

適切な AMP 操作に必要なサーバアドレス

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[適切な AMP 操作に必要なサーバアドレス](#)

[サーバの場所](#)

[北米](#)

[ヨーロッパ](#)

[アジア・太平洋、日本、中国](#)

[スタティック IP アドレス](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Advanced Malware Protection (AMP) 製品での更新、ルックアップ、レポートの伝達および実行を可能にするために必要なサーバについて説明します。操作を正常に行うためには、ファイアウォールでコネクタから必要なサーバへの接続を許可する必要があります。

注意： すべてのサーバが、ロード バランシング、耐障害性、および稼働時間にラウンドロビン IP アドレス スキーマを使用します。したがって、IP アドレスは変更される可能性があるため、ファイアウォールは IP アドレスではなく CNAME を使用して設定することをお勧めします。

前提条件

要件

Cisco Firepower Management Center (別名 *Defense Center*) および次の AMP 製品に関する知識があることが推奨されます。

- Cisco AMP アプライアンス
- Cisco AMP for Firepower
- Cisco AMP for Network Virtual Appliance
- Cisco FireAMP Private Cloud Virtual Appliance
- Cisco FireAMP for Endpoints

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

適切な AMP 操作に必要なサーバアドレス

サーバの場所

AMP サーバは次の 3 つの場所にあります。

- 北米
- ヨーロッパ
- 日本

北米

この表は北アメリカのためのサーバ ロケーションをリストしたものです。アカウントの作成日付に基づいて、サーバアドレスは異なるかもしれません：

[Category]	目的	サーバ	port
	クラウド上のサーバー	4.x Windows だけ: cloud-ec.amp.cisco.com	4.x: TCP 443 または 3213
	クラウド欧州共同体	asn.amp.cisco.com	
	クラウド欧州共同体	est.amp.cisco.com	TCP 443
	FireAMP コンソール	console.amp.cisco.com	TCP 443
	管理サーバ	mgmt.amp.cisco.com	TCP 443
	イベント サーバ	intake.amp.cisco.com	TCP 443
	ポリシー	policy.amp.cisco.com	TCP 443
	コネクタのダウンロードと更新	upgrades.amp.cisco.com	TCP 80 およ び 443
	エラー レポート	crash.amp.cisco.com	TCP 443
	エンドポイントIOC	ioc.amp.cisco.com	TCP 443
	TETRA 更新サーバ	update.amp.cisco.com	TCP 80 およ び 443
	OSX クラム定義	defs.amp.sourcefire.com	TCP 80
	高度カスタム検出	カスタムsignatures.amp.cisco.com	TCP 443
	リモートファイル フェッチ	rff.amp.cisco.com	TCP 443
Android コネクタ	クラウド上のサーバー	android.amp.sourcefire.com	TCP 443
	Cloud アップストリーム サーバ <v2.4	cloud-pc.amp.sourcefire.com	TCP 443 ま は 32137
AMP	Cloud アップストリーム サーバ >v2.4	クラウド パソコンest.amp.cisco.com クラウド パソコンasn.amp.cisco.com クラウドpc.amp.cisco.com	TCP 443
	Yum サーバ	packages.amp.sourcefire.com packages-v2.amp.sourcefire.com	TCP 443 TCP 443
	サポート セッション	packages.amp.cisco.com support-sessions.amp.sourcefire.com	TCP 443 TCP 22
Firesight/Firepower	クラウド上のサーバー	5.x: cloud-dc.amp.sourcefire.com 6.x: クラウドsa.amp.sourcefire.com	TCP 443 ま は 32137

	FireAMP イベント	export.amp.sourcefire.com	TCP 443
	FireAMP API	api.amp.sourcefire.com	TCP 443
	ダイナミック分析	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443
ESA/WSA	ファイル評判	cloud-sa.amp.sourcefire.com (レガシー) クラウドsa.amp.cisco.com	TCP 443 または 32137
Meraki	クラウド上のサーバー	クラウド Merakiasn.amp.cisco.com クラウド Merakiest.amp.cisco.com	TCP 443

ヨーロッパ

この表はヨーロッパのためのサーバロケーションをリストしたものです。アカウントの作成日付に基づいて、サーバアドレスは異なるかもしれません:

