

属性ベースのアクセス制御

属性は設定で使用するカスタマイズされたネットワーク オブジェクトです。Cisco ASA 設定で、VMware vCenter の管理対象 VMware ESXi 環境の 1 つ以上の仮想マシンに関連付けられるトラフィックをフィルタリングするために、属性を定義し使用できます。属性により、1 つ以上の属性を共有する仮想マシンのグループからのトラフィックにポリシーを割り当てるアクセス コントロール リスト（ACL）を定義することができます。ESXi 環境内の仮想マシンに属性を割り当て、HTTPS を使用して vCenter または 1 つの ESXi ホストに接続する、属性エージェントを設定します。エージェントは、仮想マシンのプライマリ IP アドレスに特定の属性に関連する 1 つ以上のバインディングを要求および取得します。

属性ベースのアクセス制御は、すべてのハードウェア プラットフォームと、ESXi、KVM または HyperV ハイパーバイザで動作するすべてASA 仮想のプラットフォームでサポートされます。属性は、ESXi ハイパーバイザ上で動作する仮想マシンからのみ取得できます。

- 属性ベースのネットワーク オブジェクトのガイドライン （1 ページ）
- 属性ベースのアクセス制御の設定 （2 ページ）
- 属性ベースのネットワーク オブジェクトのモニタリング （10 ページ）
- 属性ベースのアクセス制御の履歴 （11 ページ）

属性ベースのネットワークオブジェクトのガイドライン

IPv6 のガイドライン

- IPv6 アドレスは、vCenter では、ホストのクレデンシャルとしてサポートされていません。
- IPv6 は、仮想マシンのプライマリ IP アドレスが IPv6 アドレスである仮想マシンのバインドでサポートされます。

その他のガイドラインと制限事項

- マルチ コンテキスト モードはサポートされません。属性ベースのネットワーク オブジェクトは、シングルモード コンテキストでのみサポートされます。

- 属性ベースのネットワーク オブジェクトは、仮想マシンのプライマリ アドレスへのバインドのみをサポートします。単一の仮想マシン上の複数の vNIC へのバインドはサポートされません。
- 属性ベースのネットワーク オブジェクトは、アクセス グループに使用するオブジェクトにのみ設定できます。その他の機能（NAT など）のためのネットワーク オブジェクトはサポートされません。
- vCenter にプライマリ IP アドレスを報告するためには、仮想マシンが VMware ツールを実行している必要があります。属性の変更は、vCenter が仮想マシンの IP アドレスを知っている場合でないと、ASA には通知されません。これは、vCenter の制約事項です。
- 属性ベースのネットワーク オブジェクトは、Amazon Web Services（AWS）または Microsoft Azure のパブリック クラウド環境ではサポートされません。

属性ベースのアクセス制御の設定

次の手順は、VMware ESXi 環境内の管理対象の仮想マシン上で属性ベースのアクセス制御を実行するための一般的な流れを説明します。

手順

ステップ 1 管理対象の仮想マシンにカスタムの属性タイプと値を割り当てます。vCenter 仮想マシンの属性の設定 （2 ページ）を参照してください。

ステップ 2 vCenter サーバーまたは ESXi ホストに接続するための属性エージェントを設定します。VM 属性エージェントの設定 （4 ページ）を参照してください。

ステップ 3 展開スキームに必要な属性ベースのネットワーク オブジェクトを設定します。属性ベースのネットワーク オブジェクトの設定 （6 ページ）を参照してください。

