CHAPTER 6

DaiApp サービス

この章では、DCNM Web サービスの DaiApp サービスに対応する API メソッドについて説明します。

DaiApp サービスの概要

Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI）は、ネットワーク内の ARP パケットを検証するセキュリティ機能です。DAI は無効な IP アドレスと MAC アドレスのバインディングのない ARP パケットを代行受信し、ログを記録し、廃棄します。これによって、攻撃者がペイロード内に偽の IP と MAC のバインディングを持つ偽 ARP パケット（gratuitous ARP など）をホストまたはデフォルト ゲートウェイに送信する可能性がある man-in-the-middle 攻撃から、ネットワークを保護することができます。

bindArpAclOnVlans

ARP Access Control List（ACL; アクセス コントロール リスト）を VLAN（仮想 LAN）の収集に適用します。VLAN にすでに ARP ACL があるかどうかを検証する API です。また、API は DAI が VLAN 上でイネーブルかどうかについても検証します。DAI が VLAN 上でイネーブルの場合、API は、ARP ACL に基づいた ARP 検査が DAI によって行われる検証よりも優先されることを示す警告メッセージをスローします。つまり、ARP ACL に基づいてパケットを拒否する必要がある場合、パケットは DAI に基づいて有効である場合でも拒否されます。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- arpAclInstanceNameId がヌルか、またはタイプ ARP ACL InstanceNameId でない場合
- vlanInstanceNameIdCol がヌルまたは空の場合
- vlanInstanceNameIdCol 収集に 1 つのヌル要素が含まれるか、または収集に無効な VLAN InstanceNameId が含まれる場合

パラメータ

opContext — 動作可能なコンテキスト

arpAclInstanceNameId — ARP ACL オブジェクトの InstanceNameId

vlanInstanceNameIdCol — VLAN の InstanceNameId の収集

explicitDenyEnable — ARP ACL をスタティック ACL として設定する必要があるかどうかを示します。

戻り値

void

bindArpAclOnVlansByArpAclName

事前にプロビジョニングされた ARP ACL を VLAN の収集にバインドします。ARP ACL を VLAN の収集にバインドするために、ARP ACL をデバイスに物理的に設定する必要はありません。ARP ACL の名前を使用するだけで、ARP ACL を収集にバインドできます。この API は、この事前プロビジョニング設定に対応しています。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- 渡された引数 arpAclName がヌルの場合
- vlanInstanceIds 収集がヌルまたは空の場合
- vlanInstanceIds 収集に 1 つのヌル要素が含まれるか、または収集に無効な VLAN インスタンス名 ID が含まれる場合
- vlanInstanceIds 収集に、データベースに存在しない VLAN のインスタンス ID が含まれる場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- arpAclName に無効な ARP ACL 名ストリングが含まれる場合

例

- ARP ACL 名がアルファベットで始まらない場合（[2acl_test] など）
- ARP ACL 名にスペース、疑問符、または引用符の文字が含まれる場合（[acl test2]、[acl?test2]、または [acl'test] など）

パラメータ

opContext — 動作可能なコンテキスト

arpAclName — ARP ACL の名前。この ACL をデバイスに設定する必要はありません。

vlanInstanceIds — デバイスに設定されるネットワーク要素にある VLAN の InstanceNameId の収集

explicitDenyEnable — ARP ACL をスタティック ACL として設定する必要があるかどうかを示します。

戻り値

void

bindArpAclOnVlansForRange

事前にプロビジョニングされた ARP ACL を事前にプロビジョニングされた VLAN の収集にバインドします。ARP ACL を VLAN の収集にバインドするために、ARP ACL と VLAN の両方をデバイスに設定する必要はありません。ユーザは ARP ACL 名を VLAN の収集にバインドし、のちの段階で ARP ACL とバインドされた VLAN の両方を作成することができます。この API は、この事前プロビジョニング設定に対応しています。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- 渡された引数 arpAclName がヌルの場合
- 渡された引数 vlanRange がヌルの場合
- networkElementId がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合
- networkElementId によって InstanceNameId を与えられたネットワーク要素がデータベースに存在しない場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- 引数 arpAclName として与えられた ARP ACL 名が有効な ARP ACL 名ストリングではない場合

