

Configurazione di SD-AVC su SD-WAN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Introduzione](#)

[Cos'è SD-AVC?](#)

[Cos'è Cisco Cloud Connector?](#)

[Configurazione](#)

[Abilita Cloud Connector](#)

[Abilita SD-AVC su vManage](#)

[Abilita SD-AVC Cloud Connector su vManage](#)

[Abilita connettore cloud SD-AVC, versione precedente alla 20.10](#)

[Abilita SD-AVC Cloud Connector, tramite 20.13](#)

[EnableSD-AVC Cloud Connector, 20.14 e versioni successive](#)

[Configurazione criteri](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare Software Defined-Application Visibility and Control (SD-AVC) su una rete WAN SD (Software-Defined Wide Area Network).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN
- SD-AVC

La macchina virtuale di Cisco vManage deve disporre delle seguenti risorse minime:

- RAM: 32 GB
- Storage: 500 GB
- vCPU:16

Componenti usati

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

- Cisco vManage versione 20.3.x o successive.
- vManage versione 20.6.3
- vBond versione 20.6.3
- vSmart versione 20.6.3
- ISR (Integrated Service Router) 4321/K9 versione 17.5.1a

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.

Introduzione

Cos'è SD-AVC?

Cisco SD-AVC è un componente di Cisco Application Visibility Control (AVC). AVC integra nei dispositivi di routing le funzionalità di riconoscimento delle applicazioni e di monitoraggio delle prestazioni tradizionalmente disponibili come appliance dedicate. Funziona come un servizio di rete centralizzato e funziona con dispositivi specifici nella rete.

Per maggiori informazioni, vedere [Caratteristiche e vantaggi di SD-AVC](#).

Cos'è Cisco Cloud Connector?

Cisco Cloud Connector è un servizio Cloud fornito da Cisco che migliora la classificazione del traffico. Vengono utilizzate le informazioni più aggiornate disponibili sull'indirizzo del server utilizzato dai siti Internet e dai servizi pubblici per migliorare la classificazione del traffico SD-AVC.

Configurazione

Abilita Cloud Connector

1. Aprire [Cisco API Console](#) e fare clic su **My Apps & Keys**.



Nota: il dispositivo ospitato dalla rete SD-AVC richiede l'accesso ai domini del server cloud Cisco SD-AVC: **api.cisco.com**, **cloudsso.cisco.com**, **prod.sdavc-cloud-api.com**.

2. Fare clic **Register a New App** come mostrato nell'immagine.

My Apps & Keys

Applications Keys Register a New App

3. Nel **Name of your application** campo, inserire un nome descrittivo per l'applicazione.
4. Selezionare la **Client Credentials** casella di controllo.
5. Selezionare la **Hello API** casella.
6. Selezionare la casella di controllo per accettare le condizioni per l'utilizzo del servizio.
7. Fare clic su Register. La pagina Cisco API Console visualizza i dettagli dell'ID e del segreto client. Tenere aperta questa pagina per completare la procedura, come mostrato nell'immagine.

My Apps & Keys

Applications Keys Register a New App

SDWAN_SDAVC_Test

Registered: 8/10/22 5:21 pm Grant Type: Client Credentials

API	KEY	CLIENT SECRET	STATUS
Hello API	ttg	aUW	active

[Edit This App](#) [Delete This App](#) [Add APIs](#)

Abilita SD-AVC su vManage


1. Passare a **Administration > Cluster Management > Service Configuration**. Fate clic su (...) **More Actions** e scegliete **Edit**.

Cisco vManage Administration - Cluster Management

Service Configuration Service Reachability

⊕ Add vManage

Hostname	IP Address	Configure Status	Node Persona	UUID	
vmanage	172.12.1.4	Ready	COMPUTE_AND_DATA		*** Device Connected Edit Remove

 Nota: non utilizzare un tunnel/trasporto VPN 0 o un'interfaccia VPN 512 per abilitare SD-AVC. È possibile utilizzare l'interfaccia cluster nella vpn 0.

