

DEPLOYMENT GUIDE

Implementing AWS Route 53 Synchronization

Table of Contents

Introduction.....	2
Infoblox and Route 53 Synchronization.....	2
Prerequisites.....	2
Create IAM User in AWS.....	2
Create IAM Policy.....	3
Create IAM User.....	6
Create User Credentials.....	8
Configure AWS Route 53 Synchronization in NIOS.....	11
Creating a User Account and AWS Credentials.....	11
Start Cloud DNS Sync Service.....	15
Creating the Route 53 Sync Group.....	15
Working with Route 53 Synchronized Zones.....	18
Configuring Infoblox Name Servers for Route 53 Synchronized Zones.....	22

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**.

The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, featuring a search bar and a navigation menu with 'Policies' highlighted. The main content area shows the 'Policies' page, which includes a header with 'Policies (1174)' and an 'Info' icon. Below the header is a search bar and a table of policies. The table has the following columns: Policy name, Type, Used as, and Description. The table lists four policies, all of which are 'Customer managed' and used as 'Permissions policy ...'.

Policy name	Type	Used as	Description
AWSLambdaBasicExecutionRole-0e07e46e-3b18-4621-8680-0ee8455db596	Customer managed	Permissions policy ...	
AWSLambdaBasicExecutionRole-17176c42-5aad-44a7-b558-0bf7862a0787	Customer managed	Permissions policy ...	
AWSLambdaBasicExecutionRole-18f278b1-768a-4752-925c-0892a70cb215	Customer managed	Permissions policy ...	
AWSLambdaBasicExecutionRole-1ba7a97b-aae8-4786-8ef2-9ad26afe7871	Customer managed	Permissions 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:

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual

JSON

Actions ▼

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [],
8       "Resource": []
9     }
10  ]
11 }

```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

- 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/*"
}

```

- 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**.

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

Guide1-R53

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

Description - optional

Add a short explanation for this policy.

Policy with minimal permissions for Infoblox AWS Route 53 synchronization.

Maximum 1,000 characters. Use alphanumeric and '+=, @-_' characters.

Permissions defined in this policy [Info](#)

Edit

Permissions in the policy document specify which actions are allowed or denied.

Search

Allow (1 of 385 services)

Show remaining 384 services

Service	Access level	Resource	Request condition
Route 53	Limited: List	Multiple	None

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**.

The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Users' selected under 'Access management'. The main content area displays 'IAM > Users' and 'Users (16) Info'. Below the header, there are buttons for 'Refresh', 'Delete', and 'Create user' (highlighted in orange). A search bar is present below the buttons. At the bottom, a table header is visible with columns for 'User name' and 'Path'.

3. Name the user.
4. Click **Next**.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

guide-r53

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

? If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **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**.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1176)

Choose one or more policies to attach to your new user. [Create policy](#)

Filter by Type

guide1-r53 All types 1 match

<input checked="" type="checkbox"/>	Policy name	Type	Attached entities
<input checked="" type="checkbox"/>	Guide1-R53	Customer managed	0

▶ Set permissions boundary - optional

Cancel Previous **Next**

9. Optionally, add tags.
10. Review the User details and Permissions.
11. Click **Create user**.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name guide-r53	Console password type None	Require password reset No
------------------------	-------------------------------	------------------------------

Permissions summary

< 1 >

Name ↗	Type	Used as
Guide1-R53	Customer managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

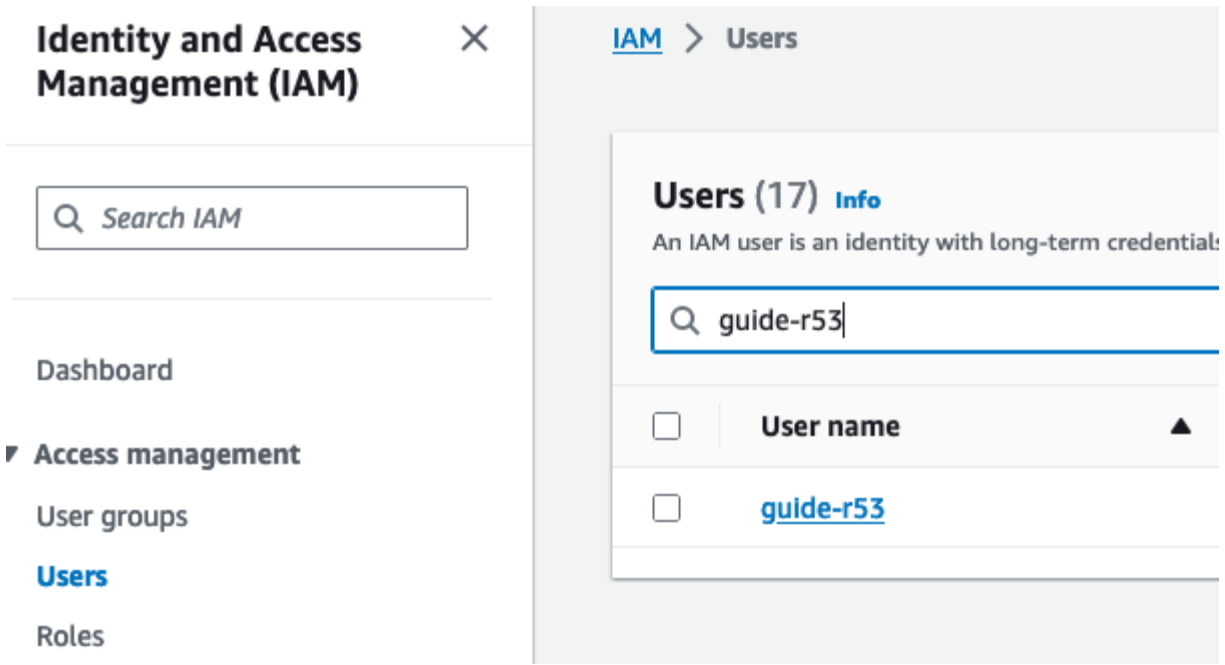
You can add up to 50 more tags.