例

- ARP ACL 名がアルファベットで始まらない場合（[2acl_test] など）
- ARP ACL 名にスペース、疑問符、または引用符の文字が含まれる場合（[acl test2]、[acl?test2]、または [acl'test] など）

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

arpAclName — ARP ACL の名前。この ACL をデバイスに設定する必要はありません。

vlanRange — VLAN の範囲を表すストリング。ストリングは、カンマとハイフンで区切った VLAN のリストを保持します。たとえば、vlanRange は 4,6,9,15-20,25 となります。

explicitDenyEnable — ARP ACL をスタティック ACL として設定する必要があるかどうかを示します。

戻り値

void

clearArpRateLimitingConfigurationInInterfaces

インターフェイスの収集で行われた ARP レート リミットとバースト間隔の設定をクリアします。また、この API は、レート リミットとバースト間隔の値をデフォルト値に戻します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- 引数 interfaceNameIds がヌルであるか、または引数がタイプ インターフェイス InstanceNameId でない場合
- 収集 interfaceNameIds 内のいずれかの InstanceNameId によって指定されたインターフェイスがデータベースに存在しない場合

パラメータ

opContext — 動作可能なコンテキスト

interfaceNameIds — インターフェイスの InstanceNameId の収集

戻り値

void

createArpAcls

ネットワーク要素に 1 つまたは複数の標準 ARP ACL オブジェクトを作成します。ネットワーク要素および ARP ACL オブジェクトのリストの InstanceNameId が与えられると、サーバ内にオブジェクトを作成し、作成された ARP ACL の InstanceNameId の収集を戻します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- neInstanceNameId がヌルか、またはタイプ ネットワーク要素 InstanceNameId でない場合
- neInstanceNameId が有効なネットワーク要素 InstanceNameId でない場合
- arpAclCol 内の ARP ACL オブジェクトに名前アトリビュート セットがない場合
- arpAclCol に ARP ACL の複製エントリが含まれない場合

次のいずれかの状況が発生した場合、javax.xml.bind.PropertyException がスローされます。

- ARP ACL の名前がアルファベットで始まらない場合
- ARP ACL にスペースまたは引用符の文字が含まれる場合
- ARP ACL の名前に 234 を超える文字が含まれる場合

次のいずれかの状況が発生した場合、IntegrityException がスローされます。

- arpAclCol に、データベースにすでに存在している ARP ACL が含まれる場合
- arpAclCol 内の ARP ACL に複製 ARP ACL エントリ オブジェクトが含まれる場合

ARP ACL との VlanExternal アソシエーションは、この API では考慮されません。ユーザは別の API を呼び出して ARP ACL を VLAN にバインドする必要があります。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

arpAclCol — 作成する ARP ACL オブジェクトの収集

戻り値

新しく作成された ARP ACL オブジェクトの収集

deleteArpAcls

1 つまたは複数の ARP ACL を削除します。ARP ACL オブジェクトの InstanceNameId が与えられると、これらのオブジェクトはサーバから削除されます。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- arpAcls 収集がヌルまたは空の場合
- arpAcls 収集にタイプ ARP ACL でない要素が含まれる場合
- arpAclCol 収集に、データベースに存在しない ARP ACL が含まれる場合

パラメータ

opContext — 動作可能なコンテキスト

arpAclInstanceNameIds — 削除する ARP ACL の InstanceNameId が含まれる収集

戻り値

void

disableDaiOnVlans

ネットワーク要素にある VLAN の特定の収集の DAI をディセーブルにします。

渡された引数がヌルであるか、またはタイプ VLAN InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

vlanIds — VLAN の InstanceNameId

戻り値

void

enableDaiOnVlans

ネットワーク要素にある VLAN の特定の収集の DAI をイネーブルにします。VLAN 上で Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）スヌーピングがイネーブルかどうかを検証します。イネーブルでない場合、DAI を機能させるために DHCP スヌーピングをイネーブルにする必要があることを示す Exception をスローします。

