Management RADIUS Authentication Using Windows NPS

AD Infrastructure

- Create New Security Group on Active Directory
RADIUS Infrastructure

- Microsoft Windows Server 2012 R2: Network Policy Server
- RADIUS Clients
Connection Request Policies
Network Policies

Switching
HP Aruba 2920: Switch

Create RADIUS Client

[Image of RADIUS Client creation settings]
- Enable this RADIUS client
- Select an existing template:
- Name and Address:
  - Friendly name: Aruba-Switch-Authentication
  - Address (IP or DNS): 172.16.0.0/16
- Shared Secret:
  - Select an existing Shared Secrets template: None
  - To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
  - Manual
  - Shared secret: ************
  - Confirm shared secret: ************
Create RADIUS Client and Enable RADIUS Standard

Aruba-Switch-Authentication Properties

Settings

Vendor
Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard

Advanced

Additional Options

- Access-Request messages must contain the Message-Authenticator attribute
- RADIUS client is NAP-capable

OK  Cancel  Apply
Create Network Policy

Aruba-Switch-Policy Properties

Policy name: [Aruba Switch Policy]

Policy State:
- [ ] Policy enabled

Access Permission:
- [ ] Grant access. Grant access if the connection request matches this policy.
- [ ] Deny access. Deny access if the connection request matches this policy.
- [ ] Ignore user account dial-in properties.

Network connection method:
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select [Unspecified].

- [ ] Type of network access server:
  - Unspecified
  - Vendor specific

Create Policy – Conditions

Aruba-Switch-Policy Properties

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Groups</td>
<td>DOMAIN\Infrastructure Net</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>PAP</td>
</tr>
</tbody>
</table>

Condition description:
The Authentication Type condition specifies the authentication methods required to match this policy.
Create Policy Constraints – Authentication Methods

Configure the constraints for the network policy. If all constraints are not matched by the connection request, network access is denied.

Constraints:

- **Authentication Methods**
- **Idle Timeout**
- **Session Timeout**
- **Called Station ID**
- **Day and time restrictions**
- **NAS Port Type**

### Authentication Methods

Allow access only to those clients that authenticate with the specified methods.

**EAP Types**

EAP types are negotiated between NFS and the client in the order in which they are listed.

**EAP Types:**

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
  - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method
- Perform machine health check only

[Add...][Edit...][Remove]
Create Policy Constraints – NAS Port Type Virtual (VPN)

Create Policy Settings – Standard Attributes

Framed-Protocol: PPP
Service-Type: Administrative
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed-Protocol</td>
<td>PPP</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Administrative</td>
</tr>
</tbody>
</table>
Network Policy – NAP Enforcement and Auto Remediation

Network Policy Overview

<table>
<thead>
<tr>
<th>Policy</th>
<th>Status</th>
<th>Access</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba-Switch-Policy</td>
<td>Enabled</td>
<td>2</td>
<td>Grant Access</td>
</tr>
<tr>
<td>Connections to Microsoft</td>
<td>Enabled</td>
<td>3</td>
<td>Deny Access</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>Enabled</td>
<td>4</td>
<td>Deny Access</td>
</tr>
</tbody>
</table>

Network Policy Condition

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Groups</td>
<td>MBDOMAIN\IT Infrastructure</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>PAP</td>
</tr>
</tbody>
</table>
### Network Policy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended State</td>
<td>&lt;Blank&gt;</td>
</tr>
<tr>
<td>Access Permission</td>
<td>Grant Access</td>
</tr>
<tr>
<td>NAS Port Type</td>
<td>Virtual (VPN)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)</td>
</tr>
<tr>
<td>NAP Enforcement</td>
<td>Allow full network access</td>
</tr>
<tr>
<td>Update Noncompliant Clients</td>
<td>True</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>PPP</td>
</tr>
<tr>
<td>Service Type</td>
<td>Administrative</td>
</tr>
<tr>
<td>BAP Percentage of Capacity</td>
<td>Reduce Multilink if server reaches 50% for 2 minutes</td>
</tr>
<tr>
<td>Ignore User Dial-In Properties</td>
<td>True</td>
</tr>
</tbody>
</table>

