DEPLOYMENT GUIDE

Implementing AWS Route 53 Synchronization

Table of Contents

Introduction

Amazon Route 53 DNS service offers limited support beyond pure Amazon Web Services environments, which means enterprises cannot create a single, unified DDI solution to serve their entire enterprise, including their on-premises networks and hybrid clouds, with Route 53 alone. Route 53 focuses on only AWS VPCs, which limits connectivity, visibility, and security when used for non-AWS cloud platforms.

Infoblox has extended our industry-leading DDI platform to integrate with AWS and Amazon Route 53 DNS, providing a unified, enterprise-grade solution for AWS and hybrid cloud deployments. Integration between Amazon Route 53 and Infoblox bridges the gap between enterprise IT and cloud teams to reduce complexity by providing a single console to manage on-premises, AWS public cloud, and private cloud deployments. This solution meets the needs of current and future Infoblox customers who are expanding to AWS and are using Amazon Route 53 for DNS.

Infoblox and Route 53 Synchronization

Infoblox and Route 53 synchronization enables the following functionality:

- Read-only synchronization of zones and record sets from AWS Route 53
- Support for Public Hosted Zones and Private Hosted Zones
- Support for A, AAAA, Alias, CNAME, MX, NS, PTR, SPF, SRV, and TXT record types
- Ability to serve synchronized Route 53 zones from an Infoblox authoritative name server

Prerequisites

The following are prerequisites for Infoblox AWS Route 53 synchronization:

- Functional Infoblox Grid with a Grid Master or standalone Infoblox member
- DNS resolution enabled for the Grid
- NTP time synchronization enabled for the Grid
- A Cloud Network Automation license installed on the Grid Master
- AWS account with Route 53 hosting at least one zone

Create IAM User in AWS

Prior to configuring Route 53 synchronization in Infoblox NIOS, you will need an IAM user with at least some minimum permissions to read DNS data in AWS Route 53. Minimum permissions required in AWS to conduct Route 53 synchronization are:

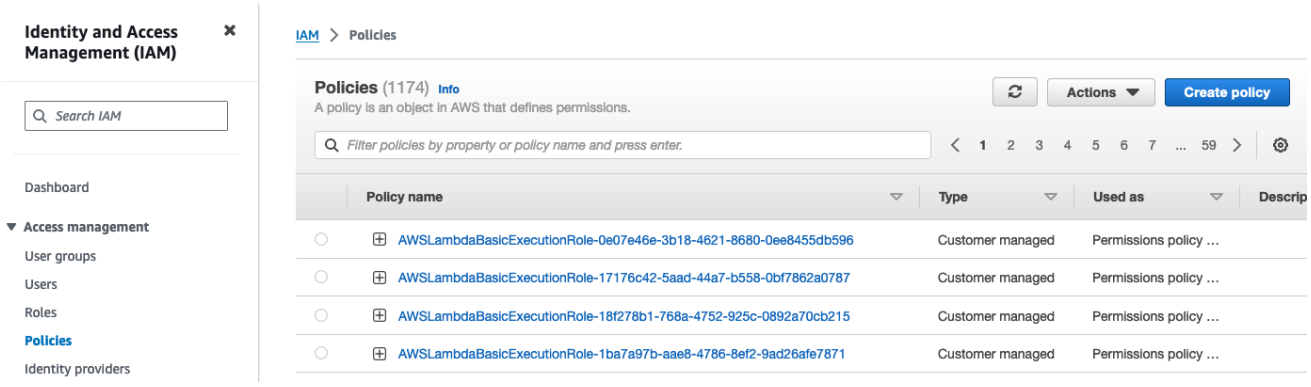
- route53:ListHostedZones
- route53:GetHostedZone
- route53:ListResourceRecordSets

Note: Instead of using IAM credentials, you can use an IAM role attached to a vNIOS instance running in AWS for Route 53 synchronization. Refer to NIOS Documentation for details on using this method.

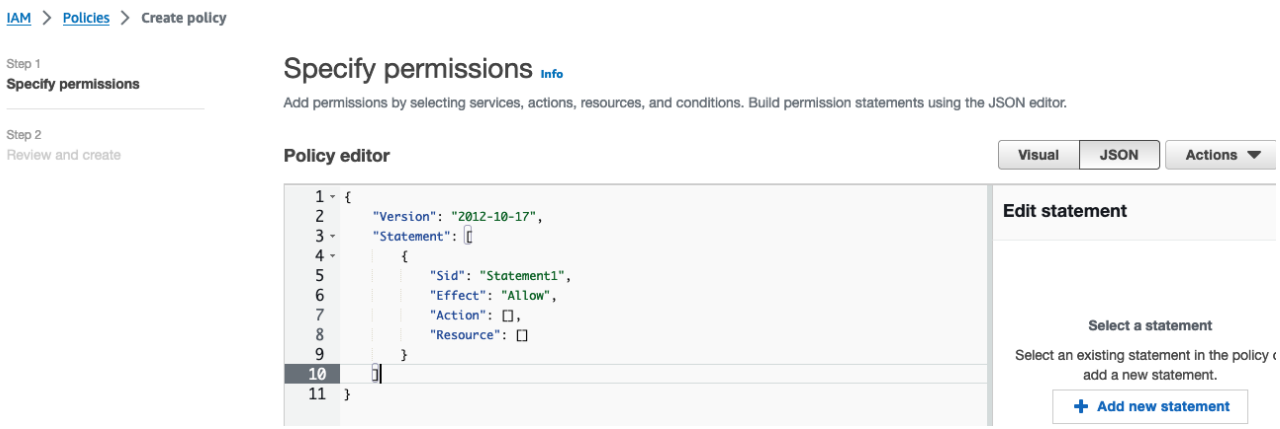
Create IAM Policy

First, we will create a custom policy with the permissions listed above to assign to an IAM user.

1. Log in to the AWS Management Console.
2. Use the Services menu to navigate to **IAM** under Security, Identity, & Compliance.
3. Select **Policies** from the IAM menu.
4. Click on **Create policy**.



5. Policies can be selected through the visual editor or defined using JSON. For this guide, we will use JSON. Click the JSON tab.
6. In the JSON editor view, you will see the base outline for a policy definition:



7. Between the square brackets for Statement, replace all text with the following to define your policy:

```
{
  "Effect": "Allow",
  "Action": "route53:ListHostedZones",
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "route53:GetHostedZone",
    "route53:ListResourceRecordSets"
  ],
  "Resource": "arn:aws:route53:::hostedzone/*"
}
```