渡された引数がヌルであるか、またはタイプ VLAN InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

vlanIds — VLAN の InstanceNameId

戻り値

特定の vlanIds のリストに対応する VLAN に関連付けられている DaiSetting オブジェクトの InstanceNameId のリスト

enableDaiOnVlansByRange

事前にプロビジョニングされた VLAN で DAI をイネーブルにします。VLAN ID を使用するだけで DAI をイネーブルにできます。DAI をイネーブルにする必要がある VLAN は、実際にデバイスに存在している必要はありません。この API は、この事前プロビジョニング設定に対応しています。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- 渡された引数 networkElementId がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合
- 渡された引数 vlanRange がヌルの場合

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

vlanRange — VLAN の範囲を表すストリング。ストリングは、カンマとハイフンで区切った VLAN のリストを保持します。たとえば、vlanRange は 4,6,9,15-20,25 となります。

戻り値

void

getArpAclsInNetworkElement

ネットワーク要素の InstanceNameId が与えられると、特定のネットワーク要素で設定されたすべての ARP ACL の収集を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

ネットワーク要素にあるすべての ARP ACL オブジェクトのリスト。戻されたオブジェクトのリストでは、次のアソシエーションのみが残され、ほかのアソシエーションはクリアされます。

- 戻された ARP ACL オブジェクトのすべての関連付けられた Access Control Entry（ACE; アクセス制御エントリ）
- 戻された ARP ACL オブジェクトを参照している VLAN
- 戻された ARP ACL が設定されているネットワーク要素

getArpAclsInVlans

VLAN InstanceNameIds の収集が与えられると、この API は関連付けられた ARP ACL（ある場合）を戻します。

パラメータ

opContext — 動作可能なコンテキスト

vlanInstanceNameIdCol — VLAN の InstanceNameId の収集

戻り値

VLAN に関連付けられた ARP ACL のリスト。パラメータ収集内に VLAN に関連付けられた ARP ACL がない場合、リストには対応する位置にあるヌル要素が含まれます。

getArpAclsWithoutAcesInNetworkElement

ネットワーク要素の InstanceNameId が与えられると、特定のネットワーク要素で設定されたすべての ARP ACL の収集を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

ネットワーク要素にあるすべての ARP ACL オブジェクトのリスト。戻されたオブジェクトのリストでは、すべてのアソシエーションがクリアされます。

getDaiDisabledVlansInNetworkElement

特定のネットワーク要素内のすべての DAI ディセーブル VLAN を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

DAI ディセーブル VlanExternal オブジェクトのリスト。戻されたオブジェクトのリストでは、次のアソシエーションのみが残され、ほかのアソシエーションはクリアされます。

- DaiSetting アソシエーション
- ARP ACL アソシエーション。この ARP ACL に ARP ACL エントリがない場合、これらのアソシエーションはクリアされます。

getDaiEnabledVlansInNetworkElement

特定のネットワーク要素内のすべての DAI イネーブル VLAN を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

DAI イネーブル VlanExternal オブジェクトのリスト。戻されたオブジェクトのリストでは、次のアソシエーションのみが残され、ほかのアソシエーションはクリアされます。

- DaiSetting アソシエーション
- ARP ACL アソシエーション。この ARP ACL に ARP ACL エントリがない場合、これらのアソシエーションはクリアされます。

getDaiGlobalSettingsInNetworkElements

特定のネットワーク要素のリストの DAI グローバル設定を取得します。ネットワーク要素の InstanceNameId が与えられると、DAI グローバル設定の収集を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

neInstanceNameIds — ネットワーク要素の InstanceNameId

戻り値

DaiGlobalSetting オブジェクトのリスト。戻されたリストには、特定のネットワーク要素のリストに関連する DaiGlobalSetting オブジェクトが含まれます。

getDaiSettingOnVlans

特定の VLAN のリストに関連する DAI 設定のリストを戻します。

渡された引数がヌルであるか、またはタイプ VLAN InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

vlanIds — VLAN の InstanceNameId

戻り値

DaiSetting オブジェクトのリスト。戻されたオブジェクトのリストでは、次のアソシエーションのみが残され、ほかのアソシエーションはクリアされます。

- VLAN アソシエーション
- DAI 設定に関連付けられた VLAN に関連付けられた ARP ACL。この ARP ACL に ARP ACL エントリがない場合、これらのアソシエーションはクリアされます。

getInterfacesWithArpRateLimitingInNetworkElement

ARP レートおよびバースト間隔が設定された特定のネットワーク要素にあるすべてのインターフェイスを戻します。これらのインターフェイスには、ARP レート リミットとバースト間隔に設定された値があります。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

