Installazione di FireSIGHT Management Center su VMware ESXi

Sommario

Introduzione Prerequisiti Componenti usati Configurazione Distribuire un modello OVF Accensione e completamento dell'inizializzazione Configurazione delle impostazioni di rete Esegui installazione iniziale Informazioni correlate

Introduzione

Questo documento descrive la configurazione iniziale di un centro di gestione FireSIGHT (noto anche come centro di difesa) che viene eseguito su VMware ESXi. Un centro di gestione FireSIGHT consente di gestire una o più appliance FirePOWER, Next-Generation Intrusion Prevention System (NGIPS) Virtual Appliance e Adaptive Security Appliance (ASA) con servizi FirePOWER.

Nota: Questo documento è un supplemento alla Guida all'installazione e manuale dell'utente del sistema FireSIGHT. Per una domanda specifica relativa alla configurazione e alla risoluzione dei problemi di ESXi, consultare la knowledge base e la documentazione di VMware.

Prerequisiti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti piattaforme:

- Cisco FireSIGHT Management Center
- Appliance virtuale Cisco FireSIGHT Management Center
- VMware ESXI 5.0

In questo documento, il termine "dispositivo" si riferisce alle seguenti piattaforme:

- Appliance Sourcefire FirePOWER serie 7000 e appliance serie 8000
- Sourcefire NGIPS Virtual Appliance per VMware ESXi
- Cisco ASA serie 5500-X con servizio FirePOWER

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.

Configurazione

Distribuire un modello OVF

- 1. Scaricare Cisco FireSIGHT Management Center Virtual Appliance dal sito Cisco Support & Downloads.
- 2. Estrarre il contenuto del file tar.gz in una directory locale.
- 3. Connessione al server ESXi con un client VMware

| | VMv | ware vSphere Cli | ent | — |
|----------|--|---|----------------------------------|----------|
| | vmware [.] VMware vSphere Client | | | |
| | To directly manage a singl To manage multiple hosts, vCenter Server. | e host, enter the IP ad enter the IP address | ddress or host n or name of a | ame. |
| | IP address / Name: | | - | |
| | User name: | | | |
| | Password: | | | |
| | | Use Windows se | ssion credential | s |
| vSphere. | | Login | Close | Help |

4. Una volta eseguito il login al client vSphere, scegliere **File > Distribuisci modello**

| d | 2 | | | | | |
|------|------|-----------------------|----------|---------|----------|-----------|
| [| File | Edit View Inventory | Administ | tration | Plug | -ins Helj |
| | | New | • | ntory | Þ 🗊 | Inventory |
| | | Deploy OVF Template | | | | |
| | | Export | • | | | |
| | | Report | • | localh | ost. Vŀ | 1ware ES |
| | | Browse VA Marketplace | | Gettir | ng Start | ed Sum |
| | | Print Maps | Þ | | | |
| OVF. | | Exit | | | | |

5. Fare clic su **Sfoglia** e individuare i file estratti nel passaggio 2. Scegliere il file OVF Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X-xxx.ovf e fare clic su **Avanti**.

| 0 | Deploy OVF Template |
|--|--|
| Source Select the source location. | |
| Source OVF Template Details Name and Location Datastore Disk Format Ready to Complete | Deploy from a file or URL C:\Temp\Sourcefire_Defense_Center_Virtual64_VMware-5.3 Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. |
| Help | < Back Next > Cancel |

6. Nella schermata **Dettagli modello OVF**, fare clic su **Avanti** per accettare le impostazioni predefinite.

| Ø | Deploy | y OVF Template | | |
|---|--|---|---------------|--------|
| OVF Template Details Verify OVF template details | | | | |
| Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete | Product: Version: Vendor: Publisher: Download size: Size on disk: Description: | VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned) 250.0 GB (thick provisioned) Sourcefire Defense Center Virtual64 Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046 | | |
| Help | | | < Back Next > | Cancel |

7. Specificare un nome per il centro di gestione e fare clic su

Avanti.

| Ø | Deploy OVF Template | - | × |
|---|---------------------|---|---|
| | | | |

Name and Location

Specify a name and location for the deployed template

| OVF Template Details VirtualDC64 Name and Location Datastore Disk Format Network Mapping Ready to Complete VirtualDC64 | Source | Name: |
|--|---|---|
| The name can contain up to 80 characters and it must be unique within the inventory folder. Network Mapping Ready to Complete | OVF Template Details | VirtualDC64 |
| | Name and Location Datastore Disk Format Network Mapping Ready to Complete | The name can contain up to 80 characters and it must be unique within the inventory folder. |

