# BeyondInsight for Unix & Linux 22.3 RNS Deployment Guide

# Table of Contents

# RNS Deployment with BIUL

This document outlines the use of BeyondInsight for Unix & Linux (BIUL) to deploy and manage a Privilege Management for Unix and Linux (PMUL) installation using the Registry Name Service (RNS) and Client Registration Profiles (CRP). Additionally, it provides an overview of Policy Management and configuration.

A minimum deployment of RNS can involve just a single host, but to better illustrate features and BIUL integration, this guide provides a more robust example.

The objective of this document is to deploy an RNS network using CRP that utilizes synchronized role-based policies with policy and log server redundancy. All required keys are managed by the system and REST connectivity with BIUL is established automatically.

> 📌 ***Note:*** *This document assumes that BIUL has been deployed and that it has access to PMUL 10.3 or greater. It further assumes general working understanding of PMUL and BIUL.*

# Overview of CRPs and RNS

## Client Registration Profiles

Installation of Privilege Management for Unix and Linux (PMUL) has historically required manual steps, such as editing settings files or copying keys and settings from machine to machine. Client Registration Profiles (CRP) simplify PMUL deployments by allowing the user to configure some environmental settings during an installation.

> *Example: A profile can be used to copy encryption keys from machine to machine to enable communication. It can also copy a settings file or join Registry Name Service (RNS) groups immediately.*

Without using CRP, administrators need to manually provision files, keys, etc., on every host. CRP provides a centralized, customizable definition of what an installation looks like and handles that provisioning.

> *Note: CRP can be used with or without RNS; however, in RNS environments, CRP is required.*

## Registry Name Service

Registry Name Service is an alternative installation mode for PMUL. Historically, there has been no formal way to provide an entire PMUL network topology (what clients are involved, what policies they are receiving, etc.) or synchronization of important elements.

RNS provides a host registry that allows the user to define service groups and to manage members of those groups.

> *Example: The administrator may create a **custom_policy** group that is in the category **policy**. This group, which is responsible for managing and delivering policy, is assigned members of three possible **roles**:*
> - ***Primary:** Responsible for handling policy writes and synchronization*
> - ***Secondaries:** Maintain copies of policy and can be used for delivery*
> - ***Clients:** Customers of this policy*

### RNS Registry Primary

The **RNS Registry Primary** server is the primary in the **Registry** group, of which there is only one per PMUL network. This server provides the Client Registration Profiles for subsequent installations and is the source of the network map for the deployment.

# Prepare for Installation

## Prepare an Action Plan

Before deployment, you should make a few decisions and create an action plan. In this example, our objective is the following:

- Use a host (**rns-primary.biul.qa**) as the primary Registry Name Service (RNS) server.
- Use role-based policy.
- Use Client Registration Profiles (CRP) to onboard new machines to the RNS network.
- Use the default RNS log group, but create a custom policy group (**custom_policy**).

> 📌 **Note:** *The step above is not required. It is merely to illustrate the process.*

- Use a host (**services-primary.biul.qa**) as the primary log and policy host.
- Use a second host (**services-secondary.biul.qa**) as the secondary for the previous.
- Use BIUL to deploy a client to this RNS network. It writes to the log server and gets policy from the policy server.

## Create Action Plan Steps

Based on the objectives above, you can now create action plan steps and follow through the logical order:

1. Discover hosts.
2. Manage credentials.
3. Profile hosts.
4. Deploy the RNS primary.
5. Create the custom policy group.
6. Configure Client Registration Profiles.
7. Deploy the group primaries.
8. Enable and configure role-based policy.
9. Deploy the group secondaries.
10. Deploy the client.
11. Execute policy.

> 📌 **Note:** *The remainder of this guide goes into further detail for each step listed above. For more information about a certain step, please see the appropriate topic in the guide.*

# Discover Hosts After Authentication

You can discover and manage hosts from the **Host Inventory** page in BIUL.

