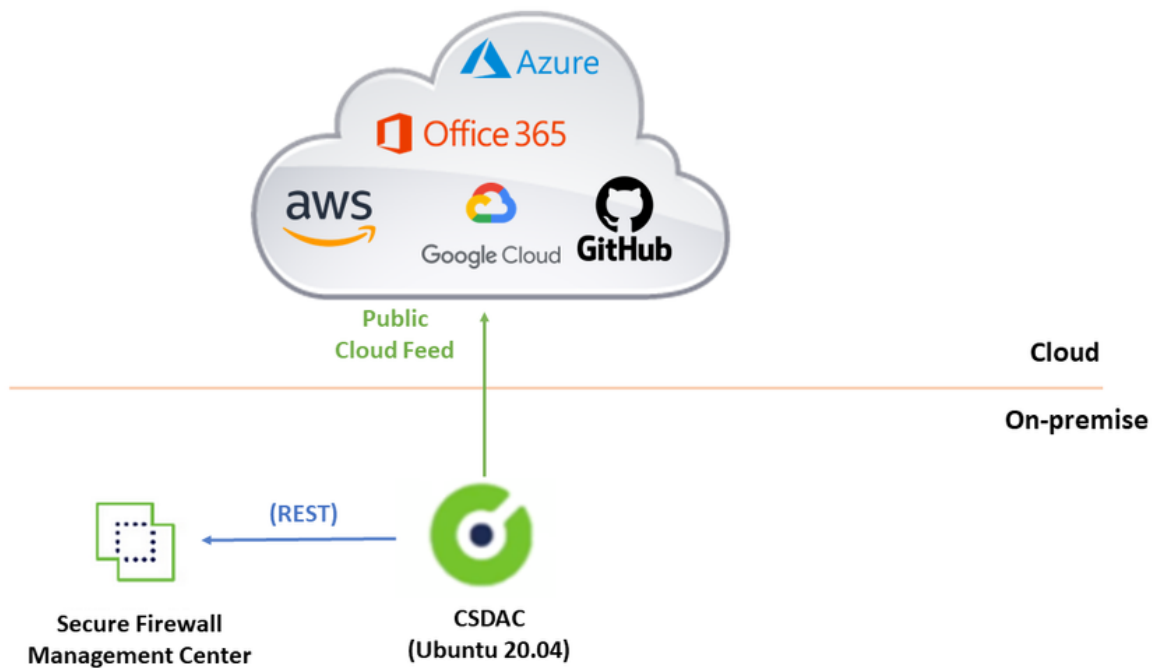


## Configurazione

Questa sezione è suddivisa nelle sezioni seguenti:

- Distribuzione CSDAC su Ubuntu 20.04.
- Creare il connettore di Office 365.
- Creare vCenter Connector.

## Esempio di rete



## Distribuzione CSDAC su Ubuntu 20.04

In questa sezione viene descritto come installare i prerequisiti software su Ubuntu.

Passaggio 1: Convalida Docker non installata.

```
root@tac:/home/tac# docker --version
```

```
Command 'docker' not found.
```

---

**⚠** Avviso: se è installato Docker, consultare la documentazione Docker per disinstallarlo.

---

Passaggio 2: Aggiornare i repository Ubuntu.


```
root@tac:/home/tac# sudo apt -y update && sudo apt -y upgrade
```

```
Hit:1 http://security-ubuntu-site/ubuntu focal-security InRelease
Hit:2 http://ubuntu-repository-web-site/ubuntu focal InRelease
Hit:3 http://ubuntu-repository-web-site/ubuntu focal-updates InRelease
Hit:4 http://ubuntu-repository-web-site/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
334 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree
....
```

### Passaggio 3: Confermare la versione Python.

```
root@tac:/home/tac# /usr/bin/python3 --version
Python 3.8.10
```

---

 **Avviso:** se la versione Python è precedente alla 3.6, è necessario installare la versione 3.6 o successiva.

---

### Passaggio 4: Installare le librerie comuni.

```
root@tac:/home/tac# sudo apt -y install software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
...
```

### Passaggio 5: Installare Ansible.


```
root@tac:/home/tac# sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible
Hit:1 http://security-ubuntu-site/ubuntu focal-security InRelease
Get:2 http://personal-package-archive-site/ansible/ansible/ubuntu focal InRelease [18.0 kB]
Hit:3 http://ubuntu-repository-web-siteubuntu focal InRelease
Hit:4 http://ubuntu-repository-web-site/ubuntu focal-updates InRelease
Hit:5 http://ubuntu-repository-web-site/ubuntu focal-backports InRelease
Get:6 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main amd64 Packages [1 132 B]
Get:7 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main i386 Packages [1 132 B]
Get:8 http://personal-package-archive-site/ansible/ansible/ubuntu focal/main Translation-en [756 B]
Fetched 21.1 kB in 3s (7 526 B/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
...
```

