



# Cisco Elastic Service Controller のインストール引数

ESC インスタンスを起動するには、次の *bootvm.py* スクリプト引数を指定する必要があります。

引数	説明
<code>esc_hostname</code>	ESC VM インスタンスのホスト名を指定します。
<code>--image</code>	ESC インスタンスを起動するために OpenStack Glance で使用されるイメージ ID を指定します。
<code>--boot_volume</code>	ESC インスタンスを起動するブート可能な外部ボリュームのボリューム名または ID を指定します。
<code>--ignore-ssl-errors</code>	「ignoreSslErrors」を「yes」に設定します。信頼できるルート証明書がインストールされていない場合に、開発環境またはテスト環境への展開に役立ちます。
<code>--managers</code>	SNMP トラップが配信される場所のカンマ区切りリストです。次の形式で指定する必要があります。 <code>udp:ipv4/port</code> or <code>udp:[ipv6]/port</code>
<code>--net</code>	ESC が接続する OpenStack 内のネットワーク ID または名前を指定します。
<code>--ipaddr</code>	(任意) ネットワークで ESC に割り当てられる IP アドレスを指定します。  (注) この IP アドレスは、 <code>--net</code> 引数の <code>net_id</code> に対応している必要があります。
<code>--gateway_ip</code>	(任意) ESC のデフォルトゲートウェイの IP アドレスを指定します。

引数	説明
--os_auth_url	(任意) os_auth_url によって認証に使用される OpenStack Keystone の URL を指定します。
--os_username	(任意) os_username によって認証に使用される OpenStack Keystone のユーザ名を指定します。
--os_password	(任意) os_password によって認証に使用される OpenStack Keystone のパスワードを指定します。
--os_tenant_name	(任意) os_tenant_name によって ESC 展開に使用される OpenStack テナント名を指定します。
--bs_os_auth_url	(任意) bs_os_auth_url によって認証に使用される OpenStack Keystone の URL を指定します。
--bs_os_username	(任意) bs_os_username によって認証に使用される OpenStack Keystone のユーザ名を指定します。
--bs_os_password	(任意) bs_os_password によって認証に使用される OpenStack Keystone のパスワードを指定します。
--bs_os_tenant_name	(任意) bs_os_tenant_name によって ESC 展開に使用される OpenStack テナント名を指定します。
--flavor	(任意) ESC VM を起動するための OpenStack フレーバーの ID を指定します。
--security_rules_file	(任意) ESC VM のセキュリティルール (IP、ポートセキュリティ) を定義するファイルを指定します。
--etc_hosts_file	(任意) ESC VM の hosts ファイル (/etc/hosts) にエントリを追加するためのファイルを指定します。
--avail_zone	(任意) ESC 展開に使用される OpenStack ゾーンを指定します。
--esc_params_file	(任意) ESC 展開用のデフォルトパラメータファイルを指定します。
--etsi_params_file	(任意) ESC 展開用の ETSI プロパティファイルを指定します。
--db_volume_id	(任意) ESC HA アクティブ/スタンバイ (ESC-HA アクティブ/スタンバイ) のデータベースストレージにマウントするための Cinder ボリューム ID を指定します。