8. Your JSON policy definition should look like this:

Policy editor

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "route53:ListHostedZones",
7              "Resource": "*"
8          },
9          {
10             "Effect": "Allow",
11             "Action": [
12                 "route53:GetHostedZone",
13                 "route53:ListResourceRecordSets"
14             ],
15             "Resource": "arn:aws:route53:::hostedzone/*"
16         }
17     ]
18 }
```

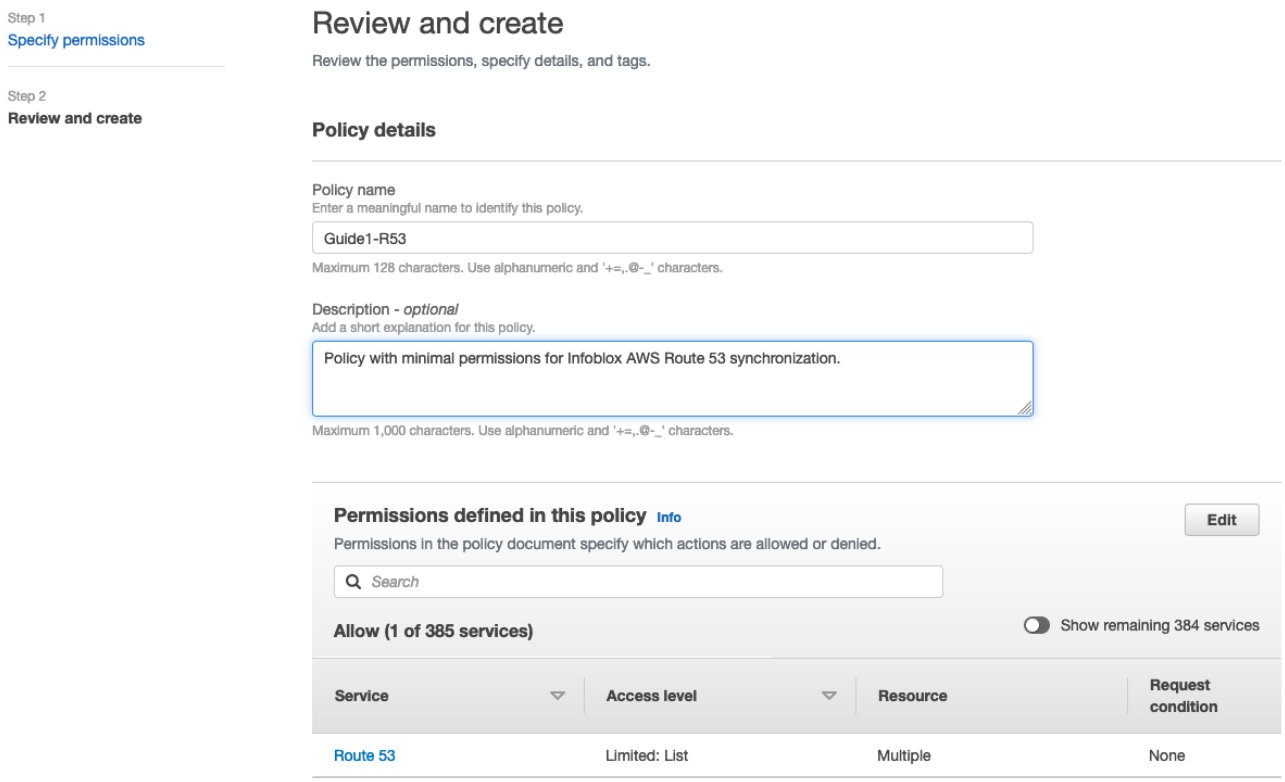
9. Click **Next**.

10. Name your policy.

11. Optionally, add a description.

12. Review the Summary.

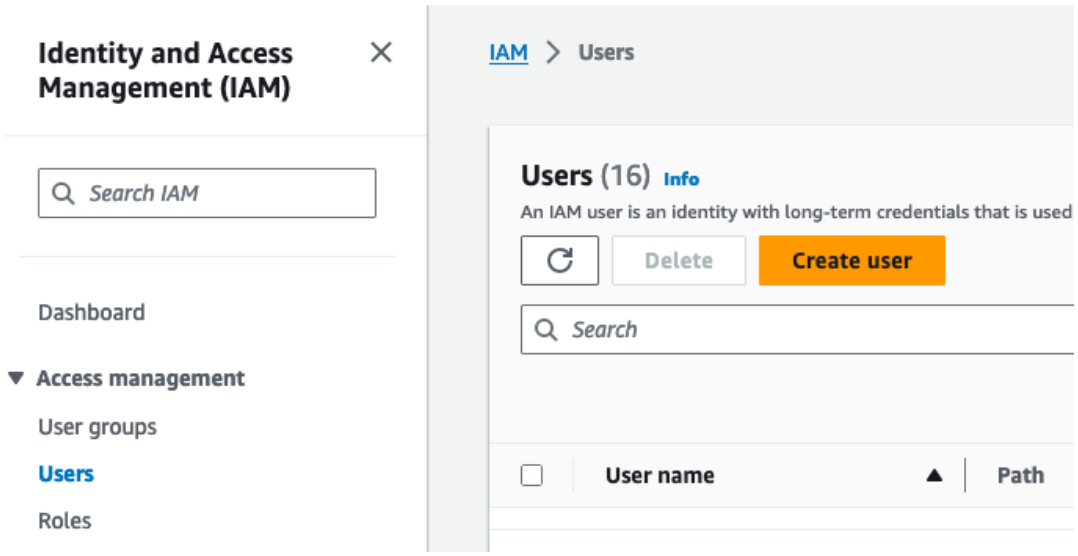
13. Scroll down to click **Create policy.**



Create IAM User

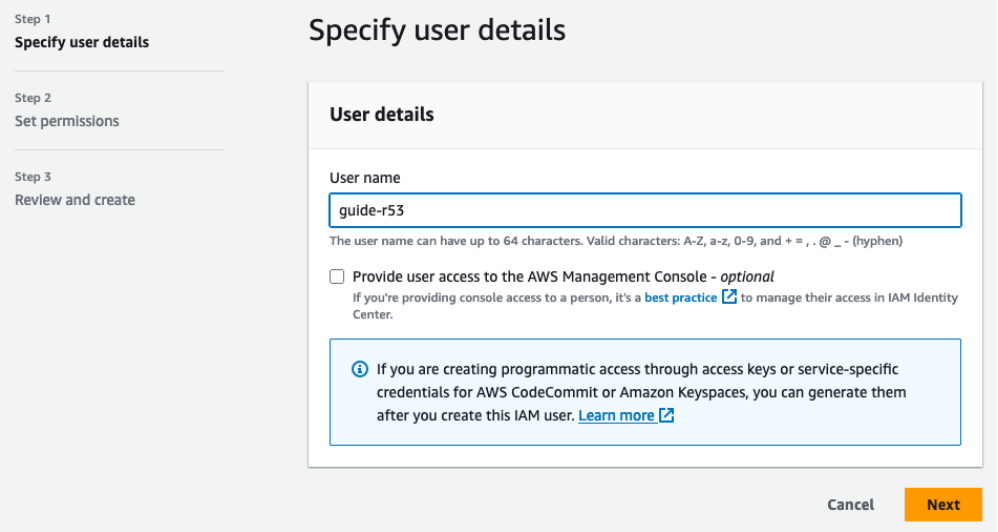
Next, we will create a user with an access key that can be used to authenticate for Route 53 synchronization jobs.

1. Select **Users** from the IAM menu.
2. Click **Create user**.



3. Name the user.

4. Click **Next**.

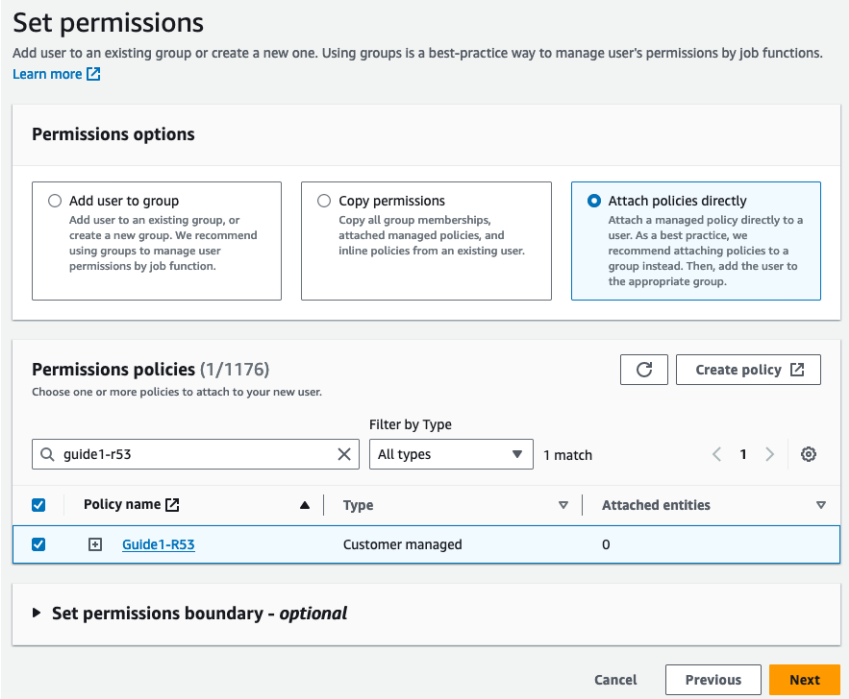


5. Under Permissions options, select **Attach existing policies directly**.

6. Enter the name of your policy in the search bar or scroll down to locate your policy.

7. Check the box next to your Route 53 policy.

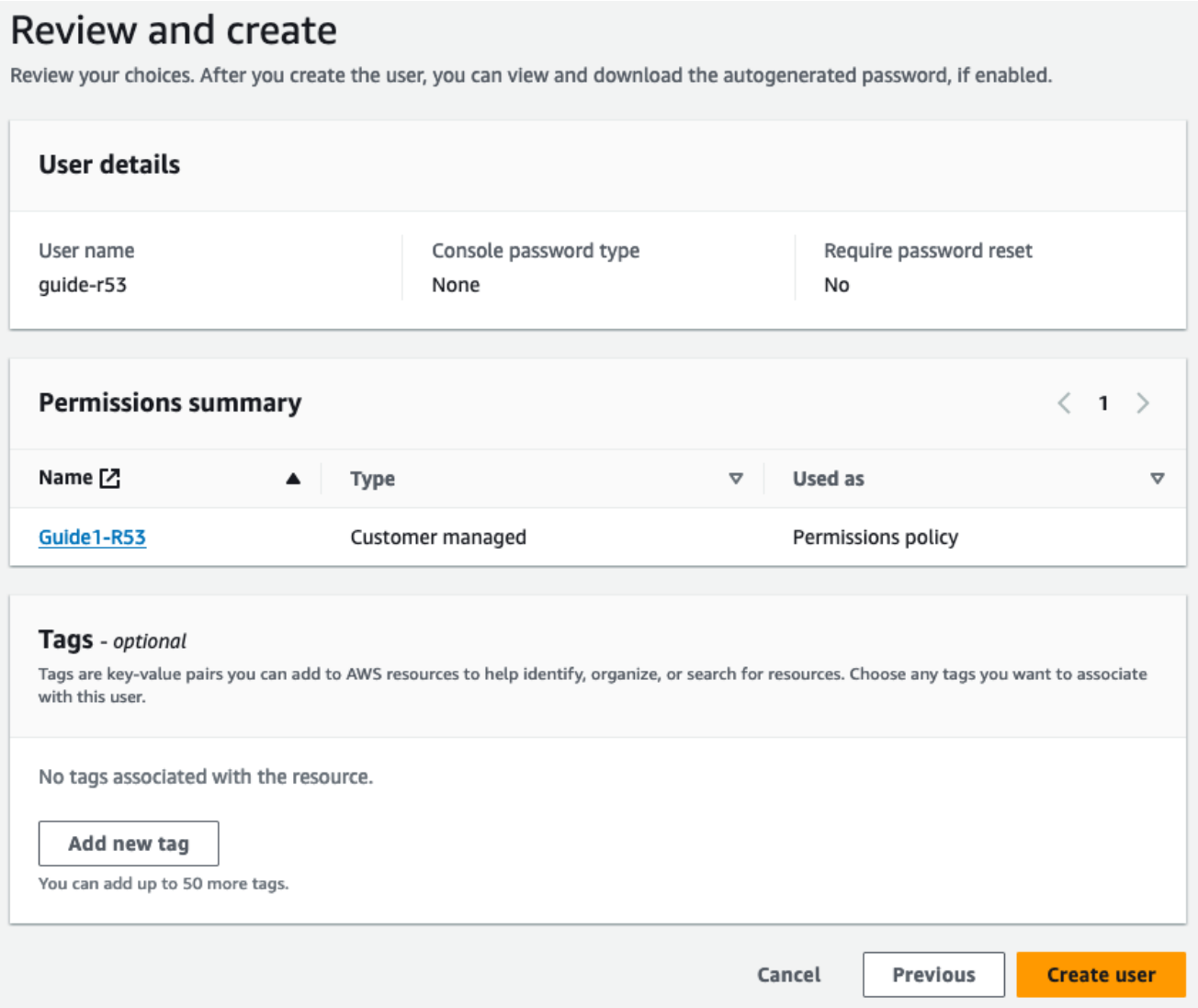
8. Click **Next**.



9. Optionally, add tags.

10. Review the User details and Permissions.

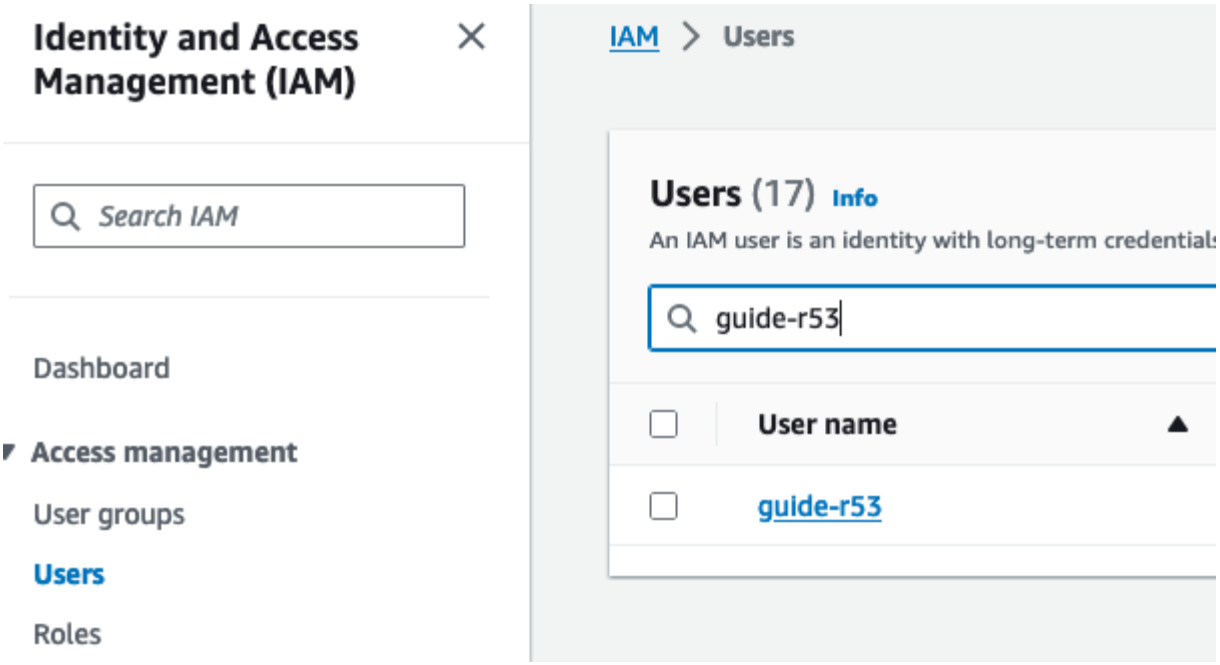
11. Click **Create user**.



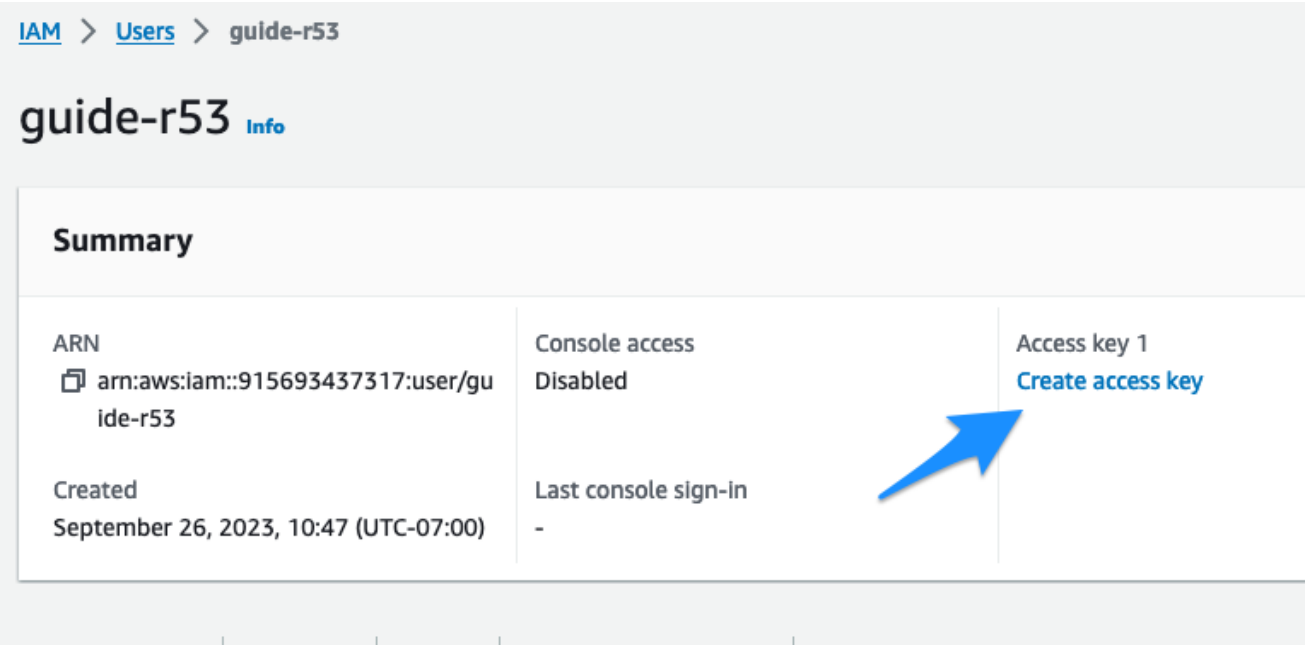
Create User Credentials

In this section, we will create an access key for the user.

1. On the **IAM** → **Users** tab, locate your new user and click on the name.