Cancel [Previous](#) **Create user**

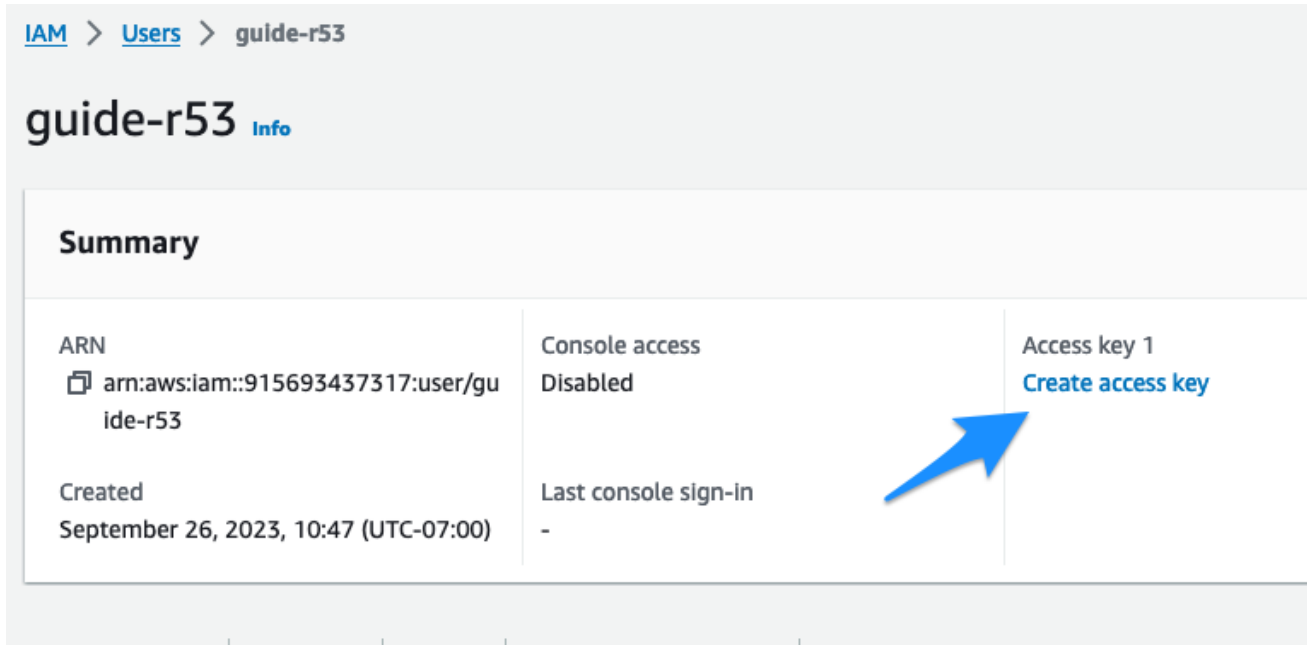
Create User Credentials

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**.

Step 1
Access key best practices & alternatives

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Other
Your use case is not listed here.

It's okay to use an access key for this use case, but follow the best practices:

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Cancel Next

- On Step 2, optionally enter a description.
- Click **Create access key**.

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
Set description tag

Step 3
Retrieve access keys

Set description tag - optional Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Used for Infoblox Route 53 sync, guide

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel Previous Create access key

- Copy and save or download the credentials.

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Retrieve access keys Info

Access key
 If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIA5KM4VAGC7IX6LVUI	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

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.

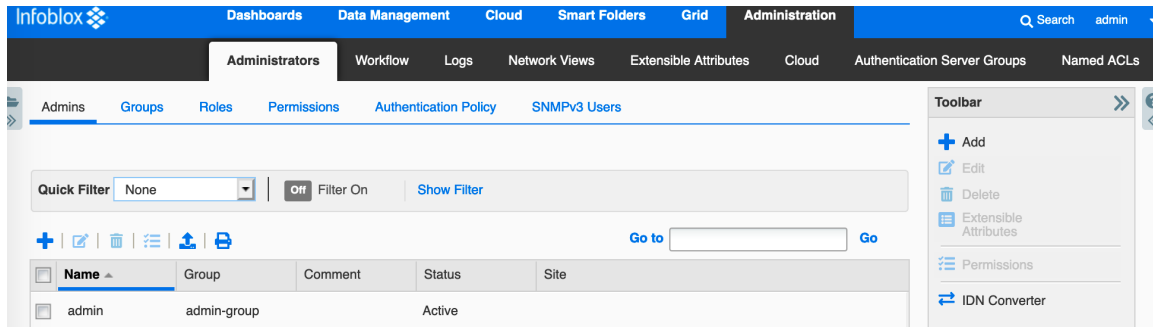
Configure AWS Route 53 Synchronization in NIOS

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**.