引数	説明
--ha_node_list	<p>(任意) アクティブ/スタンバイクラスタに含まれる HA アクティブ/スタンバイノードの IP アドレスのリストを指定します。複数のネットワークインターフェイスを持つ ESC ノードの場合、これらの IP は、データ同期に使用されるネットワーク内のアドレスである必要があります。</p> <p>(注) この引数は、レプリケーションベースの HA アクティブ/スタンバイソリューションのみに使用されます。</p>
--kad_vip	<p>(任意) keepalived VIP (仮想 IP) の IP アドレスと keepalived VIP のインターフェイスを指定します (ESC-HA アクティブ/スタンバイ)。</p> <p>VIP のインターフェイスを指定する形式の例として、--kad_vip 192.0.2.1:eth2 や --kad_vip [2001:cc0:2020::fc]:eth2 があります。</p>
--kad_vif	<p>(任意) keepalived 仮想 IP と keepalived VRRP のインターフェイスを指定します (ESC-HA アクティブ/スタンバイ)。VIP インターフェイスが引数 <i>kad_vip</i> を使用してすでに指定されている場合は、引数 --kad_vif を使用して keepalived VRRP のインターフェイスのみを指定することもできます。</p>
--kad_vri	<p>VRRP インスタンスの仮想ルータ ID を指定します。kad_vri に指定できる値は 0 ~ 254 です。同じ HA アクティブ/スタンバイ内の ESC VM は、同じ kad_vri 番号を使用する必要があります。L3 HA アクティブ/スタンバイに kad_vip が使用されない場合は、kad_vir を使用する必要があります。それ以外の場合は、kad_vri 引数を省略できます。</p>
--route	ESC VM のルーティング設定を指定します。
--ntp_server	(任意) NTP サーバのアドレスを指定します。
--rsyslog_server	(任意) ESC がログを送信する rsyslog サーバの IP アドレスを指定します。
--rsyslog_server_port	(任意) ESC がログを送信する rsyslog サーバのポートを指定します。
--rsyslog_server_protocol	(任意) サーバにログを転送するために ESC によって使用されるプロトコルを指定します。

引数	説明
--secure	(任意) セキュリティの設定を有効にします。次の値を指定できます。 <ul style="list-style-type: none"><li>• <b>A</b> : root が完全にロックアウトされます。コンソールからでも root としてログインすることはできません。</li><li>• <b>B</b> : SELinux が強制モードで実行されます。</li><li>• <b>C</b> : IPv4/IPv6 テーブルが開始されます。</li><li>• <b>D</b> : SSH パスワード認証が無効になります。ESC VM に SSH でログインするには、秘密キーが必要です。</li><li>• <b>E</b> : confd のホストキーが再作成されます。</li></ul>
--host_mapping_file	(任意) VNF 展開用のホストマッピングファイルを指定します。
--version	(任意) bootvm.py のバージョンを出力して終了します。
--rng_virtio	RNG Virtio デバイスを使用した Libvirt/KVM での ESC VM のインストールと展開を有効にします。デフォルト値は次のとおりです。device=/dev/random rate_period=1000 rate_bytes=1024

引数	説明
--user_pass	

引数	説明
	<p>--user_confid_pass とともに、3.0 以降に必須の引数です。</p> <p>この引数により、ESC VM にアクセスするユーザが追加されます。管理者権限を持たないユーザ（非管理者/非 root ユーザ）を指定するには、この引数を使用します。user_name: password の形式を使用します。Linux（SSH/コンソールアクセス）用の管理者アカウントを作成するには、bootvm.py コマンドに少なくとも 1 つの user_pass 引数を含めることが必要です。必須のユーザクレデンシャル引数の構文は、次のとおりです。</p> <pre>--user_pass admin:'PASSWORD-OR-HASH'[:OPTIONAL-PUBLIC-KEY-FILE][:OPTIONAL-ROLE]</pre> <p>このユーザは次の操作のみを実行できます。</p> <ul style="list-style-type: none"> <li>• SSH を使用して ESC にログインする。</li> <li>• Netconf CLI (esc_nc_cli、netconf-console など) にアクセスして操作する。</li> <li>• /var/logs/esc から ESC 関連ログを読み取る。</li> <li>• ローカルホスト経由で REST インターフェイスにアクセスする。</li> </ul> <p>このユーザは次の操作を実行できません。</p> <ul style="list-style-type: none"> <li>• ESC DB にアクセスし、ESC システムを再設定する。</li> <li>• システムレベルのログにアクセスする。</li> <li>• rsyslog、keepalived、DRDB などのシステムレベルのコンポーネントを設定する。</li> <li>• 暗号化キーと、REST インターフェイスまたは ESC ログからの値にアクセスする。</li> </ul> <p>次に、管理者アカウント用の --user_pass と、より強力なクリアテキストパスワードの例を示します。シェルの予約済み文字との競合を回避するには、引用符を使用します。</p> <pre>-user_pass admin:'Strong4Security!'</pre> <p>ESC をインストールする別の方法として、両方の管理者アカウントにパスワードハッシュを使用する例を示します。シェルの予約済み文字との競合を回避するには、引用符を使用します。</p> <pre>--user_pass admin:'\$algorithm\$salt\$hash-of-salt-password'</pre> <p>ESC 2.1 以降では、この属性の公開キーが受け入れられます。たとえば、次の例では、ユーザ「admin」のパスワードとして「admin321」が生成され、キーファイルとして /tmp/abc.pub を使用して公開キーが挿入されます。</p>