2. Nella sezione Indirizzo IP vManage, fare clic sull'indirizzo IP. Selezionare un indirizzo IP non tunnel nella VPN 0. Immettere le credenziali, selezionare la **Enabled SD-AVC** casella di controllo e fare clic su Update, come mostrato nell'immagine.

Node Persona ⓘ

Compute + Data
 (Up to 5 nodes each)

Compute
 (Up to 5 nodes)

Data
 (Up to 10s of nodes)

vManage IP Address

172.12.1.4

Username

admin


Password

••••••••

Enable SD-AVC

Cancel **Update**

3. Una volta confermato l'aggiornamento, fare clic su OK per riavviare il dispositivo come mostrato nell'immagine.

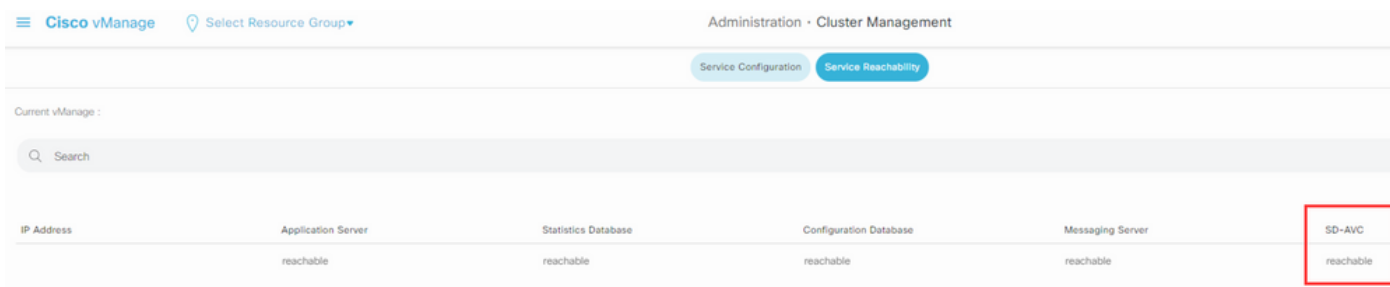
 **In order to apply these changes the device will need to be rebooted.**

Do you want to make these changes?

OK

Cancel

4. Dopo il riavvio di vManage, passare a Administration > Cluster Management > Service Reachability. Viene visualizzato SD-AVC Reachable.



The screenshot shows the Cisco vManage interface. At the top, there is a navigation bar with 'Cisco vManage' and 'Select Resource Group'. Below that, the breadcrumb 'Administration > Cluster Management' is visible. Two tabs are present: 'Service Configuration' and 'Service Reachability', with the latter being active. A search bar is located below the tabs. The main content area displays a table with the following columns: IP Address, Application Server, Statistics Database, Configuration Database, Messaging Server, and SD-AVC. The 'SD-AVC' column shows the status 'reachable' for the selected resource group.

IP Address	Application Server	Statistics Database	Configuration Database	Messaging Server	SD-AVC
	reachable	reachable	reachable	reachable	reachable

Abilita SD-AVC Cloud Connector su vManage

Abilita connettore cloud SD-AVC, versione precedente alla 20.10

1. Nella sezione GUI di vManage, spostarsi su Administration > Settings > SD-AVC Cloud Connector e fare clic su **Edit**.
2. Per SD-AVC Cloud Connector, fare clic sul pulsante di opzione Enabled. Immettere i valori in questi campi generati nella sezione Abilita connettore cloud, come mostrato nell'immagine.