- After authenticating into BIUL, click the **Host Inventory** tile on the home page.
- Next, click the **Add Hosts** dropdown menu grid item.
- Select **Scan for Hosts**. An additional card appears, with fields you can edit to add a new host.

Provide the IP addresses of the machines being used in this deployment. You can provide a file, an IP range, or a single IP. Enable **Automatically accept SSH fingerprints** for demo purposes.

**HOST INVENTORY**

Perform actions on managed hosts
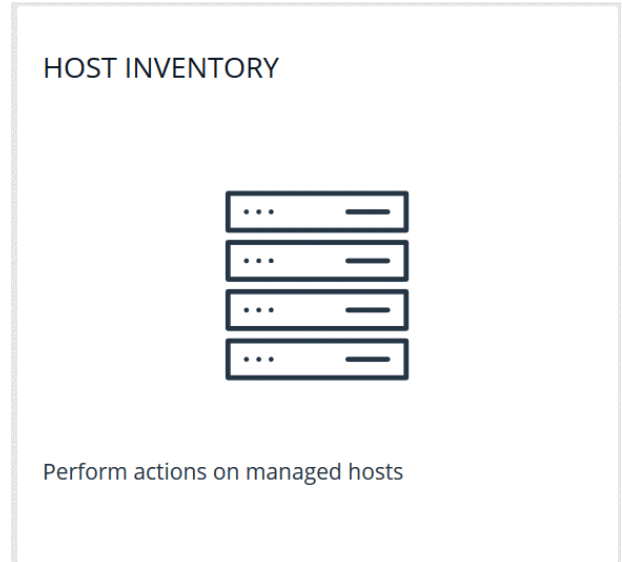
**SCAN FOR HOSTS**  ✖

Scan hosts by IP (10.100.1.0), a hyphen-separated IP range (10.100.1.0-10.100.1.20), or CIDR notation (10.100.1.0/24)

Address

SSH Port
22

SSH Host Public Key SHA256 Fingerprint (optional - single IP disc...

☑ Automatically accept SSH fingerprints

SCAN FOR HOST
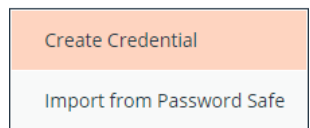
# Manage Credentials

To install software credentials, you are required to copy files to the server and execute commands.

From the left navigation menu, select the **Hosts** page, and then select the **Host Credentials** tile.

HOST CREDENTIALS

Manage credentials for accessing remote hosts
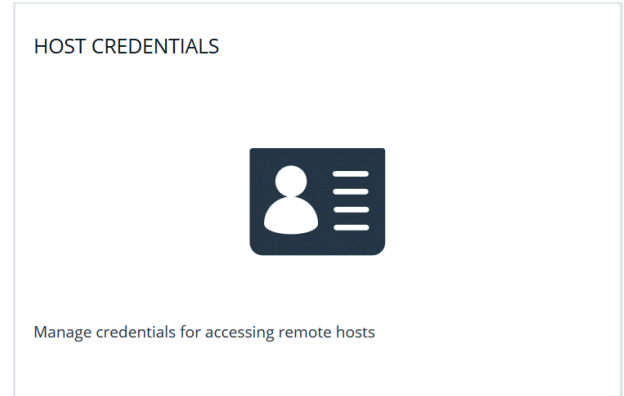
On the far right of the **Credentials** grid, click **Manage Credentials** to open the dropdown menu. Next, select **Create Credential**. Create credentials for each of your hosts. For demo purposes, it may be useful to manage one set of credentials replicated on each machine.
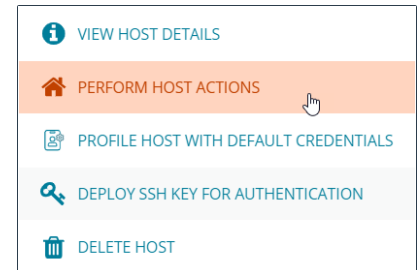
MANAGE CREDENTIALS ⊕

Create Credential

Import from Password Safe

📌 ***Note:*** *In real-world scenarios, you could use distinct credentials or **Password Safe** to manage secrets.*

# Profile Hosts

BIUL must do an initial scan of the hosts to capture some basic information. Navigate to the **Hosts Inventory** tile from the **Hosts** page. The discovered hosts become visible in the grid.