引数	説明
	<pre>--user_pass admin:admin321:/tmp/abc.pub</pre>
--user_confid_pass	<p>confd ユーザを変更するために使用されます。ConfD (netconf/cli アクセス) 用の管理者アカウントを作成するには、bootvm.py コマンドに少なくとも 1 つの user_confid_pass を含めることが必要です。必須のユーザクレデンシャル引数の構文は、次のとおりです。</p> <pre>--user_confid_pass admin:'PASSWORD-OR-HASH'[:OPTIONAL-PUBLIC-KEY-FILE]</pre> <p>次に、管理者アカウント用の --user_confid_pass と、より強力なクリアテキストパスワードの例を示します。シェルの予約済み文字との競合を回避するには、引用符を使用します。</p> <pre>--user_confid_pass:'Strong4Security!'</pre> <p>ESC をインストールする別の方法として、両方の管理者アカウントにパスワードハッシュを使用する例を示します。シェルの予約済み文字との競合を回避するには、引用符を使用します。</p> <pre>--user_confid_pass:'\$algorithm\$salt\$hash-of-salt-password'</pre> <p>ESC 2.1 以降では、この属性の公開キーが受け入れられます。たとえば、次の例では、ユーザ「admin」のパスワードとして「admin321」が生成され、キーファイルとして /tmp/abc.pub を使用して公開キーが挿入されます。--user_confid_pass:admin321:/tmp/abc.pub</p>
--esc_portal_startup	(任意) ESC ポータルを開始します。
--log	(任意) ログファイルを指定します。デフォルトでは、stdout にログが記録されます。
--esc_monitor_check_ips	(任意) esc_monitor によってモニタする必要がある IP アドレスを指定します (HA アクティブ/スタンバイフェールオーバーの場合)。
--enable-https-rest	(任意) 作成された ESC VM のセキュアな REST インターフェイスを有効にします。
--enable-http-rest	(任意) 作成された ESC VM の非セキュアな REST インターフェイスを有効にします。
--disable-rest-auth	<p>(任意) REST API 認証を無効にします。</p> <p>(注) 実稼働環境で REST 認証を無効にすることはできません。</p>

引数	説明
--enable-snmp-agent	(任意) SNMPサービスの自動起動を有効にします。デフォルト値は [いいえ (False) ] です。
--ha_mode	HA アクティブ/スタンバイインストールのための ESC HA アクティブ/スタンバイモードを指定します。HA アクティブ/スタンバイで使用可能な次のオプションのいずれかを指定します。 <b>no_ha</b> : HA なし、 <b>cinder</b> : 共有 Cinder ボリューム、 <b>drbd</b> : 組み込み DRBD、 <b>drbd_on_cinder</b> : Cinder ボリュームによる DRBD
--enable-https-etsi	(任意) 作成された ESC VM 用のセキュアな ETSI REST インターフェイスを有効にします。
--enable-http-etsi	(任意) 作成された ESC VM 用の非セキュアな ETSI REST インターフェイスを有効にします。実稼働環境でこのインターフェイスを有効にすることは推奨されません。
--encrypt_key	暗号用のキーを指定します。
--proxy	特定のポートでプロキシを使用します。
--noproxy	プロキシを使用しないホストを一覧表示します。
--kad_unicast_src_ip	ユニキャストの送信元 IP アドレスを指定します。これは ESC VM がユニキャスト (L3) VRRP 通信に使用するインターフェイスの IP アドレスです。 例 : --kad_unicast_src_ip 10.0.0.1
--kad_unicast_peer	ユニキャストのピア IP アドレスを指定します。これは ESC ピア VM がユニキャスト (L3) VRRP 通信に使用するインターフェイスの IP アドレスです。 例 : --kad_unicast_peer 10.0.0.1