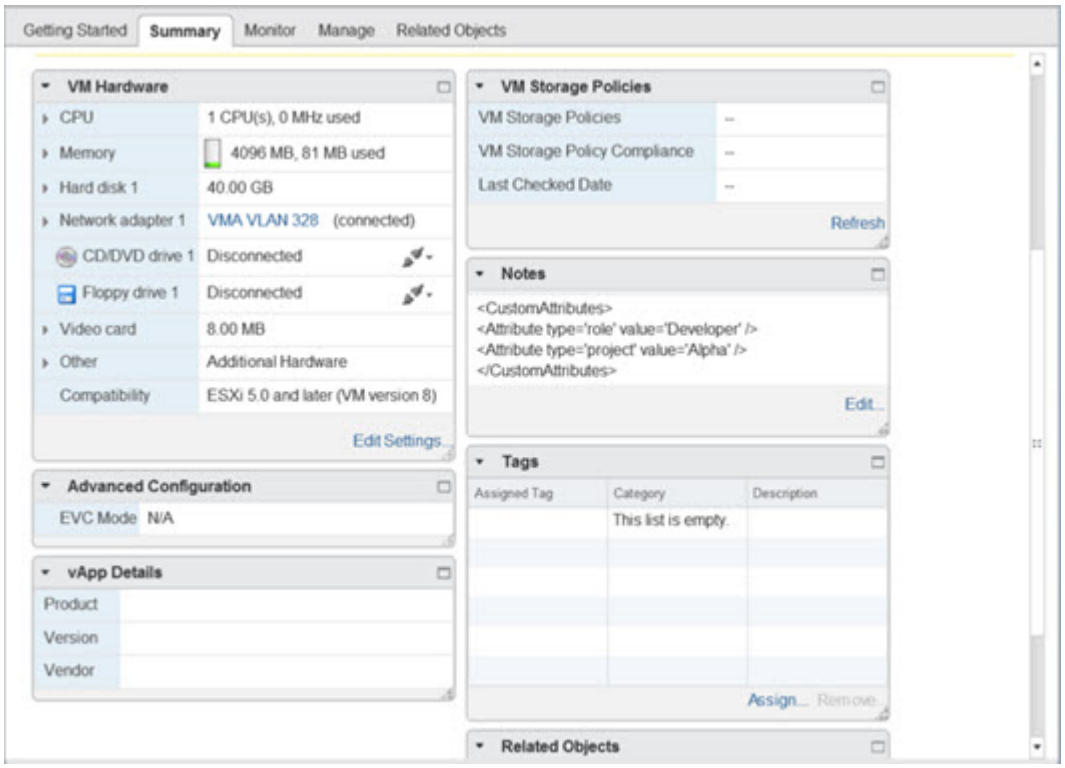
ステップ 4 アクセス コントロール リストとルールを設定します。属性ベースのネットワーク オブジェクトを使用したアクセス制御の設定 （8 ページ）を参照してください。

vCenter 仮想マシンの属性の設定

仮想マシンにカスタムの属性タイプと値を割り当て、それらの属性をネットワーク オブジェクトに関連付けます。すると、これらの属性ベースのネットワーク オブジェクトを使用して、共通のユーザー定義の特徴を持つ一連の仮想マシンに ACL を適用することができます。たとえば、開発者が構築したマシンをテストマシンから隔離したり、仮想マシンをプロジェクトおよび/または場所でグループ化したりすることができます。ASA が属性を使用して仮想マシンをモニターできるようにするには、vCenter が管理対象の仮想マシンから属性を取得できるようにする必要があります。そうするには、vCenter の仮想マシンの [Summary] ページにある [Notes] フィールドにフォーマットされたテキスト ファイルを挿入します。

[Notes] フィールドについては、次の図を参照してください。

図 *1 : vCenter* の仮想マシンの *[Summary]* タブ



カスタム属性を指定するには、適切にフォーマットした XML ファイルを仮想マシンの [Notes] フィールドにコピーします。ファイルの形式は次のとおりです。

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

上記の 2 行目を繰り返すと、単一の仮想マシンに複数の属性を定義することができます。各行には、一意の属性タイプを 1 つしか指定できないことに注意が必要です。同じ属性タイプを複数の属性値で定義すると、その都度、当該の属性タイプのバインドアップデートにより、その前の値が上書きされます。

文字列の属性値については、オブジェクト定義に関連付けられている値は、仮想マシンから vCenter に報告される値と完全に一致している必要があります。たとえば、属性値 *Build Machine* は、仮想マシンのアノテーション値である *build machine* には一致しません。この属性については、host-map にバインドが追加されることはありません。