1. At the right of the server hostname row, click the ellipsis menu icon, and then select **Perform Host Actions**.
2. Select **Profile** under **Step 1: Primary Action**. Click **Next Step**. Since the other steps are not needed here, they are skipped.
3. In **Step 4: Credential Selection**, choose the appropriate credential from the dropdown menu and select from the provided delegation tools.

> ℹ️ VIEW HOST DETAILS
> 🏠 PERFORM HOST ACTIONS
> 📄 PROFILE HOST WITH DEFAULT CREDENTIALS
> 🔍 DEPLOY SSH KEY FOR AUTHENTICATION
> 🗑️ DELETE HOST

> 📌 *Note: If your credentials are the same on each machine, you can select all hosts that they apply to in the grid, and instead choose Actions > Perform Host Actions from the Hosts Inventory page.*

4. At **Step 5: Summary**, you can review the information you've provided before you continue. Click **Finish** to finalize your actions and run the profile.

## Review on the Task Page

5. Review the **Task** page, and verify the completed status of attempted actions under **Task Summary**.
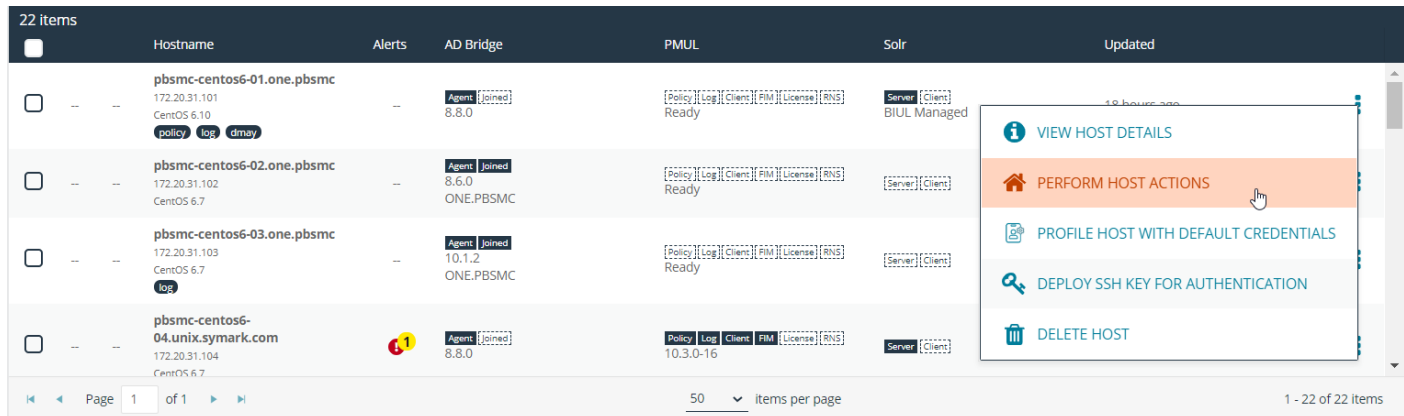6. Click **Task Details** to view more information about **Task Status**.

> 📌 *Note: Task information is always available via the Tasks navigation element.*

**SALES:** www.beyondtrust.com/contact    **SUPPORT:** www.beyondtrust.com/support    **DOCUMENTATION:** www.beyondtrust.com/docs

8

# Deploy the RNS Primary from Hosts Inventory

On the **Hosts Inventory** page, at the right of the server hostname row, click the vertical ellipsis icon in the **Inventory** grid to display a dropdown menu that displays the following menu items: **View Host Details**, **Perform Host Actions**, **Profile Host with Default Credentials**, **Deploy SSH Key for Authentication**, and **Delete Host**.

