ルートチューニングのためのルートマップおよびその他のオブジェクト

さまざまなルーティングプロトコルにより、ルートの配布や集約などのアクティビティを微調整できます。一部のチューニング機能では、ルートマップまたはその他のオブジェクトを使用して、チューニングポリシーの対象となるルートを識別します。ルートマップには、一致するルートに関するオプションを設定する追加機能があります。これにより、ネクストホップルータがカスタム動作を適用するために使用できるルートに変更を加えることができます。

これらのオブジェクトを作成する必要があるかどうかは、実装するルーティングプロトコルの動作を微調整するために必要なものに基づいて決まります。最初に要件を評価することによって、設定する調整コマンドに必要なオブジェクトのタイプを決定します。

ルートマップの設定

ルートマップはさまざまな目的で使用でき、一部のルーティングプロトコルは他のプロトコルよりも多くの用途をサポートしています。最も一般的な用途は、別のルーティングプロトコルへのルート再配布を微調整することです。

ルートマップの permit 句と deny 句

ルートマップは、1 つ以上の **permit** 句または **deny** 句で構成されます。これらの句の順序は重要です。ルートはマップのトップダウンで評価され、最初の一致が優先されます。ルートがどの句とも一致しない場合、ルートマップと一致しないと見なされます。

各 permit 句には、0 個以上の **match** ステートメントおよび **set** ステートメントを含めることができます。**match** ステートメントはどのルートが句と一致するのかを決定しますが、**set** ステートメントはルートのいくつかの特性（ルートメトリックなど）を変更します。set ステートメントは必要ありません。ルートを変更することなく、再配布（または別のサービス）のためにルートを照合できます。

各 deny 句には、0 個以上の match ステートメントを含めることができます。ただし、「拒否された」ルートは単にルートマップと一致しないため、set アクションを適用できないことから、set 句を含めても意味がありません。

ルートマップの match ステートメントと set ステートメント

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ルートの一部の属性を変更します。

たとえば、再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。ルートが基準に一致する場合、そのルートは permit 句または deny 句に従って再配布または拒否されます。permit 句と一致する場合、ルートの属性の一部は、set コマンドからの値によって変更される可能性があります。ルートが基準に一致しない場合、この句はルートに適用されず、システムはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。一致する句がない場合、ルートはルートマップに一致しないと見なされます（拒否アクションと同等）。

1 つの句内の match ステートメントおよび set ステートメントについては、次のようになります。

- 複数の match ステートメントは AND 演算されます。つまり、ルートが句に一致するには、そのルートが各ステートメントを満たす必要があります。
- 1 つの match ステートメントに含まれる複数の値は OR 演算されます。つまり、ルートがある match 句内のいずれかの値と一致する場合、そのルートはその句と全体として一致すると見なされます。
- match ステートメントがない場合、すべてのルートが句と一致します。
- ルートマップの permit 句に set ステートメントがない場合、機能（再配布など）は、ルートの現在の属性を変更せずに、ルートに適用されます。
- deny 句内の set ステートメントは無視されます。「拒否された」ルートは単にルートマップと一致しないため、set アクションを適用できないことから、set 句を含めても意味がありません。
- match ステートメントまたは set ステートメントがない空の句は、それより前の句と一致しなかったすべてのルートと一致します。次に例を示します。

- 空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。
- 空の deny 句では、残りのルートを再配布できません。これは、ルートマップがすべてスキャンされたときに明示的な一致が見つからなかった場合のデフォルトアクションです。

ルートマップの設定

ルートマップはさまざまな目的で使用でき、一部のルーティングプロトコルは他のプロトコルよりも多くの用途をサポートしています。最も一般的な用途は、別のルーティングプロトコルへのルート再配布を微調整することです。

ルートマップは、1 つ以上の **permit** 句または **deny** 句で構成されます。これらの句の順序は重要です。ルートはマップのトップダウンで評価され、最初の一致が優先されます。ルートがどの句とも一致しない場合、ルートマップと一致しないと見なされます。

各 permit 句には、0 個以上の **match** ステートメントおよび **set** ステートメントを含めることができます。**match** ステートメントはどのルートが句と一致するのかを決定しますが、**set** ステートメントはルートのいくつかの特性（ルートメトリックなど）を変更します。set ステートメントは必要ありません。ルートを変更することなく、再配布（または別のサービス）のためにルートを照合できます。

各 deny 句には、0 個以上の match ステートメントを含めることができます。ただし、「拒否された」ルートは単にルートマップと一致しないため、setアクションを適用できないことから、set 句を含めても意味がありません。

match ステートメントと set ステートメントの評価方法の詳細については、ルートマップの match ステートメントと set ステートメント （2 ページ） を注意深く参照してください。

