IPS 5.x及更高版本:IPS上的NTP配置示例

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>相關產品</u> <u>慣例</u> <u>組態</u> <u>將思科路由器配置為NTP伺服器</u> <u>將感測器配置為使用NTP時間源</u> <u>驗證</u> <u>疑難排解</u> <u>相關資訊</u>

<u>簡介</u>

本文提供使用網路時間協定(NTP)將思科安全入侵防禦系統(IPS)時鐘與網路時間伺服器同步的範例 組態。 Cisco路由器配置為NTP伺服器,IPS感測器配置為NTP伺服器(Cisco路由器)用作時間源 。

<u>必要條件</u>

<u>需求</u>

嘗試此組態之前,請確保符合以下要求:

• 啟動此NTP配置之前,必須能夠從Cisco IPS感測器訪問NTP伺服器。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- Cisco 4200系列IPS裝置(運行軟體版本7.0及更高版本)
- Cisco IPS Manager Express(IME)版本7.0.1及更高版本注意:IME可用於監控運行Cisco IPS 5.0及更高版本的感測器裝置,但只有運行Cisco IPS 6.1或更高版本的感測器才支援在IME中提供的一些新特性和功能。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下硬體和軟體版本:

- Cisco 4200系列IPS裝置,運行軟體版本6.0及更低版本
- Cisco IPS管理員Express(IME)版本6.1.1

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u> 組態</u>

<u>將思科路由器配置為NTP伺服器</u>

如果感測器要使用NTP伺服器作為時間源,則需要與NTP伺服器進行身份驗證連線。感測器僅支援 用於金鑰加密的MD5雜湊演算法。使用以下過程啟用作為NTP伺服器的Cisco路由器,並使用其內 部時鐘作為時間源。

完成以下步驟,將思科路由器設定為充當NTP伺服器:

- 1. 登入路由器。
- 2. 進入配置模式。

router#configure terminal

3. 建立金鑰ID和金鑰值。

router(config)#ntp authentication-key key_ID md5 key_value

鍵ID可以是一個介於1和65535之間的數字。鍵值是文本(數字或字元)。 稍後會加密。例如 :

router(config)#ntp authentication-key 12345 md5 123

註:感測器僅支援MD5鍵。金鑰可能已經存在於路由器上。使用show running配置命令檢查其 他金鑰。您可以在步驟4中將這些值用於受信任金鑰。

4. 將您在步驟3中剛剛建立的金鑰指定為受信任金鑰(或使用現有金鑰)。 router(config)#**ntp trusted-key key_ID**

受信任的金鑰ID與步驟3中的金鑰ID的數字相同。例如: router(config)#ntp trusted-key 12345

5. 指定路由器上感测器將與之通訊的介面。 router(config)#**ntp source interface_name**

router(config)#ntp source FastEthernet 1/0

6. 指定要分配給感測器的NTP主層編號,如下所示: router(config)#**ntp master stratum_number**

例如:

例如:

注意:NTP主層編號標識伺服器在NTP層次結構中的相對位置。可以選擇介於1和15之間的數字。對於感測器而言,選擇哪個數字並不重要。

將感測器配置為使用NTP時間源

完成本節中的步驟,將感測器配置為使用NTP時間源(在本示例中,Cisco路由器是NTP時間源)。

感測器需要一致的時間源。建議使用NTP伺服器。使用以下過程將感測器配置為使用NTP伺服器作 為其時間源。您可以使用已驗證或未驗證的NTP。

注意:對於經過身份驗證的NTP,必須從NTP伺服器獲取NTP伺服器IP地址、NTP伺服器金鑰ID和 金鑰值。

完成以下步驟,將感測器配置為使用NTP伺服器作為其時間源:

- 1. 使用具有管理員許可權的帳戶登入到CLI。
- 2. 進入配置模式,如下所示: sensor#configure terminal
- 3. 進入服務主機模式。

sensor(config)# service host

 A. NTP可以配置為已驗證和未驗證的NTP。完成以下步驟以配置未經驗證的NTP:進入NTP配置 模式。

sensor(config-hos)#ntp-option enabled-ntp-unauthenticated

指定NTP伺服器IP地址。 sensor(config-hos-ena)#**ntp-server ip_address**

在本示例中,NTP伺服器的IP地址為10.1.1.1。 sensor(config-hos-ena)#**ntp-server 10.1.1.1**

以下是使用Cisco IPS Manager Express配置未經驗證的NTP的過程:選擇**Configuration > Corp-IPS > Sensor Setup > Time**。然後,在提供NTP伺服器的IP地址後,按一下 **Unauthenticated NTP**旁邊的單選按鈕,如螢幕截圖所示。按一下「**Apply**」。