8. Scegliere un **archivio dati** in cui creare la macchina virtuale e fare clic su Avanti

| | ai ili. | | | | | | |
|---|---|--------------------------|--------------------|-------------|----------------|-------------------|--------|
| 2 | | Deplo | oy OVF Templa | ate | | | |
| I | Datastore Where do you want to st | tore the virtual machine | files? | | | | |
| | Source | Select a datastore in | which to store the | VM files: | | | |
| | OVF Template Details Name and Location | Name | Capacity F | Provisioned | Free Type | Thin Provisioning | Access |
| | Datastore | [datastore2] | 1.29 TB | 866.14 GB | 469.36 GB VMFS | Supported | Single |
| | Disk Format Network Mapping Ready to Complete | [datastore1] | 459.75 GB | 563.00 MB | 459.20 GB VMFS | Supported | Single |
| | | < | | | | | > |
| | Help | | | | < Back | Next > C | ancel |

9. Fare clic sul pulsante di opzione **Thick provisioning format** per **Disk Format** e fare clic su **Next** (Avanti). Il formato Thick Provisioning alloca lo spazio su disco necessario al momento della creazione di un disco virtuale, mentre il formato Thin Provisioning utilizza lo spazio su richiesta.

| 2 | Deploy OVE Template |
|---|---|
| Disk Format In which format do you v | vant to store the virtual disks? |
| Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete | Information about the selected datastore: Name: datastore2 Capacity: 1.3 TB Free space: 469.4 GB Select a format in which to store the virtual machines virtual disks: C Thin provisioned format The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks. Estimated disk usage: 1.4 GB C Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB |
| Help | < Back Next > Cancel |

10. Nella sezione **Mappatura di rete**, associare l'interfaccia di gestione di FireSIGHT Management Center a una rete VMware e fare clic su **Avanti**.

| <u>e</u> Template Details and Location | Map the networks used in this OVF tem | plate to networks in your inventory | |
|--|--|-------------------------------------|--------|
| tore | Source Networks | Destination Networks | |
| ormat | Management | VM Network | - |
| ork Mapping | | VM Network | |
| y to complete | | VM Network 2 | |
| | Description: The Management network | | ^ ~ |
| | | | |

11. Per completare la distribuzione del modello OVF, fare clic su **Fine**.

Ø

Network Mapping

What networks should the deployed template use?



Accensione e completamento dell'inizializzazione

 Passare alla macchina virtuale appena creata. Fare clic con il pulsante destro del mouse sul nome del server e scegliere Accensione per avviare il server per la prima volta.



2. Per monitorare la console del server, passare alla scheda **Console**. Viene visualizzato il menu di avvio

| LILO. | | |
|-----------------------------|--|--|
| VirtualDC64 | | |
| Getting Started Summary Res | source Allocation Performance Events Console Permissions | |
| | | |
| | | |
| | LILO 22.8 Boot Menu | |
| | | |
| | 3D-5.3.0 | |
| | | |
| | Hit any key to cancel timeout 00:00 | |
| | Enter choice & options, hit CR to boot | |
| | | |
| boot: | | |
| Loading 3D-5.3.0 | ·····- | |
| | | |

Una volta completato il controllo dei dati del BIOS, viene avviato il processo di inizializzazione. Poiché il database di configurazione viene inizializzato per la prima volta, il completamento del primo avvio potrebbe richiedere più tempo.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh
                                                                       E
                                                                          OK
                                                                               ]
                                                                               ]
                                                                       E
                                                                          OK
Executing S04async_syslog_dc.sh
                                                                       E
                                                                               ]
Executing S04fix-httpd.sh
                                                                          OK
                                                                       Ľ
                                                                               ]
Executing S05set-MgMnt-port
                                                                          OK
                                                                               ]
                                                                       E
                                                                          OK
Executing S06addusers
                                                                       E
                                                                          OK
                                                                               ]
Executing S07uuid-init
                                                                       ſ
                                                                          OK
                                                                               ]
Executing S09configure_mysql
************ Attention ********
   Initializing the configuration database. Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.
************ Attention ********
Executing S10database
```

Al termine, potrebbe essere visualizzato un messaggio per Nessun dispositivo di questo tipo.

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
```

3. Premere Invio per ottenere una richiesta di

accesso.

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
Sourcefire3D login: _
```

Nota: Viene visualizzato il messaggio "WRITE SAME failed. Azzeramento manuale." potrebbe apparire dopo il primo avvio del sistema. Questo non indica un difetto, ma indica correttamente che il driver di storage VMware non supporta il comando WRITE SAME. Il sistema visualizza questo messaggio e procede con un comando di fallback per eseguire la stessa operazione.

Configurazione delle impostazioni di rete

- Al prompt di accesso di Sourcefire3D, utilizzare le seguenti credenziali per eseguire l'accesso: Per la versione 5.xUsername: adminPassword: SourcefirePer la versione 6.x e successiveUsername: adminPassword: Admin123Suggerimento: È possibile modificare la password predefinita durante il processo di configurazione iniziale nella GUI.
- 2. La configurazione iniziale della rete viene eseguita con uno script. È necessario eseguire lo script come utente root. Per passare all'utente root, immettere il comando sudo su insieme alla password Sourcefire o Admin123 (per 6.x). Prestare attenzione quando si accede alla riga di comando di Management Center come utente root. admin@sourcefire3D:~\$ sudo su -

Password:

3. Per iniziare la configurazione di rete, immettere lo script **configure-network** come root. root@Sourcefire3D:~# configure-network

Do you wish to configure IPv4? (y or n) y

Verrà richiesto di specificare un indirizzo IP di gestione, una netmask e un gateway predefinito. Una volta confermate le impostazioni, il servizio di rete viene riavviato. Di conseguenza, l'interfaccia di gestione si interrompe e poi