引数	説明
--placement_hint	<p>この引数と、サーバグループ、samehost、differenthost フィルタを使用して、ESCHA アクティブ/スタンバイ仮想マシンの配置を指定します。</p> <p>例 :</p> <ul style="list-style-type: none"> <li>• --placement_hint different_host=2b299428-e7a7-4528-8566-9a4970183c6a (ID は VM UUID である必要があります)</li> <li>• --placement_hint same_host=2b299428-e7a7-4528-8566-9a4970183c6a (ID は VM UUID である必要があります)</li> <li>• --placement_hint group=4c7758ab-e9cb-4cf0-8f02-344ec666365b (ID はサーバグループ UUID である必要があります)</li> </ul>
--format {json}	<p>この引数を使用して、出力内の成功および障害メッセージをキャプチャします。</p> <p>例 : <code>\$. /bootvm.py --image ESC-2_3_0_8 --net network --format json --test-0</code></p> <pre>{ "status" : "Success", "vm_uuid" : "UUID" }</pre>
--user_rest_pass	REST API にアクセスするユーザを追加します。形式は <code>username: password</code> です。このオプションは繰り返し指定できます。
--user_portal_pass	ポータルユーザを追加します。形式は <code>username: password</code> です。このオプションは繰り返し指定できます。
--user_etsi_pass	ETSI REST API にアクセスするユーザを追加します。形式は <code>username:password</code> です。指定できるユーザは1人だけです。
--etsi_oauth2_pass	ETSI REST API にアクセスするための OAuth2 クライアントを追加します。Format <code>clientId:clientSecret</code> 。このオプションは繰り返し指定できます。

引数	説明
--no_vim_credentials	<p>VIM ログイン情報を渡さずに ESC を展開するには、この引数を使用します。この引数を使用すると、次のパラメータはインストール中に渡されません。</p> <ul style="list-style-type: none"> <li>• --os_auth_url</li> <li>• --os_username</li> <li>• --os_password</li> <li>• --os_tenant_name</li> </ul> <p>展開が完了した後、ユーザは、ESC の VIM/VIM ユーザ API (REST/Netconf) を使用して、これらの VIM ログイン情報を設定できます。REST API および Netconf を使用した設定の詳細については、「インストール後のタスク」の章にある「ESC インストール後の VIM ログイン情報の設定」を参照してください。</p>

### Cisco Elastic Service Controller インストーラファイルの参照

ファイル	説明
security_rules_file	<p>このファイルには次のものが含まれています。</p> <ul style="list-style-type: none"> <li>• テナントのセキュリティグループを作成するためのセキュリティルール。</li> <li>• テナントへのトラフィックを許可する設定。</li> </ul>
etc_hosts_file	<p>このファイルには、/etc/hosts ファイルに追加する 1 つ以上のエントリが含まれています。</p>
esc_params_file	<p>このファイルには、ESC のさまざまなパラメータを設定するための情報が含まれています。esc_params_file で設定できるパラメータの詳細については、下の表で説明します。</p>
host_mapping_file	<p>このファイルには、ホストに基づいてネットワークをマッピングするための情報が含まれています。</p>

### ESC 設定パラメータ

このファイルを使用して、インストール時にさまざまな ESC パラメータを設定できます。設定可能なパラメータを表に示します。

このファイルを使用した設定の例を次に示します。

```
openstack.endpoint=adminURL
affinity.filter=ServerGroupAffinity
```

