外部 Syslog サーバにアラートを送信するための FireSIGHT システムの設定

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>侵入アラートの送信</u> <u>ヘルス アラートの送信</u> <u>パート 1: syslog アラートを作成する</u> <u>パート 2: ヘルス モニタ アラートを作成する</u> 影響フラグ アラート、検出イベント アラート、マルウェア アラートの送信

概要

FireSIGHT システムでは、イベントのさまざまなビューが Web インターフェイスで提供されま すが、重要なシステムの継続的なモニタリングを容易にするために外部イベント通知を設定する こともできます。次のいずれかが発生したときに、電子メール、SNMP トラップ、または syslog で通知するアラートを生成するように FireSIGHT システムを設定できます。この記事では、外部 の syslog サーバにアラートを送信するように FireSIGHT Management Center を設定する方法に ついて説明します。

前提条件

要件

syslog および FireSIGHT Management Center に関する知識があることが推奨されます。また、 ファイアウォールで syslog ポート(デフォルトは 514)を許可する必要があります。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 5.2 以降に基づくものです。

注意:このドキュメントの情報は、特定のラボ環境内のアプライアンスから作成され、初期 (デフォルト)設定の状態から開始しています。対象のネットワークが実稼働中である場合 には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要 があります。

侵入アラートの送信

- 1. FireSIGHT Management CenterのWebユーザインターフェイスにログインします。
- 2. [Policies] > [Intrusion] > [Intrusion Policy] に移動します。
- 3.適用するポリシーの横にある[Edit] をクリックします。
- 4. [Advanced Settings] をクリックします。

5.リストで[Syslog Alerting] を見つけて、[Enabled] に設定します。

Overview Analysis Policie	es Devices Objects FireAMP		Health Sys	tem Help 🔻 admin 🔻
Access Control Intrusion > In	ntrusion Policy Network Discovery	Application Detectors Files	s Users Cor	relation Actions •
Edit Policy				
Policy Information	Advanced Settings			< Back
Variables	Performance Sattings			
Rules	Served Duran Configuration			a can
FireSIGHT Recommendations	Event Queue Configuration	🖲 Enabled 🕓	Disabled	J Edit
⊕ Advanced Settings	Latency-Based Packet Handling	🔘 Enabled 🛛 🖲	Disabled	
Policy Layers	Latency-Based Rule Handling	C Enabled	Disabled	
	Performance Statistics Configuration	🖲 Enabled 🛛	Disabled	🥜 Edit
	Regular Expression Limits	Enabled	Disabled	🥜 Edit
		•		0.00
	Rule Processing Configuration	🖲 Enabled 🕓	Disabled	J Edit
	📡 External Responses			
	SNMP Alerting	🔘 Enabled 🛛 🖲	Disabled	
	Syslog Alerting	Enabled	Disabled	🖉 Edit

- 6. [Syslog Alerting] の右側にある[Edit] をクリックします。
- 7. syslogサーバのIPアドレスを[Logging Hosts] フィールドに入力します。

8.ドロップダウンメニューから適切な[Facility] と[Severity] を選択します。 特定のファシリティ または重大度のアラートを受け入れるように syslog サーバを設定するのではないかぎり、これら はデフォルト値のままにしておくことができます。

Overview Analysis Policie	S Devices Ob	ojects FireAMP		Health	System Help	▼ admin ▼
Access Control Intrusion > In	trusion Policy	Network Discovery	Application Detectors	Files Users	Correlation	Actions •
Edit Policy						
Policy Information	Syslog Alerting					< Back
Variables	Settings					
Rules	Jecoles Heste		icia ele in-		a sector of Harith	
FireSIGHT Recommendations	Logging Hosts		(Single IP a	oddress or comma-sep	larated list)	
Advanced Settings	Facility Al	UTH 🔻				
Back Orifice Detection	Priority EM	MERG V				
Checksum Verification				_		
DCE/RPC Configuration			Revert to Defaults			
DNS Configuration						
Event Queue Configuratio						
FTP and Telnet Configurat						
Global Rule Thresholding						
GTP Command Channel Co						

