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

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 （5 ページ）を参照してください。

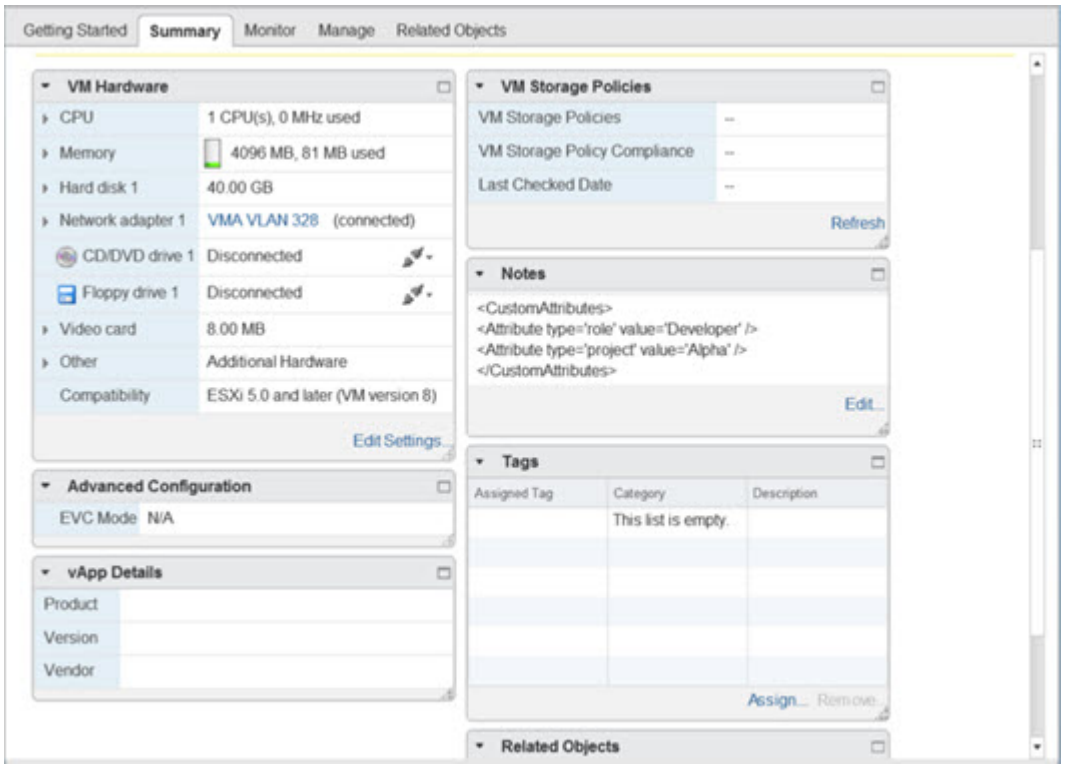
ステップ 4 アクセス コントロール リストとルールを設定します。属性ベースのネットワーク オブジェクトを使用したアクセス ルールの設定 （6 ページ）を参照してください。

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。

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 **[Configuration]** > **[Firewall]** > **[VM Attribute Agent]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Host Information] エリアで、次を実行します。

a) IP アドレスと認証クレデンシャルを有効にするかどうかを選択します。
b) DNS ホスト名または IP アドレスを入力します。
c) ユーザー名を入力します。
d) パスワード タイプとして [Clear Text]、[UnEncrypted]、[Encrypted] のいずれかを選択します。
e) パスワードを入力します。

ステップ 4 [Keepalive Information] エリアで、次を実行します。

a) [Retry Interval] に再試行間隔を入力します。1 ～ 65535 の値を入力します。デフォルトは 30 です。
b) [Retry Count] に再試行回数を入力します。1 ～ 32 の範囲で値を入力します。デフォルトは 3 です。

ステップ 5 [OK] をクリックします。

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 [Configuration] > [Firewall] > [Access Rules] > [Advanced Options] を選択します。

