Installazione del connettore Cisco Secure Endpoint Linux

Sommario

Introduzione Prerequisiti Requisiti Componenti usati RHEL/CentOS/Amazon Linux 2/SUSE 15 Configurazioni Come importare il tasto GPG Ubuntu Configurazioni Come importare il tasto GPG Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento descrive come installare e verificare il connettore Cisco Secure Endpoint Linux per i sistemi basati su Red Hat Enterprise Linux (RHEL) e Debian.

Contributo di Juan Carlos Castillero e curato da Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

Computer Linux su un sistema operativo supportato da un connettore Linux

Componenti usati

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

- Un programma di installazione del connettore Linux dell'endpoint sicuro Red Hat Package Manager (RPM)
- Un programma di installazione per il connettore Linux dell'endpoint sicuro Debian Package Manager (dpkg)

- Una chiave GNU Privacy Guard (GPG) per verificare gli aggiornamenti (opzionale)
- Un programma di installazione del connettore Linux DPKG (Debian Package Management System)

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.

RHEL/CentOS/Amazon Linux 2/SUSE 15

Configurazioni

Passaggio 1. Scaricare il pacchetto Linux RPM dal Cisco Secure Endpoint Portal, come mostrato nell'immagine.

👌 Linux	Ortal Linux Policy			
	Flash Scan on Install			
	Distribution SUSE Enterprise/Leap 15 \vee			
	Connector V Amazon Linux 2			
Show GPG Public Key	St RHEL/CentOS 6			
	RHEL/CentOS 7			
	RHEL/CentOS 8			
	✓ SUSE Enterprise/Leap 15			
	Ubuntu 20.04			
	Ubuntu 18.04			

Nota: È importante tenere presente che la distribuzione del sistema operativo è importante in quanto entrambi i connettori hanno architetture completamente diverse.

Passaggio 2. Spostare il pacchetto RPM nell'endpoint in questione, scaricarlo direttamente dal dashboard o spostarlo manualmente negli endpoint. In questo esempio viene utilizzata un'interfaccia utente grafica (UI, Graphic User Interface), sebbene sia possibile, e spesso comune, lavorare con un'installazione minima. In questo caso, è necessario sapere come gestire il terminale Linux e trovare il pacchetto RPM.

< > ← ✿ Home	Downloads +	۹	:	= -	٥	×
O Recent	Name			Size	Modif	ied 🔺
	amp_juanc2ProxyGroup_rhel-centos-7.rpm			16.1 MB		17:38
Documents	Connector.rpm			15.7 MB	25 Oct	t 2015
🕹 Downloads	cisco.gpg			1.0 kB	25 Oc	t 2015
də Music						
Pictures						
H Videos						
🗊 Trash						
+ Other Locations						
	"amp_juanc2ProxyGroup_rhe	el-cento	s-7.rp	m" select	ed (16.1	MB)

Passaggio 3. Per installare il connettore Linux, eseguire il comando: **sudo yum localinstall** [pacchetto rpm] -y (o **sudo zypper install -y** [pacchetto rpm] su SUSE 15)

dove [rpm package] è il nome del file, ad esempio "amp_Audit.rpm". È necessario installare il pacchetto RPM durante l'esecuzione del servizio atd.

The Edit View Search Terrino []enutoring/search-line men- model parameter for Jenutian Loaded plogies: Languetke, This system is not register Executing ang junc/drivesystem Marking ang junc/drivesystem Marking therester(jet) 	a ship ta bhanlandt \$ "! aradust-if. samot wa with an artitle ag stal.conton.7.0 a, chai.conton.7.0 rit tar.a88_04 0:1.30 tar.a88_04 0:1.32 alutlas	obs you localing this and local - disabled reges, solid particu- ment percer. You can use balance rgm: clocksappendentice-1.12.7 as an update to clocksappend 2.030-3.017 will be an opdated 2.032-3.017 will be an opdated	ProvyGradu rhvl-contex J.rpw (y) nanoger ription-nanoger ta register. dol-1.el7.dbh 64 ector I.bb.2.400-3.el7.x88_64	
Package	Arch.	WEFELDE	Fegocitory	BLCC
Updating: discomponenter Transaction Summary Upgrade 1 Package	18.54	5.17.7.682-1.el7	/wwp_jumezFrenyGranp_rhel.com(us-7	43.8
Total size: 49 M Downloading packages: Numling transaction theck numming transaction test Transaction test succeeded Aurning transaction Publicy served to /opt/clacs/	ung.entcapelicy.ent	Langeauxe		