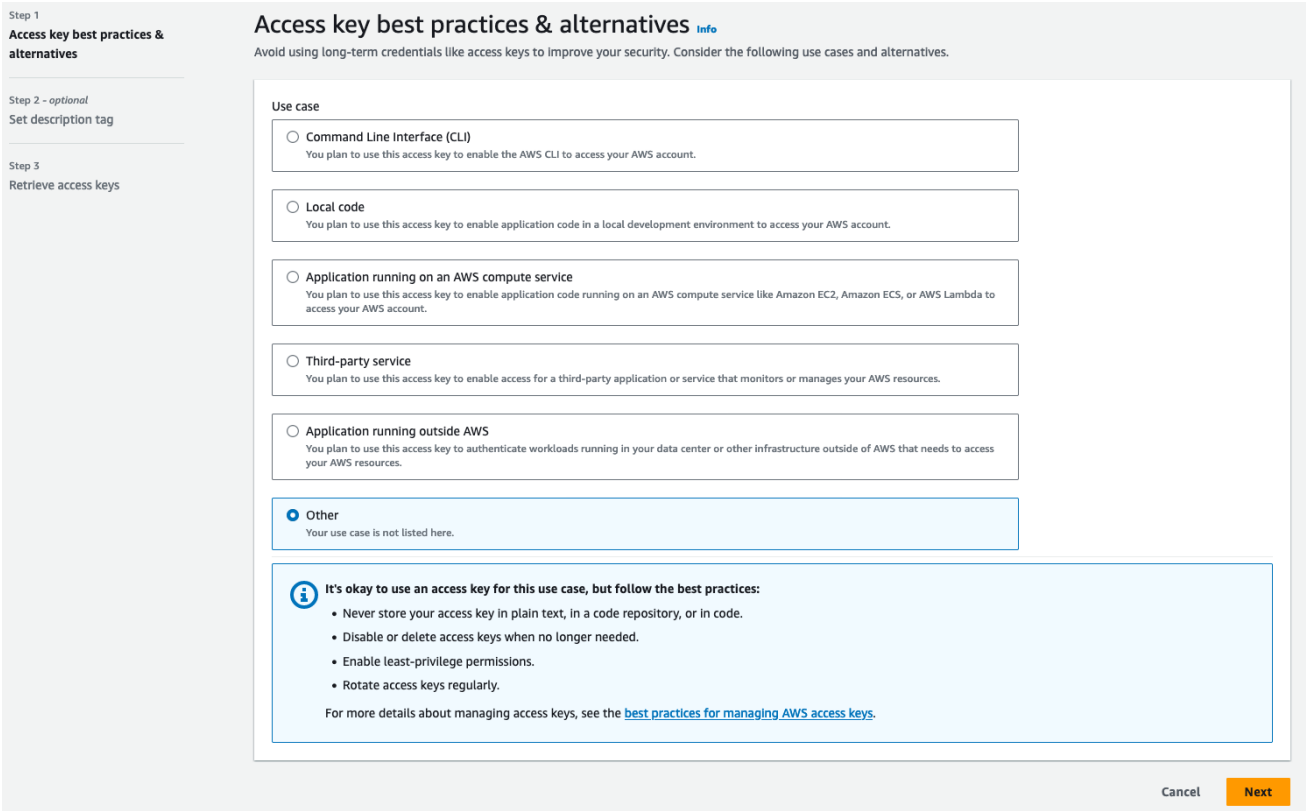


2. Click on **Create access key**.



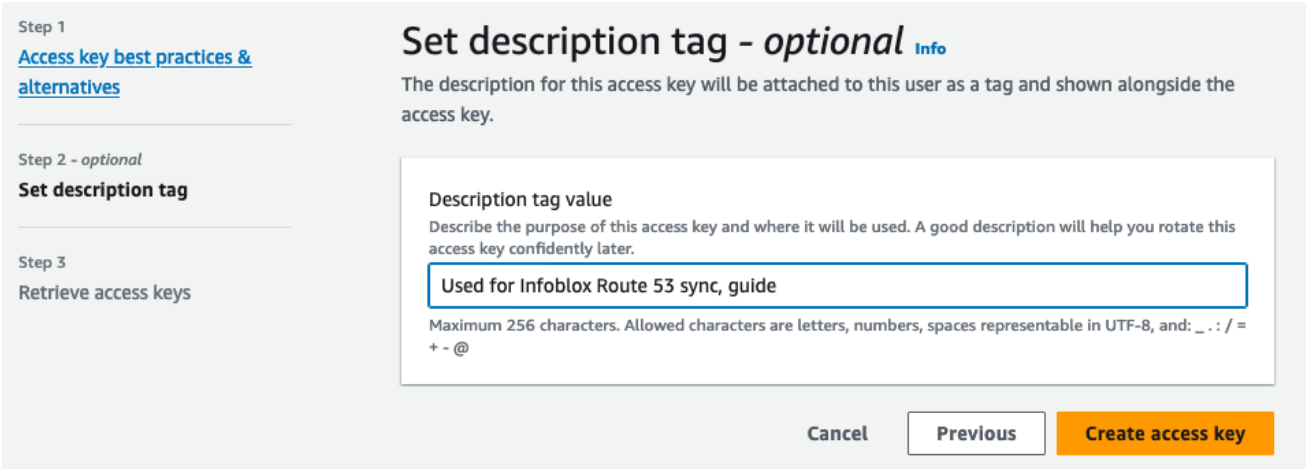
3. On Step 1, select **Other**.

4. Click **Next**.

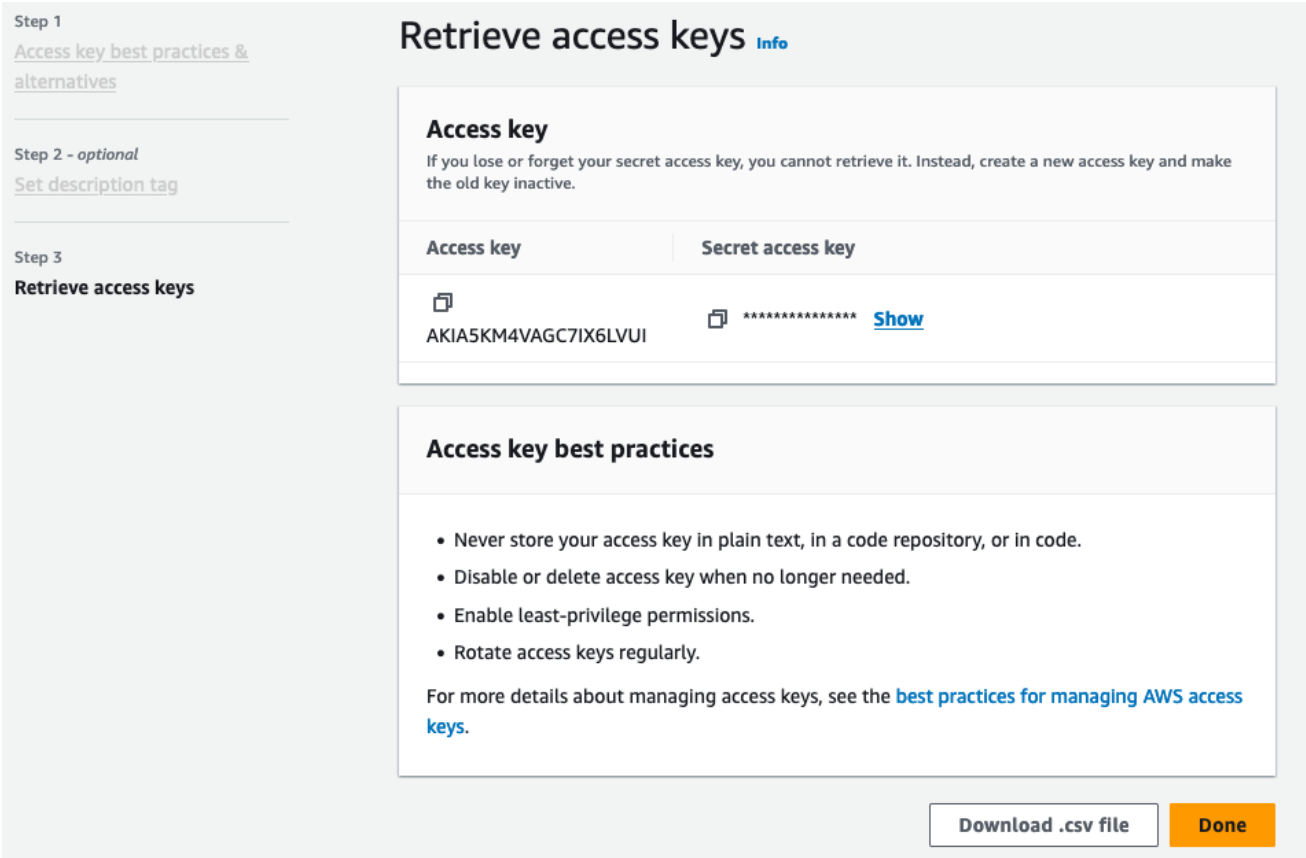


5. On Step 2, optionally enter a description.

6. Click **Create access key**.



7. Copy and save or download the credentials.



Note: This is the only opportunity to download or view these credentials. If you do not save them, or lose them later, you will have to create new access keys for this user.

8. Click **Done**.

Configure AWS Route 53 Synchronization in NIOS

An administrator needs to configure credentials and synchronization tasks for Route 53 synchronization. Once these are configured, synchronization will begin on the specified schedule and Infoblox DNS servers can serve synchronized zones when configured as the name servers for the zones.

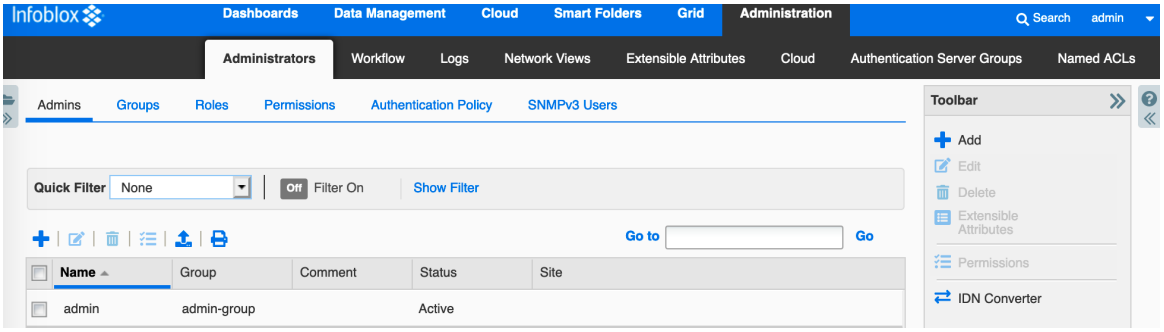
Creating a User Account and AWS Credentials

This section describes the steps to configure the required accounts and credentials for AWS Route 53 synchronization.

1. Log into your Infoblox Grid Manager GUI.

2. Navigate to the **Administration** → **Administrators** → **Admins** tab.

3. Click + **Add**.

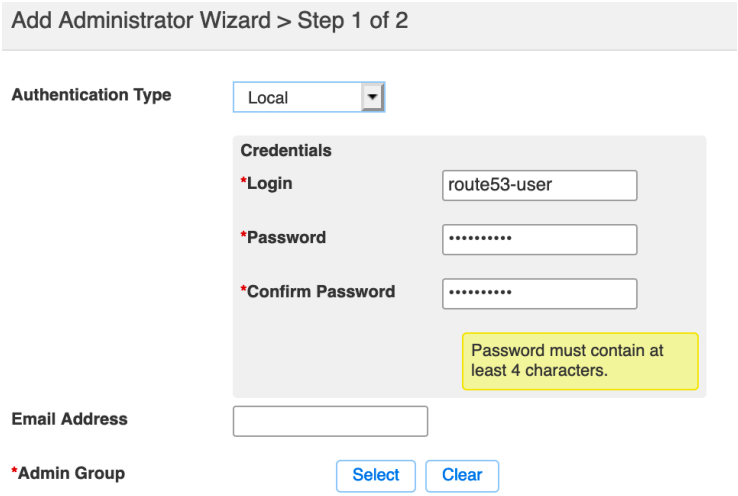


4. On Step 1 of the Add Administrator Wizard, ensure that **Local** is selected for Authentication Type.

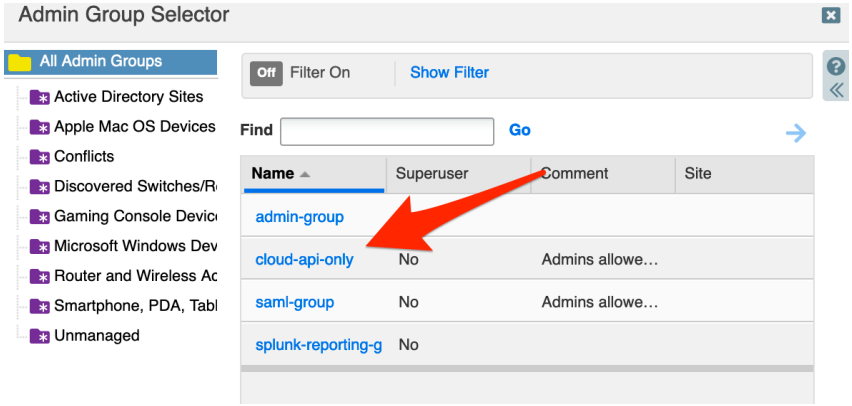
5. Next to Login, enter a name for the user.

6. Enter a password for the user and confirm.

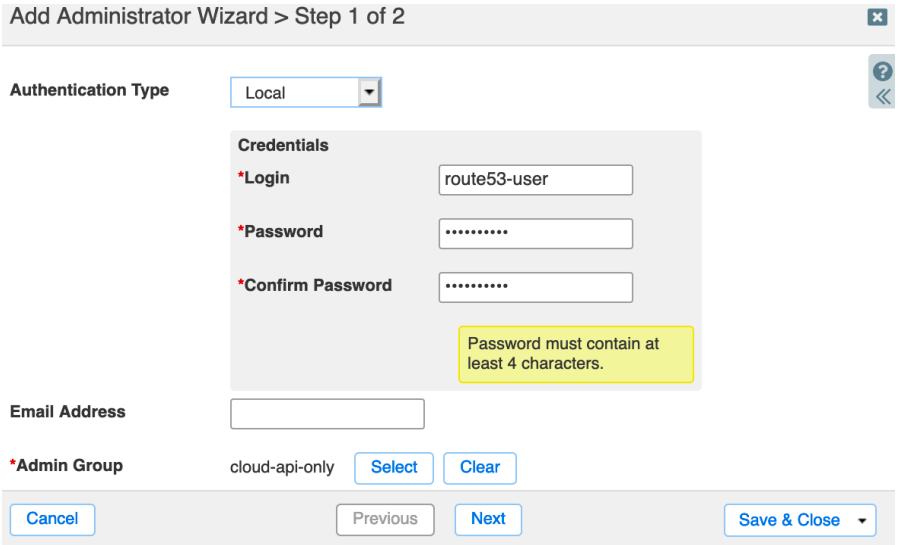
7. Next to Admin Group, click **Select**.



8. In the Admin Group Selector window, click on the **cloud-api-only** group.