表 1: ESC 設定パラメータ

esc_param.conf	タイプ	デフォルト値	説明
default.vm_recovery_retries_max	数値	3	許容されるリカバリの試行回数 (VMあたり)。
openstack.endpoint	文字列	publicURL	<p>ESC の keystone エンドポイント値を設定するパラメータ。オプション: adminURL、publicURL</p> <p>CLI または REST サービスを使用して、デフォルト値を変更できます。</p> <p>CLI を使用:</p> <pre>\$ sudo escadm escmanager config set --key openstack.endpoint --value publicURL { "category": "OPENSTACK", "type": "STRING", "value": "publicURL", "key": "ENDPOINT" }</pre> <p>REST を使用:</p> <pre>\$ curl -X PUT http://172.16.0.1:8080/ESCManager/v0/config/openstack/endpoint/publicURL</pre>
log_level	文字列	INFO	ロギングのレベル。オプション: INFO、Trace、DEBUG
affinity.filter	文字列	SameHostFilter	<p>PolicyEngine を構築し、VM ポリシーテーブルを初期化するために使用される定数文字列。</p> <p>オプション: SameHostFilter、ServerGroupAffinity</p>
anti_affinity.filter	文字列	DifferentHostFilter	<p>PolicyEngine を構築し、VM ポリシーテーブルを初期化するために使用される定数文字列。</p> <p>オプション: DifferentHostFilter</p>



- (注) ESC の場合、ESC ポリシーエンジンに対してデフォルトで SameHostFilter と DifferentHostFilter が使用されますが、OpenStack の場合、デフォルトではこれらのフィルタが設定されないことがあります。その場合、OpenStack の nova サービスの /etc/nova/nova.conf ファイルにある次のスケジューラオプションに、SameHostFilter と DifferentHostFilter を追加する必要があります。

```
scheduler_default_filters = RetryFilter, AvailabilityZoneFilter, RamFilter, ComputeFilter,
ComputeCapabilitiesFilter,
ImagePropertiesFilter, ServerGroupAntiAffinityFilter, ServerGroupAffinityFilter,
DifferentHostFilter, SameHostFilter
```

## OpenStack 用の ServerGroupAntiAffinityFilter

ESC は、OpenStack 用の ServerGroupAntiAffinityFilter の使用に対応できます。

### REST

```
PUThttp://localhost:8080/ESCManager/v0/config/anti_affinity/filter/ServerGroupAntiAffinity
```

```
PUThttp://localhost:8080/ESCManager/v0/config/affinity/filter/ServerGroupAffinity
```

### CLI

```
sudo escadm escmanager config set --key ANTI_AFFINITY.FILTER --value
ServerGroupAntiAffinity
sudo escadm escmanager config set --key AFFINITY.FILTER --value ServerGroupAffinity
```

### 重要なポイント

OpenStack の ServerGroupAntiAffinityFilter は、inter-dep anti-affinit、scaling の使用や、servergroup とデフォルトフィルタ (samehost/differenthost) の混合使用をサポートしていません。

ServerGroupAntiAffinity フィルタを使用している場合、VM グループ内での配置は許可されません。VM ベースの配置ポリシーには <placement\_group> のみを使用できます。vm\_group ごとに 1 つの VM を使用できます。2 つの異なる placement\_group に単一の VM グループを追加することはできません。

## ESC サービス、ポート、およびセキュリティグループの概要

表 2: 外部サービス (External Services)

	サービス	カンファレンスの公開/非公開 (Visibility)	任意かどうか	インターフェイス	プロトコル	ポート
1	sshd	外部 (オーケストレーション)	いいえ	0.0.0.0	TCP	22
2	ESC Web UI/ポータル (HTTPS)	外部 (オーケストレーション)	はい (代わりに REST および/または Netconf を使用可)	0.0.0.0	TCP	443 (以前は 9001)
3	ESC Netconf API	外部 (オーケストレーション)	はい (代わりに REST および/またはポータルを使用可)	0.0.0.0	TCP	830