Click **Perform Host Actions**.



On the expanded **Perform Action** card, choose Privilege Management for Unix and Linux from the list of software under **Step 1: Primary Action**. Click **Next Step**.

On the **Step 2: Secondary Action** card, set the secondary action to **Install**. Click **Next Step**.

On the **Step 3: Action Requirements** card, select **Primary Registry Server and All Components** from the **Installation Template** dropdown menu. Choosing this option assigns the host the **Primary** role in the Registry Name Service group.

After selecting the **Primary Registry Server and All Components** template, select **Install Primary Registry Server** from the **Client Registration Server** dropdown. Click **Next Step**.

In the **Step 4: Credential Selection** card, select the appropriate host connection credential in the **Credential** field along with the appropriate delegation tool from the available options. Click **Next Step**.

In the **Step 5: Summary** card, review all of the previous entries before finalizing your changes.

Click **Finish** to proceed to **Step 6: Review Task Details** which displays the **Task** page. Review the completed status of the performed actions under the displayed **Task Summary**. Click **Task Details** to view expanded details about the actions. Errors are displayed during these steps to assist with troubleshooting.

**IMPORTANT!**

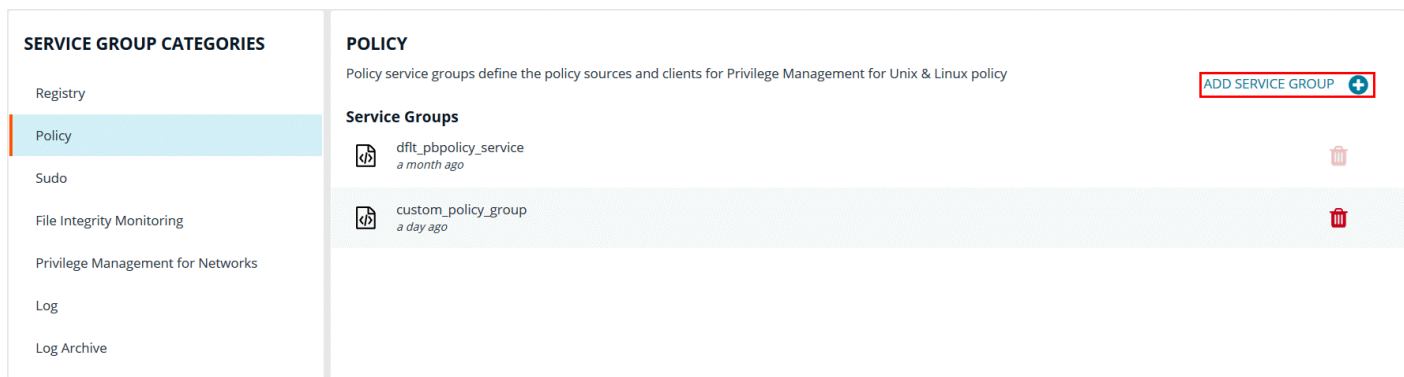*Each RNS deployment must have exactly one Primary Registry Server.*

# Create an RNS Custom Policy Group

As noted previously, this step is entirely optional and is included only to illustrate functionality. Rather than using the **dflt_policy_service** group, which is always available in the Registry Name Service (RNS), create a custom group and use it in the deployment.

From the **Hosts** landing page, select **Registry Name Service**.