Add Administrator Wizard > Step 1 of 2

Authentication Type: Local

Credentials

*Login: route53-user

*Password:

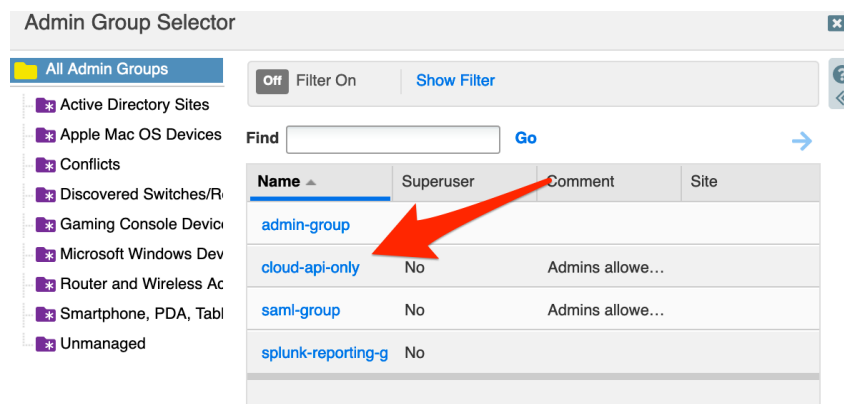
*Confirm Password:

Password must contain at least 4 characters.

Email Address:

*Admin Group: Select Clear

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



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

Add Administrator Wizard > Step 1 of 2

Authentication Type: Local

Credentials

*Login: route53-user

*Password:

*Confirm Password:

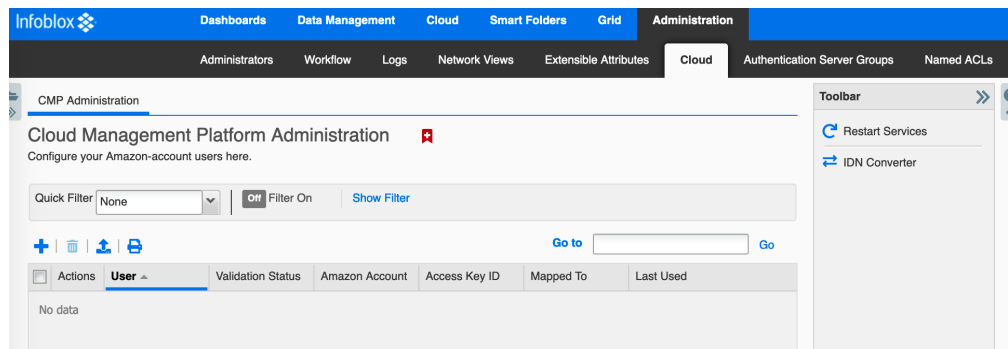
Password must contain at least 4 characters.

Email Address:

*Admin Group: cloud-api-only

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**.

Add Amazon User Wizard > Step 1 of 1

*Username

*Access key ID

*Secret access key

*Amazon account

Mapped to NIOS user

16. Click on the new admin user you created.

Select NIOS User

Off Filter On Show Filter

Find Go

Name	Comment	Site
admin		
route53-user		

17. Click Save & Close.

Add Amazon User Wizard > Step 1 of 1

*Username

*Access key ID

*Secret access key

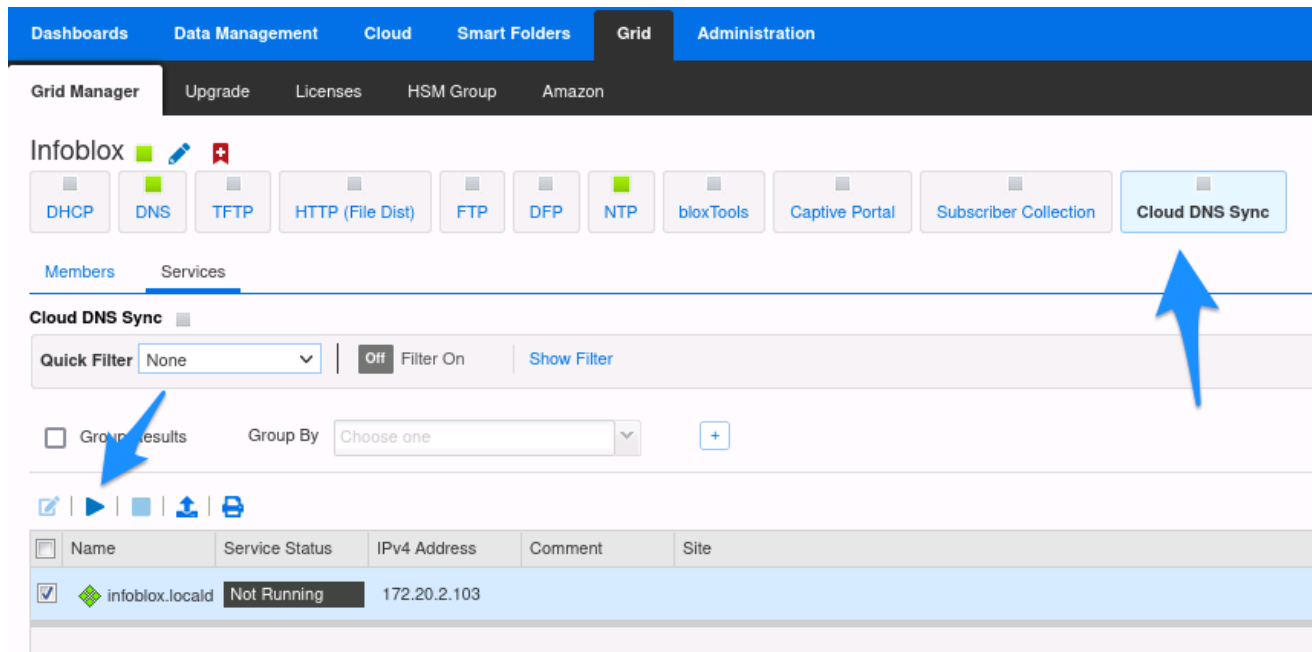
*Amazon account

Mapped to NIOS user route53-user

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.