始める前に

アクセスリスト、ASパスアクセスリスト、コミュニティリスト、ポリシーリスト、プレフィックスリストといった他のさまざまなオブジェクトをルートマップで使用して、一致基準を定義することができます。ルートマップを作成する前に、これらのオブジェクトを作成する必要があります。

ACL 照合の場合、IPv4 アドレスには標準 ACL または拡張 ACL を使用できますが、IPv6 アドレスに使用できるのは拡張 ACL のみです。match 句は IPv4 または IPv6 のみに基づいているため、ACL に match ステートメントの正しいアドレススキームがあることを確認してください。

また、他のルーティングプロトコルと比較すると BGP の一致および設定基準が異なることに注意してください。ルートマップを使用するルーティングプロセスに関して正しい一致/設定基準を選択していることを確認してください。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLI テンプレート（CLI Template）] として [ルートマップ（Route Map）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**route-map** コマンド内）のルートマップ名としても入力されることに注意してください。

ステップ 6 最初の句を作成します。

a) [redistribution] 変数をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、このルートマップを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **sequence-number** 変数をクリックし、句の番号を 1 ー 65535 の範囲で入力します。

この番号は、ルートマップ内の他の番号付き句に関連しています。一般的な方法は、カウントを 10 ずつスキップし（つまり、10、20、30）、将来新しい句を挿入する余地を残すことです。

ステップ 7 [無効を表示（Show Disabled）] をクリックし、句の **match** ステートメントを設定します。

a) **configure** *clause* コマンドを有効にするには、コマンドの横にある [+] をクリックします。

b) [clause] をクリックし、**bgp-match-clause**（BGP ルートマップの場合）または **match-clause**（他のすべてのルーティングプロトコルの場合）を選択します。

c) （BGP ルートマップ）次の **match** ステートメントの任意の組み合わせを設定して、この句でターゲットとする特定のルートを識別します。設定しないコマンドについては、必ず、[-] アイコンをクリックして無効にしてください。

- **match as-path**：変数をクリックし、照合する自律システム番号を定義するASパスオブジェクトを選択します。
- **match community**を使用して無効にすることができます。変数をクリックし、照合するコミュニティを定義するコミュニティ リスト オブジェクトを選択します。
- **match policy-list**を使用して無効にすることができます。変数をクリックし、句の一致基準を定義するポリシーリストオブジェクトを選択します。
- **match tag**を使用して無効にすることができます。変数をクリックし、照合するルートタグ値を0ー4294967295の範囲で入力します。

d) （他のすべてのルーティングプロトコル）次の**match**ステートメントの任意の組み合わせを設定して、この句でターゲットとする特定のルートを識別します。設定しないコマンドについては、必ず、[-]アイコンをクリックして無効にしてください。これらのコマンドの一部を有効にするには、[+] をクリックする必要がある場合があります。

- **match interface**を使用して無効にすることができます。変数をクリックし、照合するルート内のすべてのインターフェイスを選択します。
- **configure match ipv4/ipv6 ip address** *list-type*：IPバージョンに適したコマンドを有効にします。次に、[list-type]変数をクリックし、**access-list**または**prefix-list**に基づいてルートのIPアドレスを照合するかどうかを選択します。これにより**match ipv4/ipv6 address**コマンドが追加されます。このコマンドの変数をクリックし、照合するIPアドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **configure match ipv4/ipv6 ip next-hop** *list-type*：[list-type]変数をクリックし、**access-list**または**prefix-list**に基づいてルートのネクストホップルータのIPアドレスを照合するかどうかを選択します。これにより**match ipv4/ipv6 next-hop**コマンドが追加されます。このコマンドの変数をクリックし、照合するIPアドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **configure match ipv4/ipv6 ip route-source** *list-type*：[list-type]変数をクリックし、**access-list**または**prefix-list**に基づいてルートのルート送信元のIPアドレスを照合するかどうかを選択します。これにより**match ipv4/ipv6 route-source**コマンドが追加されます。このコマンドの変数をクリックし、照合するIPアドレスを定義するアクセスリストまたはプレフィックスリストを選択することができます。
- **match metric**：変数をクリックし、照合するルーティングメトリックを1ー4294967295の範囲で入力します。
- **match route-type**：（OSPF、EIGRP）変数をクリックし、ルートタイプを選択します。
  - **external-1**、**external-2**：OSPFまたはEIGRPの外部タイプ1またはタイプ2ルート。
  - **internal**を使用して無効にすることができます。OSPFエリア内およびエリア間ルート、またはEIGRP内部ルート
  - **local**を使用して無効にすることができます。ローカルに生成されたBGPルート。

- **nssa-external-1**、**nssa-external-2**：外部 Not So Stubby Area（NSSA）タイプ 1 またはタイプ 2 ルート。