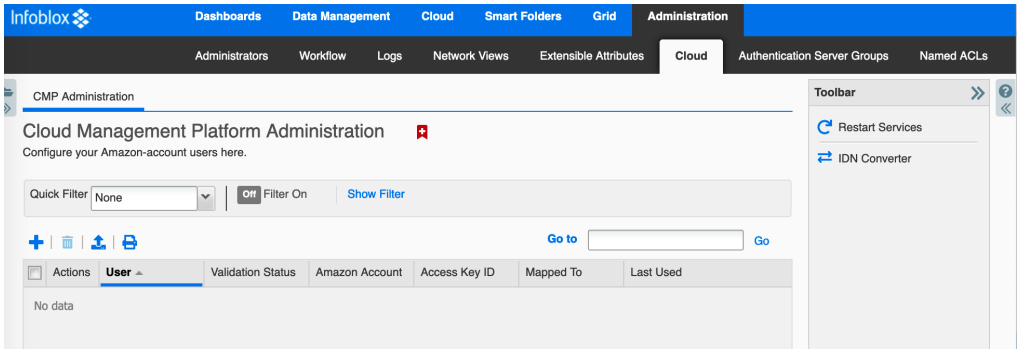


9. Click **Save & Close** in the Add Administrator Wizard.



10. Navigate to the **Administration** → **Cloud** tab.

11. Click the ✚ (add button).



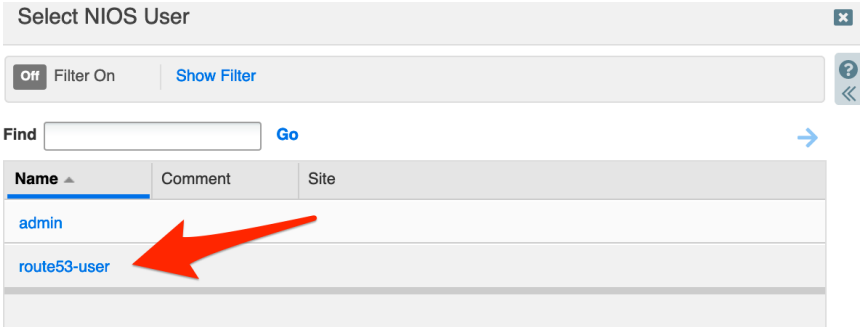
12. In the Add Amazon User Wizard, enter a **Username**.

13. Copy and paste the **Access key ID** and **Secret access key** from the AWS IAM user CSV file you saved earlier.

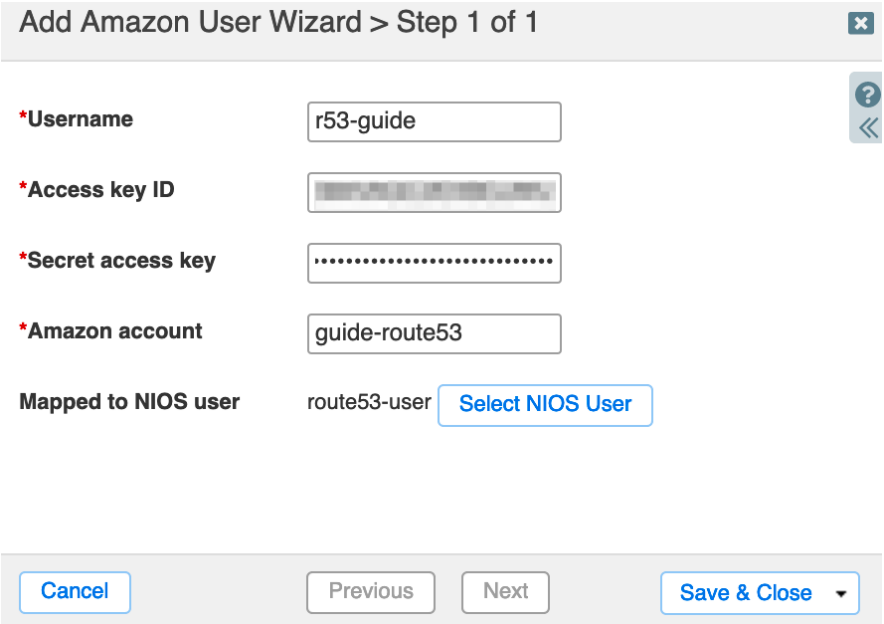
14. Type the name of the **AWS account** into the Amazon account box.

15. Click **Select NIOS User**.

16. Click on the new admin user you created.



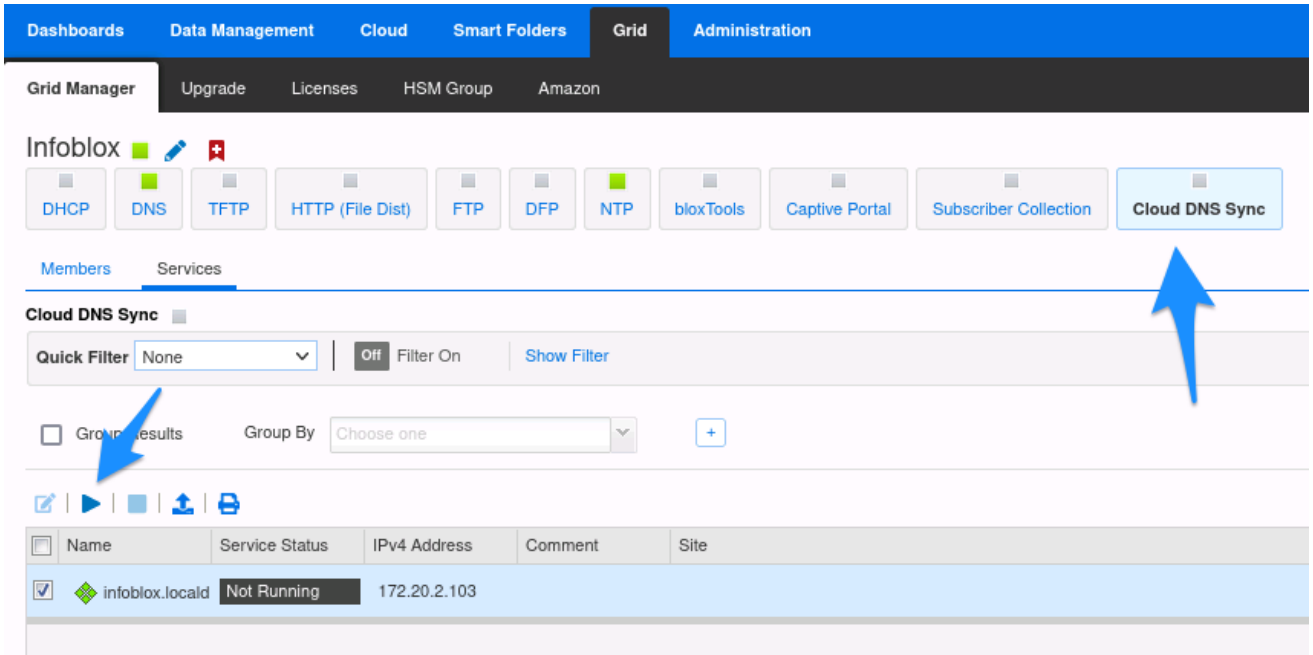
17. Click **Save & Close**.



Start Cloud DNS Sync Service

With NIOS 8.6.3 and later, the Cloud DNS Sync service must be started on the member which will be used to conduct the sync.

1. Navigate to the **Grid** → **Grid Manager** tab.
2. Click on the **Cloud DNS Sync** service.
3. Select the member you will use for Route 53 sync.
4. Click the **Start** button.

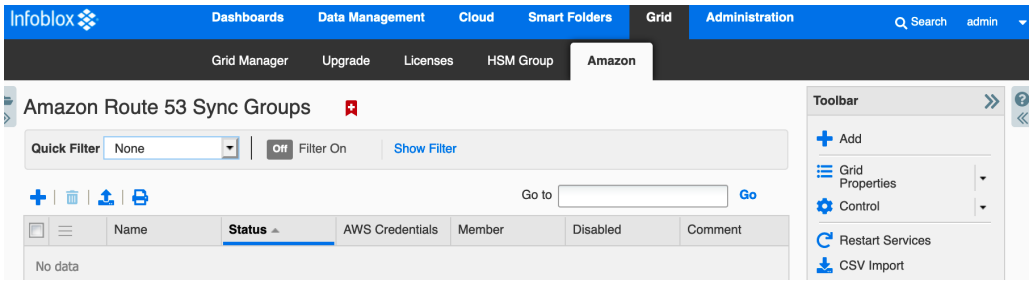


5. Click **Yes** in the confirmation window.

Creating the Route 53 Sync Group

This section describes the steps to configure a Route 53 Sync Group, which can contain multiple Sync Tasks. A separate Sync Task is required for each AWS account and for each unique set of filters you want to use for zone synchronization.

6. Navigate to the **Grid** → **Amazon** tab.
7. Click **Add**.



8. In the Amazon Sync Wizard, enter a **Sync Group Name**.

9. Click the **Select** button next to Member and select the Grid member to conduct the sync. Note: If your Grid has only one member it will be selected automatically.