```
ritorna.
 Do you wish to configure IPv4? (y or n) y
 Management IP address? [192.168.45.45] 192.0.2.2
Management netmask? [255.255.255.0]
Management default gateway? 192.0.2.1
 Management IP address?
                                  192.0.2.2
 Management netmask?
                                  255.255.255.0
 Management default gateway? 192.0.2.1
 Are these settings correct? (y or n) y
 Do you wish to configure IPv6? (y or n) n
 e1000: eth0: e1000_watchdog_task: NIC Link is Up 1000 Mbps Full Duplex, Flow Con
 trol: None
 ADDRCONF(NETDEV_UP): eth0: link is not ready
 ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Updated network configuration.
 Updated comms. channel configuration.
 Please go to https://192.0.2.2/ or https://[]/ to finish installation.
 root@Sourcefire3D:~# _
```

Esegui installazione iniziale

- Dopo aver configurato le impostazioni di rete, aprire un browser Web e individuare l'indirizzo IP configurato tramite HTTPS (in questo esempio, all'indirizzo <u>https://192.0.2.2</u>). Se richiesto, autenticare il certificato SSL predefinito. Per accedere, usare queste credenziali:Per la versione 5.x Username: adminPassword: SourcefirePer la versione 6.x e successiveUsername: adminPassword: Admin123
- 2. Sullo schermo seguente, tutte le sezioni di configurazione GUI sono facoltative ad eccezione della modifica della password e dell'accettazione dei termini del servizio. Se le informazioni sono note, si consiglia di utilizzare l'installazione guidata per semplificare la configurazione iniziale di Management Center. Una volta configurata, fare clic su Apply (Applica) per applicare la configurazione al Management Center e ai dispositivi registrati. Di seguito è riportata una breve panoramica delle opzioni di configurazione. Cambia password: Consente di modificare la password per l'account amministratore predefinito. È necessario modificare la password. Impostazioni di rete: Consente di modificare le impostazioni di rete IPv4 e IPv6 configurate in precedenza per l'interfaccia di gestione dell'accessorio o della macchina virtuale. Impostazioni ora: È consigliabile sincronizzare il centro di gestione con una fonte NTP affidabile. I sensori IPS possono essere configurati tramite criteri di sistema per sincronizzare l'ora con il centro di gestione. L'ora e il fuso orario possono essere impostati manualmente. Importazioni aggiornamento regole ricorrenti: Abilitare gli aggiornamenti ricorrenti delle regole Snort e installarli ora durante l'installazione iniziale Aggiornamenti geolocalizzazione ricorrenti: Abilita gli aggiornamenti ricorrenti delle regole di geolocalizzazione e facoltativamente installa ora durante la configurazione iniziale. Backup automatici: Pianificare backup di configurazione automatici. Impostazioni licenza: Aggiungere la licenza per le funzionalità. Registrazione dispositivo: Consente di aggiungere, concedere in licenza e applicare policy di controllo dell'accesso iniziali ai dispositivi

preregistrati. Il nome host/indirizzo IP e la chiave di registrazione devono corrispondere all'indirizzo IP e alla chiave di registrazione configurati nel modulo FirePOWER IPS.**Contratto di licenza con l'utente finale:** È necessaria l'accettazione del Contratto.

| Change Password | |
|--|---|
| Use these fields to change the password for the ad characters of mixed case and includes at least one | min account. Sourcefire recommends that you use a password that has at least eight alphanumeric numeric character. Avoid using words that appear in a dictionary. |
| New Password Confirm | |
| Network Settings | |
| Use these fields to specify network-related informa | tion for the management interface on the appliance. |
| Protocol | ⊙ IPv4 ◯ IPv6 ◯ Both |
| IPv4 Management IP | |
| Netmask | |
| IPv4 Default Network Gateway | |
| Hostname | |
| Domain | |
| Primary DNS Server | |
| Secondary DNS Server | |
| Tertiary DNS Server | |

Informazioni correlate

- Guida rapida virtuale di Firepower Management Center per VMware, versione 6.0
- Documentazione e supporto tecnico Cisco Systems