Model Based AAA

The NETCONF and RESTCONF interfaces implement the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.

Model Based AAA

Prerequisites for Model Based AAA

Working with the model based AAA feature requires prior understanding of the following :

- NETCONF-YANG
- NETCONF-YANG kill-session
- RFC 6536: Network Configuration Protocol (NETCONF) Access Control Model

Initial Operation

Upon enabling the NETCONF and/or RESTCONF services, a device that has no prior configuration of the /nacm subtree will deny read, write, and execute access to all operations and data other than the users of privilege level 15. This is described in the following configuration of the /nacm subtree:

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
      <enable-nacm>true</enable-nacm>
      <read-default>deny</read-default>
      <write-default>deny</write-default>
      <exec-default>deny</exec-default>
      <enable-external-groups>true</enable-external-groups>
      <rule-list>
        <name>admin</name>
        <group>PRIV15</group>
        <rule>
          <name>permit-all</name>
          <module-name>*</module-name>
          <access-operations>*</access-operations>
          <action>permit</action>
```

```
    </rule>
  </rule-list>
</nacm>
```

Group Membership

The group membership of a user can come from two sources- first, from the privilege level of the user as configured on the AAA server used for authorization, and second, from those configured in the /nacm/groups subtree. The names of the groups that correspond to each privilege level are as follows:

Privilege level	NACM group name
0	PRIV00
1	PRIV01
2	PRIV02
3	PRIV03
4	PRIV04
5	PRIV05
6	PRIV06
7	PRIV07
8	PRIV08
9	PRIV09
10	PRIV10
11	PRIV11
12	PRIV12
13	PRIV13
14	PRIV14
15	PRIV15

Note Traditional IOS command authorization, such as those based on privilege level, does not apply to NETCONF or RESTCONF.

Note Access granted to a NACM group based on a privilege level do not inherently apply to NACM groups with higher privilege level. For example, rules that apply to PRIV10 do not automatically apply to PRIV11, PRIV12, PRIV13, PRIV14, and PRIV15 as well.

NACM Privilege Level Dependencies

If the AAA configuration is configured with **no aaa new-model**, the privilege level locally configured for the user is used. If the AAA configuration is configured with **aaa new-model**, the privilege level is determined by the AAA servers associated with the method list **aaa authorization exec default**.

NACM Configuration Management and Persistance

The NACM configuration can be modified using NETCONF or RESTCONF. In order for a user to be able to acccess the NCAM configuration, they must have explicit permission to do so, that is, through a NACM rule. Configuration under the /nacm subtree persists when the **copy running-config startup-config** EXEC command is issued, or the **cisco-ia:save-config** RPC is issued.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-config xmlns="http://cisco.com/yang/cisco-ia"/>
</rpc>
```

Note The NACM rules that apply to a NETCONF session are those that are configured in the /nacm subtree at the time of session establishment. Modifying the /nacm subtree has no effect on NETCONF sessions as they are already established. The <kill-session> RPC or the **clear netconf-yang session** EXEC command can be used to forcibly end an unwanted NETCONF session. See NETCONF Kill Session.

Note Care should be taken when crafting rules to deny access to certain data as the same data may be exposed through multiple YANG modules and data node paths. For example, interface configuration is exposed through both **Cisco-IOS-XE-native** and **ietf-interface**. Rules that may apply to one representation of the same underlying data may not apply to other representations of that data.

Resetting the NACM Configuration

Use the following command to reset the /nacm subtree configuration to the initial configuration (see Initial Operation).

```
Router#request platform software yang-management nacm reset-config
```

Sample NACM Configuration

Note The examples in this section are for illustrative purposes only.

The following is a sample for groups configuration.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <groups>
      <group>
        <name>administrators</name>
        <user-name>admin</user-name>
        <user-name>root</user-name>
```

```
    </group>

    <group>
      <name>limited-permission</name>
      <user-name>alice</user-name>
      <user-name>bob</user-name>
    </group>
  </groups>
</nacm>
```

Table 1: Description of the Configuration Paramenters for Groups Configuration

Parameter	Description
<name>administrators</name>	Group name
<user-name>admin</user-name>	User name
<user-name>root</user-name>	User name

The following is a sample for creating module rules.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>only-ietf-interfaces</name>
    <group>limited-permission</group>
    <rule>
      <name>deny-native</name>
      <module-name>Cisco-IOS-XE-native</module-name>
      <access-operations>*</access-operations>
      <action>deny</action>
    </rule>
    <rule>
      <name>allow-ietf-interfaces</name>
      <module-name>ietf-interfaces</module-name>
      <access-operations>*</access-operations>
      <action>permit</action>
    </rule>
  </rule-list>
</nacm>
```