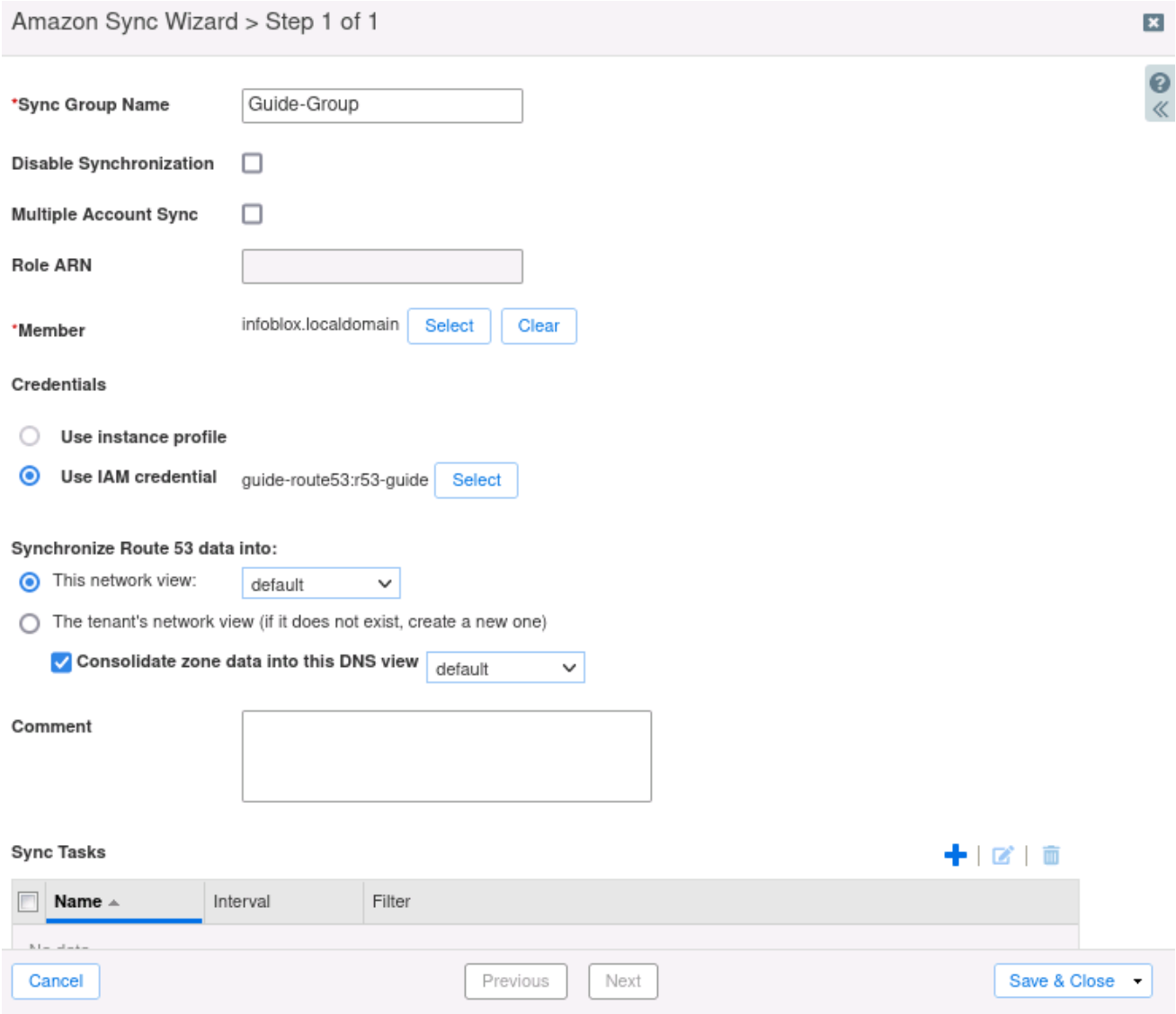
10. Under Credentials, select **Use IAM credential**. *Note: If the Grid member used for the sync is running in an AWS VPC, you can use an instance profile instead of IAM credentials. Refer to AWS documentation for assigning an instance profile to a VM instance.*

11. Click **Select** to choose the user credentials.

12. Select the Amazon user you created earlier. *Note: If you have only one cloud user, it will be selected automatically.*

13. Optionally, set the network and DNS views to synchronize data into.

14. Click the + (add button) next to **Sync Tasks**.



*Note: To sync Route 53 hosted zones from multiple accounts, you can select **Multiple Account Sync** and enter the ARN of the role from AWS that will be used. Complete setup of multi-account sync is not covered in this guide. Refer to the [Infoblox vNIOS for AWS Documentation]() for instructions on setting up multi-account sync.*

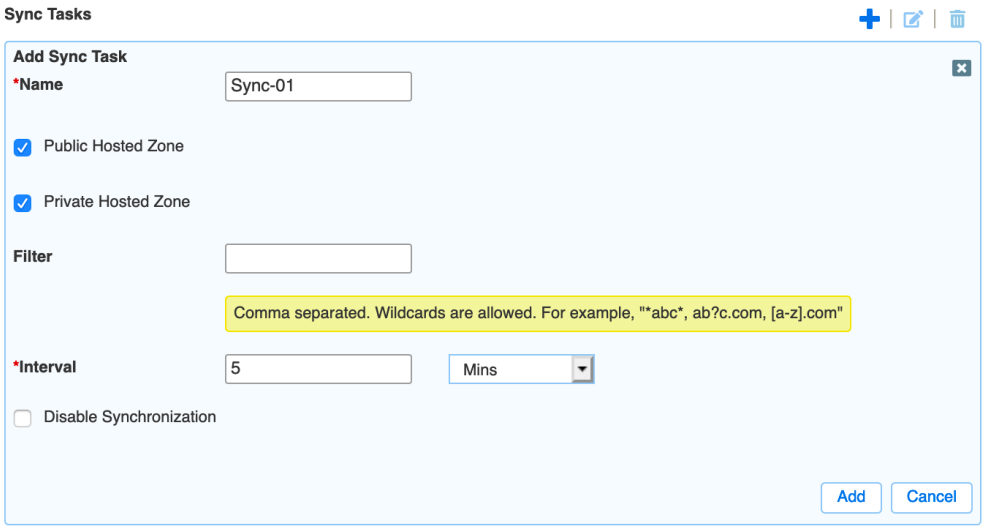
15. Enter a **Name** for the sync task.

16. Both Public Hosted Zones and Private Hosted Zones are synchronized by default. If you do not want to synchronize both types, deselect the **Public Hosted Zone** or **Private Hosted Zone** checkbox as necessary.

17. Similarly, all zones within the selected zone types are synchronized by default. If you only want to synchronize a subset of zones, specify the **filters** (comma separated) in the Filter box.

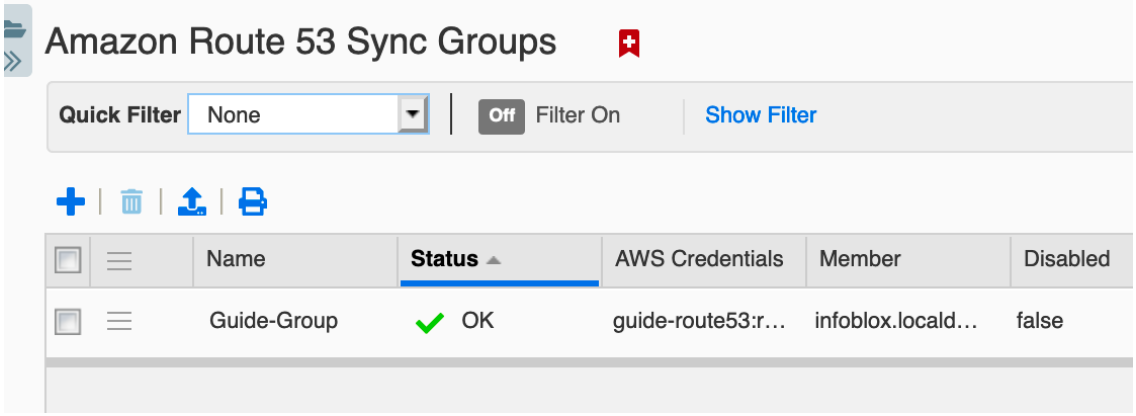
18. Specify an Interval for the task by entering a number in the box and selecting **Mins**, **Hours**, or **Days** from the dropdown.

19. Click **Add**.