1 つのファイルで固有の属性タイプを複数定義することができます。

手順

ステップ 1 vCenter インベントリから仮想マシンを選択します。

ステップ 2 その仮想マシンの [Summary] タブをクリックします。

ステップ 3 [Notes] フィールドで、[Edit] リンクをクリックします。

ステップ 4 [Edit Notes] ボックスにカスタム属性のテキスト ファイルを貼り付けます。テキスト ファイルは、XML テンプレートのフォーマットに従っている必要があります。

例：

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

ステップ 5 [OK] をクリックします。

例

次の例は、「role」および「project」に対してカスタム属性を定義する、仮想マシンへの適用が可能な適切にフォーマットされた XML テキスト ファイルを示します。

```
<CustomAttributes>
<Attribute type='role' value='Developer'/>
<Attribute type='project' value='Alpha'/>
</CustomAttributes>
```

VM 属性エージェントの設定

vCenter または単一の ESXi ホストと通信するため、VM の属性のエージェントを設定します。VMware 環境内の仮想マシンに属性が割り当てられると、属性エージェントは、どの属性が設定されたかを示すメッセージを vCenter に送信し、vCenter は、一致する属性タイプが設定されているすべての仮想マシンに関するバインド アップデートで応答します。

VM 属性エージェントと vCenter は、バインド アップデートの交換を次のように行います。

- エージェントが新しい属性タイプを含むリクエストを発行すると、vCenter は、その属性タイプが設定されているすべての仮想マシンに関するバインド アップデートで応答します。これ以降、属性値が追加または変更されると、vCenter のみが新しいバインドを発行します。
- モニター対象の属性が 1 つ以上の仮想マシン上で変更されると、バインド アップデート メッセージが受信されます。各バインド メッセージは、属性値を報告する仮想マシンの IP アドレスによって識別されます。

- 複数の属性が 1 つのエージェントによってモニターされている場合、1 件のバインドアップデートに各仮想マシンのすべてのモニター対象属性の現在の値が含まれます。
- エージェントによってモニターされている特定の属性が、ある仮想マシンには設定されていない場合、その仮想マシンについては、バインドには空の属性値が含まれます。
- ある仮想マシンにモニター対象の属性がまったく設定されていない場合、vCenter はバインドアップデートを送信しません。

各属性エージェントは、1 つの vCenter または ESXi ホストとだけ通信します。1 つの ASA には複数の属性エージェントを定義でき、それぞれを異なる vCenter と通信させるか、または複数の属性エージェントを同じ vCenter と通信させることができます。

手順

ステップ 1 vCenter と通信するための VM 属性エージェントを作成します。**attribute source-group** *agent-name* **type** *agent-type*

例：

```
hostname(config)# attribute source-group VMAgent type esxi
```

agent-name 引数は、VM 属性エージェントの名前を指定します。*type* 引数は、属性エージェントのタイプです。

（注） 現在、サポートされるエージェント タイプは ESXi のみです。

ステップ 2 vCenter ホスト クレデンシャルを設定します。**host** *ip-address* **username** *ESXi-username* **password** *ESXi-password*

例：

```
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

ステップ 3 vCenter 通信のキープアライブ設定を設定します：**keepalive retry-interval** *interval* **retry-count** *count*

例：

```
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

デフォルトのキープアライブ タイマー値は、30 秒間隔での再試行 3 回です。

ステップ 4 VM 属性エージェント設定を確認します。**show attribute source-group** *agent-name*

例：

```
hostname(config-attr)# sh attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Inactive
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
```

[Agent State] は、ネットワーク オブジェクトを設定し、そのオブジェクトと関連付けするための属性を指定するまでアクティブになりません。

ステップ 5 属性コンフィギュレーション モードを終了します。 **exit**

例：

```
hostname(config-attr)# exit
```

属性ベースのネットワーク オブジェクトの設定

属性ベースのネットワーク オブジェクトは、VMware ESXi 環境内の 1 つ以上の仮想マシンに関連付けられている属性に応じてトラフィックをフィルタリングします。アクセス コントロール リスト（ACL）を定義すれば、1 つ以上の属性を共有する仮想マシン グループからのトラフィックにポリシーを指定できます。

