詳細設定

この章では、AppNav-XE の詳細設定について説明します。内容は次のとおりです。

AppNav コントローラの設定

AppNav コントローラを設定するには、次の手順を実行します。

AppNav コントローラ グループの設定

AppNav コントローラ グループで、AppNav コントローラを設定します。AppNav コントローラ グループを設定するには、AppNav コントローラで使用する IP アドレスを入力します。

制約事項

- AppNav コントローラ グループには常に、正確に 1 つのローカル IP アドレスが含まれる必要があります。これはローカルの AppNav コントローラ（ローカル ルータ）の IP アドレスです。このローカル IP アドレスはインターフェイスに属している必要があり、AppNav コントローラ グループ内の他のすべての AppNav コントローラ、およびすべてのサービス ノードは、このインターフェイスから到達可能である必要があることに注意してください。
- AppNav コントローラ グループには、AppNav コントローラを 4 つまで含めることができます。この場合、正確に 1 つのローカル IP アドレスと、任意に最大 3 つの非ローカル IP アドレスを含める必要があります。
- GigE、VLAN インターフェイス、ループバック インターフェイスなどから IP アドレスを使用できますが、インターフェイスに VRF が設定されていないことが必要です。

（注）　デュアル RP Cisco ASR 1000 プラットフォーム上では、サブインターフェイスで **service-insertion** コマンドを使用しないでください。

- システムでは、1 つの AppNav コントローラ グループの設定だけがサポートされます。

次のコマンドを使用します。

```
(config)# [no] service-insertion appnav-controller-group group-name
```

サブモード コマンド

```
(config-service-insertion-acg)# [no] appnav-controller IP_address
```

オプションのコマンド

```
(config-service-insertion-acg)# [no] description group_description
```

サービス ノード グループの設定

サービス ノード グループでは、サービス ノードを設定する必要があります。AppNav-XE コンポーネントは、サービス ノード グループ内のサービス ノードにフローをインテリジェントに配信します。

制約事項

AppNav コントローラまたはサービス ノード IP アドレスには、VRF を使用できません。IP アドレスは、VRF なしで明示的にアクセスできる必要があります。たとえば、管理インターフェイスの IP アドレス（vrf Mgmt-intf あり）は、AppNav コントローラの IP アドレスとして使用できません。

次のコマンドを使用します。

```
(config)# [no] service-insertion service-node-group group_name
```

サブモード コマンド

```
(config-service-insertion-sng)# [no] description group_description
(config-service-insertion-sng)# [no] service-node IP_address
```

AppNav クラス マップの設定

AppNav-XE コンポーネントによって処理されるトラフィックを決定するには、AppNav クラスを使用します。次のパラメータのセットに基づいてトラフィックを分類するには、appnav タイプのクラス マップを使用します。

- アクセス リスト
- サービス ノード ピア デバイス ID
- サービス ノードでサポートされる特殊なプロトコル

指定したクラスへの接続の照合に使用するクラス マップを作成または変更するには、グローバル コンフィギュレーション モードで **class-map** コマンドを使用します。既存のクラス マップを削除するには、このコマンドの **no** 形式を使用します。**class-map** コマンドは、クラスマップ コンフィギュレーション モードを開始します。このモードでは、オプションの description コマンドと 1 つまたは複数の match コマンドを入力して、このクラスの一致基準を設定できます。

クラス マップを定義する構文は次のようになります。

```
(config)# [no] class-map type appnav [match-all | match-any] appnav_class_name
```

一致を指定しない場合、デフォルトは match-all です。

サブモード コマンド

```
(config-cmap)# [no] description description_text
(config-cmap)# [no] match access-group {ACL_number | name ACL_name}
(config-cmap)# [no] match peer device_ID
(config-cmap)# [no] match protocol app_def
```

match access-group コマンド

match access-group コマンドは、番号付きアクセスリストまたは名前付きアクセス リストを指定します。これらの内容は、パケットがこのクラスに属するかどうかを判断する際の一致基準として使用されます。アクセス リスト（ACL）番号は 1 ～ 2699 の範囲で指定できます。

match peer コマンド

match peer コマンドは、接続のクライアント側で最適化を実行するピア サービス ノードを識別します。01:23:45:67:89:ab 形式で指定する必要があります。match peer コマンドは、AppNav-XE コンポーネントがコアとして動作する、つまり、すでにピア WAAS デバイスを介した接続を受信している場合にのみ役立ちます。

match protocol コマンド

match protocol コマンドは、次のプロトコルのいずれかを取得します。

- CITRIX
- MAPI
- MS-AD-REP
- MS-EXCH-NSPI
- MS-FRS
- MS-FRSAPI
- MS-RFR
- MS-SQL
- MSN-MESSENGER
- NETLOGON

プロトコルは、サービス ノードによって提供される追加情報とともにのみ使用され、パケットを特定のアプリケーションと関連付けます。match protocol フィルタを、次に示す AppNav ポリシーの **monitor-load** キーワードと混同しないでください。