ステップ 8 （任意、permit 句のみ）許可された（つまり、一致した）ルートについて、**set** ステートメントを設定してルート属性を変更できます。ルートを変更する必要はありません。たとえば、ルートを変更せずに再配布することができます。

a) **[...] > [複製（Duplicate）]**（permit 句内の configure match-clause コマンドまたは **configure bgp-match-clause** コマンドの左横）をクリックします。新しい **configure** *clause* コマンドが permit 句の最後に追加されます。

b) [clause] をクリックし、match 句に対して選択したものに基づいて **bgp-set-clause** または **set-clause** を選択します。

c) （BGP ルートマップ）一致するルートの属性を変更するには、次の **set** ステートメントの任意の組み合わせを設定します。設定しないコマンドについては、必ず、[-]アイコンをクリックして無効にしてください。

- **configure set as-path** *options*：[options] をクリックし、**properties** を選択すると、設定する必要がある次のコマンドが追加されます。パスに項目を追加すると、AS 番号が重複していても、パスが長くなり、そのルートが最適なルートとして選択される可能性が低くなります。
  - **set as-path prepend** *as-path*：[as-path] をクリックし、ルートの AS_PATH 属性の先頭に追加する最大 10 個の自律システム番号を入力します。この変更は、アウトバウンド BGP ルートマップに適用されます。
  - **set as-path prepend last-as** *value*：[value] をクリックし、システムが AS_PATH 変数の先頭にアドバタイジングネイバーの自律システム番号を付加する回数を入力します。この変更は、インバウンド BGP ルートマップに適用されます。
  - **set as-path tag**を使用して無効にすることができます。ルートのタグを自律システム パスに変換します。BGP にルートを再配布するときのみ適用されます。
- **set community** *community-number properties*：[community-number] をクリックし、ルートのコミュニティを 1 ～ 4694967295 の範囲で入力します。必要に応じて、[properties] をクリックし、次のいずれかを追加できます。
  - **internet**：このコミュニティのあるルートは、すべてのピア（内部および外部）にアドバタイズされます。
  - **no-advertise**：このコミュニティのあるルートは、ピア（内部または外部）にはアドバタイズされません。
  - **no-export**：このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
- **set local-preference**を使用して無効にすることができます。変数をクリックし、自律システムパスのプリファレンス値を 0 ー 4294967295 の範囲で入力します。グローバル

BGP オプションで変更しないかぎり、BGP ルートのデフォルトプリファレンスは 100 です。プリファレンス値が最大のルートが優先されます。

- **set weight**を使用して無効にすることができます。変数をクリックし、ルートの重み 0 ～ 65535 の範囲で入力します。ルータが同じ宛先への複数のルートがあることを学習すると、[重要度（Weight）] 属性値が最も大きいルートが優先されます。
- **set origin** *options*：BGP ルートの起点は、メイン IP ルーティングテーブルのルートのパス情報に基づいています。これを変更するには、[options] をクリックし、BGP 送信元コードの設定方法を選択します。
  - **igp**を使用して無効にすることができます。送信元を内部ゲートウェイプロトコル（IGP）のリモートシステムに設定します。
  - **incomplete**を使用して無効にすることができます。送信元を不明な継承として設定します。
- **configure next-hop ipv4/ipv6** *options*：これらは個別のコマンドです。適切な IP バージョンの [options] をクリックし、次のいずれかを選択します。ネクストホップゲートウェイの設定は、通常、ポリシーベースのルーティングを実装するときに行います。
  - **specific-ip**を使用して無効にすることができます。このルートのネクストホップゲートウェイの IP アドレスを明示的に設定する場合は、このオプションを選択します。**set ip/ipv6 next-hop ip-address** コマンドが追加されます。変数をクリックし、ネクストホップゲートウェイの IP アドレスを入力します。スペースで区切ることにより、複数の IP アドレスを追加できます。最初のゲートウェイのアドレスに到達できない場合は次のアドレスが試行され、以降同様です。
  - **user-peer-address**を使用して無効にすることができます。ネクストホップゲートウェイを BGP ピアの IP アドレスとして設定する場合は、このオプションを選択します。このオプションを BGP ピアのアウトバウンドルートマップで使用すると、アドバタイズされた一致するルートのネクストホップをローカルルータのピアアドレスに設定し、ネクストホップ計算をディセーブルにします。このコマンドについては、追加設定は必要ありません。
- **set ipv4/ipv6 address** *prefix-list*：これらは個別のコマンドです。選択したプレフィックスリストの内容に基づいて、ルートの IP アドレスを変更します。
- **set automatic-tag**を使用して無効にすることができます。システムにルートのタグ値を自動的に計算させます。

d) （他のすべてのルーティングプロトコル）一致するルートの属性を変更するには、次の**set** ステートメントの任意の組み合わせを設定します。設定しないコマンドについては、必ず、[-] アイコンをクリックして無効にしてください。