### Passaggio 6: Verificare la versione ansible.

```
root@tac:/home/tac# ansible --version
ansible [core 2.12.10]
config file = /etc/ansible/ansible.cfg
configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
ansible python module location = /usr/lib/python3/dist-packages/ansible
ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
```

```
executable location = /usr/bin/ansible
python version = 3.8.10 (default, May 26 2023, 14:05:08) [GCC 9.4.0]
jinja version = 2.10.1
libyaml = True
```

---

 Nota: è normale per Ansible fare riferimento a Python 2.x. Il connettore utilizza ancora Python 3.6.

---

## Passaggio 7: Ottenere il software Dynamic Attributes Connector con Ansible.

```
root@tac:/home/tac# ansible-galaxy collection install cisco.csdac
Starting galaxy collection install process
Process install dependency map
Starting collection install process
Downloading https://galaxy-ansible-site/download/cisco-csdac-2.2.1.tar.gz to /root/.ansible/tmp/ansible
Downloading https://galaxy-ansible-site/download/community-crypto-2.15.1.tar.gz to /root/.ansible/tmp/a
Installing 'cisco.csdac:2.2.1' to '/root/.ansible/collections/ansible_collections/cisco/csdac'
cisco.csdac:2.2.1 was installed successfully
Installing 'community.crypto:2.15.1' to '/root/.ansible/collections/ansible_collections/community/crypt
Downloading https://galaxy-ansible-site/download/community-general-7.4.0.tar.gz to /root/.ansible/tmp/a
community.crypto:2.15.1 was installed successfully
Installing 'community.general:7.4.0' to '/root/.ansible/collections/ansible_collections/community/gener
community.general:7.4.0 was installed successfully
```

## Passaggio 8: Spostarsi nella directory csdac.

```
root@tac:/home/tac# cd ~/.ansible/collections/ansible_collections/cisco/csdac/
```

## Passaggio 9: Installare il servizio di raccolta.

```
root@tac:~/.ansible/collections/ansible_collections/cisco/csdac# ansible-playbook default_playbook.yml
BECOME password:
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'
[WARNING]: running playbook inside collection cisco.csdac

PLAY [localhost] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [cisco.csdac.csdac : Define Python Interpreter] *****
ok: [localhost]

...

TASK [cisco.csdac.csdac : verify that core services are started] *****
```

ok: [localhost]

TASK [cisco.csdac.csdac : verify that core services are started] \*\*\*\*\*  
ok: [localhost]

TASK [cisco.csdac.csdac : verify that core services are started] \*\*\*\*\*  
ok: [localhost]

TASK [cisco.csdac.csdac : verify that core services are started] \*\*\*\*\*  
ok: [localhost]

TASK [cisco.csdac.csdac : Post task] \*\*\*\*\*  
ok: [localhost] => {}

MSG:

Please login in to <https://172.16.1.53> to configure csdac application

PLAY RECAP \*\*\*\*\*  
localhost : ok=72 changed=8 unreachable=0 failed=0 skipped=35 rescued=0 ignored=0