[Category]	目的	サーバ	port
	クラウド上のサーバー	4.x Windows だけ: cloud-ec.eu.am p.cisco.com cloud-ec-asn.eu.am p.cisco.com cloud-ec-est.eu.am p.cisco.com	4.x: TCP 443 または 32137 TCP 443
	FireAMP コンソール管理サーバ	console.eu.amp.cisco.com	TCP 443
	イベント サーバ	mgmt.eu.amp.cisco.com	TCP 443
	ポリシー	intake.eu.amp.cisco.com	TCP 443
	コネクタのダウンロードと更新	policy.eu.amp.cisco.com upgrades.amp.cisco.com	TCP 443
	エラー レポート	crash.eu.amp.cisco.com	TCP 80 および 443
	エンドポイントIOC	ioc.eu.amp.cisco.com	TCP 443
	TETRA 更新サーバ	update.amp.cisco.com	TCP 80 および 443
	OSX クラム定義	defs.amp.sourcefire.com	TCP 80
	高度カスタム検出	custom-signatures.eu.am p.cisco.com	TCP 443
Android コネクタ	リモートファイル フェッチ	rff.eu.amp.cisco.com	TCP 443
	クラウド上のサーバー	android.eu.amp.sourcefire.com	TCP 443
	Cloud アップストリーム サーバ <v2.4	cloud-pc.eu.am p.sourcefire.com	TCP 443 または 32137
AMP	Cloud アップストリーム サーバ >v2.4	cloud-pc-est.eu.am p.cisco.com cloud-pc-asn.eu.am p.cisco.com cloud-pc.eu.am p.cisco.com	TCP 443
	Yum サーバ	packages.amp.sourcefire.com	TCP 443
	サポート セッション	packages-v2.amp.sourcefire.com パソコンpackages.amp.cisco.com	TCP 443
	クラウド上のサーバー	support-sessions.amp.sourcefire.com	TCP 22
	FireAMP イベント	5.x: cloud-dc.eu.am p.sourcefire.com 6.x: cloud-sa.eu.am p.sourcefire.com	TCP 443 または 32137
Firesight/Firepower	FireAMP API	export.eu.amp.sourcefire.com	TCP 443
	ダイナミック分析	api.eu.amp.sourcefire.com 5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443
ESA/WSA	ファイル評判	cloud-sa.amp.sourcefire.com (レガシー)	TCP 443 または 32137

Meraki	クラウド上のサーバー	cloud-sa.eu.amp.cisco.com cloud-meraki-asn.eu.amp.cisco.com (AW IP) cloud-meraki-est.eu.amp.cisco.com (AW IP)	TCP 443
--------	------------	---	---------

アジア・太平洋、日本、中国

この表は 2017 年 1 月 27 日からのサーバーロケーションをリストしたものです:

[Category]	目的	サーバ	port
	クラウド上のサーバー	4.x Windows だけ: クラウド ec.apjc.amp.cisco.com	4.x: TCP 443 または 32137
		クラウド欧州共同体asn.apjc.amp.cisco.com クラウド欧州共同体est.apjc.amp.cisco.com	TCP 443
	FireAMP コンソール	console.apjc.amp.cisco.com	TCP 443
	管理サーバ	mgmt.apjc.amp.cisco.com	TCP 443
	イベント サーバ	intake.apjc.amp.cisco.com	TCP 443
Windows/Mac コネクタ	ポリシー	policy.apjc.amp.cisco.com	TCP 443
	コネクタのダウンロードと更新	upgrades.amp.cisco.com	TCP 80 および 443
	エラー レポート	crash.apjc.amp.cisco.com	TCP 443
	エンドポイントIOC	ioc.apjc.amp.cisco.com	TCP 443
	TETRA 更新サーバ	update.amp.cisco.com	TCP 80 および 443
	OSX クラム定義	defs.amp.sourcefire.com	TCP 80
	高度カスタム検出	カスタムsignatures.apjc.amp.cisco.com	TCP 443
	リモートファイル フェッチ	rff.apjc.amp.cisco.com	TCP 443
Android コネクタ	クラウド上のサーバー	android.apjc.amp.cisco.com	TCP 443
AMP	Cloud アップストリーム サーバ < v2.4	cloud-pc.amp.sourcefire.com	TCP 443 または 32137
	Cloud アップストリーム サーバ	クラウド パソコンest.amp.cisco.com	TCP

	バ > v2.4	クラウド パソコン asn.amp.cisco.com クラウド pc.amp.cisco.com	443 TCP
	Yum サーバ	packages.amp.sourcefire.com packages-v2.amp.sourcefire.com パソコン packages.amp.cisco.com	443 TCP 443 TCP
	サポート セッション	support-sessions.amp.sourcefire.com	443 TCP 22
	クラウド上のサーバー	5.x: クラウド dc.apjc.amp.sourcefire.com 6.x: cloud-sa.apjc.amp.sourcefire.com (静 的な IP)	TCP 443 ま たは 32137
Firesight/Firepower	FireAMP イベント	export.apjc.amp.sourcefire.com	TCP 443
	FireAMP API	api.apjc.amp.sourcefire.com	TCP 443
	ダイナミック分析	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443 TCP
ESA/WSA	ファイル評判	cloud-sa.amp.sourcefire.com (レガシー) cloud-sa.apjc.amp.cisco.com	443 ま たは 32137
Meraki	クラウド上のサーバー	cloud-meraki-asn.apjc.amp.cisco.com (AW IP) cloud-meraki-est.apjc.amp.cisco.com (AW IP)	TCP 443

