

エンドポイント向けAMPとThreat GridのWSAとの統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[AMP統合](#)

[Threat Gridの統合](#)

[確認](#)

[トラブルシューティング](#)

[WSAがAMPページにリダイレクトされない](#)

[WSAは指定されたSHAをブロックしません](#)

[WSAがTG組織に表示されない](#)

概要

このドキュメントでは、エンドポイント用のAdvanced Malware Protection(AMP)とThreat Grid(TG)をWebセキュリティアプライアンス(WSA)と統合する手順について説明します。

著者 : Cisco TACエンジニア、Uriel Montero、編集 : Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- エンドポイントアクセス用AMP
- TGプレミアムアクセス
- ファイル分析とファイルレピュテーション機能キーを使用したWSA

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

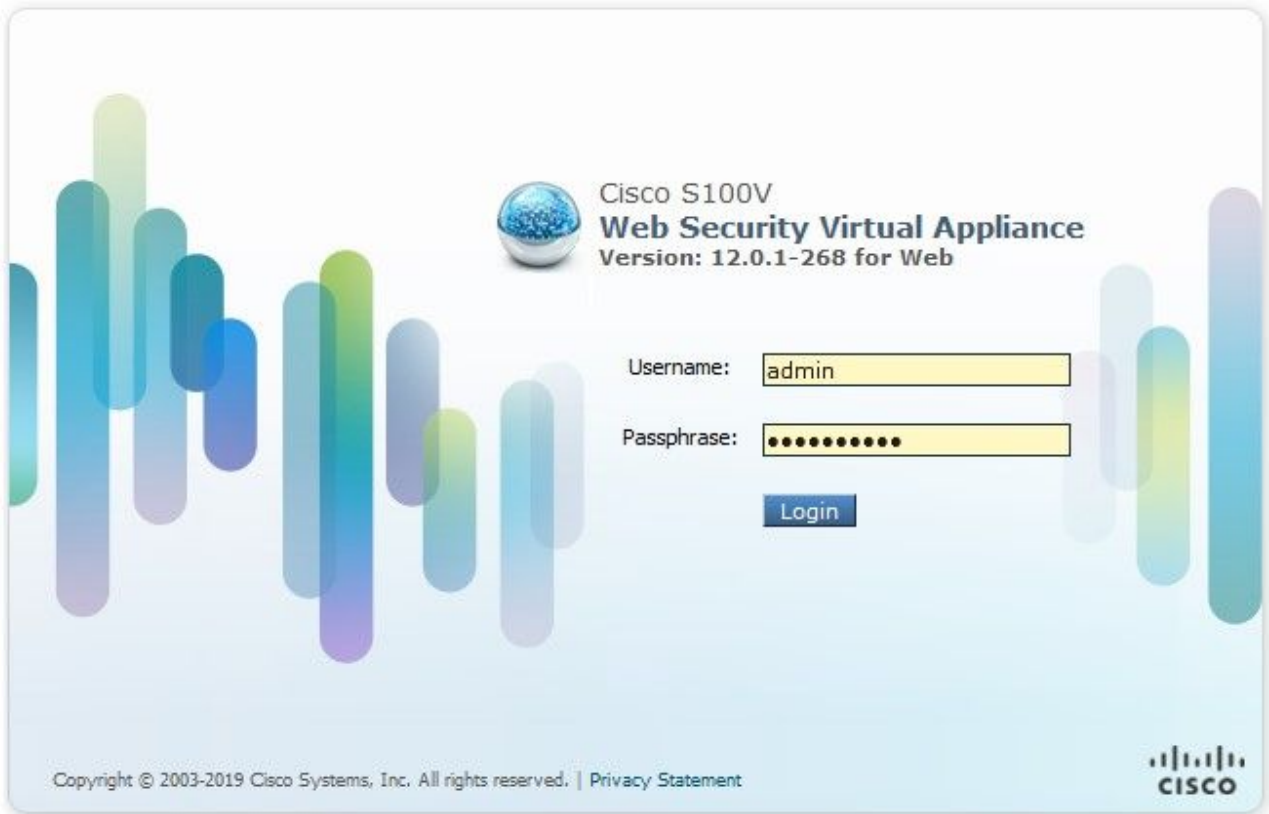
- AMPパブリッククラウドコンソール
- WSA GUI
- TGコンソール

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています

。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

WSAコンソールにログインします。



ログインしたら、[Security Services] > [Anti-Malware and Reputation]に移動します。このセクションでは、AMPとTGを統合するオプションを見つけることができます。