- ID client
- Segreto client
- Nome organizzazione
- Affinità
- Telemetria (opzionale)

SD-AVC Cloud Connector Enabled

SD-AVC Cloud Connector Enabled Disabled

Client ID

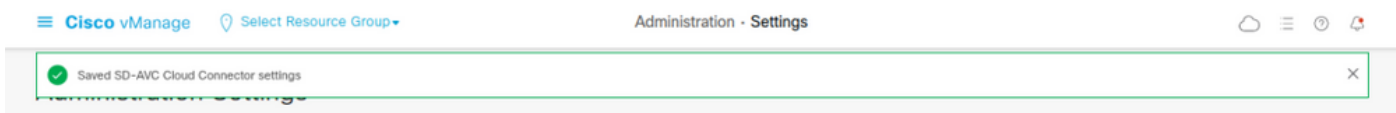
Client Secret

Organization Name

Affinity

Telemetry Disabled

3. Fare clic Save su e verificare la notifica come mostrato nell'immagine.



Abilita SD-AVC Cloud Connector, tramite 20.13

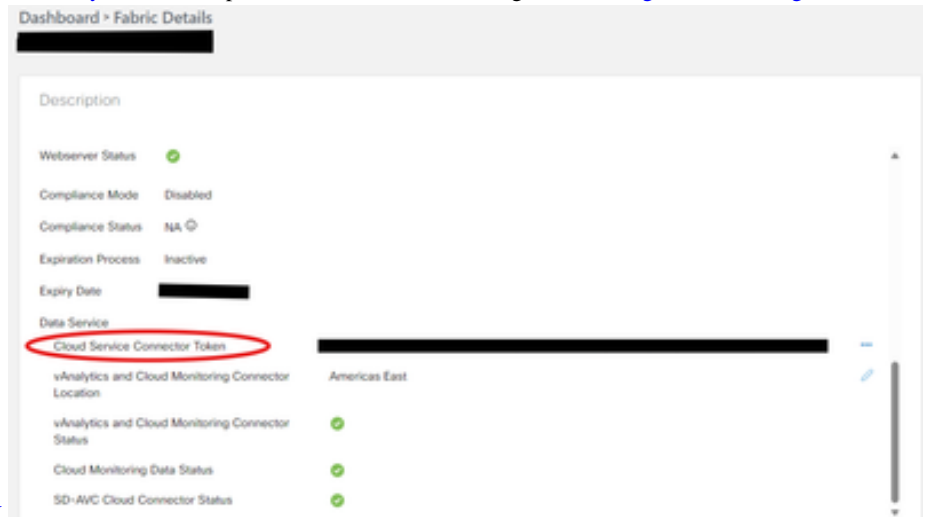
A partire dalla versione 20.10.1, l'abilitazione del connettore cloud richiede un URL del gateway cloud e una password temporanea (OTP) anziché un ID client e un segreto client.

Nelle nuove installazioni su host Cisco della versione 20.10.1 o successive, Cloud Connector è abilitato per impostazione predefinita e non è necessario immettere le credenziali.

1. Nella sezione GUI di vManage, spostarsi su Administration > Settings > SD-AVC e fare clic su **Edit**.
2. Per Cloud Connector, fare clic sul pulsante di opzione Enabled. Immettere i valori in questi campi generati nella sezione Abilita connettore cloud, come mostrato nell'immagine.

- OTP

- Cloud-hosted: usare il [portale Cisco Catalyst SD-WAN](#) per ottenere l'OTP. Per i dettagli, vedere la [guida alla configurazione del](#)



[portale Cisco Catalyst SD-WAN](#).

- In locale: apri una richiesta Cisco TAC per OTP

- URL gateway cloud

Utilizzare https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/

SD-AVC

Cloud Connector

Enabled Disabled

OTP

Cloud Gateway URL

Telemetry Disabled

Save

Cancel

3. Fare clic su Save e verificare che le impostazioni di conferma della notifica siano state applicate.

EnableSD-AVC Cloud Connector, 20.14 e versioni successive

20.14.1 introduce una nuova procedura per abilitare Cisco SD-AVC Cloud Connector dall'opzione Servizi cloud in Amministrazione > Impostazioni. Da questa release, l'abilitazione di Cloud Connector non richiede OTP né l'apertura di una richiesta TAC.

1. Nella sezione GUI di vManage, passare a Administration > Settings > Cloud Services. Confirm Cloud Services are enabled.