- **set metric**を使用して無効にすることができます。変数をクリックし、メトリック値を 0 ー 4294967295 の範囲で入力します。この値は EIGRP では使用されません。

- **set metric-type**を使用して無効にすることができます。変数をクリックし、メトリックのタイプを選択します。
  - **type-1**、**type-2**：OSPF の外部ルートのタイプ。デフォルトは type-2 です。
  - **internal**を使用して無効にすることができます。ルートのネクストホップの内部ゲートウェイプロトコル（IGP）メトリックと一致するように、外部BGP（eBGP）ネイバーにアドバタイズされるプレフィックスの Multi-Exit 識別子（MED）値を設定します。これは、生成された内部BGP（iBGP）生成ルートおよびeBGP生成ルートに適用されます。

ステップ 9 permit/deny 句を追加してルートマップを完成させます。

句を追加するには、**[...]** > **[複製（Duplicate）]**（**permit** 行または **deny** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした句の直後に新しい *redistribution sequence-number* 句が追加されます。

ルートマップの句は、オブジェクトに表示される順序ではなく、シーケンス番号の順序で評価されますが、新しい句を順番に挿入することで、オブジェクトの編集が容易になります。オブジェクト内で句を移動することはできません。

句を複製すると新しい空の句が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

ルートマップを必要とする機能のために、ルーティングプロセス設定（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

アクセスリストの設定

アクセス リスト オブジェクトは、アクセス コントロール リスト（ACL）とも呼ばれ、トラフィックに適用されるサービスを選択します。アクセス リスト オブジェクトを使って、ルート マップなどの機能を設定します。ACL で許可されたトラフィックはサービスを利用できますが、「ブロックされた」トラフィックはサービスから除外されます。サービスから除外されたトラフィックが必ずしも完全にドロップされるわけではありません。

次のタイプの ACL を設定できます。

- 拡張：送信元と宛先アドレスおよびポートに基づいてトラフィックを識別します。IPv4アドレスと IPv6 アドレスをサポートしています。
- 標準：宛先アドレスのみに基づいてトラフィックを識別します。IPv4のみサポートしています。

ACL は 1 つまたは複数のアクセス コントロール エントリ（ACE）またはルールで構成されます。ACE の順番は重要です。パケットを「許可」 ACE と照合して ACL を評価する際、ACL

に登録されているACEの順番どおりに照合します。一致が見つかると、ACEはそれ以上チェックされません。たとえば、10.100.10.1 と一致させ、10.100.10.0/24 の残りを除外する場合、10.100.10.1 の許可エントリは 10.100.10.0/24 の拒否エントリの前に配置する必要があります。通常、具体性の高いルールを ACL の上部に置きます。

許可エントリに一致しないパケットは、拒否されるか、照合から除外されると見なされます。

次に、ACL オブジェクトの設定方法について説明します。

拡張アクセスリストの設定

送信元および宛先アドレス、プロトコル、およびポートに基づいて、あるいはトラフィックが IPv6 の場合にトラフィックを照合するには、拡張 ACL オブジェクトを使用します。

始める前に

オブジェクトに作成する ACE に必要なネットワークオブジェクトまたはポートオブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [拡張アクセスリスト（Extended Access List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**access list** コマンド内）の ACL 名としても入力されることに注意してください。

ステップ 6 ACL の最上位のルールとなる ACE を作成します。

1 つの **configure access list entry** コマンドに含まれるコマンドの各リストは基本的に 1 つの ACE ですが、展開すると、特に複数のネットワークオブジェクトを含める場合、システムがコマンドを一連の ACE に分割することがあります。

a) configure access list entry コマンドで、[action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このACEに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このACEに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、この ACL を使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **permit/deny network** コマンドで、変数をクリックし、接続の送信元 IP アドレスと宛先 IP アドレスを定義するネットワークオブジェクトを選択します。複数のオブジェクトを選択できます。「任意の」アドレスを指定するには、any-ipv4 オブジェクトおよび any-ipv6 オブジェクトを選択します。

オブジェクトまたはオブジェクトグループにFQDNを含めることはできません。オブジェクトはIPアドレスのみを指定する必要があります。FQDNオブジェクトは、アクセス制御ルールでのみ有効です。

c) **configure permit/deny port** コマンドで、[options] をクリックし、次のいずれかを選択します。これにより、関連付けられた permit/deny コマンドがテンプレートに追加されます。