AppNav ポリシー マップの設定

AppNav クラス マップを設定したら、AppNav ポリシー マップを使用してアクションを割り当てることができます。候補最適化トラフィックのサービス ポリシーを定義するポリシー マップを作成または変更するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。

```
(config)# [no] policy-map type appnav appnav_policy_name
```

サブモード コマンド

```
(config-pmap)# [no] description description_text
(config-pmap)# [no] class appnav_class_name
```

上記の **class** コマンドは、ポリシーマップクラス コンフィギュレーション サブモードを開始します。

```
(config-pmap-c)# [no] distribute service-node-group SNG_name
(config-pmap-c)# [no] monitor-load application_accelerator_name
(config-pmap-c)# [no] pass-through
```

distribute コマンド

distribute コマンドは、このクラスの最も一般的なアクションです。システムは、指定した *SNG_name* パラメータで識別したサービス ノード グループに、クラス マップに一致するトラフィックを送信します。サービス ノード グループが使用できない場合、または、distribute が指定されていない場合、デフォルトのアクションはトラフィックのパススルーです。

monitor-load コマンド

monitor-load コマンドは、モニタする負荷値を決定します。アプリケーション アクセラレータをモニタする場合は、AppNav コントローラがそのアプリケーション アクセラレータの過負荷をチェックし、過負荷がかかっているサービス ノードに新しいフローを送信しないようにします。フローはサービス ノード グループの別のサービス ノードに送信されます。

このコマンドは任意です。これを使用すると、システムは *application_accelerator_name* パラメータで示されるアプリケーション アクセラレータをモニタします。このコマンドを使用しない場合、システムは TFO アクセラレータのステータスをモニタします。アプリケーション アクセラレータを指定すると、既存の monitor-load（存在する場合）が置き換えられます。

次のアプリケーション アクセラレータがサポートされます。

- MS-port-mapper（Microsoft Endpoint Port Mapper の負荷のモニタリング）
- cifs（SMB または CIFS アクセラレータの負荷のモニタリング）
- http（HTTP アクセラレータの負荷のモニタリング）
- ica（ICA アクセラレータの負荷のモニタリング）
- mapi（MAPI アクセラレータの負荷のモニタリング）
- nfs（NFS アクセラレータの負荷のモニタリング）
- ssl（SSL アクセラレータの負荷のモニタリング）
- video（ビデオ アクセラレータの負荷のモニタリング）

pass-through コマンド

pass-through コマンドは、リダイレクトが発生しないことを明示的に示すために使用します。**pass-through** コマンドは、**distribute** または **monitor-load** コマンドとともに使用することはできません。**pass-through** コマンドを使用すると、システムは **distribute** または **monitor-load** コマンドのアクションをブロックし、エラー メッセージを表示します。**distribute** または **monitor-load** コマンドのいずれかを使用する場合、システムは **pass-through** コマンドのアクションをブロックします。

サービス コンテキストの設定

サービス コンテキストは、AppNav コントローラ グループ、サービス ノード グループ、および AppNav ポリシー マップをまとめて関連付けるために使用されます。

サービス コンテキストを作成するには、次のコマンドを使用します。

```
(config)# service-insertion service-context waas/interface_ID
```

interface_ID は、すべてのサービス コンテキストで一意の番号です。これは、AppNav-Compress*interface_ID* および AppNav-UnCompress*interface_ID* と呼ばれる自動作成される仮想インターフェイスの名前を決定します。

サブモード コマンド

```
(config-service-insertion-context)# [no] appnav-controller-group ACG_name
(config-service-insertion-context)# [no] authentication sha1 key authentication_key
(config-service-insertion-context)# [no] service-node-group SNG_name
(config-service-insertion-context)# [no] service-policy appnav_policy_name
(config-service-insertion-context)# [no] vrf { name VRF_name | default | global}
(config-service-insertion-context)# [no] enable
```

appnav-controller-group コマンド

ACG_name は、このサービス コンテキストが属する AppNav コントローラ グループの名前です。各サービス コンテキストに対して 1 つの AppNav コントローラ グループだけを設定できます。

authentication sha1 key コマンド

authentication-key は、AppNav コントローラからサービス ノードへの登録時に使用される共有認証キーです。同じサービス コンテキスト内のサービス ノードには、同一のキーを設定する必要があります。現在、AppNav コントローラ グループは、1 つの認証キーだけをサポートしています。すべてのサービス コンテキストが認証を使用する必要があります。そうでない場合、サービス コンテキストは認証を使用できません。

service-node-group コマンド

SNG_name は、サービス コンテキストの一部である 1 つまたは複数のサービス ノード グループの名前です。AppNav ポリシーで使用されているものをクロス チェックするために、リストが使用されます。2 つのサービス コンテキスト間で同じサービス ノード グループを共有できないことに注意してください。

service-policy コマンド

appnav_policy_name は、サービス コンテキストの AppNav ポリシーの名前です。

vrf name コマンド

VRF_name は、AppNav-XE コンポーネントによって認識されるトラフィックのための LAN インターフェイス上の VRF の名前です。複数の VRF 名を入力できます。最大 64 の VRF 名を定義できますが、サポートされる VRF の数に制限はありません。VRF グローバルは、VRF なしのトラフィックを識別することを除けば、他の VRF 定義と同じです。VRF 名は、次のような順番に一覧表示されます。

```
vrf name v1
vrf name v2
vrf name v3
vrf global
```