スタティック IP アドレス

ファイアウォールがポート 443 の発信 TCP 接続をブロックしている場合 (通常はブロックしない)、ポリシーを更新する前にファイアウォール設定を変更する必要があります。アカウントが 2016 年 2 月以降に確立された場合、既に標準ポリシーに書かれている静的な IP アドレスがあります。アカウントが 2016 年 2 月以前に確立された場合、静的な IP アドレスにポリシーの移行を要求するために Cisco Technical Assistance Center (TAC) に連絡できます。

注: オペレーションの継続を確認し、検出する ファイル malware 開封が Firepower Management Center の両方に同じ、プライマリおよびセカンダリ管理センターであることを確認することはこの資料にリストされているサーバにアクセスできなければなりません。

北アメリカの静的な IP アドレス	ヨーロッパの静的な IP アドレス	APJC の静的な IP アドレス
23.23.197.169	46.51.181.139	54.250.127.0
23.23.198.191	46.51.182.195	52.197.2.58
23.23.224.83	46.51.182.202	52.197.22.41
50.16.244.193	46.137.99.242	52.69.16.172
52.0.55.209	52.16.63.115	13.112.137.80
52.2.63.194	52.16.95.58	52.198.208.254
52.2.128.246	52.16.105.95	13.112.162.167
52.3.149.24	52.16.166.193	54.249.244.218
52.3.178.163	52.16.177.94	54.249.246.210

52.3.190.47		54.249.243.85
52.4.98.101	52.16.193.225	54.249.240.219
52.4.151.41	52.16.220.180	54.248.98.94
52.4.245.162	52.17.93.43	176.34.47.0
52.4.246.178	52.17.102.100	52.192.82.189
52.5.92.125	52.17.106.35	52.68.180.106
52.6.103.57	52.17.179.163	52.196.247.47
52.6.197.200	52.17.211.190	52.196.185.158
52.20.14.163	52.17.233.49	52.197.74.4
52.20.123.238	52.18.9.153	52.69.39.127
52.20.141.147	52.18.28.229	54.248.113.224
52.21.52.149	52.18.79.226	54.238.55.12
52.21.117.50	52.18.109.209	54.249.248.16
52.21.134.210	52.18.187.129	52.197.50.93
52.22.64.192	52.18.187.166	52.193.124.132
52.22.156.183	52.18.223.41	52.69.108.228
52.23.13.34	52.19.84.244	52.197.72.147
52.23.16.199	52.19.167.56	52.197.22.165
52.23.73.146	52.30.25.70	52.68.82.200
52.23.87.4	52.30.74.163	52.197.35.73
52.23.107.89	52.30.124.82	52.197.39.251
52.23.134.105	52.30.160.113	52.68.251.104
52.23.140.222	52.30.175.205	54.249.253.42
52.70.11.137	52.30.179.236	54.249.253.65
52.70.13.27	52.30.196.206	176.34.60.211
52.70.35.37	52.30.208.114	52.192.198.119
52.70.47.45	52.30.217.4	52.196.96.41
52.70.56.136	52.30.217.226	54.248.116.199
52.70.58.10	52.30.255.133	52.196.117.29
52.70.59.59	52.31.30.249	52.196.134.7
52.70.59.121	52.31.66.59	176.34.60.30
52.70.60.74	52.31.83.94	52.192.145.214
52.70.61.174	52.31.119.97	52.192.221.107
52.70.61.181	52.31.122.77	52.193.182.191
52.70.61.193	52.31.127.190	52.193.201.169
52.70.63.25	52.31.137.201	52.193.223.43
54.83.45.221	54.195.248.52	52.193.233.17
54.88.208.235	54.195.249.18	52.196.115.166
54.221.210.7	54.217.232.226	52.196.31.86
54.221.255.190	54.217.232.234	52.197.121.237
54.225.226.117	54.217.232.241	52.198.147.230
54.225.227.9	54.217.232.244	52.198.195.125
54.225.227.30	54.217.232.249	52.198.202.24
54.225.227.45	54.228.250.255	52.198.221.53
54.225.227.105	54.246.88.192	52.198.223.169
54.225.228.145	54.247.189.117	52.198.225.221
54.225.228.166	54.74.229.75	52.198.226.104
54.225.228.244	54.74.195.196	52.198.26.36
54.227.247.102	107.21.250.31	52.198.94.104
107.20.158.55	107.21.236.143	52.199.124.11
107.20.203.8	52.2.128.246	52.199.127.80
107.20.229.191	52.18.202.103	52.199.92.142
107.20.234.220	52.18.119.87	52.68.1.146

107.21.212.157
107.21.217.202
107.21.218.60
128.177.8.0/24
174.129.203.65
54.161.128.60
54.234.131.176
52.206.206.244
34.225.208.192
52.22.120.193
34.199.250.32
34.199.238.4
34.194.224.132
34.198.112.150
34.224.236.198
52.20.233.31

54.248.107.84
54.248.109.124
54.248.126.98
54.248.236.127
54.248.236.141
54.248.236.144
54.248.236.151
54.248.237.93
54.249.246.7
54.250.127.131

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)