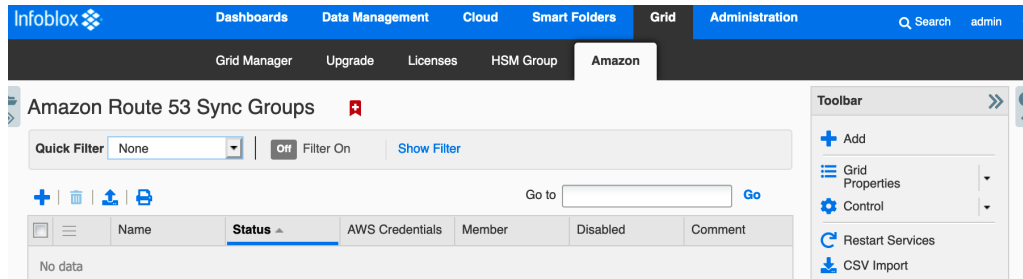
The screenshot shows the Infoblox Grid Manager interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Cloud', 'Smart Folders', 'Grid', and 'Administration'. The 'Grid' tab is active, and the 'Grid Manager' sub-tab is selected. Below the navigation bar, there are several service tiles: DHCP, DNS, TFTP, HTTP (File Dist), FTP, DFP, NTP, bloxTools, Captive Portal, Subscriber Collection, and Cloud DNS Sync. The 'Cloud DNS Sync' tile is highlighted with a blue arrow. Below the service tiles, there are tabs for 'Members' and 'Services'. The 'Cloud DNS Sync' section is expanded, showing a 'Quick Filter' dropdown set to 'None', a 'Filter On' toggle set to 'Off', and a 'Show Filter' link. Below the filter controls, there is a 'Group By' dropdown set to 'Choose one' and a '+' button. A blue arrow points to the '+' button. Below the group controls, there are icons for refresh, play, stop, and delete. At the bottom, there is a table with columns: Name, Service Status, IPv4 Address, Comment, and Site. The table contains one entry: 'infoblox.locald' with a status of 'Not Running' and an IPv4 address of '172.20.2.103'.

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**.

Amazon Sync Wizard > Step 1 of 1

*Sync Group Name

Disable Synchronization

Multiple Account Sync

Role ARN

*Member

Credentials

Use instance profile

Use IAM credential

Synchronize Route 53 data into:

This network view:

The tenant's network view (if it does not exist, create a new one)

Consolidate zone data into this DNS view

Comment

Sync Tasks + | ✎ | 🗑

<input type="checkbox"/>	Name ▲	Interval	Filter

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.

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

- 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**.

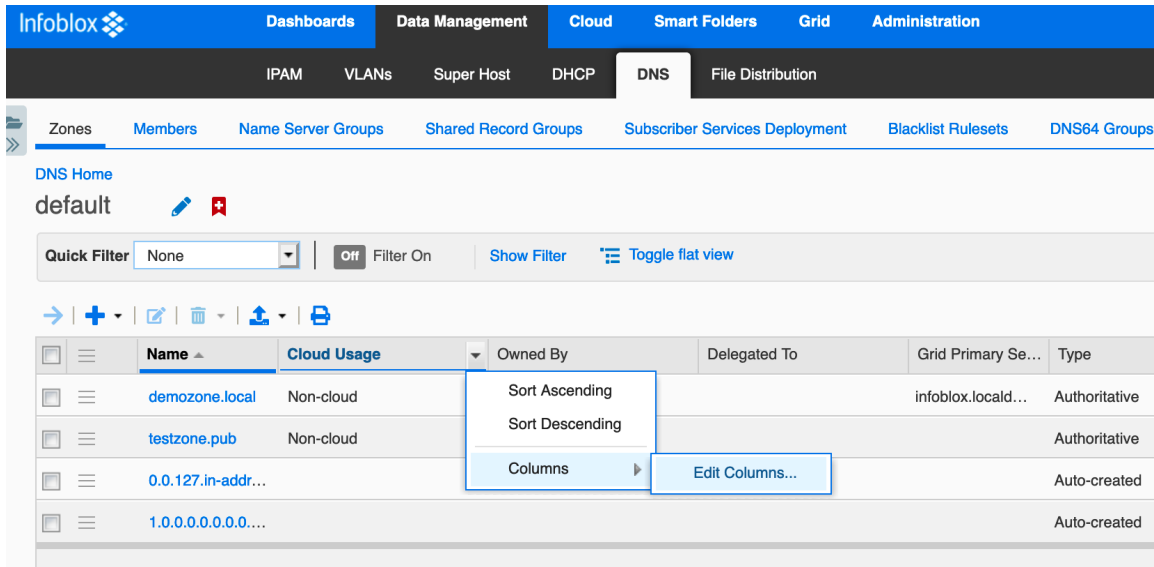
Name	Status	AWS Credentials	Member	Disabled
Guide-Group	OK	guide-route53:r...	infoblox.locald...	false