20. Back in the Amazon Sync Wizard, click **Save & Close**.

Once the sync group has been saved the synchronization proceeds automatically on the specified schedule. A successful synchronization shows a status of **OK**.



Working with Route 53 Synchronized Zones

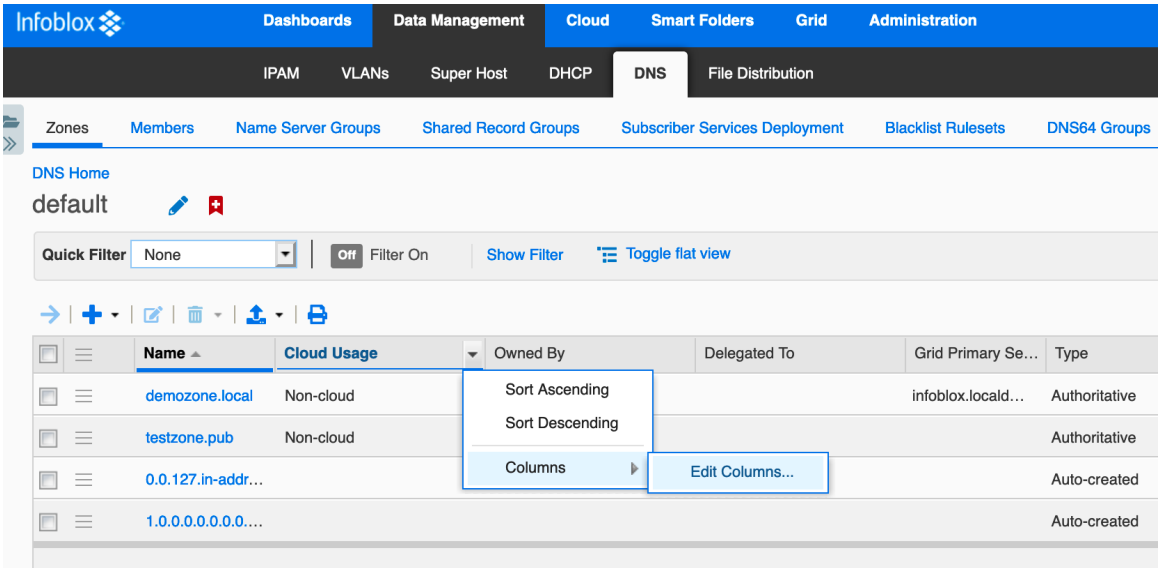
Route 53 Public Hosted Zones are synchronized into the default DNS view. A new Extensible Attribute (EA), **DNS Source**, is available to identify Route 53 zones in the system.

1. Navigate to the **Data Management** → **DNS** → **Zones** tab.

2. To add the DNS Source extensible attribute to your view, hover over any column.

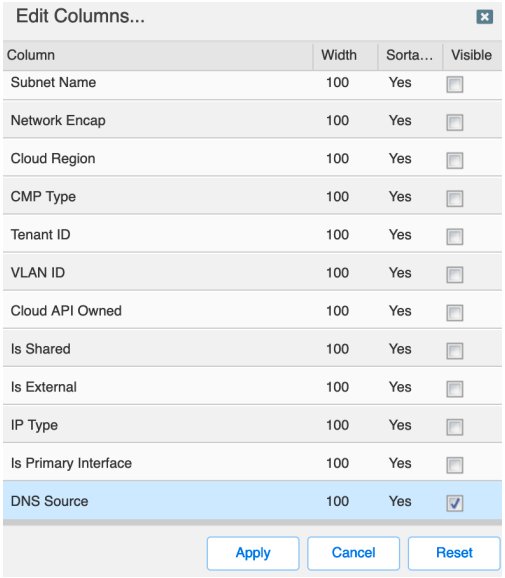
3. Click the dropdown and select Columns.

4. Click on **Edit Columns**.



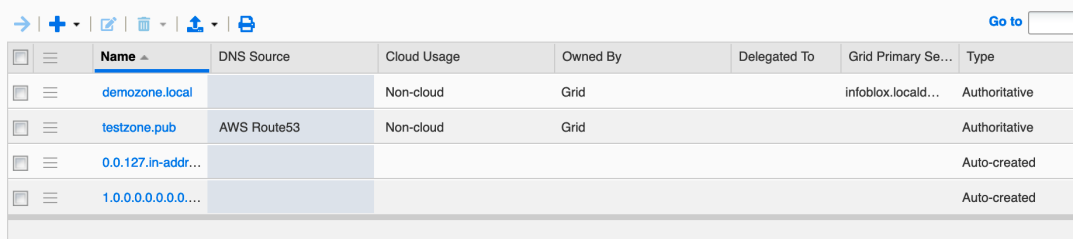
5. Scroll down to locate the **DNS Source** EA. Click in the checkbox under Visible.

6. Click **Apply**.

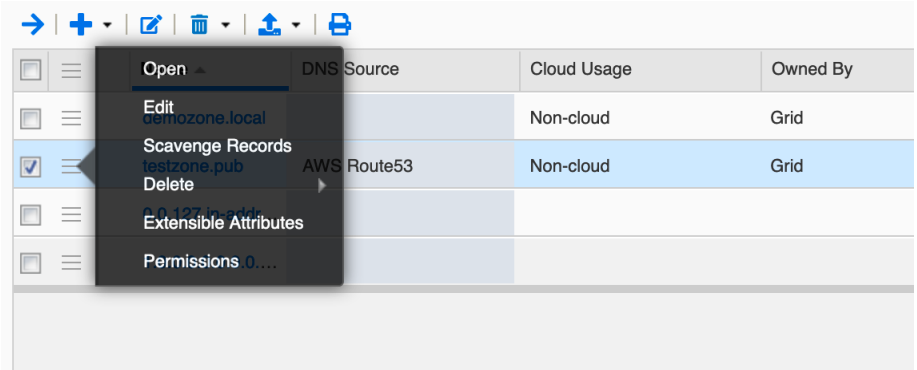


7. Back on the Zones tab, scroll right to find the DNS Source column.

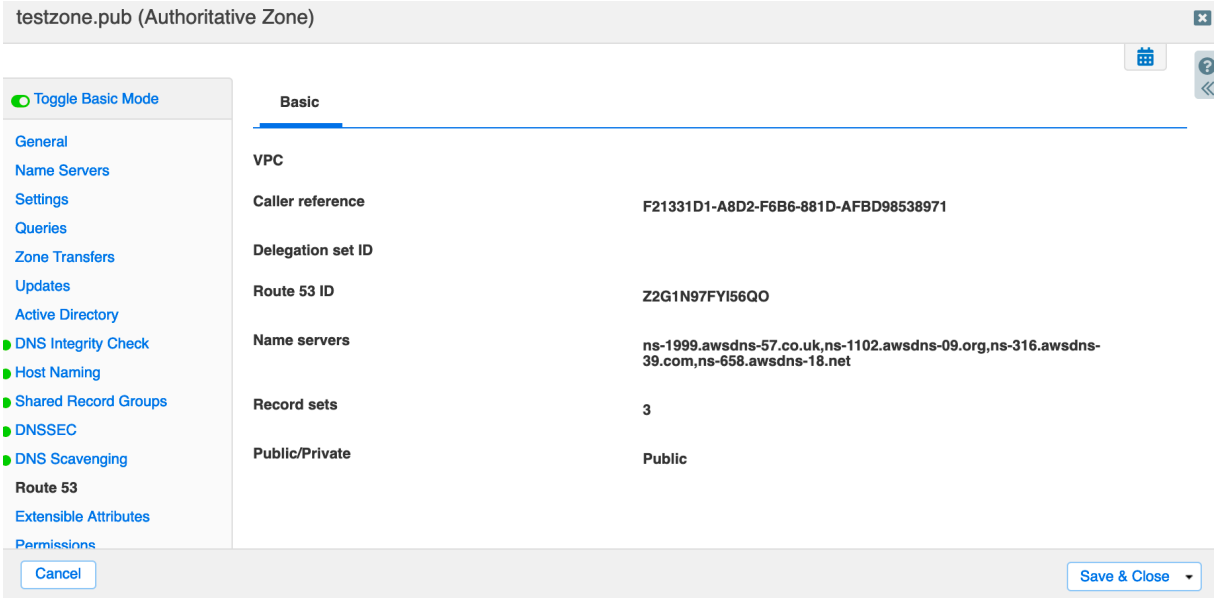
8. Click and drag the column to the desired location.



9. To view information on a zone synchronized from Route 53, select your Public Hosted Zone from the list and click **Edit** in the action menu.



10. Click the **Route 53** tab in the zone edit dialog. This shows information associated with the Route53 zone. In the case of a Public Hosted Zone it includes identifying information about the zone from within Route 53 and the AWS public name servers associated with the zone.



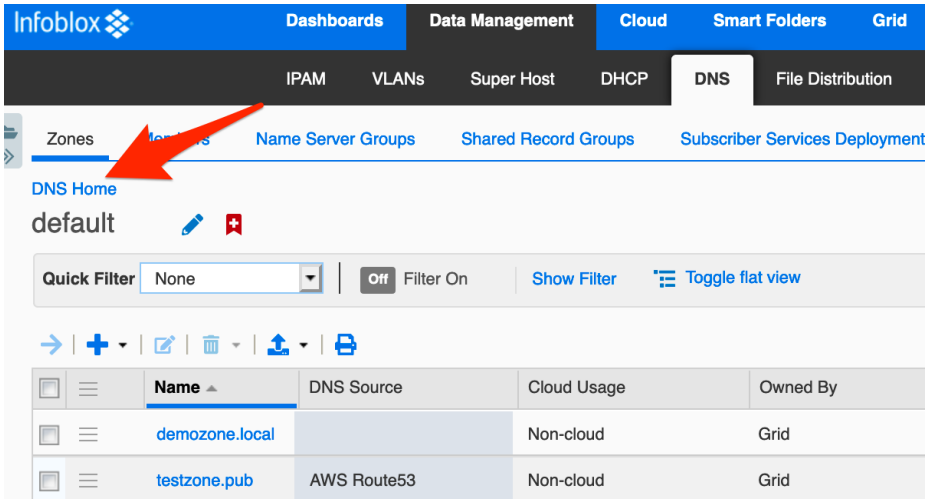
11. Click **Cancel** to exit the zone edit dialog.