REGISTRY NAME SERVICE

Manage Privilege Management for Unix & Linux Registry Name Service systems
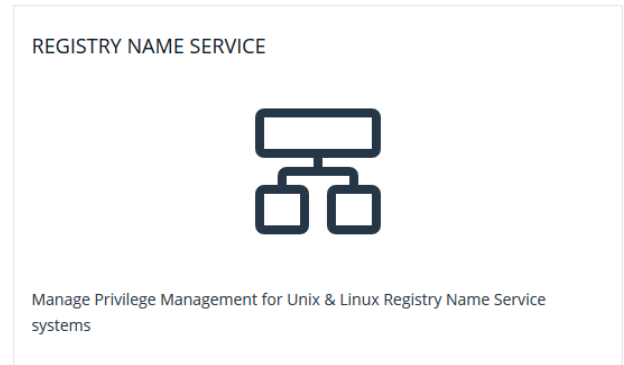
Choose the primary that was just installed from the presented list in the grid. A new list of categories appears under **Service Group Categories**. Select the **Policy** category and choose **Add Service Group**. In the expanded **Service Groups** card, name the new group **custom_policy_group** and click **Create**.

| SERVICE GROUP CATEGORIES | POLICY |
|---|---|
| Registry | Policy service groups define the policy sources and clients for Privilege Management for Unix & Linux policy |
| Policy | ADD SERVICE GROUP |
| Sudo | **Service Groups** |
| File Integrity Monitoring | dflt_pbpolicy_service — a month ago |
| Privilege Management for Networks | custom_policy_group — a day ago |
| Log | |
| Log Archive | |

> **Note:** This interface can be used in the future for all RNS network group management. For example, you can use it for adding clients or promoting secondaries to primaries.

TC: 12/7/2022

# Configure Client Registration Profiles

In a Registry Name Service (RNS) deployment, Client Registration Profiles (CRP) are always retrieved from the Primary Registry group. Because of this, create the profiles there.

After installation, navigate back to the **Hosts** landing page and click **Hosts Inventory**. Click the vertical ellipsis icon on the Primary Registry host to reveal a dropdown menu. Select **View Host Details**.
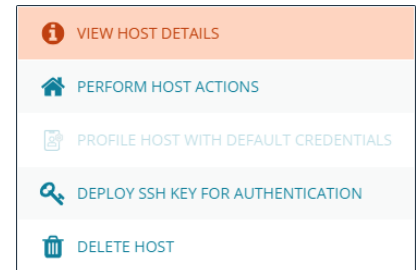


Choose **Client Registration Profiles** to enter the editor.



Make three new Registration Profiles:

- **rns_primaries:** Assigned to **Group Primaries**
- **rns_secondaries:** Assigned to **Group Secondaries**
- **rns_clients:** Assigned to **Clients**

To do this, follow the same action three times by cloning the default profile for each new Registration Profile.

> 📌 **Note:** Rather than starting a new profile from scratch, clone the **default** profile for all three profiles. This allows you to take advantage of its existing capabilities.

## Clone Each Profile

To clone each profile:

1. Select the **default** profile and choose **Clone**. Give the profile a meaningful name, such as **rns_primaries**, **rns_secondaries**, or **rns_clients**.
2. With one of the three profiles selected, expand **Role Registrations**. You should see two registrations already configured using two of the default services groups.
3. Change the **Role** field for each of these to match the desired type. For example, **primary** for the **rns_primaries group**.
4. Change the group name of the policy service group from **dflt_policy_service** to the one defined in the previous step. In this case, it is **custom_policy_group**.

> ℹ️ For more information, please see *"Create an RNS Custom Policy Group" on page 12*.

# Deploy the RNS Group Primaries

The deployment of the Group Primaries is explained in this section. On the **Hosts** page, click **Hosts Inventory**, choose the desired host, and click on the vertical ellipsis icon to select **Perform Host Actions**.

On the expanded **Perform Action** card, choose Privilege Management for Unix and Linux from the list of software under **Step 1: Primary Action**. Click **Next Step**.

**Step 1: Primary Action**
Choose a primary action to perform on the selected hosts

◯ Profile

◯ Active Directory Bridge

◯ Privilege Management for Unix & Linux

◯ Solr

ⓘ  Software actions are disabled when the software is unavailable. You can review available software versions and upload additional installers on the Software page.

**Selected Hosts**

pbsmc-

**NEXT STEP** ❯

On the **Step 2: Secondary Action** card, set the secondary action to **Install**. Click **Next Step**.