ARP レート リミットとバースト間隔が設定されたインターフェイス オブジェクトの収集

getTrustStateSettingInInterfaces

信頼状態設定オブジェクトの収集を戻します。インターフェイス InstanceNameId の収集が与えられると、信頼状態設定オブジェクトの収集を戻します。

渡された引数がヌルであるか、またはタイプ インターフェイス InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

interfaceInstanceIds — インターフェイスの InstanceNameId

戻り値

TrustStateSetting オブジェクトの収集

getUntrustedInterfacesWithDefaultRateInNetworkElement

ネットワーク要素の InstanceNameId が与えられると、デフォルトの ARP レートとバースト間隔の値を持つ特定のネットワーク要素にあるすべての信頼されないインターフェイスを戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

デフォルトのレート リミットとバースト間隔を持つ信頼されないインターフェイス オブジェクトの収集

getVlansWithDaiSettingNetworkElement

特定のネットワーク要素内の DaiSetting オブジェクトを持つすべての VLAN を戻します。

渡された引数がヌルであるか、またはタイプ ネットワーク要素 InstanceNameId でない場合、ValidationException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

networkElementId — ネットワーク要素の InstanceNameId

戻り値

DaiSetting オブジェクトを持つ VLAN のリスト。戻されたオブジェクトのリストでは、次のアソシエーションのみが残され、ほかのアソシエーションはクリアされます。

- DaiSetting アソシエーション
- ARP ACL アソシエーション。この ARP ACL に ARP ACL エントリがない場合、これらのアソシエーションはクリアされます。

modifyAclSequence

開始シーケンス番号およびシーケンス番号を増加させるステップに基づいて、ACL 内の ACE のシーケンス番号を修正します。

パラメータ

opContext — 動作可能なコンテキスト

aclInstanceNameIdCol — 1 つまたは複数の ACL の InstanceNameId

再シーケンスは、プラットフォーム タイプが Nexus 7000 シリーズ スイッチの場合にのみサポートされます。

startSeqNo — この初期値を使用して、アクセス リスト エントリが再シーケンスされます。

increment — シーケンス番号が変更される幅。たとえば、increment の値が 5 で、開始シーケンス番号が 20 の場合、その後のシーケンス番号は、25、30、35、40 などになります。

戻り値

void

modifyArpAcls

1 つまたは複数の既存の ARP ACL オブジェクトを修正します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- arpAcls 収集がヌルまたは空の場合
- arpAcls 収集にタイプ ARP ACL でないオブジェクトが含まれる場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- arpAcls 収集内の ARP ACL の名前が修正された場合

次のいずれかの状況が発生した場合、IntegrityException がスローされます。

- arpAclCol 収集に、データベースに存在しない ARP ACL オブジェクトが含まれる場合
- arpAcls 収集内の ARP ACL に複製 ARP ACL エントリ オブジェクトが含まれる場合

この API は ARP ACL オブジェクトの VLAN アソシエーションを考慮しません。ユーザは別の API を呼び出して ARP ACL を VLAN にバインドする必要があります。

パラメータ

opContext — 動作可能なコンテキスト

arpAcls — データベース内の既存の ARP ACL オブジェクトに取って代わる修正された ARP ACL オブジェクトの収集

戻り値

void

modifyDaiGlobalSettingsInNetworkElements

特定のネットワーク要素の収集内の 1 つまたは複数の既存の DAI グローバル設定オブジェクトを修正します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- networkElementIds 収集がヌルまたは空の場合
- networkElementIds 収集に 1 つのヌル要素が含まれるか、または収集に無効なネットワーク要素 InstanceNameId が含まれる場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- daiGlobalSettings 収集で、いずれか 1 つの daiGlobalSetting アトリビュートが有効でない場合