In Route 53 it is possible to have multiple identically named Private Hosted Zones if they are associated with different VPCs. In Infoblox, it is not possible to have non-unique zone names within one DNS view. For this reason Private Hosted Zones are synchronized into separate DNS views by default. These views are

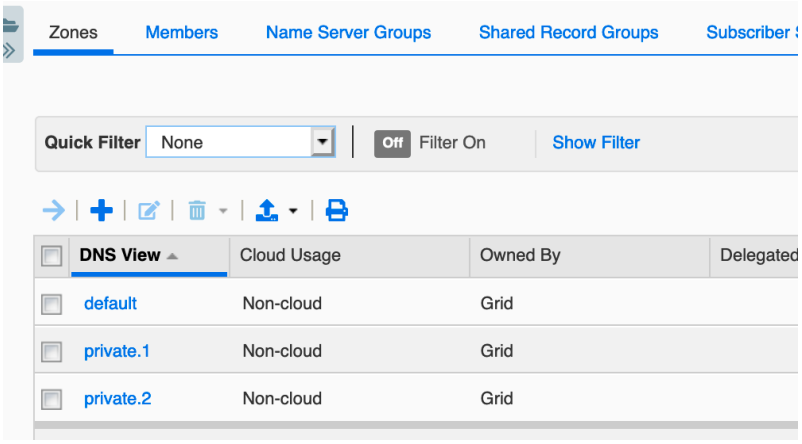
named private.n. A separate view will be created for every unique combination of VPCs associated with a Private Hosted Zone.

For example: Assume there are three VPCs: VPC1, VPC2, and VPC3; and three Private Hosted Zones: zone 1, zone 2, and zone 3. zone1 is associated with VPC1, zone 2 with VPC2, and zone 3 with both VPC2 and VPC3. This will result in three private views: one for "VPC1," one for "VPC2," and one for "VPC2 and VPC3." If a new zone is added (zone 4) and associated with VPC3 only, a new view will be created since there is no existing "VPC3" related view.

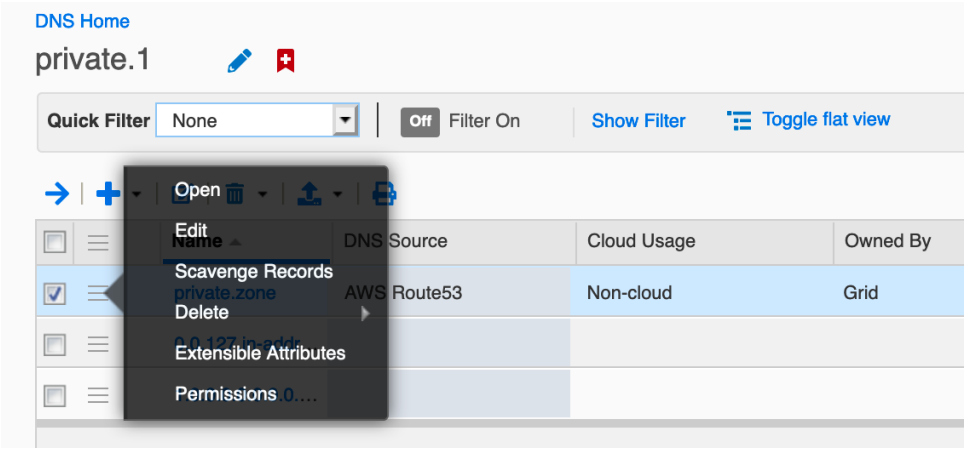
12. To view a Private Hosted Zone, click on **DNS Home**.



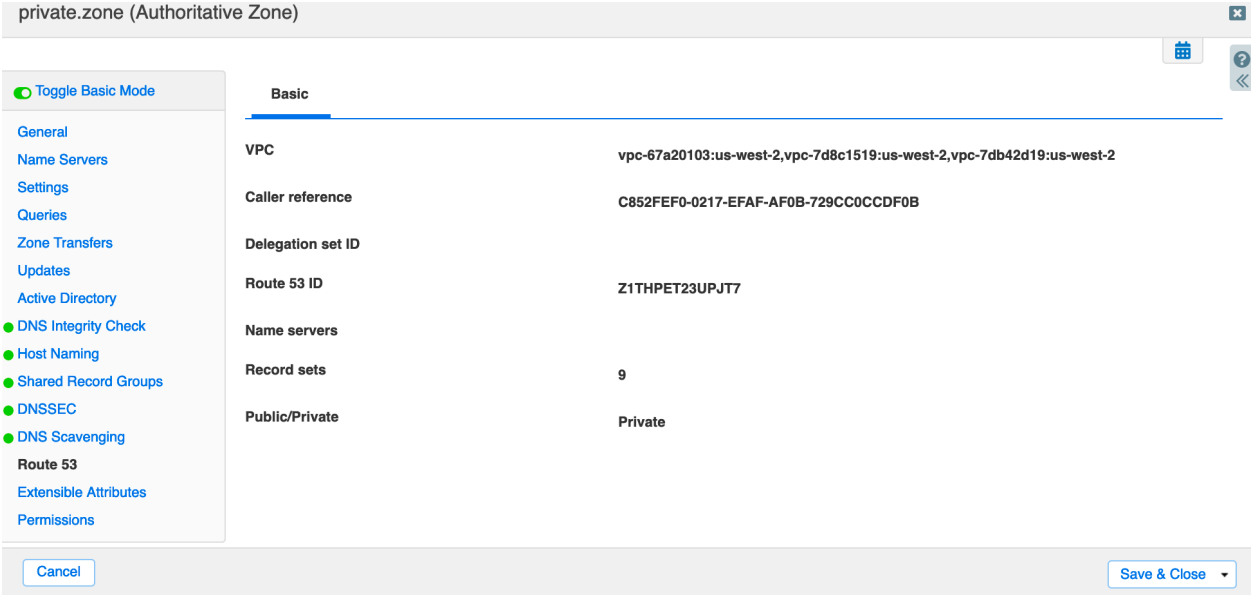
13. Click on one of the **private.n** DNS Views.



14. Select your Private Hosted Zone from the list and click **Edit** in the action menu.



15. Click the **Route 53** tab in the zone edit dialog, which shows information associated with the private Route 53 zone. This includes the list of VPC associations for the zone.



16. Click **Cancel** to exit the zone edit dialog.

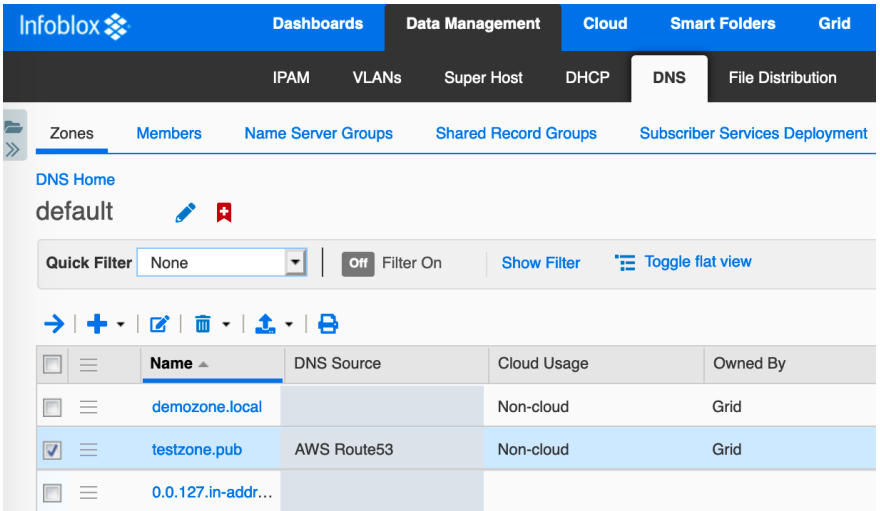
Warning: It is possible to make changes to a Route 53 synchronized zone within the Infoblox Grid Manager interface. However, when the zone is next synchronized from Route 53, any changes will be lost and the zone will revert to the zone data from Route 53.