9.この画面の左上にある[Policy Information] をクリックします。

10. [Commit Changes] ボタンをクリックします。

11.侵入ポリシーを再適用します。

注:アラートを生成するには、アクセス制御ルールでこの侵入ポリシーを使用します。 設 定されているアクセス制御ルールがない場合は、この侵入ポリシーをアクセス制御ポリシー のデフォルト アクションとして使用するように設定し、アクセス制御ポリシーを再適用し ます。

そのポリシーで侵入イベントがトリガーされると、侵入ポリシーに設定されている syslog サーバ にもアラートが送信されます。

ヘルス アラートの送信

パート1: syslog アラートを作成する

1. FireSIGHT Management CenterのWebユーザインターフェイスにログインします。

2. [Policies] > [Actions] > [Alerts] に移動します。

Overview	/ Analysis	Policie	s Devi	ces Ob	jects F			Healt	th S	System	Help 🔻	admin 🔻	
Access Control Intrusion • Files		Files	Network Discovery		Application Detectors		Users (Correlation		Actions + Alerts		
				Policies	Rule Editor	White List	Traffic Profiles	Alerts	Remediat	tions	Groups	Health Mon	itor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts				Advanced Malware Protection Alerts									
											0	Create Aler	t•
Name	Name					Туре	e	In U	Jse	Enabled			

3. Webインターフェイスの右側にある[Create Alert] を選択します。



4. [Create Syslog Alert] をクリックします。設定ポップアップ ウィンドウが表示されます。

5.アラートの名前を指定します。

6. syslogサーバのIPアドレスを[Host] フィールドに入力します。

7. syslogサーバで必要に応じてポートを変更します(デフォルトのポートは514です)。

8.適切な[Facility] と[Severity] を選択します。

Create Syslog Alert Configuration ? X

Name

Host

Port

514

Facility

ALERT

Severity

ALERT

Tag

Save

Cancel

9. [Save] ボタンをクリックします。[Policies] > [Actions] > [Alerts] ページに戻ります。



10. Syslog設定を有効にします。

パート 2: ヘルス モニタ アラートを作成する

次の手順では、(前の項で)作成した syslog アラートを使用するヘルス モニタ アラートの設定 手順について説明します。

1. [Policies] > [Actions] > [Alerts] ページに移動し、ページの上部近くにある[Health Monitor Alerts] を選択します。

Overview	Analysis	Policie	s Dev	vices Ol	bjects	FireAMP			Health	System	Help 🔻	admin 🔻
Access Control Intrusion • Fi		Files	iles Network Discovery			tion Detectors	Use	Users Corr		Actions	 Alerts 	
				Policies	Rule Edit	or White List	Traffic Profiles	Alerts I	Remediation	s Groups	Health Moni	itor Alerts
Alerts Impact Flag Alerts Discovery Event Alerts					Advanced Malware Protection Alerts							
										0	Create Alert	•
Name							Туре	a Ir	Use	Enabled		

2.ヘルスアラートに名前を付けます。

3. [Severity] を選択します(Ctrlキーを押しながらクリックすると、複数の重大度タイプを選択できます)。

4. [Module] 列から、syslogサーバにアラートを送信するヘルスモジュールを選択します(たとえば、[Disk Usage])。

5. [Alerts] 列から、以前に作成したsyslogアラートを選択します。

6. [Save] ボタンをクリックします。

影響フラグ アラート、検出イベント アラート、マルウェア アラ ートの送信

特定の影響フラグを含むイベント、特定タイプの検出イベント、特定タイプのマルウェア イベントの syslog アラートを送信するように FireSIGHT Management Center を設定することもできます。これを行うには、「<u>パート 1:syslog アラートを作成する」を実行してから、syslog サーバに送信するイベントのタイプを設定する必要があります。</u>そのためには、[Policies] > [Actions] > [Alerts] **に移動し、目的のアラートタイプのタブを選択します。**

Overview	/ Analysi	s Polici	es De	vices	Object	s F	ireAMP			He	alth	System	Help 🔻	admin 🔻
Access Control Intrusion • Files		Netwo	Network Discovery		Application Detectors		Users		Correlation		Actions	Alerts		
				Polic	cies Rule	Editor	White List	Traffic Profiles	Alerts	Remed	iations	Groups	Health Mon	itor Alerts
Alerts	ts Impact Flag Alerts Discovery Event Alerts				erts	Advanced Malware Protection Alerts								
												0	Create Aler	t •
Name									Тур	pe	In	Use	Enabled	

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。