AMP統合

[Anti-Malware Scanning Services]セクションで、図に示すように[Edit Global Settings]をクリックします。

Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90

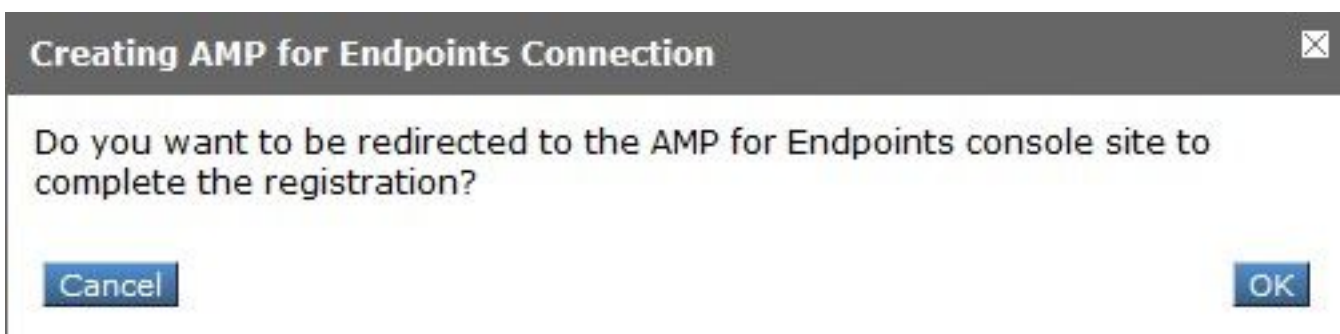
 [Edit Global Settings...](#)

[Advanced] > [Advanced Settings for File Reputation]セクションを検索して、展開すると、一連のクラウドサーバオプションが表示され、最寄りのロケーションを選択します。

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
File Reputation Server:	<input type="text" value="AMERICAS (cloud-sa.amp.cisco.com)"/> <ul style="list-style-type: none"> AMERICAS (cloud-sa.amp.cisco.com) AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com) EUROPE (cloud-sa.eu.amp.cisco.com) APJC (cloud-sa.apjc.amp.cisco.com) Private Cloud
AMP for Endpoints Console Integration ?	
SSL Communication for File Reputation:	<input type="text" value="Server:"/> Port: <input type="text" value="80"/> <input type="text" value="Username:"/> <input type="text" value="Passphrase:"/> <input type="text" value="Retype Passphrase:"/> <input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ?
Heartbeat Interval:	<input type="text" value="15"/> minutes
Query Timeout:	<input type="text" value="15"/> seconds
File Reputation Client ID:	67f8cea0-c0ec-497d-b6d9-72b17eabda5d

クラウドを選択したら、[Register Appliance with AMP for Endpoints]ボタンをクリックします。

図に示すように、AMPコンソールにリダイレクトするポップアップが表示され、[Ok]ボタンをクリックします。



図に示すように、有効なAMPクレデンシャルを入力し、[ログイン]をクリックする必要があります。



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
-  Threat Grid
-  Threat Response
and more...

Log In

[Use Single Sign-On](#)

[Can't access your account?](#)

デバイス登録を受け入れ、クライアントIDをメモします。これは、後でコンソールでWSAを見つけるのに役立ちます。

Authorize VLNWS

The VLNWS [redacted] (WSA endpoint) is requesting the following authorizations:

- Device Registration

Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.

WSAコンソールに戻り、図に示すように、[Amp for Endpoints Console Integration]セクションにチェックが表示されます。

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)
Cloud Domain:	cloud-sa.amp.cisco.com
AMP for Endpoints Console Integration ?	VLNWSA [redacted] ? Deregister SUCCESS

注:[送信]をクリックして変更を確定することを忘れないでください (プロンプトが表示された場合)。そうしないと、もう一度プロセスを実行する必要があります。

Threat Gridの統合

[セキュリティサービス] > [マルウェアとレピュテーションの対策]に移動し、Anti-Malware Protection Servicesで[グローバル設定の編集]ボタンをクリックします (図を参照)。

Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90

 [Edit Global Settings...](#)

[Advanced] > [Advanced Settings for File Analysis]セクションを検索して展開し、図に示すように、場所に最も近いオプションを選択します。

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
Advanced Settings for File Analysis	
File Analysis Server:	AMERICAS (https://panacea.threatgrid.com)
Proxy Settings:	AMERICAS (https://panacea.threatgrid.com) EUROPE (https://panacea.threatgrid.eu) Private Cloud
File Analysis Client ID:	02_VLNWS [redacted]

[Submit]をクリックし、変更を[Commit]をクリックします。

アプライアンスがAMP/TGと正常に統合された場合は、TGポータル側で[Users]タブの下でWSAデバイスを検索します。

Users - vrt/wsa/EC2ACF1150F19CCEF2DB-178D3EFDBAD1

+ New User Feedback

Filter										
Q Search on Login, Name, Email, Title, CSA Registration Key										
Login	Name	Email	Title	Organization	Role	Status	Integration	Type	Actions	
484c72c8-5321-477c-...	WSA Device			vrt/wsa/EC2ACF1150F...	user	Active	WSA	device	...	