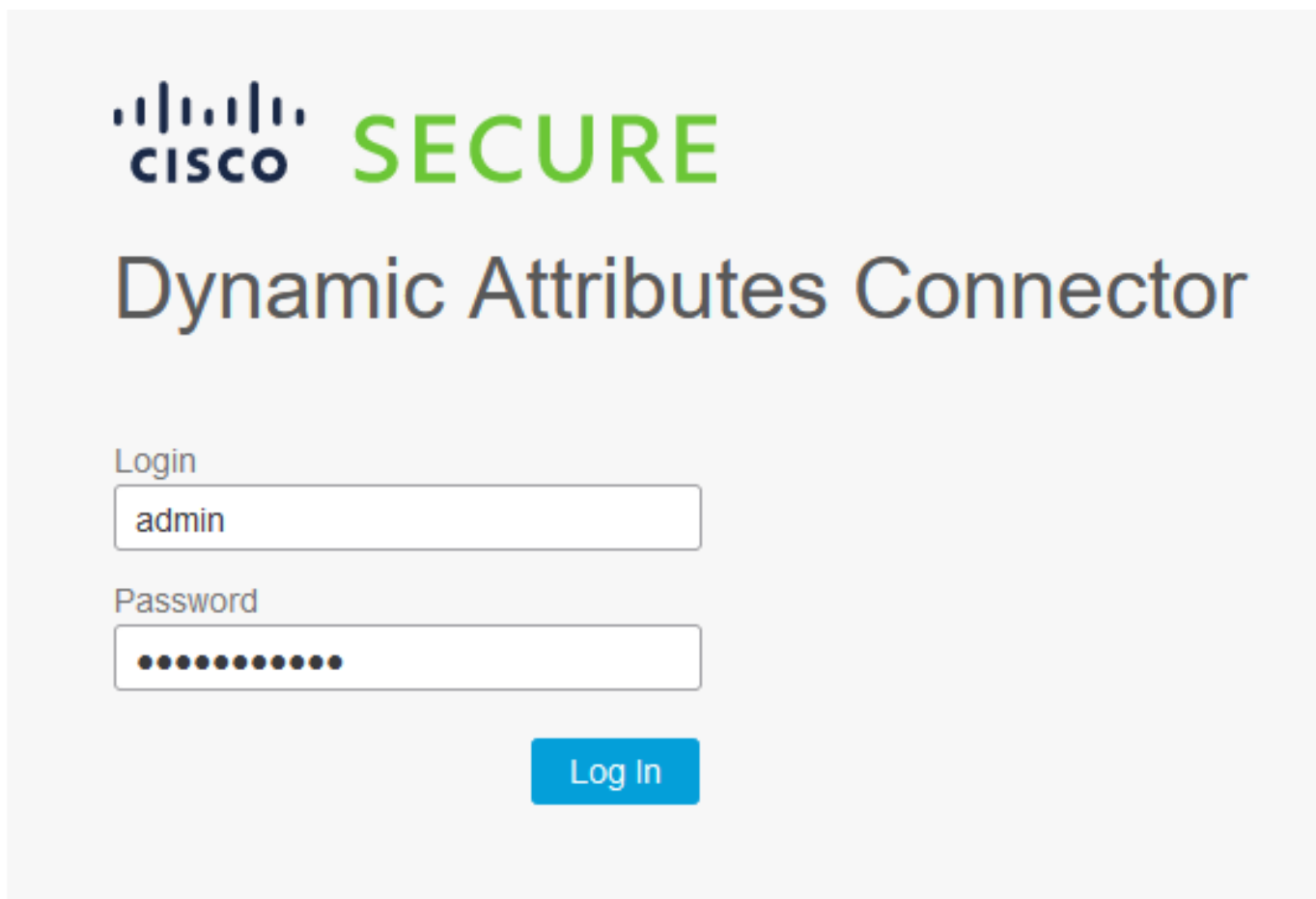


---

Avviso: in caso di errore di installazione causato da 'Autorizzazioni negate con il socket del daemon del Docker', prendere in considerazione l'ID bug Cisco [CSCwh58312](#) o contattare Cisco TAC.


---

Passaggio 10: Accedere al connettore utilizzando l'indirizzo IP CSDAC con il protocollo HTTPS.



The screenshot shows the login interface for the Cisco Secure Dynamic Attributes Connector. At the top left is the Cisco logo, followed by the word "SECURE" in green. Below this is the title "Dynamic Attributes Connector" in a large, dark blue font. The login form consists of two input fields: "Login" with the text "admin" entered, and "Password" with a series of black dots representing a masked password. A blue "Log In" button is positioned below the password field.

---

 Nota: l'accesso iniziale è il nome utente 'admin' e la password 'admin'. Il sistema chiede di cambiare la password dopo il primo login riuscito.

---

## Crea un connettore di Office 365

Passaggio 1: accedere al connettore degli attributi dinamici.