	サービス	カンファレンスの公開/非公開 (Visibility)	任意かどうか	インターフェイス	プロトコル	ポート
4	ESC SNMP	外部 (オーケストレーション)	はい (カスタムユーザデータ/esc-config.yamlのみで設定可能)	0.0.0.0	TCP	2001
5	ESC DRBD (HA アクティブ/スタンバイレプリケーション)	外部 (オーケストレーション)	いいえ。HA アクティブ/スタンバイの設定に必要。	0.0.0.0	TCP	7789
6	ESC ConfD CLI	External	○ esc_product_confid.conf を変更してリロードすることで設定可能	0.0.0.0	SSH	2024
7	ESC REST API (HTTPS)	外部 (オーケストレーション)	はい (代わりにポータルおよび/または Netconf を使用可)	0.0.0.0	TCP	8443
8	ESC Keepalived	外部 (オーケストレーション)	いいえ。HA アクティブ/スタンバイの設定に必要。	0.0.0.0	マルチキャスト VRRP	該当なし
9	ETSI-VNFM (HTTP)	外部	はい (etsi-productionproperties を使用して設定可)	0.0.0.0	TCP	8250
10	ETSI-VNFM (HTTPS)	外部	はい (etsi-productionproperties を使用して設定可)	0.0.0.0	TCP	8251
11	ETSI-VNFM (Prometheus)	外部	はい (etsi-productionproperties を使用して設定可)	0.0.0.0	TCP	8252

	サービス	カンファレンスの公開/非公開 (Visibility)	任意かどうか	インターフェイス	プロトコル	ポート
12	ETSI-VNFM (アーティファクトのダウンロード用の追加の HTTPS ポート)	外部	はい ( <code>etsi-production-properties</code> を使用して設定可)	0.0.0.0	TCP	8253
13	ESC ヘルス API	外部 (オーケストレーション)	いいえ	0.0.0.0	TCP	ESC 5.2 以降の場合、8060 ESC 5.1 以前の場合、60000
14	ETSI Health API	内線				Local のみ
15	D-MONA REST API	外部	いいえ	0.0.0.0	TCP	8443
16	Consul サービス <a href="#">1</a>	外部	いいえ	0.0.0.0	TCP	8300、8301、8302
17	Consul サービス <a href="#">2</a>		いいえ	0.0.0.0	TCP および UDP	8301 8302 8600
18	ConfD	外部 <a href="#">3</a>	A/A セットの場合 はいいいえ	ESC ノード IP に限定 <a href="#">4</a>	TCP	4565
19	PostgreSQL	外部 <a href="#">5</a>	A/A セットの場合 はいいいえ	ESC ノード IP に限定 <a href="#">6</a>	TCP	7878
20	ESCManager RMI レジストリ <a href="#">7</a>	外部	A/A セットの場合 はいいいえ	ESC ノード IP に限定	TCP	8679

	サービス	カンファレンスの公開/非公開 (Visibility)	任意かどうか	インターフェイス	プロトコル	ポート
21	ESCManager RMI サービス <sup>8</sup>	外部	A/A セットの場合はいいえ	ESC ノード IP に限定	TCP	8680
22	ESCManager Prometheus メトリック	外部 <sup>9</sup>	はい (application.properties)	0.0.0.0	TCP	8088
23	MONA Prometheus	外部 <sup>10</sup>	はい (application.properties)	0.0.0.0	TCP	8092
24	VIMManager Prometheus メトリック	外部 <sup>11</sup>	はい (application.properties)	0.0.0.0	TCP	8097
25	DHCP	外部  DHCP は、ESC インターフェイスの IP アドレスの解決に限定されます。	いいえ	0.0.0.0	UDP	66、67

<sup>1</sup> A/A ESC セットのみが必要です。それ以外の場合、ポートはリッスンしません。

<sup>2</sup> A/A ESC セットのみが必要です。それ以外の場合、ポートはリッスンしません。

<sup>3</sup> ESC 5.0 以降のみに導入

<sup>4</sup> ESC A/A セット (3 VM)

<sup>5</sup> ESC 5.0 以降のみに導入

<sup>6</sup> ESC A/A セット (3 VM)

<sup>7</sup> A/A ESC セットのみが必要です。それ以外の場合、ポートはリッスンされません。

<sup>8</sup> A/A ESC セットのみが必要です。それ以外の場合、ポートはリッスンされません。

<sup>9</sup> ESC 5.2 以降

<sup>10</sup> ESC 5.2 以降

<sup>11</sup> ESC 5.2 以降