### Create Connection Request Policy

**Aruba-Switch-Access Properties**

- **Policy name:** Aruba-Switch-Access
- **Policy State:** If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evaluate this policy.
- **Network connection method:**
  - Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
  - **Type of network access server:** Unspecified
  - **Vendor specific:**
    - 10
Configuring AAA on Aruba 2920 Switch

Enable and Specify RADIUS Authentication Server

radius-server host 172.16.4.117 key "Welcome123!" acct-port 1646 auth-port 1645
radius-server retransmit 2

Enable SSH Login via RADIUS

aaa authentication ssh login radius local
aaa authentication ssh enable radius local
Enable Web Login via RADIUS

```
aaa authentication web login radius
aaa authentication web enable radius
aaa authentication web-based peap-mschapv2
```

Enable Authentication and Accounting Parameters

```
aaa accounting commands interim-update radius
aaa authentication num-attempts 7
aaa authentication login privilege-mode
```

PS: The following command is what will get everything working for you as without it; you will get the error below;

```
Access denied: no user’s authorization info supplied by the RADIUS server
```

Golden Command to allow SSH Sessions to Switch

```
aaa authorization commands commands none
```

Verify and Troubleshoot

Check Switch RADIUS Authentication

```
Aruba-Edge-Switch# show radius authentication
```

<table>
<thead>
<tr>
<th>Status and Counters - RADIUS Authentication Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS Identifier : Aruba-Edge-Switch</td>
</tr>
<tr>
<td>Invalid Server Addresses : 0</td>
</tr>
<tr>
<td>Server IP Addr</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>172.16.4.117</td>
</tr>
</tbody>
</table>
Check Recent SSH Logins

```
Aruba-Edge-Switch# show authentication last-login

+----------------+-------+-----------------+-----------------+
| Username       | Priv  | Last Login      | Last Login IP Address |
|----------------+-------+-----------------+-----------------+
| jsmith         | Mgr   | 2019-03-21 13:18:28 | 172.16.122.120   |
| sarif          | Mgr   | 2019-03-21 09:56:57 | 172.16.122.196   |
```

On Microsoft NPS Server 2012 R2 – Launch Events Viewer

![Image of Event Viewer](image)

Check Authentication Informational Log Reporting

```
<table>
<thead>
<tr>
<th>Level</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>21/03/2019 13:52:39</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:52:39</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:52:17</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:40:36</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:40:36</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:29:31</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:29:31</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:53</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:53</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:21</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:21</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:13</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:08</td>
</tr>
<tr>
<td>Information</td>
<td>21/03/2019 13:28:08</td>
</tr>
</tbody>
</table>
```
Network Policy Server granted access to a user.

**User:**
- Security ID: MercuryLabs\soppong
- Account Name: soppong
- Account Domain: MercuryLabs
- Fully Qualified Account Name: MercuryLabs\soppong

**Client Machine:**
- Security ID: NULL SID
- Account Name: -
- Fully Qualified Account Name: -
- OS-Version: -
- Called Station Identifier: -
- Calling Station Identifier: 172.16.122.109

**NAS:**
- NAS IPv4 Address: 172.16.122.19
- NAS IPv6 Address: -
- NAS Identifier: Aruba-Edge-Switch
- NAS Port-Type: Virtual
- NAS Port: -

**RADIUS Client:**
- Client Friendly Name: Aruba-Switch-Auth-Corp
- Client IP Address: 172.16.122.19

**Authentication Details:**
- Connection Request Policy Name: Aruba-Switch-Access
- Network Policy Name: Aruba-Switch-Corp-Policy
- Authentication Provider: Windows
- Authentication Server: NPS-Server.expertnetworkconsultant.com
- Authentication Type: PAP
- EAP Type: -
- Account Session Identifier: -
- Logging Results: Accounting information was written to the local log file.

**Quarantine Information:**
- Result: Full Access
- Session Identifier: -