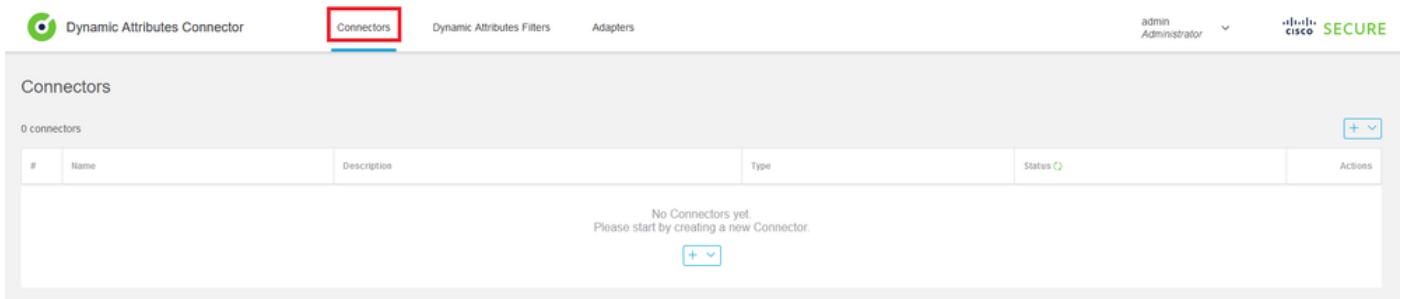
# Dynamic Attributes Connector

Login

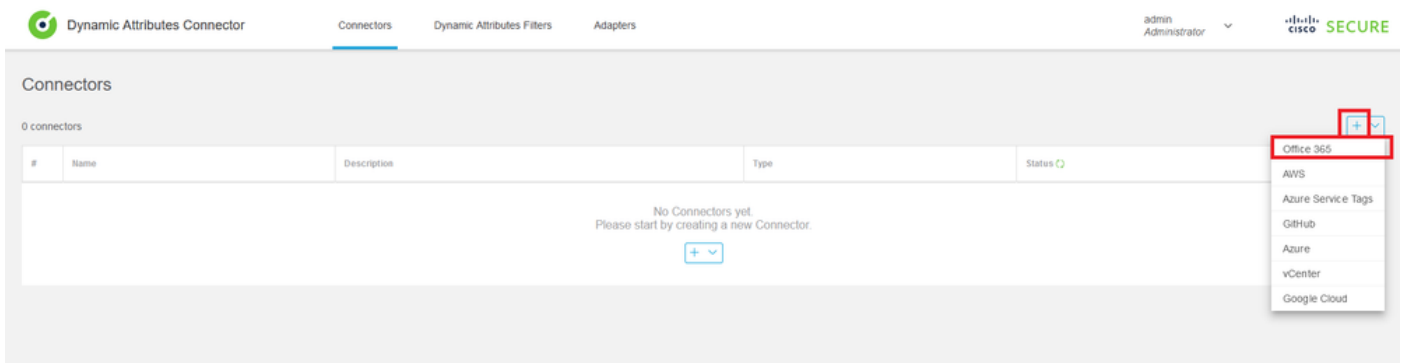
Password

Log In

Passaggio 2: fare clic su 'Connettori'.



Passaggio 3: Aggiungere un connettore di Office 365: fare clic sull'icona Aggiungi (+), quindi su 'Office 365'.



Passaggio 4: configurare il connettore con il nome, l'URL dell'API di base, il nome dell'istanza e

abilitare o disabilitare gli IP facoltativi.

## Add Office 365 Connector

Name\*

Cisco TAC

Description

Pull interval (sec)

30

Base API URL\*

https://endpoints.office.com

Instance name\*

Worldwide

Disable optional IPs\*



Test

Cancel

Save

Consideriamo quanto segue:

- L'intervallo di pull predefinito è 30 secondi.
- L'URL API di base è l'URL per il recupero delle informazioni di Office 365. Consultare [l'indirizzo IP di Office 365 e il servizio Web URL](#) nella Guida alla documentazione di Microsoft.

Passaggio 5: fare clic su 'Test' e verificare che il test abbia esito positivo prima di salvare la configurazione del connettore.

## Add Office 365 Connector

Name\*

Description

Pull interval (sec)

Base API URL\*

Instance name\*

Disable optional IPs\*

Test again

✓ *Test connection succeeded*

Cancel

Save

Passaggio 6: salvare e verificare che lo stato sia 'OK'.

Dynamic Attributes Connector Connectors Dynamic Attributes Filters Adapters admin Administrator Secure CISCO

Connectors

1 connector +

| # | Name      | Description | Type       | Status | Actions |
|---|-----------|-------------|------------|--------|---------|
| 1 | Cisco TAC |             | Office 365 | Ok     |         |

## Crea connettore vCenter

Passaggio 1: accedere al connettore degli attributi dinamici.



# Dynamic Attributes Connector

Login

Password

Log In

Passaggio 2: fare clic su 'Adattatori'.

The screenshot shows the Cisco Secure Dynamic Attributes Connector interface. The navigation menu at the top includes 'Connectors', 'Dynamic Attributes Filters', and 'Adapters', which is highlighted with a red box. The main content area is titled 'Adapters' and shows '0 adapters'. A table with columns for '#', 'Name', 'Description', 'Type', 'Status', and 'Actions' is present. Below the table, a message states: 'No Adapters yet. Please start by creating a new Adapter.' with a '+ v' button.

Passaggio 3: Aggiungere una nuova scheda: fare clic sull'icona Aggiungi (+), quindi su 'Centro gestione firewall locale'.