- **any**：ポートが問題ではない場合に使用します。つまり、任意のタイプのIPトラフィックが照合されます。
- **any-source**：送信元TCP/UDPポートは問題ではないが、宛先ポートを指定する場合に使用します。**permit/deny port** コマンドの [destination-port] 変数をクリックし、ポートオブジェクトを選択します。
- **any-destination**：宛先TCP/UDPポートは問題ではないが、送信元ポートを指定する場合に使用します。**permit/deny port** コマンドの [source-port] 変数をクリックし、ポートオブジェクトを選択します。
- **source-destination**：送信元 TCP/UDP ポートと宛先 TCP/UDP ポートの両方が問題である場合に使用します。**permit/deny port** コマンドで [source-port] 変数と [destination-port] 変数をクリックし、ポートオブジェクトを選択します。

d) **configure logging** コマンドで、**disabled** を選択します。ロギングはアクセス制御に使用される ACL に適用され、これらのオブジェクトをアクセス制御に使用することはできません。そのため、ロギングオプションは選択内容に関係なく無視されます。

ステップ 7 ACE を追加して ACL を完成させます。

ACE を追加するには、**[...]** > **[複製（Duplicate）]**（**configure access list entry** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした ACE の直後に新しい ACE グループが追加されます。

そのため、オブジェクトに多数のACEがある場合は、「複製」するACEを慎重に選択してください。オブジェクト内ではACEを移動できないため、間違えた場合は、ACEを正しい場所で手動で再作成する必要があります。

ACE を複製すると新しい空の ACE が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

拡張ACLを必要とする機能のために、ルートマップオブジェクト（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

標準アクセスリストの設定

宛先 IPv4 アドレスのみに基づいてトラフィックを照合する場合や、設定している機能が標準 ACL をサポートする場合は、標準 ACL オブジェクトを使用します。それ以外の場合は、拡張 ACL を使用します。

始める前に

オブジェクトに作成する ACE に必要なネットワークオブジェクトを作成します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [標準アクセスリスト（Standard Access List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**access list** コマンド内）の ACL 名としても入力されることに注意してください。

ステップ 6 ACL の最上位のルールとなる ACE を作成します。

1 つの **configure action** コマンドに含まれるコマンドの各リストは、1 つの ACE です。

a) **configure action** コマンドで、[action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このACEに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このACEに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであること

に注意してください。たとえば、ルートマップでは、この ACL を使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) **permit/deny host** コマンドで、変数をクリックし、接続の宛先 IP アドレスを定義するネットワークオブジェクトを選択します。このオブジェクトは、ネットワークまたはホストアドレスを指定できます。**permit/deny host** コマンドごとに 1 つのオブジェクトを選択できます。コマンドで **[...]** > **[複製（Duplicate）]** をクリックして追加のアドレスを指定すると、同じアクションを持つ一意の ACE になります。「任意の」アドレスを指定するには、any-ipv4 オブジェクトを選択します。

ステップ 7 ACE を追加して ACL を完成させます。

ACE を追加するには、**[...]** > **[複製（Duplicate）]**（**configure action** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックした ACE の直後に新しい ACE グループが追加されます。

そのため、オブジェクトに多数の ACE がある場合は、「複製」する ACE を慎重に選択してください。オブジェクト内では ACE を移動できないため、間違えた場合は、ACE を正しい場所で手動で再作成する必要があります。

ACE を複製すると新しい空の ACE が挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

標準ACLを必要とする機能のために、ルートマップオブジェクト（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

AS パスアクセスリストの設定

AS パスアクセスリストを使用して、BGP ネイバーの更新を、更新内の自律システム番号に基づいてフィルタ処理できます。許可された AS 番号の場合は更新が受け入れられますが、拒否された AS 番号の場合は更新が拒否されます（つまり、更新はルーティングテーブルに追加されない）。

また、アウトバウンド方向に AS パスフィルタ処理を適用して、ネイバーに送信する更新をフィルタ処理することもできます。

さらに、BGP アドレス集約のルートマップで AS パスオブジェクトを使用できます。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [ASパス（ASPath）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、1 ー 500 の範囲の数値にする必要があります。この名前は、CLI テンプレートの最初の行（**as-path** コマンド内）の AS パスアクセスリスト名としても入力されることに注意してください。

ステップ 6 AS パスエントリを設定します。

各エントリは、*action* オプションで始まる単一の行に含まれます。

a) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このオブジェクトを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) [regex] をクリックし、このエントリに一致する AS 番号を定義する正規表現を入力します。

最も単純な形式では、正規表現は単に完全な AS パス番号であり、単一の自律システムからのルート更新を許可または拒否します。

AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。AS 番号は固有に割り当てられた値であるため、インターネットの各ネットワークが識別されます。システムは、RFC 5396 で定義されている asplain および asdot 表記をサポートしています。使用する必要がある表記は、BGP グローバル設定で **bgp asnotation dot** コマンドを有効にするかどうかによって異なります。