例

- logBufferSize アトリビュートに 0 ～ 1024 の値が含まれていない場合
- logInterval アトリビュートに 0 ～ 86400 の値が含まれていない場合

次のいずれかの状況が発生した場合、IntegrityException がスローされます。

- 収集 networkElementIds と収集 daiGlobalSettings のサイズが等しくない場合

パラメータ

opContext — 動作可能なコンテキスト

networkElementIds — DAI グローバル パラメータを修正する必要があるネットワーク要素の InstanceNameId

daiGlobalSettings — 修正された DAI グローバル設定オブジェクト

戻り値

void

modifyDaiOnVlans

1 つまたは複数の既存の DAI 設定オブジェクトを修正します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- modifiedDaiSettings 収集がヌルまたは空の場合
- modifiedDaiSettings 収集にタイプ DaiSetting でないオブジェクトが含まれる場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- 修正された DAI 設定オブジェクト内の VLAN の参照が変更された場合

パラメータ

opContext — 動作可能なコンテキスト

modifiedDaiSettings — データベース内の既存の DAI 設定オブジェクトに取って代わる修正された DaiSetting オブジェクトの収集

戻り値

void

modifyDaiSettingsAndArpAclBindingsOnVlans

特定の VLAN の収集内の DAI 設定と ARP ACL バインディングを修正します。渡された VLAN オブジェクトには、修正された DAI 設定と修正された ARP ACL バインディングが含まれます。

ARP ACL エントリの修正は、この API ではサポートされていません。modifyArpAcls（リスト arpAcls）API を使用し、ARP ACL の ARP ACL エントリを修正します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- modifiedVlanObjects 収集がヌルまたは空の場合
- modifiedVlanObjects に、データベースに存在しない VLAN が含まれている場合
- modifiedVlanObjects 収集内の要素に対応するデータベース内の VLANに DAI 設定が含まれない場合

DAI 設定のアトリビュートまたは modifiedVlanObjects 内の VLAN に関連付けられた ARP ACL のアトリビュートのいずれかが有効でない場合、PropertiesException がスローされます。

パラメータ

opContext — 動作可能なコンテキスト

modifiedVlanObjects — DAI 設定と ARP ACL 参照を持つ修正された VLAN オブジェクトの収集

戻り値

void

modifyTrustStateSettings

特定のネットワーク インターフェイスの収集内の 1 つまたは複数の既存の信頼状態設定オブジェクトを修正します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- interfaceInstanceIds 収集がヌルまたは空の場合
- interfaceInstanceIds 収集に 1 つのヌル要素が含まれるか、または収集に無効なインターフェイス InstanceNameId が含まれる場合
- trustStateSettings 収集がヌルまたは空の場合
- trustStateSettings 収集にタイプ TrustStateSetting でない要素が含まれる場合

次のいずれかの状況が発生した場合、PropertiesException がスローされます。

- trustStateSettings 収集で、いずれかの trustStateSetting アトリビュートが有効でない場合

例

- arpRate アトリビュートに 0 ～ 2048 の値が含まれていない場合
- burstInterval アトリビュートに 0 ～ 15 の値が含まれていない場合

次のいずれかの状況が発生した場合、IntegrityException がスローされます。

- interfaceInstanceIds 収集と trustStateSettings 収集のサイズが等しくない場合
- trustStateSettings 収集にタイプ TrustStateSetting でないインターフェイスが含まれる場合

パラメータ

opContext — 動作可能なコンテキスト

interfaceInstanceIds — インターフェイスの InstanceNameIds

trustStateSettings — 修正された TrustStateSetting オブジェクト

戻り値

void

unbindArpAclFromVlans

VLAN の収集内の ARP ACL とのアソシエーションを削除します。

次のいずれかの状況が発生した場合、ValidationException がスローされます。

- vlanInstanceNameIds 収集がヌルまたは空の場合
- vlanInstanceNameIdCol 収集に 1 つのヌル要素が含まれるか、または収集に無効な VLAN インスタンス名 ID が含まれる場合

パラメータ

opContext — 動作可能なコンテキスト

vlanNameIds — ARP ACL アソシエーションを削除する必要がある VLAN の InstanceNameId

戻り値

void