Se la GUI è in uso, aprire il terminale, come mostrato nell'immagine.



Una volta avviata l'installazione, non è necessario alcun input da parte dell'utente, ma si tratta di un processo automatico, come mostrato nell'immagine.



Come importare il tasto GPG

La chiave pubblica GPG può essere copiata dalla pagina Download Connector per verificare la firma del pacchetto RPM. Il connettore può essere installato senza il tasto GPG; tuttavia, un utente deve importare la chiave GPG nel database RPM se prevede di eseguire il push degli aggiornamenti del connettore tramite criteri RHEL.

Nota: A partire dalla versione 1.17.0 del connettore, il tasto GPG utilizzato per verificare i pacchetti di aggiornamento durante gli aggiornamenti del connettore viene installato automaticamente.

Passaggio 1. Verificare la chiave GPG, quindi fare clic sul collegamento Chiave pubblica GPG nella pagina Download Connector. Confrontare la chiave con quella su **/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp**.

Derosen Avenue - Out	GPG Public Key	×	Jaan Castillers Det Sac 7 Montes 7
Download Connec	BEEIN PGP PUBLIC KEY BLOCK Version: GnuPS v1.4.12 (DMS/Linix)		
Genue Mark Providence	Approximate a subscription of the second sec	10.0	
No. contrainer retaine age	Jo yi 1 2 2 2 2 3 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4	四寸 おりに 回 つ 四 フ	Varials COX Facts Scient at Italial resolute Variani, 1.12,2.733 Package Parenat: CMIG Reserved: CMIG
§ Linux	b- Jr vxxQ4 END PGP PUBLIC KEY BLOCK	q	Verda Antend Prester Verden: 1.1.2.40
Show OPG Public Key	Duwen	tan	Itom LPL Download

Out	GF	Opening cisco.gpg		×K	
nec	 Ve mQ 7w Lk Jd	You have chosen to open: cisco.gpg which is: PGP/MIME-encrypted message header (1.0 KB) from: https://console.amp.cisco.com			
re upc	yI lx ZU ZW BE eS zI	Open with Text Editor (default) Save File Do this <u>a</u> utomatically for files like this from now on.	~		Flash Scan on onnector Version: Package Format
	bl be JH =Xt	Cancel END PGP PUBLIC KEY BLOCK	OK		• Vanilla Android
ey			Down	nload	Show URL

Passaggio 2. Eseguire il comando da un terminale per importare la chiave: **sudo rpm —import** /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp.

[]enutern@jenuter.lin.ees.lab rpm-gpg[% pwd /ept/cisco/amp/stc/rpm-gpg []enutern@jenuter.lin.mes.lab rpm-monit. []]enutern@composition	Open + A Oktaget Same B - B -
Version: Gendro v2.0.14 (SWE/Linux)	version: 6maP6 v1.4.12 (000/Linux)
T 	0 m 0 y 1 y 1 y 1 y 1 y 1 y 1 y 1 y 1
[]sustorr0]sistorr-lin-mes-lab rpm-ppg]5 []sustorr0]sistorr-lin-mes-lab rpm-ppg]5 []sustorr0]sistorr-lin-mes-lab rpm-ppg]1	Plan Test + Tab Weth 8 + Un 1 Cel 1 + Inc