ステップ 7 エントリを追加して AS パスアクセスリストを完成させます。

エントリを追加するには、**[...]** > **[複製（Duplicate）]**（*action* 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

そのため、オブジェクトに多数のエントリがある場合は、「複製」するエントリを慎重に選択してください。オブジェクト内ではエントリを移動できないため、間違えた場合は、エントリを正しい場所で手動で再作成する必要があります。ルールはトップダウンで評価され、最初の一致が優先されます。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ASパスアクセスリストを必要とする機能のために、BGPオブジェクト、ルートマップオブジェクト（またはFlexConfigオブジェクト）でオブジェクトを使用できるようになりました。

コミュニティリストの設定

BGPプロセスでコミュニティ情報を送信できるようにすると、ルートマップでコミュニティリストをmatch句として使用して、一致するルートで属性を設定できます。たとえば、特定のコミュニティのルート優先度を変更できます。

コミュニティとは、共通するいくつかの属性を共有する宛先グループに関してアドバタイズされたルートにサービスプロバイダーが添付するオプションの属性またはラベルです。特定のコミュニティ番号はISPがアドバタイズするものであり、それらの番号とその意味をISPから取得し、ルートマップを使用してそれらを処理する方法を選択する必要があります。

コミュニティリストは順序付けられており、一致は、アクセスリストやプレフィックスリストと同様に、トップダウン（最初の一致が優先される）方式によって決定されます。

コミュニティリストには次の2つのタイプがあります。

- 標準：特定の既知のコミュニティ（サービスプロバイダーから取得したコミュニティなど）を対象とする場合は、標準リストを使用します。
- 拡張：正規表現照合に基づいて一連のコミュニティを照合する場合は、拡張リストを使用します。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（  ）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（  ）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [標準コミュニティリスト（Standard Community List）] または [拡張コミュニティリスト（Expanded Community List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**community-list** コマンド内）のコミュニティリスト名としても入力されることに注意してください。

ステップ 6 （標準リスト）コミュニティリストエントリを設定します。

各エントリは、*action* オプションで始まる単一の行に含まれます。

a) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このルートを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

b) [community-number] をクリックし、最大 10 個のコミュニティをスペースで区切って入力します。1 つのルールに含まれる複数のコミュニティは AND 演算されるため、ルート内のすべてのコミュニティが一致する場合にのみ一致します。

BGP プロセスに関して有効になっている番号付け方法に基づいてコミュニティを 10 進形式（1 ～ 4294967295）または AA:NN 形式（各値は 1 ～ 66535）で入力します。これらの番号は、ISP またはその他の BGP ネイバーから取得してください。

c) （オプション）[properties] をクリックし、他の既知のコミュニティをルールに追加します。

- **internet**：このコミュニティのあるルートは、すべてのピア（内部および外部）にアドバタイズされます。
- **no-advertise**：このコミュニティのあるルートは、ピア（内部または外部）にはアドバタイズされません。
- **no-export**：このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。

ステップ 7 （拡張リスト）コミュニティリストエントリを設定します。

a) [action] をクリックし、**permit** または **deny** を選択します。これらのアクションについては、前述しています。

b) [regex] をクリックし、このエントリに一致するコミュニティを定義する正規表現を入力します。

* または + の文字を使用した照合の順序は、最長のコンストラクトが最初になります。入れ子のコンストラクトは外側から内側へと照合されます。連結コンストラクトは左側から順に照合されます。ある正規表現が、1 つの入力ストリングの異なる 2 つの部分と一致す

る可能性がある場合、早く入力された部分が最初に一致します。正規表現の表記の詳細については、『Cisco IOS Terminal Services Configuration Guide』の付録「Regular Expressions」を参照してください。

ステップ 8 エントリを追加してコミュニティリストを完成させます。

エントリを追加するには、**[...]**>**[複製（Duplicate）]**（*action* 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

そのため、オブジェクトに多数のエントリがある場合は、「複製」するエントリを慎重に選択してください。オブジェクト内ではエントリを移動できないため、間違えた場合は、エントリを正しい場所で手動で再作成する必要があります。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

コミュニティリストを必要とする機能のために、ルートマップやルーティングプロセス（または FlexConfig オブジェクト）でオブジェクトを使用できるようになりました。

ポリシー リストの設定

ルートマップではポリシーリストを 1 つ以上の match 句の代わりに使用できます。そのため、再利用したい一連の match 句がある場合、ポリシーマップによって設定が簡素化され、各ルートマップで match 句を繰り返す必要がなくなります。BGP のポリシーリストを参照するルートマップを使用できます。