[Login]をクリックすると、該当するアプライアンスの情報にアクセスできます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

AMPとWSAの統合が成功したことを確認するには、AMPコンソールにログインし、WSAデバイスを検索します。

[管理] > [コンピュータ]に移動し、[フィルタ]セクションで[Web Security Appliance]を検索し、フィルタを適用します

▼ Filters

Hostname	<input type="text" value="Hostname or Connector GUID"/>	Group	<input type="text"/>
Operating System	<input type="text"/>	Policy	<input type="text"/>
Connector Version	<input type="text" value="web"/>	Internal IP	<input type="text" value="Single IPv4 or CIDR"/>
Flag	<input type="checkbox"/> All <input type="checkbox"/> Web Security Appliance	External IP	<input type="text" value="Single IPv4 or CIDR"/>
Fault	<input type="text" value="None Selected"/>	Last Seen	<input type="text" value="Any Date"/>
Fault Severity	<input type="text"/>	Definitions Last Updated	<input type="text" value="None Selected"/>
Isolation Status	<input type="text" value="None Selected"/>	Sort By	<input type="text" value="Hostname"/>
Orbital Status	<input type="text" value="None Selected"/>	Sort Order	<input type="text" value="Ascending"/>

複数のWSAデバイスが登録されている場合は、ファイル分析クライアントIDを使用してそれらを識別できます。

デバイスを展開すると、そのデバイスが属するグループが表示され、適用されたポリシーとデバイスGUIDを使用してデバイストラジェクトリを表示できます。

VLNWSA [redacted] in group [redacted]-Group			
Hostname	VLNWSA [redacted] ...	Group	[redacted]-Group
Operating System	Web Security Appliance	Policy	[redacted].policy
Device Version		Internal IP	
Install Date		External IP	
Device GUID	67f8cea0-c0ec-497d-b6d9-72b17eabda5d	Last Seen	2020-05-20 03:51:32 CDT

[Diagnostics](#) [View Changes](#)

[Diagnose...](#) [Move to Group...](#) [Delete](#)

[Policy]セクションでは、デバイスに適用される[Simple Custom Detection]および[Application Control - Allowed]を設定できます。

Edit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

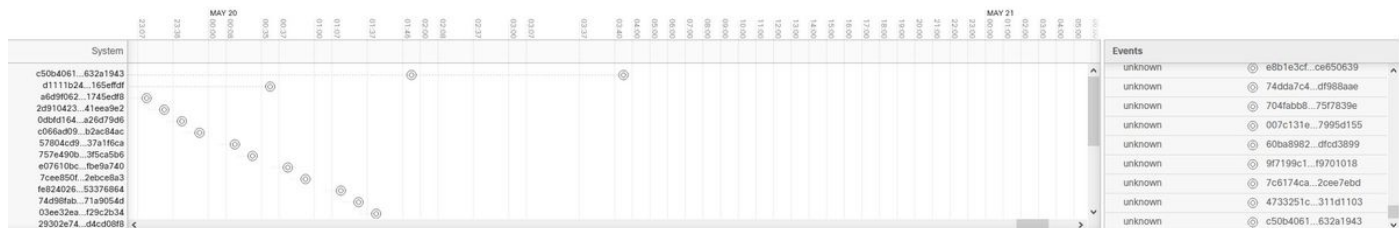
Application Control - Allowed:

WSAの[Device Trajectory]セクションを表示するには、別のコンピュータの[Device Trajectory]を開いて[Device GUID]を使用する必要があります。

変更は、図に示すようにURLに適用されます。

<https://console.amp.cisco.com/computers/c359f0b9-b4be-4071-9570-7d10c50df5bd/trajectory2>

<https://console.amp.cisco.com/computers/67f8cea0-c0ec-497d-b6d9-72b17eabda5d/trajectory2>



Threat Gridでは、しきい値は90です。この数値を下回るファイルにスコアが付いた場合、悪意のあるファイルはプッキングされませんが、WSAでカスタムしきい値を設定できます。

Advanced Routing Table: Management

Advanced Settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server: AMERICAS (https://panacea.threatgrid.com) ▾

Proxy Settings:

Use File Reputation Proxy

Server: Port:

Username:

Passphrase:

Retype Passphrase:

File Analysis Client ID: 02_VLNWSA [REDACTED]

Advanced Settings for Cache

Threshold Settings

File Analysis Threshold Score:

Use value from cloud service: 90

Enter custom value:

(valid range 1 through 100)

トラブルシューティング

WSAがAMPページにリダイレクトされない

- AMPに必要なアドレスがファイアウォールで許可されていることを確認します。ここをクリックします。
- 適切なAMPクラウドを選択していることを確認します (レガシークラウドを選択しないでください)。

WSAは指定されたSHAをブロックしません

- WSAが正しいグループにあることを確認します。
- WSAが正しいポリシーを使用していることを確認します。
- SHAがクラウド上でクリーンでないことを確認します。そうでないと、WSAはクラウドをブロックできません。

WSAがTG組織に表示されない

- 適切なTGクラウド (アメリカまたはヨーロッパ) を選択していることを確認します。
- ファイアウォールでTGに必要なアドレスが許可されていることを確認します。
- ファイル分析クライアントIDをメモします。
- [Users]セクションで検索します。
- 見つからない場合は、シスコサポートに連絡して、組織間での移行を支援してください。