**Step 2: Secondary Action**

⦿ Install
Deploy and configure Privilege Management for Unix & Linux on your selected hosts.

◯ Upgrade
Upgrade Privilege Management for Unix & Linux using the existing configuration on your selected hosts.

◯ Uninstall
Remove Privilege Management for Unix & Linux from the selected hosts.

◯ Deploy PMUL Network and REST encryption key files
Copy the network and REST Privilege Management for Unix & Linux key files to the selected hosts.

◯ Configure a SIEM for use with one or more Privilege Management for Unix & Linux servers
Configure an existing SIEM as a destination for events generated by Privilege Management for Unix & Linux servers

❮ **PREVIOUS STEP**          **NEXT STEP** ❯

In the **Step 3: Action Requirements** card, choose an installation template. Select **All Components** from the **Installation Template** dropdown menu.

> 📌 ***Note:*** *Choosing **All Components** installs policy, log, and client components.*



For the **Client Registration Server**, choose the RNS Primary that was configured previously. A **Primary Registry Server** label and an icon are provided to help identify it. Choosing this sever to the Registry Name Service (RNS) network.

In the **Client Registration Profile** dropdown menu, choose the **rns_primaries** profile. After you choose the server and click **Next Step**, PMUL installs and uses the profile to perform some additional steps.

> 📌 ***Note:*** *PMUL copies the settings file and keys required for encrypted communications. It also automatically joins this host to the **dflt_pbpolicy_service** and **dflt_log_service** as the group primary.*

When the installation is complete, verify the configuration by visiting the **Hosts** main page and selecting **Registry Name Service**. Choose your primary from the presented list. A new list of categories appears on a new page under **Service Group Categories**. Choose the **Policy** category, which lists all policy groups. Select **dflt_policy_service**. A list of all hosts and their roles are displayed; the host you just installed is registered here as the group primary.

> 📌 ***Note:*** *This interface can be used to create new groups, add or remove hosts to existing groups, and to promote hosts in the group.*

# Enable and Configure Role-Based Policy

Before continuing the deployment, you must first configure policy.

📌 **Note:** *This can be done after deployment is complete, but with it in place, this policy is **immediately** synced when the secondary is in place, rather than be re-synced later.*

1. On the left side menu, click **Policy**.
2. Using the filtering options (or from the list), select a **server** (host).
3. At the right of the server hostname row, click the ellipsis menu icon, and then select **Server Details**.

📌 **Note:** *In the Registry Name Service (RNS) deployments, you only write changes to **primaries**. If you had chosen a **secondary**, the policy would not be available for editing.*

## Enable RBP

To enable RBP, click the **Settings & Configuration** tile.

| | Discovered: | 22 Nov 2021 14:48:20 UTC | Last Profiled: | 2 hours ago | IP: | |
| Operating System: | Linux CentOS 7.9.2009 | Architecture: | x86_64 | Default Gateway: |
| Tags: | | | |

| POLICY | FILE INTEGRITY MONITORING | PRIVILEGE MANAGEMENT FOR NETWORKS | SETTINGS & CONFIGURATION |
|---|---|---|---|
| Manage Privilege Management for Unix & Linux Policies | Manage File Integrity Monitoring Policies | Manage Privilege Management for Networks Policies | Configure Privilege Management for Unix & Linux |

On the **Privilege Management for Unix & Linux Policy Settings** page, click **Enable Role-Based Policy**.

Privilege Management for Unix & Linux Policy Settings

**Policy Mode**
This Policy Server is operating in Script Policy Mode. To enable Role-Based Policy Mode choose the option below.

Note: Switching to Role-Based Policy Mode will disable Script Policy and Script Policies will no longer be available to requesting clients. Policies are not removed when switching modes. This option can be changed at any time.

**ENABLE ROLE-BASED POLICY**

# Configure RBP

After you swap modes, select **Server Details** at the top of the page to configure a policy. Click the **Policy** tile to access more options.