The screenshot shows the same interface as in the previous step, but with the '+ v' button in the top right corner of the table area highlighted with a red box. A dropdown menu is open, showing two options: 'On-Prem Firewall Management Center' and 'Cloud-Delivered Firewall Management Center'. The first option is selected and highlighted with a red box.

Passaggio 4: configurare la scheda con nome, indirizzo IP, porta e utente/password.


## Add On-Prem Firewall Management Center Adapter

|                     |   |
|---------------------|---|
| Name*               | <input type="text" value="Cisco TAC On-Prem FMC"/>  |
| Description         | <input type="text"/>                                |
| Domain              | <input type="text"/>                                |
| IP*                 | <input type="text" value="firepower.ciscotac.com"/> |
| Port*               | <input type="text" value="443"/>                    |
| User*               | <input type="text" value="TAC"/>                    |
| Password*           | <input type="password" value="●●●●●●●●"/>           |
| Secondary IP        | <input type="text"/>                                |
| Secondary Port      | <input type="text"/>                                |
| Secondary User      | <input type="text"/>                                |
| Secondary Password  | <input type="password"/>                            |
| Server Certificate* | <input type="text"/>                                |
|                     | <input type="button" value="Get certificate"/>      |


Test

Cancel

Save

 **Avviso:** creare un nuovo utente FMC nell'interfaccia utente dedicata alla connessione della scheda. L'utilizzo di un utente esistente potrebbe creare disconnessioni impreviste nell'interfaccia utente di CSDAC o di Centro gestione firewall locale.

---

 Nota: la configurazione del ruolo utente deve avere i ruoli 'Amministratore', 'Amministratore accesso' o 'Amministratore rete'. Utilizzare il nome di dominio completo (FQDN) di Centro gestione firewall locale nel campo dell'indirizzo IP.

---

Passaggio 5: aprire l'interfaccia utente di Centro gestione protetta firewall locale.