Working with Route 53 Synchronized Zones

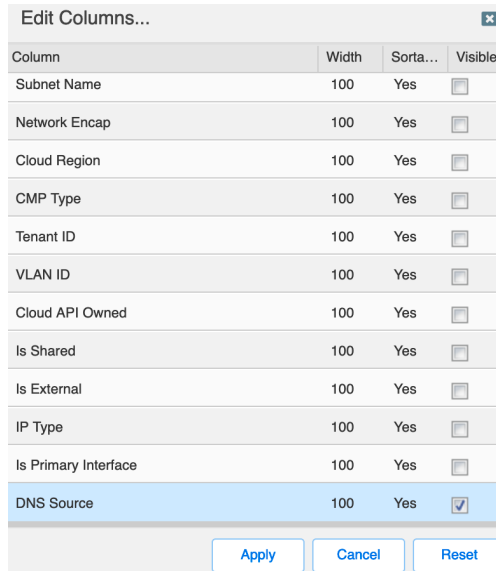
Route 53 Public Hosted Zones are synchronized into the default DNS view. A new Extensible Attribute (EA), **DNS Source**, is available to identify Route 53 zones in the system.

- Navigate to the **Data Management** → **DNS** → **Zones** tab.
- To add the DNS Source extensible attribute to your view, hover over any column.
- Click the dropdown and select **Columns**.

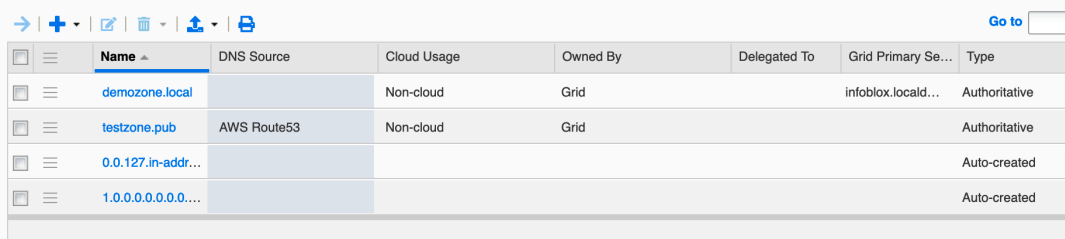
4. Click on **Edit Columns**.



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

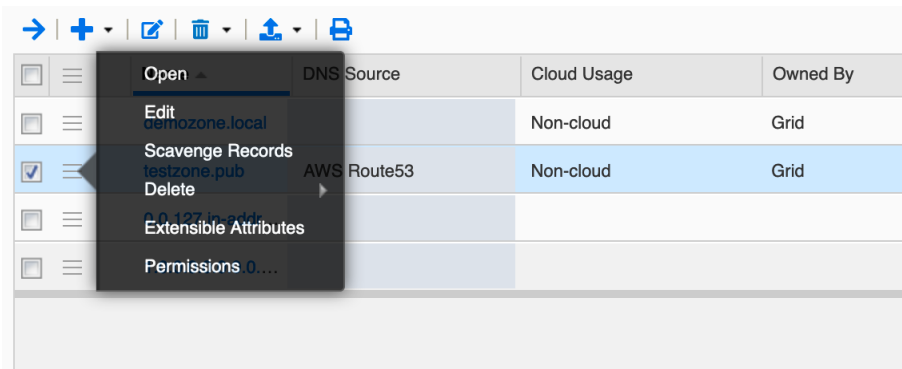


7. Back on the Zones tab, scroll right to find the **DNS Source** column.
8. Click and drag the column to the desired location.