Cisco IPS Manager Express	7.0.1		
File View Tools Help			
Home 😥 Configuration 🏧 E	ivent Monitoring 🚮 Reports 🦿 Help		
Configuration > Corp-IPS > Sense	or Setup > Time		
Corp-IPS			
Sartup Weard Network Allowed Hosts/Networks Time Structures	Specify local date and time settings for the sensor. O Sensor Local Date November > 10 > 2009 >	lick Apply Time to Sensor to set the date and time. Sensor Local Time 22 : 47 : 08 bhommess	
	Standard Time Zone		
	UTC Offset: 0 minutes		
	NTP Server		
	IP Address: 10.1.1.1	Summertime	
	O Authenticated NTP	Enable Summertime	
	Key ID:	Configure Summertime	
	O Unauthenticated NTP		
Sensor Setup			
Interfaces			
Policies			
Sensor Management			
Sensor Monitoring		C	
		Apply Reset Apply	Time to Sensor

這將完成未經身份驗證的NTP配置。完成以下步驟以配置經過身份驗證的NTP:進入NTP配置 模式。

sensor(config-hos)#ntp-option enable

指定NTP伺服器IP地址和金鑰ID。金鑰ID是一個介於1和65535之間的數字。這是您在NTP伺服器上設定的金鑰ID。

sensor(config-hos-ena)#ntp-servers ip_address key-id key_ID

在本示例中,NTP伺服器的IP地址為10.1.1.1。

sensor(config-hos-ena)#ntp-server 10.1.1.1 key-id 12345

指定NTP伺服器的鍵值。

sensor(config-hos-ena)#ntp-keys key_ID md5-key key_value

鍵值為文本(數字或字元)。這是已在NTP伺服器上設定的金鑰值。例如: sensor(config-hos-ena)#**ntp-keys 12345 md5-key 123**

以下是使用Cisco IPS Manager Express配置已驗證NTP的過程:選擇**Configuration > Corp-**IPS > Sensor Setup > Time。然後,在提供NTP伺服器的IP地址後,按一下Authenticated NTP旁邊的單選按鈕,如螢幕截圖所示。提供必須與NTP伺服器中提到的金鑰和金鑰ID。在本 示例中,金鑰為123,金鑰ID為12345。按一下「Apply」。

ome 2 Configuration	Event Monitoring 📆 Reports 🦻 Help		
suration > Form TPS > Sens	(II) o		
orp-IPS			
Sartup Wizard Network Allowed Hosts/Networks	Specify local date and time settings for the sensor. O Sensor Local Date	Click Apply Time to Sensor to set the date and time.	
(upers)	Standard Time Zone		
	Zone Name: UTC UTC Offset: 0 minutes	M	
	NTP Server IP Address: 10.1.1.1	Summertime	
	Authenticated NTP Key: 123	Configure Summertime	
	Key ID: 12345 O Unauthenticated NTP		
Server Setur			
interfaces			
iensor Management			
Sensor Monitoring	2	Andy Recat	me to Series

這將完成已驗證的NTP配置。

5. 退出NTP配置模式。

sensor(config-hos-ena)# exit

sensor(config-hos)# exit

Apply Changes:?[yes]

6. 按Enter應用更改,或輸入no放棄更改。這樣即可完成配置任務。

<u>驗證</u>

本節提供的資訊可用於確認您的組態是否正常運作。

驗證經過身份驗證的NTP設定。這可確保已驗證的NTP配置正確完成。

sensor(config-hos-ena)#show settings

enabled

ntp-keys (min: 1, max: 1, current: 1)

key-id: 12345

md5-key: 123
.....
ntp-servers (min: 1, max: 1, current: 1)
.....
ip-address: 10.1.1.1
key-id: 12345
.....

sensor(config-hos-ena)#

要顯示當前子模式中包含的配置內容,請在任何服務命令模式下使用<u>show settings</u>命令。這驗證未 身份驗證NTP配置是否正確完成。

sensor(config-hos-ena)#show settings

enabled-ntp-unauthenticated

ntp-server: 10.1.1.1

sensor(config-hos-ena)#

要顯示系統時鐘,請在執行模式下使用<u>show clock</u>命令,如下所示。此示例顯示已配置和同步的 NTP:

sensor#show clock detail

11:45:02 CST Tues Jul 20 2011

Time source is NTP

sensor#

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- <u>思科入侵防禦系統支援頁面</u>
- <u>Cisco IPS管理員Express支援頁面</u>
- 網路時間協定(NTP)

• <u>要求建議 (RFC)</u> • <u>技術支援與文件 - Cisco Systems</u>