ルートマップ内には、ポリシーリストに加えて他の match 句を含めることができます。ポリシーリストの match 句は、着信属性でのみ照合されます。

ポリシーリストは IPv4 アドレスの照合のみをサポートします。IPv6 アドレスは照合できません。

ポリシーマップ内の match 句については、次のようになります。

- 複数の match 句は AND 演算されます。つまり、ルートがポリシーリストに一致するには、そのルートが各句を満たす必要があります。
- 1 つの match 句内の複数の値は OR 演算されます。つまり、ルートがある match 句内のいずれかの値と一致する場合、そのルートはその句と全体として一致すると見なされます。

始める前に

アクセスリスト、プレフィックスリスト、または AS パスアクセスリストに関する match 句を設定する場合は、ポリシーリストを作成する前にそれらのオブジェクトを作成する必要があります。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLI テンプレート（CLI Template）] として [ポリシーリスト（Policy List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**policy-list** コマンド内）のポリシーリスト名としても入力されることに注意してください。

ステップ 6 **policy-list** コマンドで [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このリストに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このリストに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このオブジェクトを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

ステップ 7 テンプレートの上にある [無効を表示（Show Disabled）] をクリックして match コマンドを表示します。有効にする match ステートメントの左側にある [+] アイコンをクリックする必要があります。次の match ステートメントの任意の組み合わせを設定して、ターゲットとするルートを定義します。

- **match as-path**を使用して無効にすることができます。変数をクリックし、照合する自律システム番号を定義する AS パスオブジェクトを選択します。
- **configure match ip address** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートの IP アドレスを照合するかどうかを選択します。これにより **match ip address** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。
- **configure match ip next-hop** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのネクストホップルータの IP アドレスを照合するかどうかを選択します。これにより **match ip next-hop** コマンドが追加されます。このコマンドの変

数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。

- **configure match ip route-source** *list-type*：[list-type] 変数をクリックし、**access-list** または **prefix-list** に基づいてルートのルート送信元の IP アドレスを照合するかどうかを選択します。これにより **match ip route-source** コマンドが追加されます。このコマンドの変数をクリックし、照合する IP アドレスを定義する標準アクセスリストまたは IPv4 プレフィックスリストを選択することができます。
- **match community** *community-list options*：[community-list] 変数をクリックし、照合するコミュニティを定義するコミュニティ リスト オブジェクトを選択します。リスト内のすべてのコミュニティが一致した場合にのみルートをコミュニティリストと一致させる場合は、[options] をクリックし、**exact-match** を選択します。
- **match interface**を使用して無効にすることができます。変数をクリックし、照合するルート内のすべてのインターフェイスを選択します。
- **match metric**を使用して無効にすることができます。変数をクリックし、照合するルーティング Multi-Exit 識別子（MED）メトリックを 1 ー 4294967295 の範囲で入力します。
- **match tag**を使用して無効にすることができます。変数をクリックし、照合するルートタグ値を 0 ー 4294967295 の範囲で入力します。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

BGP ルーティングで使用するためにオブジェクトをルートマップオブジェクトで使用できるようになりました。

プレフィックス リストの設定

プレフィックスリストはアクセス制御リストと似ています。プレフィックスリストは、許可/拒否ルールの順序付きリストです。ここで、「許可」はリストと一致する必要があるアドレスプレフィックスを示し、「拒否」はリストと一致してはならないアドレスプレフィックスを示します。システムは一致をトップダウン方式で評価し、必ずしも最も一致したルールに基づかず、最初に一致したルールに基づいてアクションを割り当てます。そのため、必要な一致を確実に得るには、シーケンス番号を慎重に指定する必要があります。

OSPF フィルタリングや BGP、OSPF、または EIGRP ルートマップのプレフィックスリストを使用して、ルートの再配布または注入、あるいは BGP ネイバーフィルタ処理を行うことができます。

IPv4 アドレス用と IPv6 アドレス用の個別のプレフィックスリストがありますが、リストの構造は同じです。

手順

ステップ 1 **[デバイス（Device）]** > **[詳細設定（Advanced Configuration）]** で [設定の表示（View Configuration）] をクリックします。

ステップ 2 コンテンツテーブルから **[スマート CLI（Smart CLI）]** > **[オブジェクト（Objects）]** を選択します。

ステップ 3 次のいずれかを実行します。

- オブジェクトを作成するには、[+] ボタンをクリックします。
- オブジェクトを編集するには、オブジェクトの編集アイコン（）をクリックします。

参照されていないオブジェクトを削除するには、オブジェクトの [ごみ箱（trash can）] アイコン（）をクリックします。

ステップ 4 [CLIテンプレート（CLI Template）] として [IPv4プレフィックスリスト（IPv4 Prefix List）] または [IPv6プレフィックスリスト（IPv6 Prefix List）] を選択します。