サービス コンテキストに VRF を設定しなかった場合、システムは自動的に **vrf default** のデフォルト設定を適用します。**vrf default** の目的は、設定された VRF 名または **vrf global** に一致しないトラフィックを一致させることです。

パケットに対する適切なサービス コンテキストの選択には、次のロジックが使用されます。システムは、サービス コンテキストに設定されている VRF 名（または **vrf global**）と、パケットが通過する LAN インターフェイス上の VRF を比較します。一致が検出されると、システムは対応するサービス コンテキストを選択します。一致が存在しない場合、システムは **vrf default** のサービス コンテキスト（使用可能な場合）を選択します。このようなサービス コンテキストがない場合、システムはパケットをパススルーします。

AppNav 代行受信のイネーブル化

現在、AppNav-XE コンポーネントによってサポートされているサービスは WAAS のみです。

AppNav-XE コンポーネントをイネーブルにするには、WAN インターフェイスを識別し、**service-insertion** コマンドを使用します。

（注）　デュアル RP Cisco ASR 1000 プラットフォーム上では、サブインターフェイスで **service-insertion** コマンドを使用しないでください。

```
(config)# interface if_name
(config-if)# [no] service-insertion waas
```

（注）　インターフェイスの、着信と発信の両方の TCP トラフィックは、その VRF と、VRF で識別されるサービス コンテキストに関連付けられたサービス ポリシーに基づき、AppNav 処理に従います。

AppNav サービス ノード自動検出機能の設定（Cisco CSR 1000V シリーズのみ）

ここでは、次の内容について説明します。

AppNav サービス ノード自動検出機能のイネーブル化（Cisco CSR 1000V シリーズのみ）

AppNav サービス ノード自動検出機能を設定するには、次の手順を実行します。

手順

ステップ 1　Cisco IOS-XE では、次のコマンドを入力します。*SNG_name* パラメータには、AppNav サービス ノード自動検出機能をイネーブルにするサービス ノード グループの名前を入力します。WAAS デバイスが AppNav-XE コンポーネントと同じサブネット内にあることを確認します。

```
router(config)# service-insertion service-node-group SNG_name
```

ステップ 2　次のコマンドを入力して、機能をイネーブルにします。

```
router(config-service-insertion-sng)# node-discovery enable
```

ステップ 3　WAAS デバイス上では、次のコマンドを入力します。

```
WAAS(config)# service-insertion service-node
```

ステップ 4　使用するインターフェイスを選択し、それが AppNav-XE サービスの要求元と同じサブネット内にあることを確認します。インターフェイスが指定されていない場合、デフォルトは GigabitEthernet0/0 です。

```
WAAS(config)# node-discovery enable GigabitEthernet 0/1
```

ステップ 5　次のコマンドを入力して、AppNav サービス ノード自動検出機能を設定およびイネーブル化します。

```
WAAS(config)# enable
```

AppNav サービス ノード自動検出機能のディセーブル化（Cisco CSR 1000V シリーズのみ）

次のいずれかを実行して、AppNav サービス ノード自動検出機能をディセーブルにします。

- Cisco IOS-XE に移動し、次のコマンドを入力して、システム全体のサービス ノード自動検出機能をディセーブルにします。

```
router(config)# service-insertion service-node-group sng
router(config-service-insertion-sng)# no node-discovery enable
```

- 次のように、WAAS ノードのサービス応答機能をディセーブルにします。

```
router(config)# service-insertion service-node
router(config)# no enable
```

AppNav-XE 設定の削除

AppNav-XE 設定を削除するには、次の手順を実行します。

手順

ステップ 1　コンフィギュレーション モードで、WAN インターフェイスから代行受信を削除します。次の CLI コマンドを使用します。

```
router(config)# interface GigabitEthernet0/0/1
router(config-if)# no service-insertion waas
router(config-if)# exit
```

ステップ 2　AppNav サービス コンテキストをディセーブルにします。次の CLI コマンドを使用します。

```
router(config)# service-insertion service-context  waas/1
router(config-service-insertion-context)# no enable
router(config-service-insertion-context)# exit
```

ステップ 3　AppNav サービス コンテキスト、サービス ノード グループ、および AppNav コントローラ グループを削除します。次の CLI コマンドを使用します。

```
router(config)# no service-insertion service-context  waas/1
router(config)# no service-insertion service-node-group ISR-WAAS-SNG
router(config)# no service-insertion appnav-controller-group ISR-WAAS-SCG
```

ステップ 4　AppNav ポリシー マップ、クラス マップ、およびアクセス リストを削除します。次の CLI コマンドを使用します。

```
router(config)# no policy-map type appnav ISR-WAAS
router(config)# no class-map type appnav match-any ISR-WAAS
router(config)# no ip access-list extended ISR-WAAS
router(config)# end
```