ステップ 2 [Enable Object Group Search Algorithm] チェックボックスをオンにします。

VM 属性を設定するには、オブジェクト グループ検索を有効にする必要があります。

ステップ 3 [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択します。

ステップ 4 次のいずれかを実行します。

- [Add] > [Network Object Attributes] を選択し、新しい属性ベースのネットワーク オブジェクトを追加します。名前を入力し、任意で説明を入力します。
- 既存の属性ベースのネットワーク オブジェクトを選択し、[Edit] をクリックします。

ステップ 5 新しい属性ベースのネットワーク オブジェクトの場合は、次のフィールドに値を入力します。

a) **[Agent Name]**：参照ボタンをクリックして VM 属性エージェントを選択（または新しいものを定義）します。

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、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」の状態となります。

b) [Attribute Type]：この文字列エントリは属性タイプを定義するもので、**custom.** というプレフィックスを含める必要があります。たとえば、custom.role です。

c) [Attribute Value]：この文字列エントリは、値を属性タイプに関連付けます。

また、[Attribute Type] と [Attribute Value] のペアは、一意の属性を定義します。これにより、特定の展開スキームに適した複数の属性を定義できます。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。

ステップ 6 [OK] をクリックします。

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 ルールの設定

属性ベースのネットワーク オブジェクトを使用してアクセス ルールを適用するには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Firewall] > [Access Rules] の順に選択します。

ルールはインターフェイスおよび方向別に構成され、グローバル ルールはそれらとは別のグループにまとめられています。管理アクセス ルールを設定する場合は、このページで繰り返されます。これらのグループが、作成されてアクセス グループとしてインターフェイスまたはグローバルに割り当てられた拡張 ACL に相当します。それらの ACL も [ACL Manager] ページに表示されます。

ステップ 2 次のいずれかを実行します。

- 新しいルールを追加するには、[Add] > [Add Access Rule] の順に選択します。

- コンテナ内の特定の場所にルールを挿入するには、追加する場所の下にある既存のルールを選択して [Add] > [Insert] の順に選択するか、[Add] > [Insert After] の順に選択します。
- ルールを編集するには、ルールを選択し、[Edit] をクリックします。

ステップ 3 ルールのプロパティを入力します。選択する主なオプションを次に示します。

- [Interface]：ルールを適用するインターフェイスを指定します。 グローバル ルールを作成する場合は [Any] を選択します。ルーテッド モードのブリッジ グループでは、ブリッジ仮想インターフェイス（BVI）と各ブリッジ グループ メンバーのインターフェイスの両方にアクセス ルールを作成できます。
- [Action]：[Permit] または [Deny]：対象のトラフィックを許可するか拒否（破棄）するかを指定します。
- [Source/Destination criteria]：送信元の属性ベースのネットワーク オブジェクト（発信オブジェクト）と宛先の属性ベースのネットワーク オブジェクト（トラフィック フローの対象オブジェクト）を選択します。送信元のユーザー名またはユーザー グループ名も指定できます。また、[Service] フィールドでトラフィックの種類を指定すると、すべての IP トラフィックではなく、特定のトラフィックを対象とするルールを作成できます。Trustsec を実装している場合は、セキュリティ グループを使用して送信元と宛先を定義できます。

使用可能なすべてのオプションの詳細については、アクセス ルールのプロパティを参照してください。

ルールの定義が完了したら、[OK] をクリックしてルール テーブルに追加します。

ステップ 4 [Apply] をクリックし、アクセス ルールを設定に保存します。

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 オブジェクトについては、各オブジェクトの使用状況を分析できます。[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] フォルダにある各オブジェクトのページで、[Where Used] ボタンをクリックします。

属性ベースのネットワーク オブジェクトの場合、[Not Used] ボタンをクリックすると、どのルールでも使用されていないオブジェクトを見つけることもできます。この表示によって、未使用のオブジェクトを簡単に削除できるようになります。

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。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [Objects] > [Network Object Attributes]。 次の画面が導入されました。[Configuration] > [Firewall] > [VM Attribute Agent]。
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。