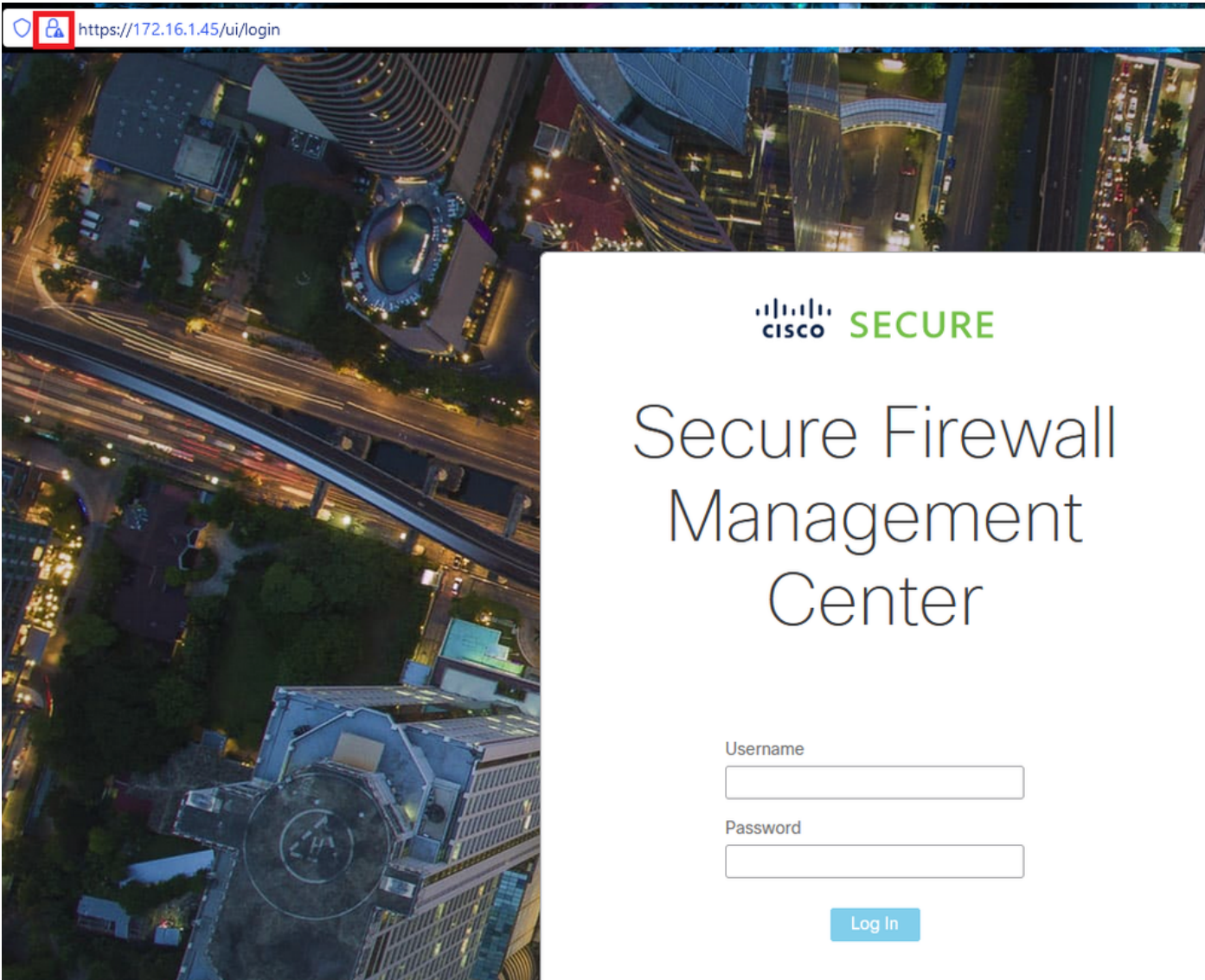
# Secure Firewall Management Center

Username

Password


Log In

Passaggio 6: Scaricare il certificato HTTPS PEM (concatenamento) dal browser: fare clic sul lucchetto HTTPS mostrato nel browser, Secure Connection, More Information, View Certificate, PEM (concatenamento).



| Miscellaneous       |  |
|---------------------|--|
| Serial Number       | 7 7C0E170000F3E6C000D97A0A2E00701C081E02E0             |
| Signature Algorithm | SHA-256 with RSA Encryption                            |
| Version             | 1  |
| Download            | <a href="#">PEM (cert)</a> <a href="#">PEM (chain)</a> |

In questo modo viene scaricato un file con estensione pem con la catena di certificati.

 Nota: la procedura per la raccolta del certificato HTTPS locale Secure Firewall Management Center appartiene al browser Firefox. Se si utilizza un altro browser, eseguire una procedura simile.

Passaggio 7: aprire il connettore degli attributi dinamici e fare clic su 'Ottieni certificato' e 'Sfoglia da file...!'

## Add On-Prem Firewall Management Center Adapter

|                     |   |
|---------------------|---|
| Name*               | <input type="text" value="Cisco TAC On-Prem FMC"/>  |
| Description         | <input type="text"/>                                |
| Domain              | <input type="text"/>                                |
| IP*                 | <input type="text" value="firepower.ciscotac.com"/> |
| Port*               | <input type="text" value="443"/>                    |
| User*               | <input type="text" value="TAC"/>                    |
| Password*           | <input type="password" value="●●●●●●●●"/>           |
| Secondary IP        | <input type="text"/>                                |
| Secondary Port      | <input type="text" value="443"/>                    |
| Secondary User      | <input type="text"/>                                |
| Secondary Password  | <input type="password"/>                            |
| Server Certificate* | <input type="text"/>                                |

Get certificate ▾

Fetch ⓘ

Browse from file... ⓘ

Passaggio 8: caricare il certificato .pem e fare clic su 'TEST' per verificare che il test abbia esito positivo.



## Add On-Prem Firewall Management Center Adapter

Name\*

Cisco TAC On-Prem FMC

Description

Domain

IP\*

firepower.ciscotac.com

Port\*

443

User\*

TAC

Password\*

●●●●●●●●●●

Secondary IP

Secondary Port

443

Secondary User

Secondary Password

Server Certificate\*

```
-----BEGIN CERTIFICATE-----  
MIID6TCCAIECFHHN4bDI8+DNjdWoruZkj8mB5p4JMA0GC  
SqGSib3DQEBCwUAMIGw
```

Get certificate ▾


✓ Updated

Test again

✓ Test connection succeeded

Cancel

Save

 **Avviso:** verificare che i server DNS configurati nel computer Ubuntu siano in grado di risolvere l'FQDN di Centro gestione firewall locale. In caso contrario, il test potrebbe non riuscire.

Passaggio 9: salvare e verificare che lo stato sia 'OK'.

Dynamic Attributes Connector

Connectors Dynamic Attributes Filters Adapters

admin Administrator

CISCO SECURE

Adapters

1 adapter

| # | Name                  | Description | Type                               | Status | Actions |
|---|-----------------------|-------------|------------------------------------|--------|---------|
| 1 | Cisco TAC On-Prem FMC |             | On-Prem Firewall Management Center | OK     |         |

Nota: non è possibile creare filtri degli attributi dinamici per Office 365.