ステップ 5 スマート CLI オブジェクトの [名前（Name）] を入力します。この名前は、CLI テンプレートの最初の行（**prefix-list** コマンド内）のプレフィックスリスト名としても入力されることに注意してください。

ステップ 6 プレフィックス リスト エントリを設定します（**seq** コマンドライン）。

各エントリは、**seq** オプションで始まる単一の行に含まれます。

a) **seq** で、[sequence-number] をクリックし、このルールの番号を 1 ー 4294967294 の範囲で入力します。この番号は、他のルールのシーケンス番号に関連し、1 のルールが最初に評価されます。一般的な方法では、カウントを 5 ずつスキップします（つまり 5、10、15 など）。これにより、他のルールのシーケンス番号を変更することなく新しいルールを挿入する余地が残ります。

b) [action] をクリックし、次のいずれかを選択します。

- **permit**：一致します。このルールに一致する接続は、設定中の機能に関して選択されます。
- **deny**：一致しません。このルールに一致する接続は、この機能から除外されます。「拒否された」トラフィックはドロップされず、サービスが適用されないだけであることに注意してください。たとえば、ルートマップでは、このルートを使用して再配布されるルートを定義すると、「拒否された」アドレス空間が再配布されないだけです。

c) [ip-address-mask] をクリックし、ネットワークアドレスおよびマスク（IPv4 の場合 CIDR 形式）または IPv6 の場合はプレフィックス長を入力します。たとえば、10.100.10.0/24（IPv4）または 2001:DB8:0:CD30::/60（IPv6）と入力します。

ge オプションまたは **le** オプションのいずれかを含めないかぎり、システムは、このアドレス/マスクの完全一致を使用します。たとえば、ルールに **ge 9** を含めないかぎり、10.100.10.10/8 は 10.100.10.0/24 と一致しません。

マスクまたはプレフィックス長は次のように設定できます。

- IPv4 = 0 ～ 32
- IPv6 = 0 ～ 128

d) （オプション）**ge** キーワードおよび **le** キーワードを使用して、IP アドレスおよびマスク/プレフィックス長よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。これらのキーワードがないときは、完全一致の場合にのみルールに一致すると見なされます。

ge *min-prefix-length* では、照合する最小プレフィックス長を指定します。この最小値は、マスク/プレフィックス長より大きく、**le** オプションで定義されている最大値以下である（存在する場合）必要があります。

le *max-prefix-length* では、照合する最大プレフィックス長を指定します。この最大値は、最小値以上である（存在する場合）か、マスク/プレフィックス長より大きい（最小値が定義されていない場合）必要があります。

上記の相対的な長さの制限に加えて、これらのオプションの長さには、次の外的制限があります。

- IPv4 = 1 ～ 32
- IPv6 = 0 ～ 128

ステップ 7 エントリを追加してプレフィックスリストを完成させます。

エントリを追加するには、**[...]**>**[複製（Duplicate）]**（**seq** 行の左横）をクリックします。[複製（Duplicate）] コマンドをクリックしたエントリの直後に新しいエントリが追加されます。

便宜上、エントリを順番に保持することをお勧めします。ただし、オブジェクト内で混ざっていても、展開するとプレフィックスリストは順番に書き換えられます。

エントリを複製すると新しい空のエントリが挿入され、それらは事前設定された特性を持ちません。「複製」を作成したら、必要に応じて、上記の説明に従って設定してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

プレフィックスリストを必要とする機能のために、ルートマップやルーティングプロセス（または FlexConfig オブジェクト）でオブジェクトを使用できるようになりました。

例

以下に、プレフィックスリストを使用してプレフィックスを照合する方法の例を示します。分かりやすくするために例ではシーケンス番号を省いています。各ルールの実

際の動作は、対象のアドレス空間のサブセットに一致するルールがそれよりも前にある場合は、それによって変更されます。

- デフォルトルート 0.0.0.0/0 を拒否する：

```
deny 0.0.0.0/0
```

- プレフィックス 10.0.0.0/8 を許可する：

```
permit 10.0.0.0/8
```

- プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する：

```
permit 192.168.0.0/8 le 24
```

- プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する：

```
deny 192.168.0.0/8 ge 25
```

- すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する：

```
permit 0.0.0.0/0 ge 8 le 24
```

- すべてのアドレス空間で 25 ビットよりも大きいマスク長を拒否する：

```
deny 0.0.0.0/0 ge 25
```

- プレフィックス 10/8 のすべてのルートを拒否する：

```
deny 10.0.0.0/8 le 32
```

- プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する：

```
deny 192.168.1.0/24 ge 25
```

- プレフィックス 0/0 のすべてのルートを許可する：

```
permit 0.0.0.0/0 le 32
```

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。