たとえば、*engineering* 属性を持つマシンに対して *eng_lab* 属性を持つマシンへのアクセスを許可するアクセス ルールを設定できます。ネットワーク管理者がエンジニアリング マシンとラボ サーバーを追加・削除できる一方で、セキュリティ管理者によって管理されるセキュリティ ポリシーは、アクセス ルールを手動で更新しなくても自動的に適用され続けます。

手順

ステップ 1 オブジェクト グループの検索を有効にします。 **object-group-search access-control**

例：

```
hostname(config)# object-group-search access-control
```

属性ベースのネットワーク オブジェクトを設定するには、object-group-search を有効にする必要があります。

ステップ 2 オブジェクト名を使用して、属性ベースのネットワーク オブジェクトを作成または編集します。**object network** *object-id*

例：

```
hostname(config)# object network dev
```

ステップ 3 オブジェクトに関連付けるエージェント、属性タイプ、および属性値を指定します。**attribute** *agent-name attribute-type attribute-value*

例：

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

agent-name は、VM 属性エージェントを指定します。<XREF> を参照してください。設定されていない属性エージェントを使用するように属性ベースのネットワーク オブジェクトを設定した場合、クレデンシャルがなく、デフォルトのキープアライブ値を持つプレースホルダ エージェントが自動的に作成されます。このエージェントは、**host** サブコマンドを使用してホスト クレデンシャルが与えられるまで、「クレデンシャル使用不可」の状態が続きます。

また、*attribute-type* と *attribute-value* のペアは、一意の属性を定義します。*attribute-type* は任意の文字列で、**custom.** というプレフィックスが含まれている必要があります。同じ属性タイプを複数の属性値で複数回定義すると、最後に定義された値でその前の値が上書きされます。

例

次の例では、開発者グループを表し、「Developer」というロールを持つ属性ベースのネットワーク オブジェクト、*dev* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.role* という属性に一致するすべての仮想マシンにバインドを返します。

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

次の例では、テスト グループを表し、「Automation」というロールを持つ属性ベースのネットワーク オブジェクト、*test* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.role* という属性に一致するすべての仮想マシンのバインドを返します。これは、前述の例と同じ仮想マシンのリストであることに注意してください。

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

次の例では、プロジェクト グループを表し、「Alpha」というロールを持つ属性ベースのネットワーク オブジェクト、*project* を作成しています。VM 属性エージェントは vCenter と通信し、*custom.project* という属性に一致するすべての仮想マシンのバインドを返します。一部のマシンに複数の属性が重複していることに注意してください。

```
hostname(config)# object network project
```

```
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

次の例は、アクティブな状態で属性リクエストが保留中の VM 属性エージェントを示します。

```
hostname(config-attr)# show attribute source-group VMAgent

   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attribute requests pending:
       'custom.project'
       'custom.role'
```

属性ベースのネットワークオブジェクトを使用したアクセス制御の設定

属性ベースのネットワーク オブジェクトは、1つ以上の属性を共有する仮想マシンのグループからのトラフィックに対してアクセス コントロール リスト（ACL）を定義するときに使用できます。アクセス リストは、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。ACE はアクセス リストの単一エントリで、ルールの許可または拒否（パケットの転送またはドロップ）を指定します。通常、許可または拒否ルールの適用対象は、プロトコル、送信元および宛先の IP アドレスまたはネットワークで、必要に応じて送信元および宛先ポートに適用されます。

属性ベースのネットワーク オブジェクトを使用すると、送信元または宛先の IP アドレスをこれらのオブジェクトに置き換えることができます。仮想マシンが導入、移動、または廃止されると、仮想マシン上の属性は更新されますが、割り当てられたアクセス制御ポリシーは、設定を変更しなくても効果を継続できます。

ACL に使用可能なすべてのオプションについては、ACL の設定を参照してください。

手順

ステップ 1 属性ベースのネットワーク オブジェクトを使用して、拡張 ACL エントリ（ACE）を作成および設定します。**access-list** *access_list_name* **extended** {**deny | permit**} *protocol_argument* **object** *source_object_name* **object** *dest_object_name*

例：

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

（注） ポリシーに必要なだけ繰り返します。

次のオプションがあります。

- *access_list_name*：新規または既存の ACL の名前。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- プロトコル：*protocol_argument* では、IP プロトコルを指定します。
  - *name* または *number*：プロトコルの名前または番号を指定します。**ip** を指定すると、すべてのプロトコルに適用されます。
  - **object-group** *protocol_grp_id*：**object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。
- 送信元オブジェクト：**object** には、**object network** コマンドを使用して作成された属性ベースのネットワーク オブジェクトを指定します。*source_object_name* には、パケットの送信元オブジェクトを指定します。
- 宛先オブジェクト：**object** には、**object network** コマンドを使用して作成された属性ベースのネットワーク オブジェクトを指定します。*dest_object_name* には、パケットの送信先オブジェクトを指定します。

ステップ 2 ACL を 1 つのインターフェイスにバインドするか、グローバルに適用します。**access-group** *access_list_name* {**in interface** *interface_name* | **global**}

例：