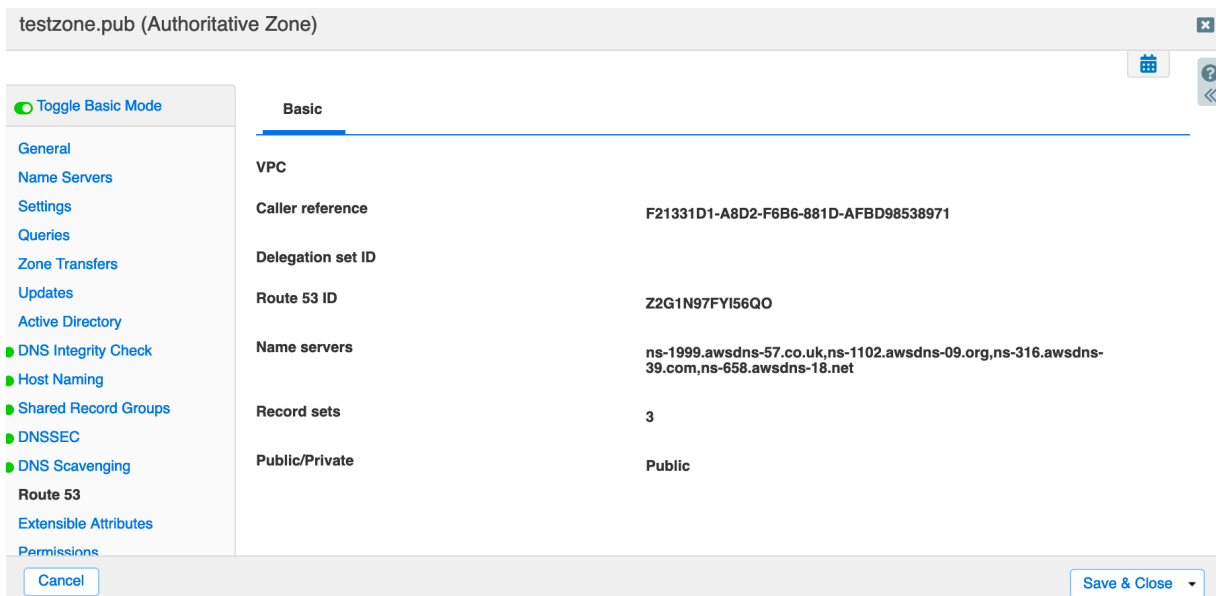


Name	DNS Source	Cloud Usage	Owned By	Delegated To	Grid Primary Se...	Type
demozone.local		Non-cloud	Grid		infoblob.local...	Authoritative
testzone.pub	AWS Route53	Non-cloud	Grid			Authoritative
0.0.127.in-addr...						Auto-created
1.0.0.0.0.0.0...						Auto-created

- 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.



- 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.



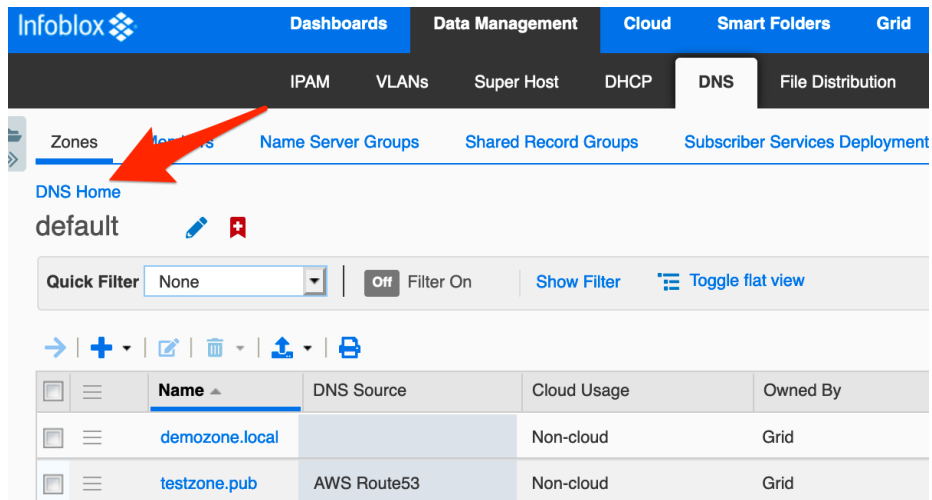
- Click **Cancel** to exit the zone edit dialog.

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

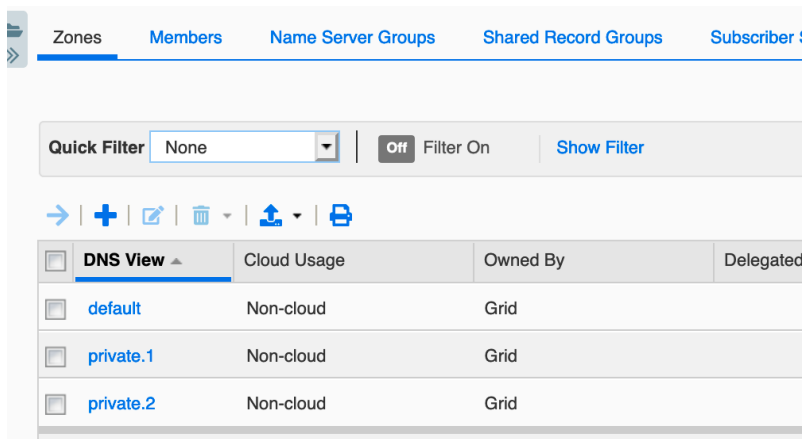
named private.n. A separate view will be created for every unique combination of VPCs associated with a Private Hosted Zone.

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.

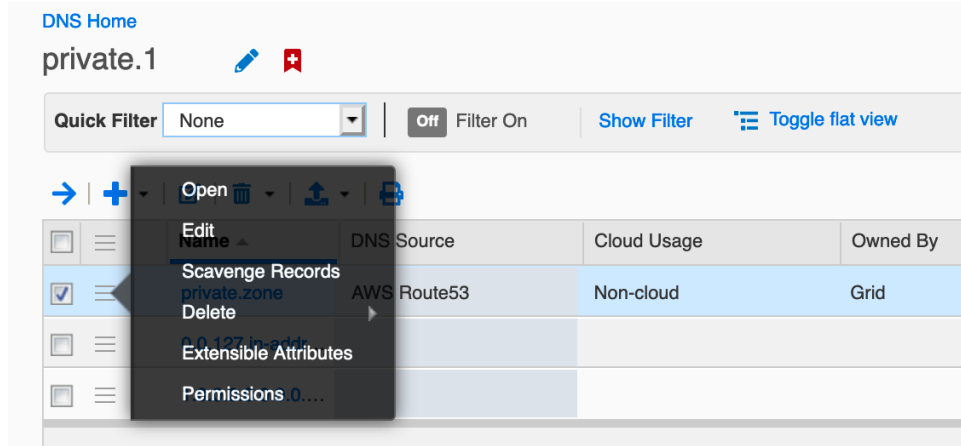
12. To view a Private Hosted Zone, click on **DNS Home**.