2. Per Cloud Connector, fare clic sul pulsante di opzioneEnabled.

Cloud Services

Cloud Services [Terms & Conditions](#)

Cisco Catalyst SD-WAN Analytics. By enabling Cisco Catalyst SD-WAN Analytics you agree to the following:

1. If you are a Cisco channel partner or reseller provisioning the Catalyst SD-WAN Analytics service on behalf of an end customer, you warrant that you have permission from the end customer for Cisco to process their data in accordance with the referenced links above.
2. All Cisco devices connecting to the Cisco Catalyst SD-WAN fabric with Catalyst SD-WAN Analytics enabled must have Cisco DNA Advantage licenses.
3. Catalyst SD-WAN Analytics is currently not available for end customers located in mainland China, Hong Kong or Macau. Therefore, you warrant that the end customer using the Catalyst SD-WAN Analytics service is not headquartered or mainly based in mainland China, Hong Kong, or Macau, and you shall ensure that end customers located in such jurisdictions do not use Catalyst SD-WAN Analytics.

Cloud Services

Analytics ⓘ

SD-AVC Cloud Connector

Telemetry

Save

Cancel

3. Fare clic su Save e verificare che le impostazioni di conferma della notifica siano state applicate.

Configurazione criteri

Dopo aver abilitato SD-AVC, è necessario creare un criterio localizzato e abilitare la visibilità dell'app.

1. Passare alla GUI vManage e scegliere **Configuration > Policies > Localized Policy > Add Policy**.

2. Passare a **Policy Overview**., Nella Policy Settings sezione, selezionare la **Application** casella di controllo e fare clic su **Save Policy**.

Localized Policy > Add Policy

Create Groups of Interest
 Configure Forwarding Classes/QoS
 Configure Access Control Lists
 Configure Route Policy
 Policy Overview

Enter name and description for your localized master policy

Policy Name:

Policy Description:

Policy Settings

Netflow
 Netflow IPv6
 Application
 Application IPv6
 Cloud QoS
 Cloud QoS Service side
 Implicit ACL Logging

Log Frequency:

FNF IPv4 Max Cache Entries:

FNF IPv6 Max Cache Entries:

[Back](#)
[Preview](#)
[Save Policy](#)
[Cancel](#)

3. Passare a Configuration > Templates. Identificare il nome del modello di Cisco Edge Router, fare clic su (...) More Actions, quindi scegliere Edit come mostrato nell'immagine.

Cisco vManage Select Resource Group

Configuration · Templates

Device Feature

Search

Create Template

Template Type: Non-Default

Total Rows: 5

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
-	-	CLI	vSmart	-	global	0	Disabled	1	-	09 Aug 2022 7:24...	In Sync
-	-	Feature	ASR1001-X	SDWAN Edge	global	13	Disabled	1	-	22 Jun 2022 9:27...	In Sync
-	-	Feature	vEdge Cloud	SDWAN Edge	global	10	Disabled	0	-	29 Jul 2022 9:09...	In Sync
-	-	Feature	ISR 1100 4GLTE* ...	SDWAN Edge	global	10	Disabled	0	-	01 Aug 2022 7:55...	In Sync
ISR4321_Template	ISR4321_Template	Feature	ISR4321	SDWAN Edge	global	11	Disabled	1	admin	18 Aug 2022 8:04...	In Sync

4. Passare a **Additional Templates**. Dall'elenco a **Policy** discesa, scegliere il criterio localizzato creato in precedenza.

sdwan/messaging-server	0.20.0	a46dc94d4993	13 months ago	71.2MB
sdavc	4.1.0	721c572475f9	14 months ago	1.17GB
sdwan/support-tools	latest	0c3a995f455c	15 months ago	16.9MB
sdwan/service-proxy	1.17.0	4e3c155026d8	15 months ago	205MB
sdwan/ratelimit	master	f2f93702ef35	16 months ago	47.6MB