Passaggio 10: iniziare a creare le regole dei criteri di controllo di accesso con gli attributi dinamici di Office 365 nell'interfaccia utente di Centro gestione firewall locale.

Add Rule

Name   Enabled Insert into Mandatory

Action Allow Time Range None

Zones Networks VLAN Tags Users Applications Ports URLs **Dynamic Attributes** Inspection Logging Comments

Available Attributes  +

Search by name or value

Dynamic Objects

o365\_Worldwide\_Common

o365\_Worldwide\_Exchange

o365\_Worldwide\_SharePoint

o365\_Worldwide\_Skype

Add to Source

Add to Destination

Selected Source Attributes (0)

any

Selected Destination Attributes (0)

any

Attributes of the same type (for example, SGT) match the rule if any attribute is matched.  
Attributes of different types match the rule only if all attributes are matched. [More info](#)

Cancel Add

## Verifica

Verificare lo stato del contenitore su Ubuntu per i servizi di base, i connettori e le schede di rete.

```
root@tac://# docker ps -a
```

| CONTAINER ID | IMAGE  | COMMAND                 | CREATED    |
|--------------|--|-------------------------|------------|
| 44f71f675ff1 | public.ecr.aws/e6e4t5f5/muster_fmc_adapter:2.2.0-latest    | "/docker-entrypoint..." | 12 hours   |
| 88826cf0742f | public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest | "/docker-entrypoint..." | 13 hours   |
| 4c2c73d351e2 | public.ecr.aws/e6e4t5f5/muster_envoy:2.2.0-latest          | "/docker-entrypoint..." | 2 days ago |
| 67f3afae2165 | public.ecr.aws/e6e4t5f5/muster_ui:2.2.0-latest             | "/docker-entrypoint..." | 2 days ago |
| 722a764c54e9 | public.ecr.aws/e6e4t5f5/muster_ui_backend:2.2.0-latest     | "/docker-entrypoint..." | 2 days ago |
| 03865454f30  | public.ecr.aws/e6e4t5f5/muster_bee:2.2.0-latest            | "/bin/sh -c /app/bee"   | 2 days ago |
| 90cfd7e3a28b | public.ecr.aws/e6e4t5f5/muster_etcd:2.2.0-latest           | "etcd"                  | 2 days ago |

Verificare lo stato del connettore dall'interfaccia utente CSDAC.

The screenshot shows the 'Connectors' page in the CSDAC interface. At the top, there are navigation tabs for 'Connectors', 'Dynamic Attributes Filters', and 'Adapters'. The user is logged in as 'admin Administrator'. Below the header, there is a table with the following data:

| # | Name      | Description | Type       | Status | Actions |
|---|-----------|-------------|------------|--------|---------|
| 1 | Cisco TAC |             | Office 365 | OK     |         |

Verificare lo stato della scheda dall'interfaccia utente CSDAC.

The screenshot shows the 'Adapters' page in the CSDAC interface. At the top, there are navigation tabs for 'Connectors', 'Dynamic Attributes Filters', and 'Adapters'. The user is logged in as 'admin Administrator'. Below the header, there is a table with the following data:

| # | Name                  | Description | Type                               | Status | Actions |
|---|-----------------------|-------------|------------------------------------|--------|---------|
| 1 | Cisco TAC On-Prem FMC |             | On-Prem Firewall Management Center | OK     |         |

Verificare gli attributi dinamici di Office 365 in Centro gestione firewall.

Creare o modificare una regola dei criteri di controllo d'accesso, fare clic su 'Attributi dinamici', su 'Attributi disponibili' e selezionare 'Oggetti dinamici'.


The screenshot shows the 'Add Rule' configuration page in the CSDAC interface. The 'Dynamic Attributes' tab is selected. The configuration includes:

- Name: [Empty field]
- Enabled:
- Insert: into Mandatory
- Action: Allow
- Time Range: None

Below the configuration, there are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes', 'Inspection', 'Logging', and 'Comments'. The 'Dynamic Attributes' tab is active, showing:

- Available Attributes: A list with a search bar and a dropdown menu. The dropdown is open, showing 'Dynamic Objects' selected. Below it are 'o365\_Worldwide\_Common', 'o365\_Worldwide\_Exchange', 'o365\_Worldwide\_SharePoint', and 'o365\_Worldwide\_Skype'. This list is highlighted with a red box.
- Selected Source Attributes (0): any
- Selected Destination Attributes (0): any

At the bottom right, there are 'Cancel' and 'Add' buttons.

 Nota: se gli oggetti dinamici di Office 365 non sono elencati, l'integrazione potrebbe causare dei problemi. Controllare la sezione risoluzione dei problemi o contattare Cisco TAC.