POLICY

Manage Privilege Management for Unix & Linux Policies

# Add Command Group

Command groups are added when the user wishes to designate a list of commands that are allowed or rejected for a specific set of users.

To add a command group:

- From the available tiles, click the **What** tile to move to the **Command Groups** page.
- In the **Command Groups** grid, click **Add Command Group** to reveal the **Command Groups** card.

WHAT

Command Groups determine which commands will be allowed or rejected

- With the **Command Groups** card revealed, type the desired command group name into the **Command Group Name** field, as well as any command group description you may want to add into the **Command Group Description**.
- In the **Change requested by [loggedInUserName]** field, enter a reason for the assignment or change.
- Click **Save** to confirm your changes.

Commands are added to a **Command Group** by entering each item under the **Commands** section.

- To delete an individual command, click the **Delete icon** beside the command.
- Otherwise, to delete an entire command group, click the **Delete** button that appears after a command group has been created.



---

🔍 ***Example:*** *For example, a user may wish to add a list of basic commands consisting of **ls**, **date**, **whoami**, and **id**. Create a command group called **Basic Commands**, and add each of the previous commands to the command group.*

---

# Create New Users

Next, you must choose users and add a new secure user.

To create a new user:

- At the top of the page, select **Role Based Policy** to navigate back to the RBP grid, and then select the **Who** tile.
- In the **Users** grid, click **Add User / Group** to reveal the dropdown menu.
- There are multiple types of user-creation options available to choose from, but for this guide select the **Secure User** option.

With the **Users and Groups** card revealed, type the desired username into the field, as well as any description you want to add into the **Description** field, and click **Save Changes**.

- Names entered into the **Username** field are entered freely.
- The username is now visible in the **Users** grid.

> 📌 **Note:** *A username can be edited or deleted at any time by left-clicking the username in the* **Users** *grid.*

## Create New Roles

Finally, create a new **Role**. Make sure to use **root** as the run user and the command group for your commands.

To create a new role:

- At the top of the page, select **Role Based Policy** to navigate back to the RBP grid, and then select the **Roles** tile.
- From the **Roles** grid, click **Add Role** to reveal the expanded **Roles** card.
- Create a new role-based policy role, and then click **Create** to finalize your changes.

# Deploy and Manage RNS Secondaries

Deploying a secondary very closely mirrors the process outlined in the *Deploy the RNS Group Primaries* section.

The primary difference is that you should change the selected Client Registration Profile (CRP) to the **rns_secondaries**, in order to make this host the secondary, for both the policy and log services.

> ℹ️ *For more information, please see "Deploy the RNS Group Primaries" on page 14.*

# Deploy Single and Multiple Clients

Like deploying a secondary, deploying a client very closely mirrors the process outlined in the *Deploy the RNS Group Primaries* section.

The primary change here, is that you will need to change the selected Client Registration Profile to the **rns_clients** in order to make this host a client of both the policy and log services.

> *For more information, please see "Deploy the RNS Group Primaries" on page 14.*

## Deploy Multiple Clients

To deploy multiple clients, select all applicable hosts in the grid and use **Actions > Perform Host Actions** to deploy multiple clients simultaneously.

**SALES:** www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

21

# Execute Policy

**SSH** into the client and run a command defined in your Role Based Policy (RBP) via **pbrun**.

> 🔍 ***Example:*** *Assuming the policy is configured to accept this command, you will see an **accept** message, or a **reject** message otherwise.*

**SALES:** www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

22

# Troubleshooting

This section serves as a reference for some of the more common issues users might experience.

## Primaries

Registry Name Service (RNS) synchronizes data every two minutes by default. As a result, changes on the primaries aren't propagated to secondaries immediately.

## Policy Mode

Policy mode is not auto synchronized. Changing from role-based policy (RBP) to script and vice-versa does not replicate. We recommend that the mode be manually toggled on secondaries when the primary changes via **Settings & Configuration**.

## Domain Names

We strongly recommend using fully qualified domain names with RNS to reduce complexity of name resolution.