Listing all containers

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS
270601fc94ec	cloudagent-v2:fb3fc5c0841	"python ./main.py"	6 weeks ago	Up 6
53bba5216b24	sdwan/ratelimit:master	"/usr/local/bin/rate..."	6 weeks ago	Up 6
59bf900edf14	sdwan/service-proxy:1.17.0	"/entrypoint.sh /run..."	6 weeks ago	Up 6
62defa38c798	sdwan/messaging-server:0.20.0	"/entrypoint.sh /mes..."	6 weeks ago	Up 6
3fbf32dd8d73	sdwan/coordination-server:3.6.2	"/docker-entrypoint..."	6 weeks ago	Up 6
c2e7b672774c	sdwan/configuration-db:4.1.7	"/sbin/tini -g -- /d..."	6 weeks ago	Up 6
f42ac9b8ab37	sdwan/statistics-db:6.8.10	"/bin/tini -- /usr/l..."	6 weeks ago	Up 1
112f3d9b578b	sdavc:4.1.0	"/usr/local/bin/scr..."	7 weeks ago	Up 7
06b09f3b030c	sdwan/host-agent:1.0.1	"python ./main.py --..."	7 weeks ago	Up 7
3484957576ee	sdwan/cluster-oracle:1.0.1	"/entrypoint.sh java..."	7 weeks ago	Up 7

Docker info

Client:

Debug Mode: false

Server:

Containers: 10

Running: 10

Paused: 0

Stopped: 0

Images: 11

Server Version: 19.03.12

Storage Driver: aufs

Root Dir: /var/lib/nms/docker/aufs

Backing Filesystem: extfs

Dirs: 149

Dirperm1 Supported: true

Logging Driver: json-file

Cgroup Driver: cgroupfs

Plugins:

Volume: local

Network: bridge host ipvlan macvlan null overlay

Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog

Swarm: inactive

Runtimes: runc

Default Runtime: runc

Init Binary: docker-init

containerd version: fd103cb716352c7e19768e4fed057f71d68902a0.m

runc version: 425e105d5a03fabd737a126ad93d62a9eeede87f-dirty

init version: fec3683-dirty (expected: fec3683b971d9)

Kernel Version: 4.9.57-ltsi

Operating System: Linux

OSType: linux

Architecture: x86_64

CPUs: 16

Total Memory: 30.46GiB

Name: vManage

ID: XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXXX

Docker Root Dir: /var/lib/nms/docker

Debug Mode: false

Registry: https://index.docker.io/v1/

Labels:

Experimental: false

Insecure Registries:

127.0.0.0/8

Live Restore Enabled: false

WARNING: No cpu cfs quota support

WARNING: No cpu cfs period support

WARNING: bridge-nf-call-iptables is disabled

WARNING: bridge-nf-call-ip6tables is disabled

WARNING: the aufs storage-driver is deprecated, and will be removed in a future release.

Nella versione 20.10 è presente una modifica del comportamento nell'output di 'request nms all status':

Quando si utilizzano i componenti di controllo SD-WAN di Cisco Catalyst versione 20.10.x o successive, in un'installazione ospitata da Cisco di Cisco Catalyst SD-WAN, i componenti SD-AVC funzionano in modo diverso rispetto alle versioni precedenti. Di conseguenza, se si esegue il comando `request nms all status` sull'istanza Cisco Catalyst SD-WAN, il componente "server SDAVC NMS" non è abilitato. Questo è il comportamento previsto e non indica alcun problema con SD-AVC. Si noti che il componente "gateway SDAVC NMS" viene visualizzato come attivato.

```
NMS SDAVC server Enabled: false Status: not running NMS SDAVC gateway Enabled: true Status: running PID
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Nei registri vManage verificare i percorsi seguenti:

```
/var/log/nms/vmanage-server.log
```

```
/var/log/nms/containers/sdavic/avc/sdavic_application.log
```

Immettere questo comando:

```
<#root>
```

```
request nms container-manager
```

```
{
```

```
status
```

```
|
```

```
diagnostics
```

```
}
```

In Cisco Edge Cisco IOS® XE, immettere i seguenti comandi:

```
<#root>
```

```
Router#
```

```
show avc sd-service info connectivity
```

```
show avc sd-service info
```

```
{  
export  
|  
import  
}
```

Informazioni correlate

[Guida introduttiva a Cisco Catalyst SD-WAN - Installazione hardware e software](#)

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).