# Risoluzione dei problemi

In caso di problemi di installazione di Secure Dynamic Attributes Connector con Ansible, raccogliere 'csdac.log' nella directory '~/.ansible/collection/ansible\_collection/cisco/csdac/logs/'.

```
root@tac://# cd ~/.ansible/collections/ansible_collections/cisco/logs/
root@tac:~/.ansible/collections/ansible_collections/cisco/csdac/logs# ls -lth
total 276K
-rw-r--r-- 1 root root 272K sep 14 15:37 csdac.log
```

In questo file sono presenti i log degli errori di installazione. Aprirlo con i comandi Linux 'cat' o 'less', esplorare i log degli errori o contattare Cisco TAC e fornire questo file.

A volte l'installazione Ansible non riesce a causa di autorizzazioni negate. Esplorare il file csdac.log e cercare i registri di autorizzazioni negate.

```
TASK [cisco.csdac.csdac : print result of csdac command line start command (stderr)] ***
ok: [localhost] => {
  "muster_cli_start_result.stderr_lines": [
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: ",
    "docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docke",
    "See 'docker run --help'.",
    "docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docke"
```

Se vengono trovati log simili, prendere in considerazione l'ID bug Cisco [CSCwh58312](#) o contattare Cisco TAC per assistenza.

Se 'docker ps -a' indica che i contenitori sono inattivi o devono essere riavviati in caso di problemi, i contenitori possono essere riavviati con il comando 'docker restart container-id'.

Esempio: riavvio di Office 365 con ID contenitore '88826cf0742f'.

```
root@tac://# docker ps -a
CONTAINER ID IMAGE COMMAND CREATED
44f71f675ff1 public.ecr.aws/e6e4t5f5/muster_fmc_adapter:2.2.0-latest "/docker-entrypoint..." 12 hour
88826cf0742f public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest "/docker-entrypoint..." 13 hour

root@tac://# docker restart 88826cf0742f
```

```
root@tac://# docker ps -a
CONTAINER ID IMAGE COMMAND CREATED
44f71f675ff1 public.ecr.aws/e6e4t5f5/muster_fmc_adapter:2.2.0-latest "/docker-entrypoint..." 12 hour
88826cf0742f public.ecr.aws/e6e4t5f5/muster_o365_connector:2.2.0-latest "/docker-entrypoint..." 13 hour
```

Verificare la connessione a CSDAC e verificare se gli oggetti sono stati creati nel Centro gestione firewall protetto.

```
> expert
sudoadmin@firepower:~$ sudo su -
Password:

root@firepower:/Volume/home/admin# cat /var/opt/CSC0px/MDC/log/operation/usmsharedsvcs.log
17-Sep-2023 17:24:58.046, [INFO], (DefenseCenterServiceImpl.java:1462)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-2
** REST Request [ CSM ]
** ID : ff3e6259-2417-48cc-8e5e-a41d0bd04b39
** URL: POST /audit
{
  "version":"7.2.5",
  "requestId":"ff3e6259-2417-48cc-8e5e-a41d0bd04b39",
  "data":{
    "userName":"TAC",
    "subsystem":"API",
    "message":"POST https://FMC-FQDN/api/fmc\_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/objct/bulldynamicobjects Created (201) - The request has been fulfilled and resulted in a new reso
    "sourceIP":"172.16.1.53",
    "domainUuid":"e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time":"1694971497660"}, "deleteList":[]
  }
}
```

## Informazioni correlate

Ulteriori documenti relativi a Cisco Secure Dynamic Attributes (CSDAC) sono disponibili qui:

Informazioni su Cisco Dynamic Attributes Connector

[https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/m\\_about-the-cisco-dynamic-attributes-connector\\_21.html](https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/m_about-the-cisco-dynamic-attributes-connector_21.html)

Installare e aggiornare Cisco Secure Dynamic Attributes Connector

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/install-the-cisco-secure-dynamic-attributes-connector.html>

Configurazione di Cisco Dynamic Attributes Connector

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/configure-the-cisco-secure-dynamic-attributes-collector.html>

Usa oggetti dinamici nei criteri di controllo di accesso

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/use-dynamic-objects-in-access-control-rules.html>

Risoluzione dei problemi relativi al connettore degli attributi dinamici

<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/220/cisco-secure-dynamic-attributes-connector-v220/troubleshoot-the-dynamic-attributes-connector.html>

Installazione di CSDAC 2.2 non riuscita: "Autorizzazione negata con socket daemon Docker" in Ubuntu 20.04.

ID bug Cisco [CSCwh58312](#).

## Informazioni su questa traduzione

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