Passaggio 3. Verificare che la chiave sia stata installata, quindi eseguire il comando dal terminale: rpm -q gpg-pubkey —qf '%{name}-%{version}-%{release} —> %{summary}\n'.

te Edt Vew Search	Terminal Help
etador egistador - 11a an	tar Bowlands(5 ym -g gog pulwy - gf "s(same) s(version) s(version) -> s(samary)/v" █ -> ggflawrafter fireAPF (fireAPF Line Corrector) same-mailer@samarine.com/relpestivn@jenuters.lin man-lah Bowlands(1

Passaggio 4. Cercare nell'output una chiave GPG di Sourcefire. Il programma di aggiornamento

viene eseguito dal daemon di inizializzazione del sistema e, quando è disponibile un aggiornamento, attiva automaticamente il processo di aggiornamento RPM. Alcune configurazioni SELinux vietano questo comportamento e causano il fallimento dell'Updater.

Se si sospetta che questo sia il caso, esaminare il registro di controllo del sistema (ad esempio, /var/log/audit/audit.log) e cercare gli eventi di rifiuto correlati a ampupdater. Potrebbe essere necessario regolare le regole SELinux per consentire il funzionamento di Updater.

Ubuntu

Configurazioni

Passaggio 1. Scaricare il pacchetto Linux DEB da Cisco Secure Endpoint Portal, come mostrato nell'immagine.

 ✓ Flash Scan on Install Distribution RHEL/CentOS 6 √ Connector V ✓ RHEL/CentOS 6 Show GPG Public Key Show URI RHEL/CentOS 7 RHEL/CentOS 8 Ubuntu 20.04 	👌 Linux	rkubik Linux Policy		
Distribution RHEL/CentOS 6 ∨ Connector V ✔ RHEL/CentOS 6 Show GPG Public Key Show URL RHEL/CentOS 7 RHEL/CentOS 8 Ubuntu 20.04		🧭 Flash Scan on Install		
Connector V < RHEL/CentOS 6 Show GPG Public Key Show URL RHEL/CentOS 7 RHEL/CentOS 8 Ubuntu 20.04		Distribution RHEL/CentOS 6 \checkmark		
Show GPG Public Key Show URL RHEL/CentOS 7 RHEL/CentOS 8 Ubuntu 20.04		Connector V < RHEL/CentOS 6		
RHEL/CentOS 8	Show GPG Public Key	Show URL RHEL/CentOS 7		
Ubuntu 20.04		RHEL/CentOS 8		
		Ubuntu 20.04		
Amazon Linux 2		Amazon Linux 2		

Passaggio 2. Spostare il pacchetto DEB sull'endpoint in questione, scaricarlo direttamente dal dashboard o spostarlo manualmente sugli endpoint. In questo esempio viene utilizzata un'interfaccia utente grafica (UI, Graphic User Interface), anche se è possibile, e spesso comune, lavorare con un'installazione minima. In questo caso, è necessario sapere come gestire il terminale Linux e trovare il pacchetto DEB.

< > Ĝi Home	Downloads 👻	Q	-	≡ _ ⊂	
() Recent	Name		Size	 Modified 	Star
★ Starred	amp_rkubik_Group_beta-ubuntu-20-04.deb		32.9 MB	13:25	☆
습 Home					
🖸 Desktop					
🗊 Documents					
🗄 Downloads					
♫ Music					
Pictures					
🖯 Videos					
💼 Trash					
☐ Share					

Passaggio 3. Per installare il connettore Linux, eseguire il comando: **sudo dpkg -i [pacchetto deb]** dove [pacchetto deb] è il nome del file, ad esempio "amp_Audit.deb". Una volta avviata l'installazione, non è necessario alcun input da parte dell'utente, ma si tratta di un processo automatico, come mostrato nell'immagine.