Configuring Infoblox Name Servers for Route 53 Synchronized Zones

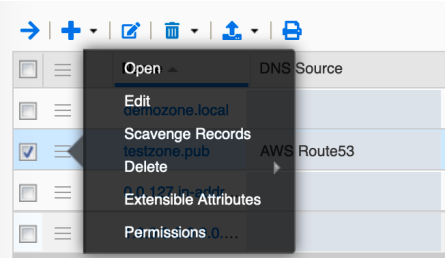
Using your Infoblox name servers, on-premises and hybrid/multi cloud clients can resolve DNS records in your Route 53 hosted zones. To make your Infoblox name servers authoritative for the Route 53 synchronized zones:

1. In the Grid Manager, navigate to the **Data Management** → **DNS** → **Zones** tab.

2. Select a Route 53 synchronized zone from the list.

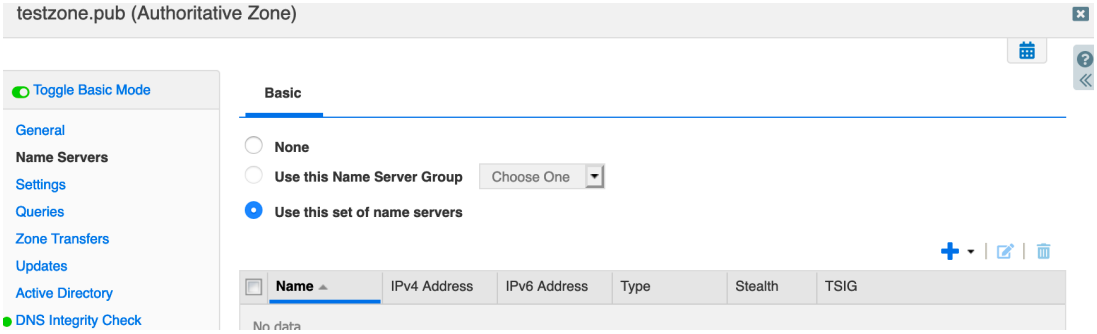


3. In the action menu for the zone, select **Edit**.



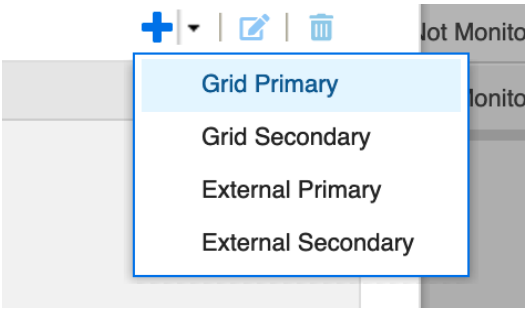
4. In the zone edit window, click **Name Servers**.

5. Select **Use this set of name servers**.



6. Click the ✚ ▾ (add) dropdown.

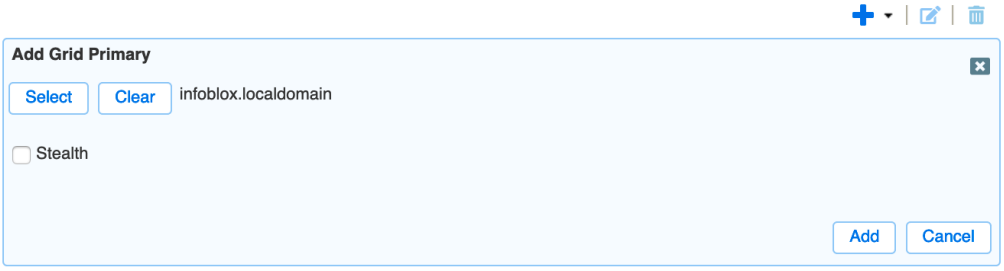
7. Select **Grid Primary** from the list.



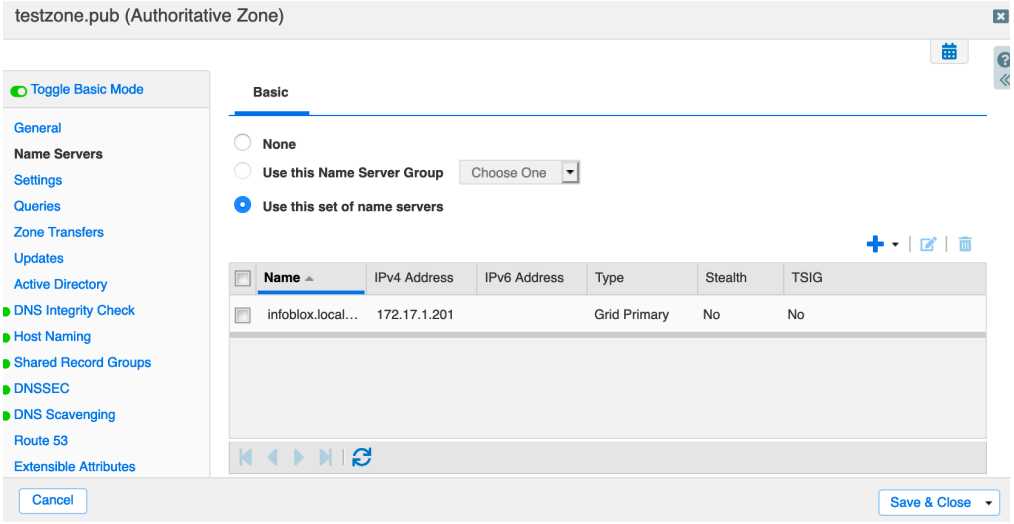
8. Click the **Select** button.

9. Choose a name server from the dialog. If the grid only consists of one member, it will be automatically selected.

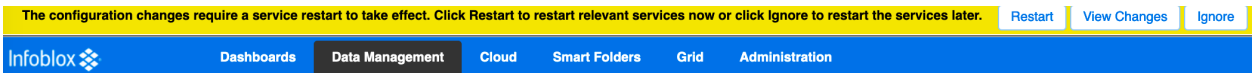
10. Click **Add**.



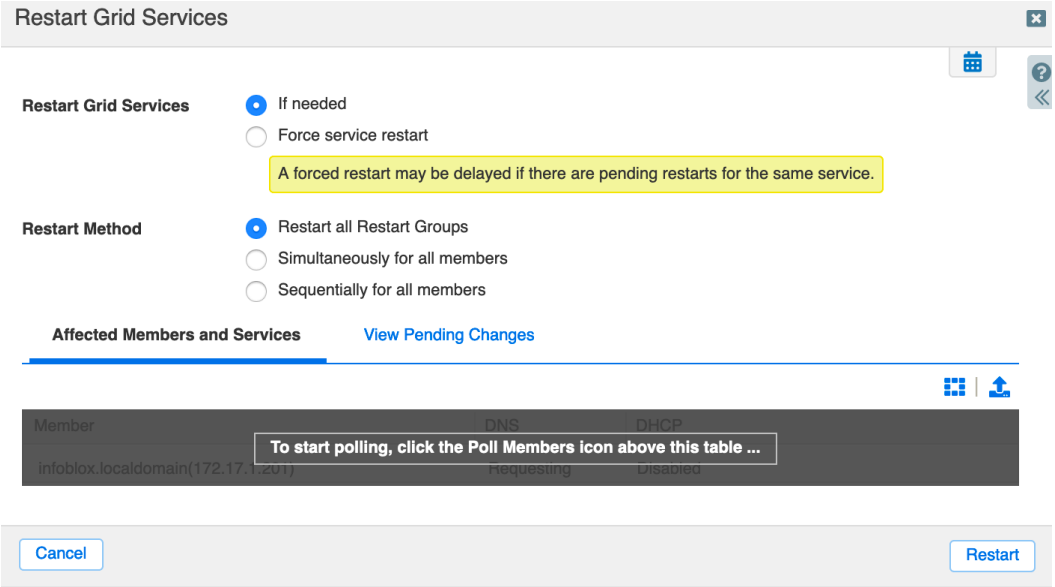
11. Click **Save & Close**.



12. Click **Restart** in the bar at the top of the Grid Manager.



13. Click **Restart** in the Restart Grid Services window.



Your Infoblox name servers will now be authoritative for the Route 53 synchronized zone. Any changes made to the zone in the AWS Route 53 management interface will synchronize on the schedule specified earlier and will become available from the selected name servers automatically.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com