```
hostname(config)# access-group lab-access in interface inside
```

インターフェイス固有のアクセス グループの場合は、次の手順を実行します。

- 拡張 ACL 名を指定します。インターフェイスごとの ACL タイプごとに 1 つの **access-group** コマンドを設定できます。
- **in** キーワードによって、ACL が着信トラフィックに適用されます。
- **interface** 名を指定します。

グローバル アクセス グループの場合は、global キーワードを指定して、すべてのインターフェイスの着信方向に拡張 ACL を適用します。

例

次の例では、属性ベースの拡張 ACL をグローバルに適用する方法を示します。

```
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0)
0x64a1be76
  access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0)
 0x64a1be76
```

属性ベースのネットワークオブジェクトのモニタリング

属性ベースのネットワーク オブジェクトをモニターするには、次のコマンドを入力します。

- **show attribute host-map**

  指定された属性のエージェント、タイプ、および値に関する属性バインドを表示します。

- **show attribute object-map**

  object-to-attribute バインドを表示します。

- **show attribute source-group**

  設定された VM 属性エージェントが表示されます。

例

次に、host-to-attribute バインドのマップの例を示します。

```
hostname# show attribute host-map /all
IP Address-Attribute Bindings Information

          Source/Attribute                          Value
=========================================================================
VMAgent.custom.project                          'Alpha'
     10.15.28.34
     10.15.28.32
     10.15.28.31
     10.15.28.33
VMAgent.custom.role                             'Automation'
     10.15.27.133
     10.15.27.135
     10.15.27.134
VMAgent.custom.role                             'Developer'
     10.15.28.34
     10.15.28.12
```

```
     10.15.28.31
     10.15.28.13
```

次に、object-to-attribute バインドのマップの例を示します。

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information

Object
         Source/Attribute                          Value
=========================================================================
dev
     VMAgent.custom.role                            'Developer'
test
     VMAgent.custom.role                            'Automation'
project
     VMAgent.custom.project                         'Alpha'
```

次に、属性エージェントの設定例を示します。

```
hostname# show attribute source-group
   Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
      'custom.role' (2)
```

属性ベースのアクセス制御の履歴

機能名	プラットフォームリリース	説明
属性ベースのネットワーク オブジェクトのサポート	9.7.(1)	現在、ネットワーク アクセスの制御には、IP アドレス、プロトコル、ポートなどの従来のネットワーク特性に加え、仮想マシンの属性も使用することができます。仮想マシンは、VMware ESXi 環境に存在している必要があります。 次のコマンドを導入しました。 **object network** *attribute* **attribute** *agent-name attribute-type attribute-value* **attribute source-group** *agent-name* **type** *agent-type* **host** *ip-address* **username** *ESXi-username* **password** *ESXi-password* **keepalive retry-interval** *interval* **retry-count** *count*

機能名	プラットフォームリリース	説明
ASA 5506-X（全モデル）、5508-X、5512-X、5516-X から VM 属性ベースのネットワークオブジェクトのサポートを除外します。	9.10(1)	ASA 5506-X（全モデル）、5508-X、5512-X、5516-X プラットフォームでは、VM 属性ベースのオブジェクトが使用できなくなりました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。