/bin/bash	-	8
/bin/bash 80x24		
Now using version go1.11.13 13:27:33 cisco~ \$ cd Downloads/ 13:27:53 cisco~/Downloads \$ sudo dpkg -i amp_rkubik_Group_beta-ubuntu-20-04.deb Selecting previously unselected package ciscoampconnector. (Reading database 252023 files and directories currently installed. Preparing to unpack amp_rkubik_Group_beta-ubuntu-20-04.deb Unpacking ciscoampconnector (1.15.999.9999-1) Setting up ciscoampconnector (1.15.999.9999-1) Verifying archive integrity 100% All good.)	
Uncompressing ampconnector installer 100% Processing triggers for libc-bin (2.31-Oubuntu9.1) Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) 13:28:02 cisco~/Downloads \$ ■		

Come importare il tasto GPG

La chiave pubblica GPG può essere copiata dalla pagina Download Connector per verificare la firma del pacchetto DEB. Il connettore può essere installato senza il tasto GPG; tuttavia, un utente dovrebbe importare la chiave GPG nel suo keyring debsig se ha intenzione di spingere gli aggiornamenti del connettore tramite la policy su Ubuntu. Per ulteriori informazioni su come importare il tasto GPG e verificare che il connettore non sia stato modificato su Ubuntu, vedere <u>https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/216524-amp-for-endpoints-ubuntu-connector.html#anc6</u>

Nota: A partire dalla versione 1.17.0 del connettore, il tasto GPG utilizzato per verificare i pacchetti di aggiornamento durante gli aggiornamenti del connettore viene installato automaticamente. Per verificare questa chiave GPG, fare clic sul collegamento Chiave pubblica GPG nella pagina Download Connector e confrontarla con la chiave installata in /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-Key-cisco-amp.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare il corretto completamento dell'installazione, eseguire AMP CLI. L'interfaccia della riga di comando del connettore Linux è disponibile in /opt/cisco/amp/bin/ampcli. Può essere eseguito in modalità interattiva oppure eseguire un unico comando e uscire. Eseguire il comando ./ampcli — per visualizzare un elenco completo delle opzioni e dei comandi disponibili. Tutti i file di registro generati dal connettore si trovano in /var/log/cisco.

File Edit Vie Lipsonterrelipsoon rept/classrompeout amptilis anno Lipsonterrelipsoon Tipesonterrelipsoon	ver Search Ternmenal. Help ser-lin-man-lab birls por ter lin-man-lab birls por ter lin-man-lab birls 16 september i septemperter itera-angehelper long-annunch in Stateline 100001.co.0.2.0 ser-lin-man-lab birls i rempetter ser-lin-man-lab birls (rempetter
ampeliz - AMP for Interactive mod	r Endpeints Connector Command Line Interface M
Bitter 191 or Ct	risc to fait
Illegger] Set au Trying to come Connected. Amplia status Scatu: Model Scan Last Scan: Prilics Common Lines Fasits Common Lines Fasits	nimum reported tog level to notice ct Connected Nameda Nameda for scan Noterie Linux (F112001 Kondbal Name

Sulla console Cisco Secure viene visualizzato anche un evento di installazione. Se sono state richieste scansioni flash durante il download del pacchetto RPM, verranno visualizzate anche queste.

T instantional	And and Deserved THE Proj. I printed	en harte	Q to the	
Conceptor Mar	(targater	Transferration and the second second		~
Comments	Committee 2018	¥.		
	durant law	(harman		
	Cither Burn		P	Dense Property Conceptency
* instructional	terrait safet see-		Q. the hand	THE R. W. LEWIS CO.
Contractor Man-	Computer .	Territorian (2)		
Comments	Strenchi GOR-	T.		
	Surrent later	(hisson)		
	Rather Bran		P	David Supervy Conceptant
T Instantional	term more reading		Le contrace	3101-88-08 10.01-81-007
Concession of Co	Conservation	07,9446		
	There are carriedly in the			
	Add Comment			
	But Gammer			

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Installare AMP for Endpoints Connector in un video Linux
 Documentazione e supporto tecnico Cisco Systems