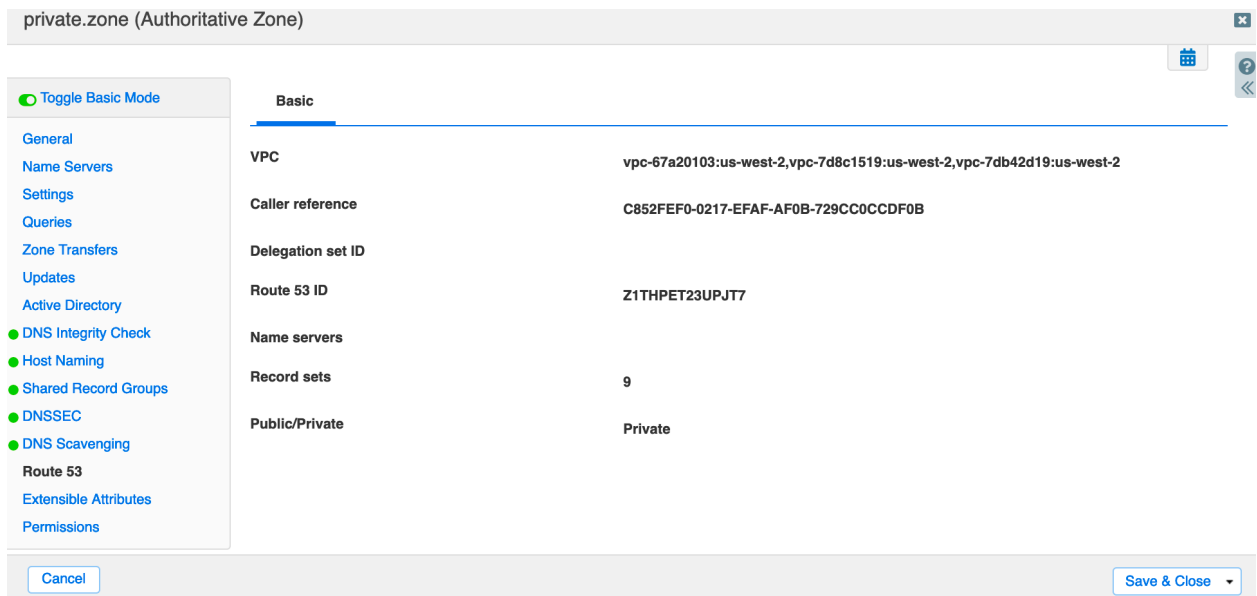
13. Click on one of the **private.n** DNS Views.



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.

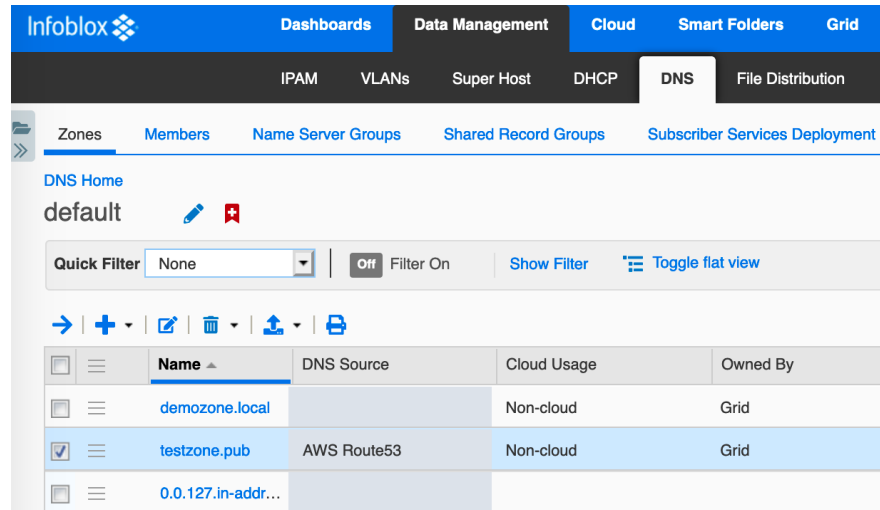
Warning: It is possible to make changes to a Route 53 synchronized zone within the Infoblox Grid Manager interface. However, when the zone is next synchronized from Route 53, any changes will be lost and the zone will revert to the zone data from Route 53.

Configuring Infoblox Name Servers for Route 53 Synchronized Zones

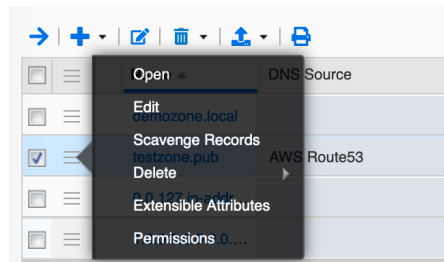
Using your Infoblox name servers, on-premises and hybrid/multi cloud clients can resolve DNS records in your Route 53 hosted zones. To make your Infoblox name servers authoritative for the Route 53 synchronized zones:

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

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

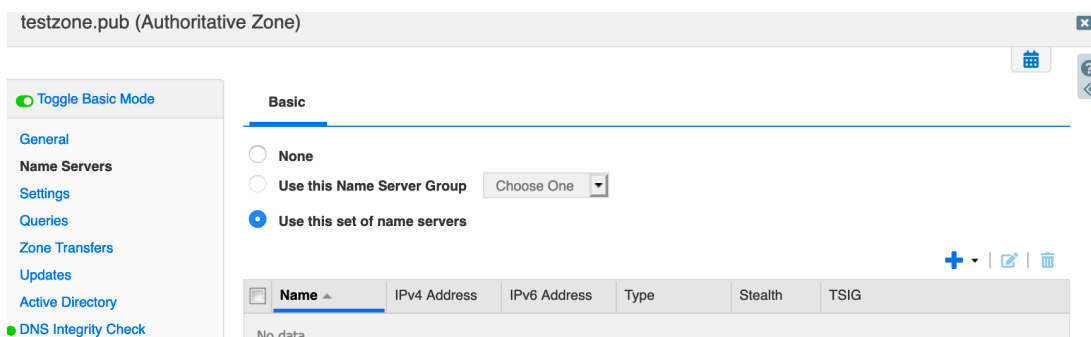


3. In the action menu for the zone, select **Edit**.

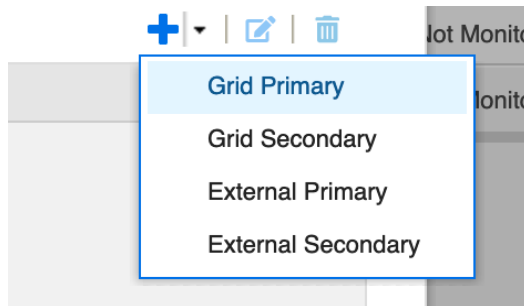


4. In the zone edit window, click **Name Servers**.

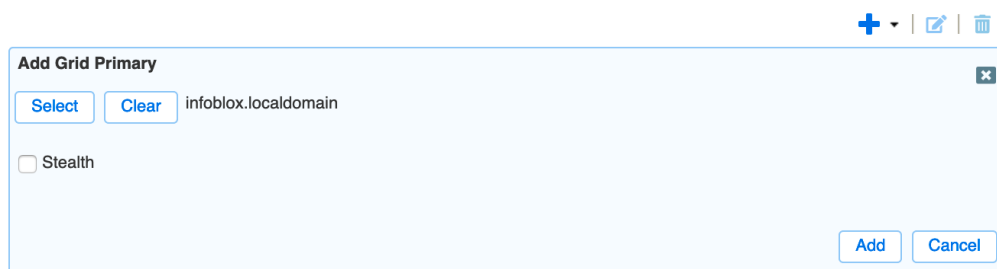
5. Select **Use this set of name servers**.



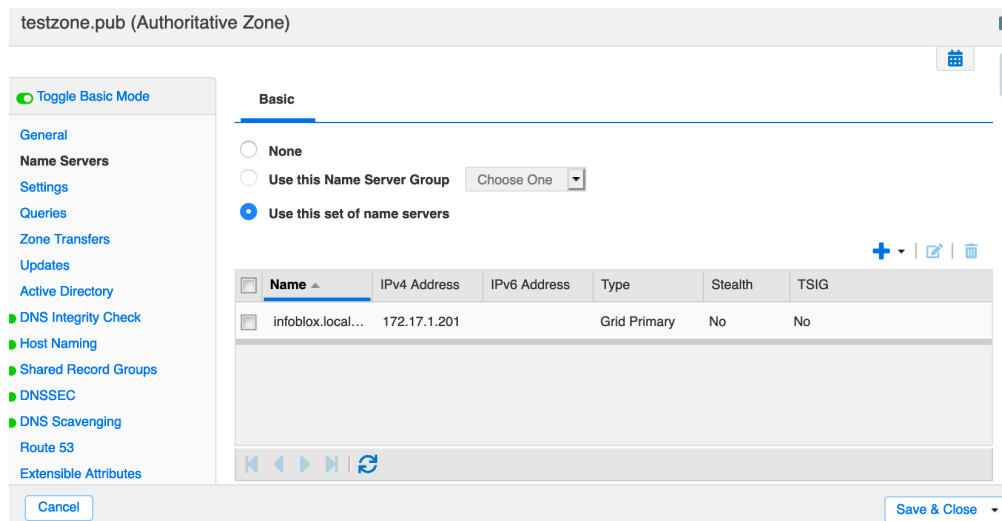
6. Click the **+ ' (add) dropdown.**
7. Select **Grid Primary** from the list.



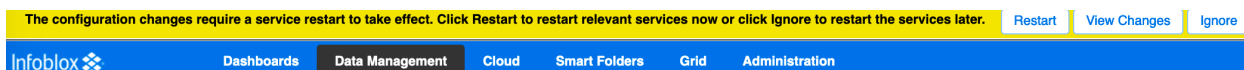
8. Click the **Select** button.
9. Choose a name server from the dialog. If the grid only consists of one member, it will be automatically selected.
10. Click **Add**.



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.

✕
📅 ? ⏪

Restart Grid Services

If needed
 Force service restart

A forced restart may be delayed if there are pending restarts for the same service.

Restart Method
 Restart all Restart Groups
 Simultaneously for all members
 Sequentially for all members

Affected Members and Services [View Pending Changes](#)

📊
📶

Member	DNS	DHCP
infoblox.localdomain(172.17.1.201)	Requesting	Disabled

To start polling, click the Poll Members icon above this table ...

Cancel
Restart

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