Table 2: Description of the Configuration Paramenters for Creating Module Rules

Parameter	Description
<name>only-ietf-interfaces</name>	Unique rule-list name
<group>limited-permission</group>	Groups that rule-list applies to
<name>deny-native</name>	Unique rule name
<module-name>Cisco-IOS-XE-native</module-name>	Name of the YANG module
<access-operations>*</access-operations>	CRUDx operation types
<action>deny</action>	Permit/deny

The following is a sample for creating protocol operation rules.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>only-get</name>
    <group>limited-permission</group>

    <rule>
      <name>deny-edit-config</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>edit-config</rpc-name>
      <access-operations>exec</access-operations>
      <action>deny</action>
    </rule>
    <rule>
      <name>allow-get</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>get</rpc-name>
      <access-operations>exec</access-operations>
      <action>permit</action>
    </rule>
  </rule-list>
</nacm>
```

Table 3: Description of the Configuration Paramenters for Creating Protocol Operation Rules

Parameter	Description
<name>only-get</name>	Unique rule-list name
<group>limited-permission</group>	Groups that rule-list applies to
<name>deny-edit-config</name>	Unique rule name
<module-name>ietf-netconf</module-name>	Name of module containing the RPC
<rpc-name>edit-config</rpc-name>	Name of the RPC
<access-operations>exec</access-operations>	Execute permission for the RPC
<action>deny</action>	Permit/deny

The following is a sample for creating data node rules.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>hide-enable-passwords</name>
    <group>limited-permission</group>

    <rule>
      <name>deny-enable-passwords</name>
      <path xmlns:ios="http://cisco.com/ns/yang/Cisco-IOS-XE-native>/ios:native/enable
      </path>
      <access-operations>*</access-operations>
      <action>deny</action>
    </rule>
  </rule-list>
</nacm>
```

Table 4: Description of the Configuration Paramenters for Creating Data Node Rules

Parameter	Description
<name>hide-enable-passwords</name>	Unique rule-list name
<group>limited-permission</group>	Groups that rule-list applies to
<name>deny-enable-passwords</name>	Unique rule name
<path xmlns:ios="http://cisco.com/ns/yang/Cisco-IOS-XE-native">/ios:native/enable</path>	Path to the data node being granted/denied
<access-operations>*</access-operations>	CRUDx operation types
<action>deny</action>	Permit/deny

The following is an example NACM configuration that permits all groups to use the standard NETCONF RPCs <get> and <get-config>, the schema download RPC <get-schema>, and read-only access to the data in the module **ietf-interfaces**:

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
      <rule-list>
        <name>readonly-protocol</name>
        <group>*</group>
        <rule>
          <name>get-permit</name>
          <module-name>ietf-netconf</module-name>
          <rpc-name>get</rpc-name>
          <access-operations>exec</access-operations>
          <action>permit</action>
        </rule>
        <rule>
          <name>get-config-permit</name>
          <module-name>ietf-netconf</module-name>
          <rpc-name>get-config</rpc-name>
          <access-operations>exec</access-operations>
          <action>permit</action>
        </rule>
        <rule>
          <name>get-schema-permit</name>
          <module-name>ietf-netconf-monitoring</module-name>
          <rpc-name>get-schema</rpc-name>
          <access-operations>exec</access-operations>
          <action>permit</action>
        </rule>
      </rule-list>
      <rule-list>
        <name>readonly-data</name>
        <group>*</group>
        <rule>
          <name>ietf-interfaces-permit</name>
          <module-name>ietf-interfaces</module-name>
          <access-operations>read</access-operations>
          <action>permit</action>
        </rule>
      </rule-list>
    </nacm>
```

Additional References for Model Based AAA

Related Documents

Related Topic	Document Title
YANG data models for various release of IOS-XE, IOS-XR, and NX-OS platforms	To access Cisco YANG models in a developer-friendly way, please clone the *GitHub repository*, and navigate to the *vendor/cisco* subdirectory. Models for various releases of IOS-XE, IOS-XR, and NX-OS platforms are available here.

Standards and RFCs

Standard/RFC	Title
RFC 6020	*YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*
RFC 6241	*Network Configuration Protocol (NETCONF)*
RFC 6536	*Network Configuration Protocol (NETCONF) Access Control Model*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Model-Based AAA

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Programmability: Data Models

Feature Name	Release	Feature Information
Model-Based AAA	Cisco IOS XE Fuji 16.8.1	This feature was implemented on the following platforms: • Cisco ASR 900 Series Aggregated Services Routers • Cisco ASR 920 Series Aggregated Services Routers • Cisco ASR 1000 Series Aggregated Services Routers • Cisco CSR 1000v Switches • Cisco ISR 1100 Series Integrated Services Routers • Cisco ISR 4000 Series Integrated Services Routers • Cisco NCS 4200 Series
	Cisco IOS XE Fuji 16.8.1a	This feature was implemented on the following platforms: • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches