

DEPLOYMENT GUIDE

DNS Scavenging Deployment Guide

Table of Contents

Introduction	2
Prerequisites	2
Limitations.....	2
Scavenging Workflow.....	2
Scavenging Properties.....	3
Best Practices	3
Deploying DNS Scavenging	3
Enabling DNS Scavenging.....	4
Setting up Scavenging Rules.....	6
Resource Record Type.....	6
Creation Time.....	6
Last Queried Time.....	7
Last Discovered Time.....	7
Record Source.....	8
Associated Records.....	9
Extensible Attributes.....	9
Creating a Scavenging Policy.....	10
Automatically Scavenging Stale Records.....	12
Manually Scavenging Stale Records.....	13
Manually Deleting Reclaimable Records.....	15
Reset Reclaimable Flag.....	16
Disabling Scavenging on Individual Resource Records.....	17
Using Multiple Matching Rules in a Scavenging Policy.....	18
Static Records Not Queried in a Year.....	18
Dynamic Records Created More Than a Month Ago.....	19
Simulate Microsoft DNS Scavenging Behavior.....	19
Recycle Bin	19
Dashboard Widget	21
Smart Folders	21

Introduction

DNS Scavenging enables NIOS to remove stale DNS records based on configured scavenging policies. The stale records can either be marked for removal by the administrator at a later time or automatically removed during scavenging operation.

Prerequisites

The following are prerequisites for Infoblox DNS Scavenging;

- Functional NIOS 7.3 or higher Infoblox Grid™ with a Grid Master
- Active Grid and DNS license
- At least one NIOS appliance acting as a Primary DNS Server

Limitations

Following general limitations apply:

- Records created by NIOS automatically (creator is SYSTEM) are never scavenged, for example NS, SOA.
- Manually created records are never scavenged automatically.
- Minimal Scavenging analysis unit is a zone; scavenging an individual record is not supported.
- There can be only one scavenging task in progress at any given time
- Scavenging is supported only for Authoritative grid primary (or unassigned) zones. Microsoft and external primary zones are not supported for scavenging.
- Scavenging is disabled by default in both new NIOS installations and upgrade use cases.

Scavenging Workflow

Scavenging is divided into two separate stages, which can be executed separately:

- Analysis
 - During this stage, resource records are marked as reclaimable and are not deleted.
- Scavenging
 - During this stage, records marked as reclaimable in the Analysis stage are deleted.

- The deletion process moves the records to the Recycle Bin if this feature is enabled.

Users may control the entire workflow by:

- Defining scavenging properties for a particular object (scavenging policies, scheduling, etc.)
- Running either a single workflow or both stages of the workflow

Scavenging Properties

Scavenging properties can be defined at the following levels:

- Grid DNS
- DNS View
- Authoritative Zone

Properties defined at a given level are inherited by subordinate levels unless overridden, following the standard NIOS inheritance pattern.

Best Practices

To get the most from Infoblox DNS Scavenging, Infoblox recommends the following best practices:

- All scavenged records end up in the Recycle Bin. The Recycle bin is not automatically emptied. An administrator should determine the frequency of emptying the recycle bin. The idea is not to run out of space.
- All rules should be tested with manual execution before configuring scavenging for automated runs.
- Automated Scavenging runs should be scheduled for non-peak hours.
- Rules should be designed to target as granular of a set of records as possible.

Deploying DNS Scavenging

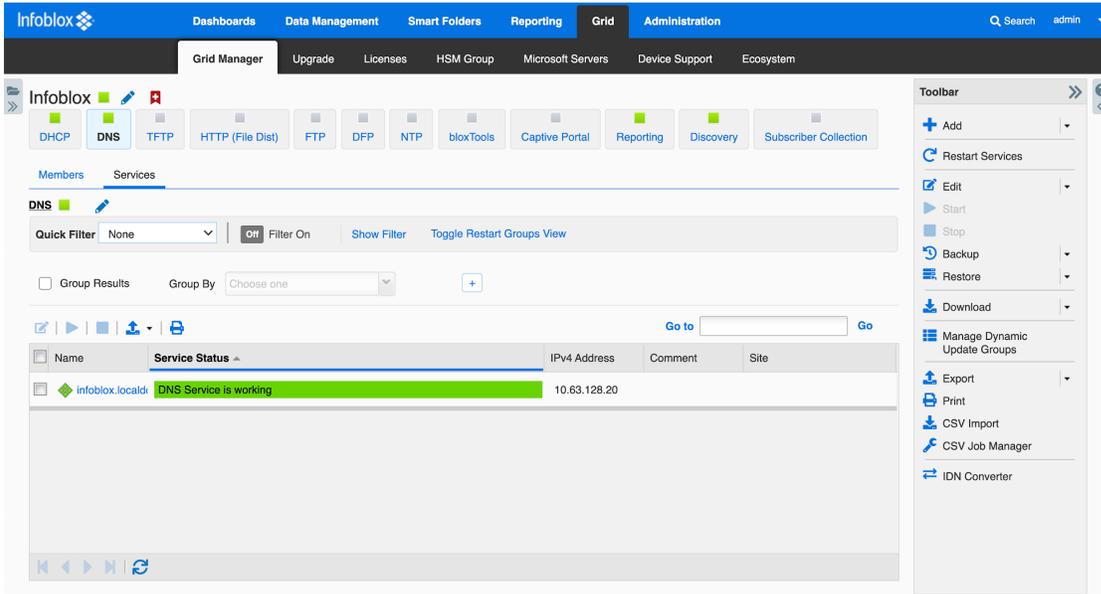
The following steps are required to enable DNS Scavenging:

1. Enable DNS Scavenging on the Grid
2. Set up the scavenging policy
3. Automatically scavenge stale DNS records
4. Manually scavenge stale DNS records

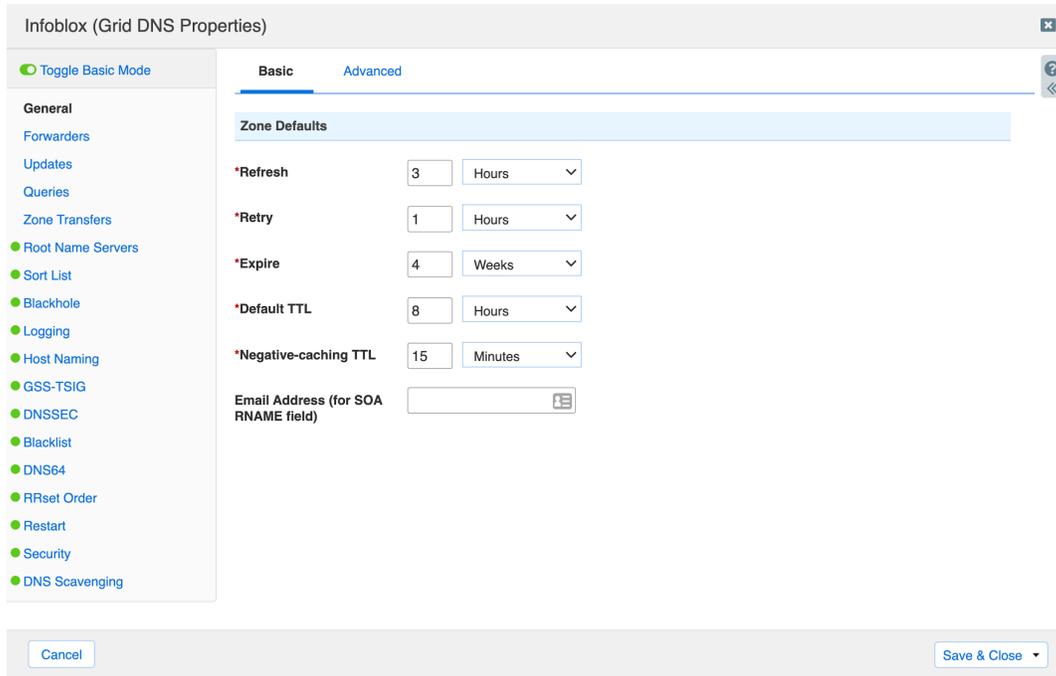
Enabling DNS Scavenging

This section describes how to enable DNS Scavenging on the Grid.

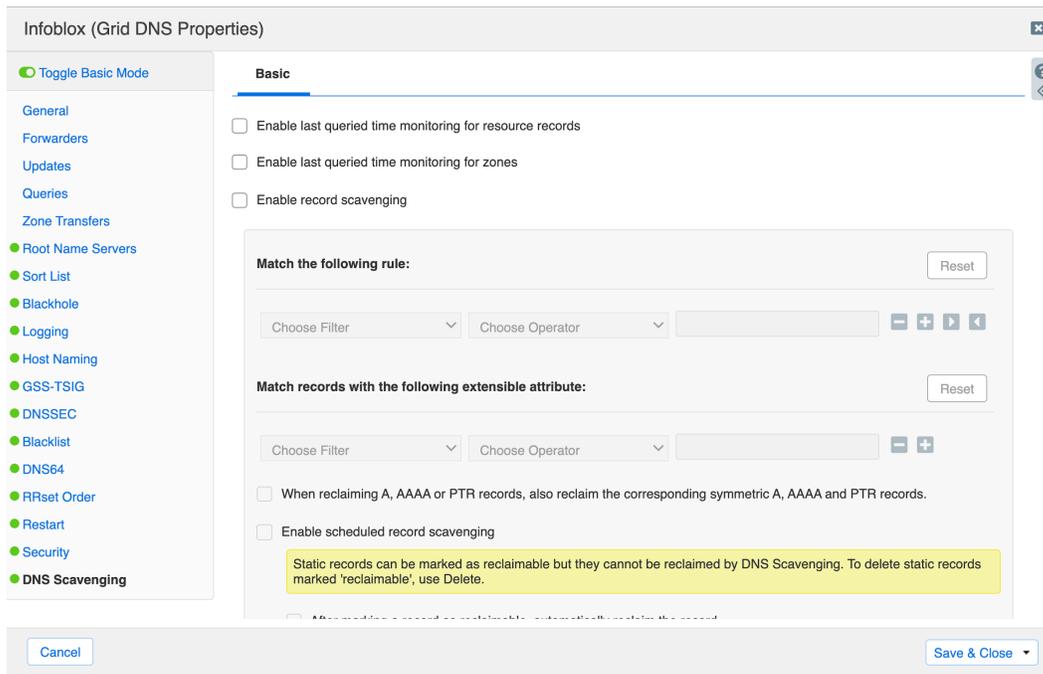
1. Go to Grid → Grid Manager → DNS → Services.



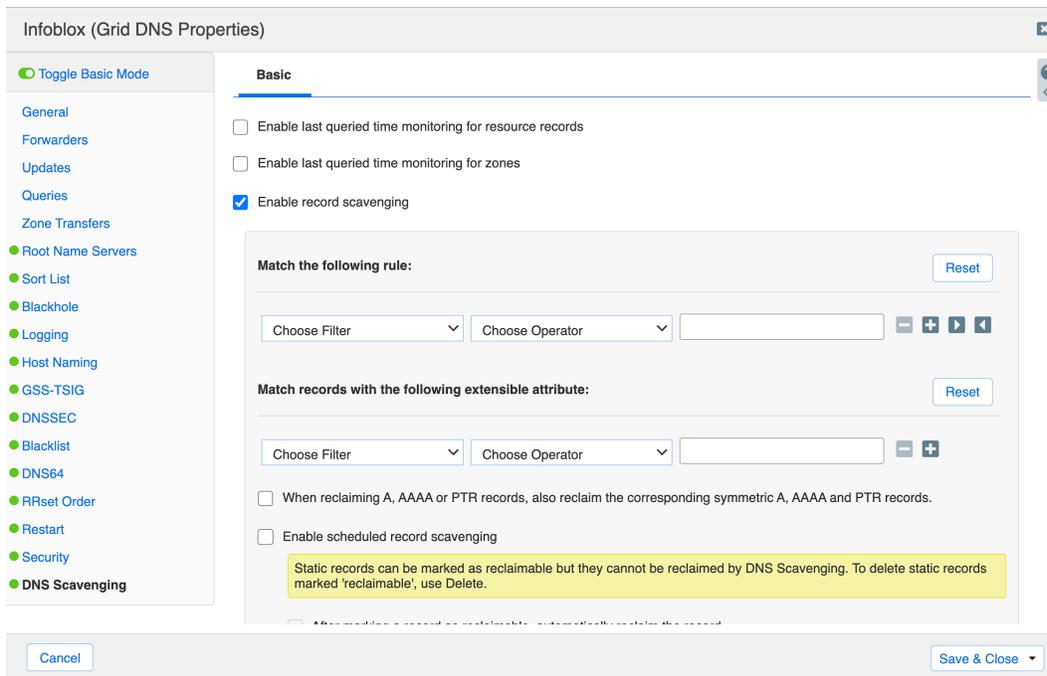
2. Select the **Edit** → **Grid DNS Properties** from the toolbar.



3. Click **Toggle Advanced Mode** to ensure that Advanced mode is on, and click the **DNS Scavenging** tab in the Grid Properties Editor.



4. Select **Enable record scavenging**.



Setting up Scavenging Rules

After enabling Infoblox DNS Scavenging, configure scavenging policies to identify which stale DNS records are going to be scavenged.

Resource Record Type

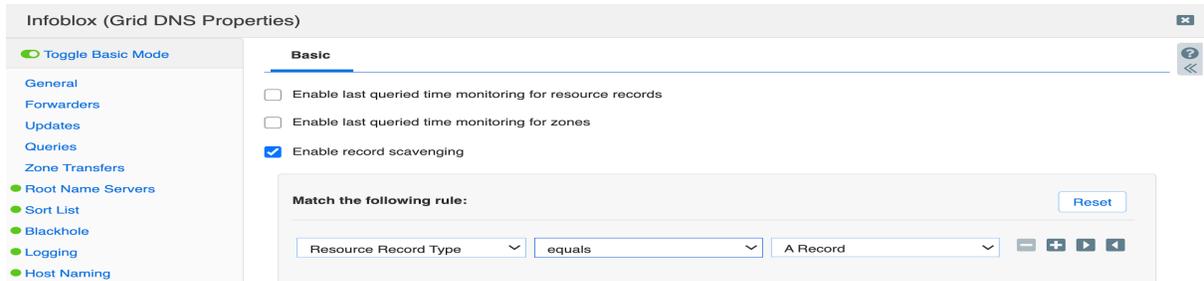
The resource record type policy allows users to define a record type for scavenging. A record is reclaimable if its type matches the type configured in the policy.

Supported types are: A, AAAA, PTR, CNAME, DNAME, MX, SRV, NAPTR, and TXT.

Note: NS, SOA, DNSSEC and HOST records are not supported for scavenging.

In the following example a scavenging policy is set for A records.

1. In the Grid DNS Properties editor, in the DNS Scavenging tab, set the **Matching** rule option so that **Resource Record Type** equals A Record.



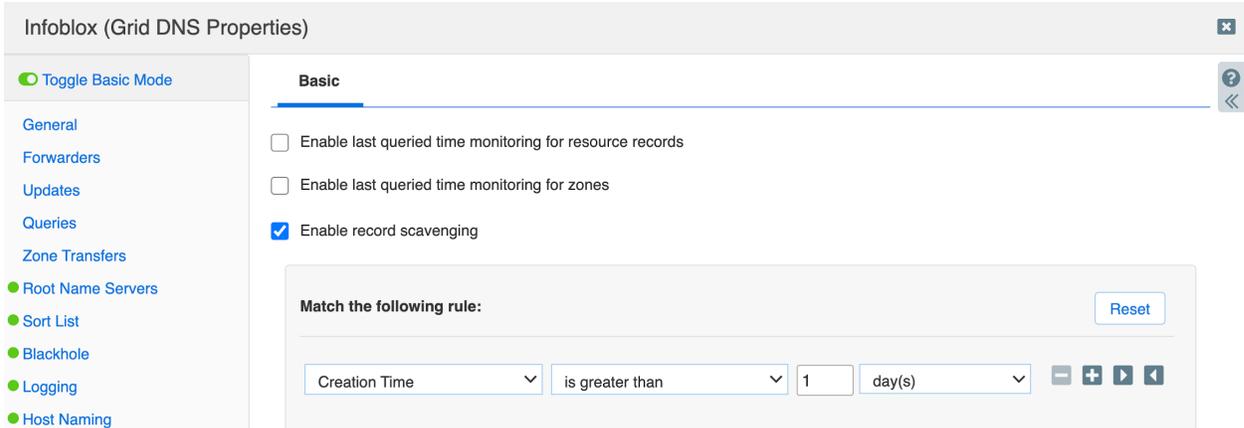
The operator values are **equals** and **does not equal**. If the operator in this example is set to **does not equal**, then all supported resource records will be scavenged except A records.

2. Click **Save & Close**.

Creation Time

The Creation Time scavenging policy is based on the record creation timestamp. If a record does not have creation time set, it will never be marked reclaimable based on this policy. In this example, the following creation time policy is set to scavenge records that are older than a day.

1. In the Grid DNS Properties editor, in the DNS Scavenging tab, set the Matching rule option so that the Creation Time is greater than 1 day.



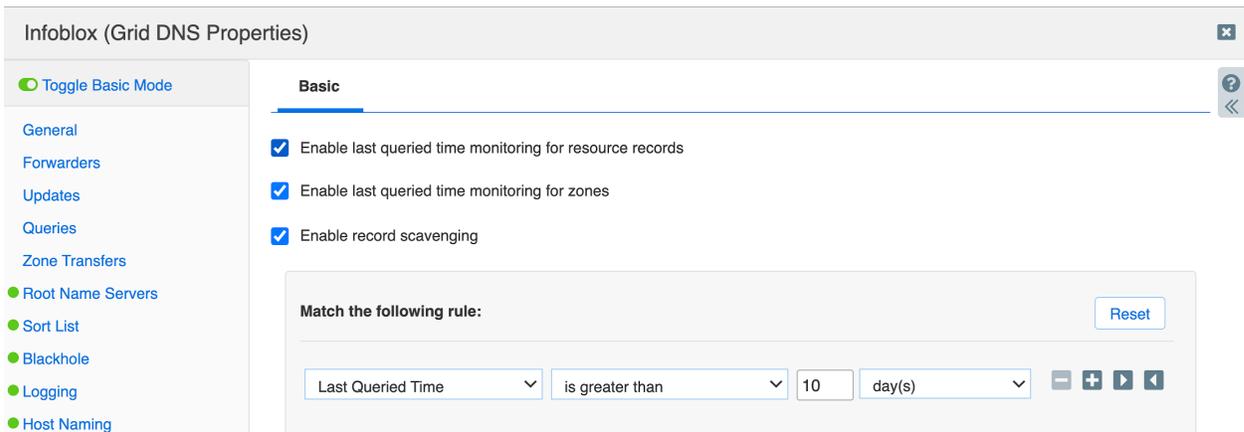
Setting the creation time to greater than 52 weeks scavenges records that are more than a year old.

2. Click **Save & Close**.

Last Queried Time

This policy allows users to define a scavenging policy based on last queried timestamp, which requires last queried enabled on zones. In this example, records that are not queried for more than ten days will be scavenged.

1. In the Grid DNS Properties editor, in the DNS Scavenging tab, select **Enable last queried time monitoring for resource records** and **Enable last queried time monitoring for zones** options. Set the Matching rule option such that Last Queried Time is greater than 10 days,

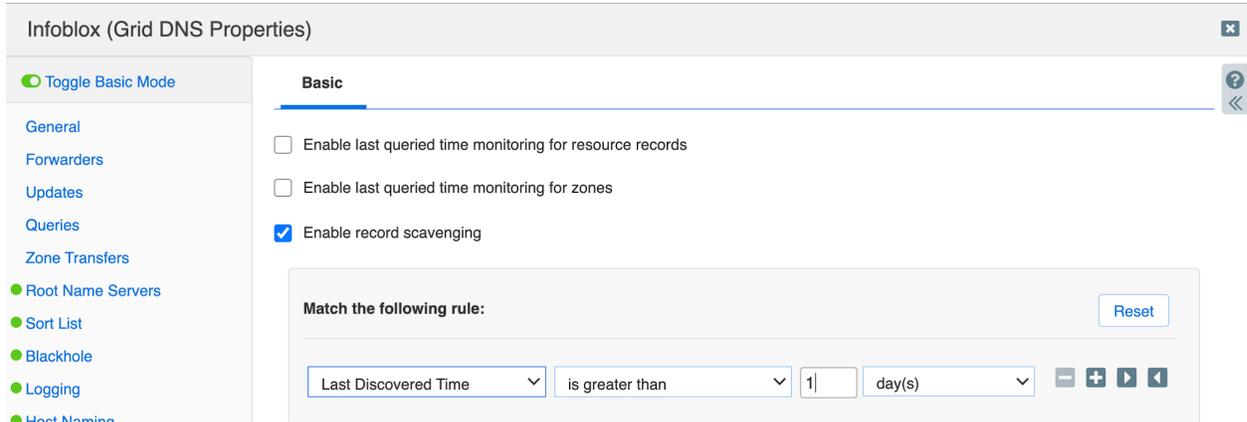


2. Click **Save & Close**.

Last Discovered Time

The Last Discovered Time policy allows users to define a scavenging policy based on last seen timestamp. This policy is for A, AAAA, and PTR records.

1. To set this policy to scavenge records last seen more than a day ago, in the Grid DNS Properties editor, in the DNS Scavenging tab, set the Matching rule option so that Last Discovered Time is greater than 1 day.



2. Click **Save & Close**.

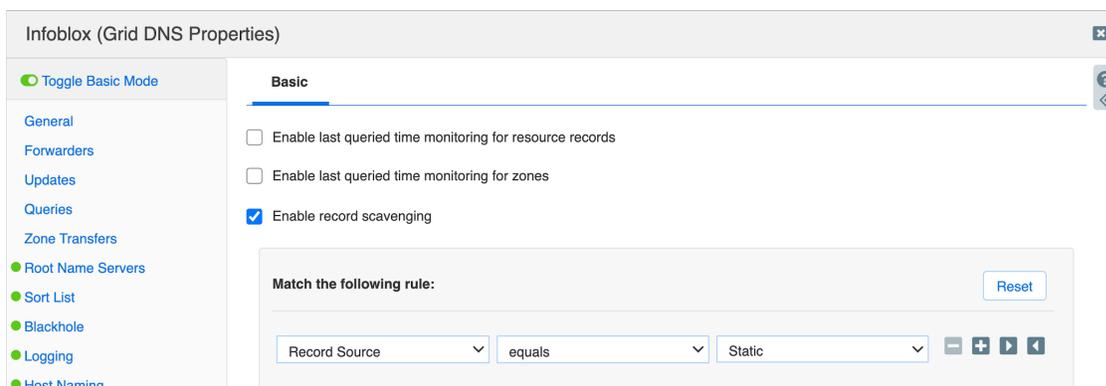
Note: To understand how the discovery process works in NIOS, refer to the chapter on “IP Discovery and vDiscovery” in the NIOS Admin Guide.

Record Source

The Record Source policy enables NIOS to scavenge records based on their source: Static or Dynamic. Static records cannot be scavenged automatically.

Note: Users can omit this rule if both Static and Dynamic records need to be scavenged.

1. To scavenge Static records only, in the Grid DNS Properties editor, in the DNS Scavenging tab, set the Matching rule option so that Records Source equals Static.

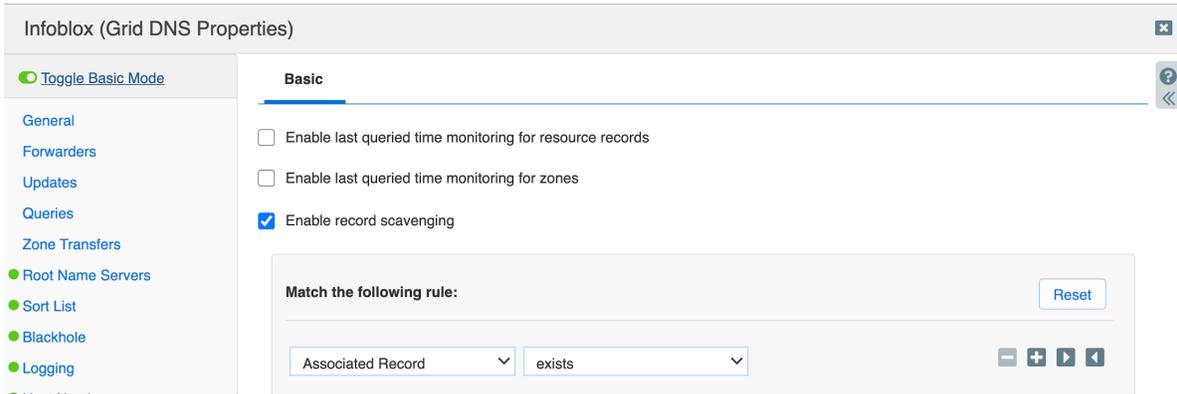


2. Click **Save & Close**.

Associated Records

The Associated Records policy specifies whether to check for associated records existence.

1. To scavenge A records (only if associated records exist), in the Grid DNS Properties editor, in the DNS Scavenging tab, set the Matching rule option so that Associated Record exists is chosen.



2. Click **Save & Close**.

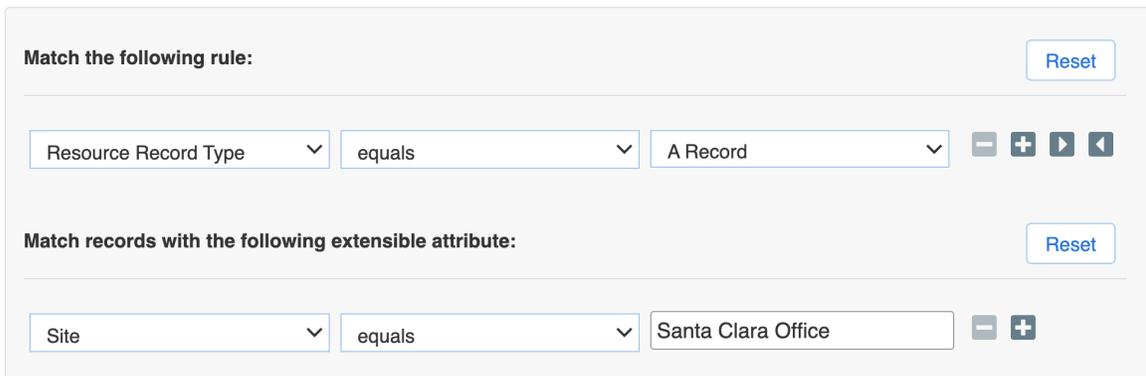
Note: Record associations are not definable and are supported only for Address records (A/AAAA/PTR).

Extensible Attributes

The Extensible Attributes scavenging policy makes a record reclaimable if it has associated Extensible Attributes as defined in the policy.

1. To scavenge A records that have Extensible Attribute Site with a value of Santa Clara Office, in the Grid DNS Properties editor, in the DNS Scavenging tab, set two Matching rule options:
 - o Resource Record Type equals A Record
 - o Site equals Santa Clara Office

Enable record scavenging



The extensible attributes matching is logical AND with the policy above.

Creating a Scavenging Policy

The scavenging policy consists of a combination of scavenging rules discussed in the previous section. The scavenging rules support AND/OR operators. The rules can also be nested to create complex scavenging policies. The same rule type can be used more than once (for example: two rules for resource record type that match A and AAAA records). The Extensible Attribute (EA) rules do not support nesting and EA rules use AND logic with the other set of rules.

Note: In the screen captures below, the words AND and OR in red have been added to make choice clear; they do not appear in the actual UI.

With the all keyword, rules at the same level have an AND between them.

The screenshot shows a configuration interface for a scavenging policy. At the top, it says "Match **all** of the following rules:" with a dropdown menu set to "all" and a "Reset" button. Below this, there are three rows of rules, each with a dropdown menu for the attribute, a dropdown for the operator, a text input for a value, a dropdown for the unit, and a set of control icons (minus, plus, right arrow, left arrow). The first row is "Resource Record Type" equals "A Record". The second row is "Creation Time" is greater than "52" "week(s)". The third row is "Last Queried Time" is greater than "30" "day(s)".

With the any keyword, rules at the same level have an OR between them.

The screenshot shows a configuration interface for a scavenging policy. At the top, it says "Match **any** of the following rules:" with a dropdown menu set to "any" and a "Reset" button. Below this, there are three rows of rules, each with a dropdown menu for the attribute, a dropdown for the operator, a text input for a value, a dropdown for the unit, and a set of control icons (minus, plus, right arrow, left arrow). The first row is "Resource Record Type" equals "A Record". The second row is "Creation Time" is greater than "52" "week(s)". The third row is "Last Queried Time" is greater than "30" "day(s)".

Scavenging rules can be nested. Users can create levels in the scavenging policy and have the option of using AND/OR operators within levels and within the same level rules for more scavenging options.

Consider this nested equation:

Rule 1 AND Rule 2 AND Rule 3 (Rule A (Rule a AND Rule b) OR Rule B (Rule c AND Rule d) AND EA Rule

Where Rule 1, Rule 2, Rule 3, and EA Rule are top-level rules with AND operations between them. Rule A and Rule B are sub-level rules with further sub-levels of rules. User have maximum flexibility in creating scavenging policies, as shown below.

The screenshot displays a DNS scavenging policy configuration interface. At the top, a section titled "Match all of the following rules:" contains a "Reset" button and a list of rules. The rules are:

- Rule 1: Creation Time is greater than 1 hour(s)
- Rule 2: Record Source equals Static
- Rule 3: any of the following rules:
 - Rule A: all of the following rules:
 - Rule a: Resource Record Type equals A Record
 - Rule b: Associated Record exists
 - Rule B: all of the following rules:
 - Rule c: Resource Record Type equals PTR Record
 - Rule d: Last Discovered Time is greater than 4 day(s)
- EA Rule: Match records with the following extensible attribute: Site equals Home

Annotations on the left side of the interface indicate the logical structure:

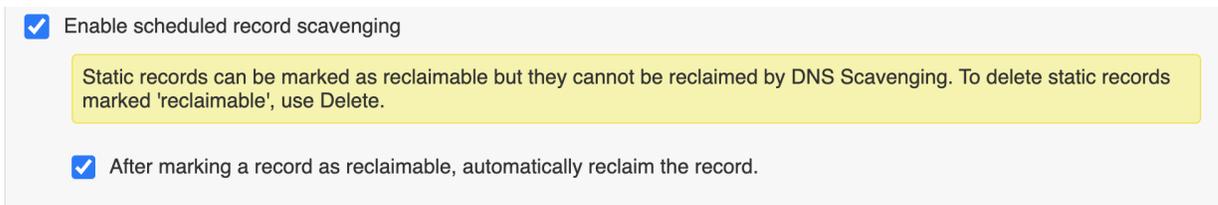
- Rule 1 AND Rule 2
- Rule 3 (AND) contains Rule A (AND) and Rule B (OR)
- EA Rule (AND) is combined with the other top-level rules.

The bottom portion of the image shows a simplified view of the same configuration, with a "Reset" button and a list of rules that matches the top section.

Automatically Scavenging Stale Records

Users can make a DNS scavenging process recurring so that it automatically runs on a set schedule.

1. In the Grid DNS Properties editor, in the DNS Scavenging tab, check the option Enable scheduled record scavenging.
2. If you also need to delete the records after marking them stale during the scavenging cycle, then check the option After marking a record as reclaimable, automatically scavenge the record. Otherwise leave the option unchecked.



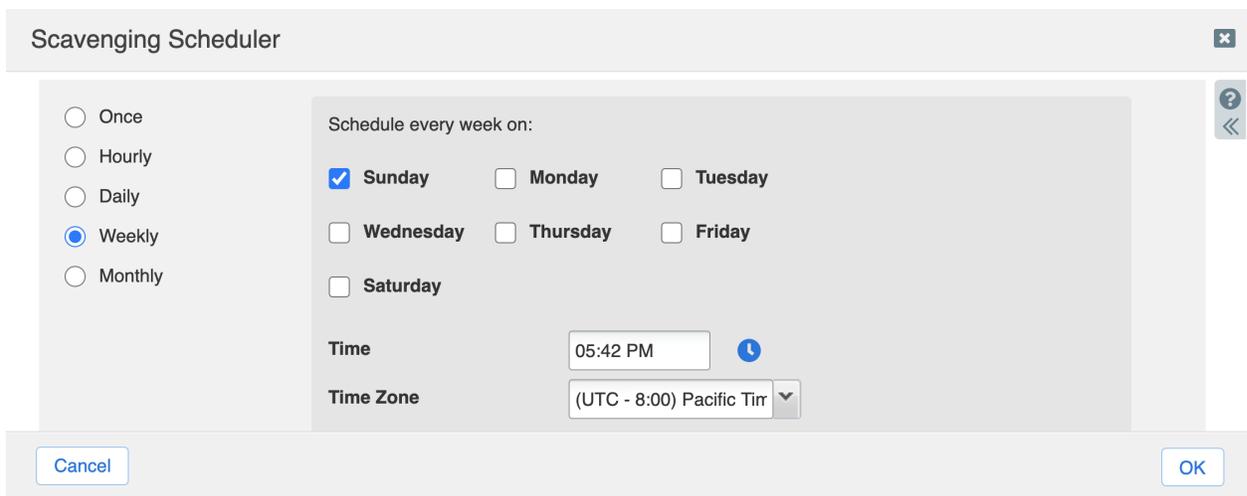
A screenshot of the DNS Scavenging configuration interface. It features a checkbox labeled "Enable scheduled record scavenging" which is checked. Below this is a yellow warning box containing the text: "Static records can be marked as reclaimable but they cannot be reclaimed by DNS Scavenging. To delete static records marked 'reclaimable', use Delete." At the bottom, there is another checked checkbox labeled "After marking a record as reclaimable, automatically reclaim the record."

Scavenging Schedule: December 31, 2020 at 05:42 PM PST 

Note: Only Dynamic records are automatically deleted.

3. To specify the schedule, click the calendar icon next to the Schedule option.
4. In the Scavenging Scheduler screen, specify the frequency on the left (Once, Hourly, Daily, Weekly, and Monthly) and associated settings on the right.

In this example, NIOS will run the scavenging process Weekly on Sunday at 10 past midnight Pacific Time.



A screenshot of the "Scavenging Scheduler" dialog box. On the left, there are radio buttons for frequency: "Once", "Hourly", "Daily", "Weekly" (selected), and "Monthly". The main area is titled "Schedule every week on:" and contains checkboxes for "Sunday" (checked), "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", and "Saturday". Below this, there are input fields for "Time" (05:42 PM) and "Time Zone" ((UTC - 8:00) Pacific Time). The dialog has "Cancel" and "OK" buttons at the bottom.

Another example specifies that the scavenging process will run Monthly every 2 months on the 29th day of that month at 10 past midnight Pacific Time.

Scavenging Scheduler
✕

Once

Hourly

Daily

Weekly

Monthly

Schedule the day of the month

Day every month(s)

Time ⌵

Time Zone ⌵

?
<<

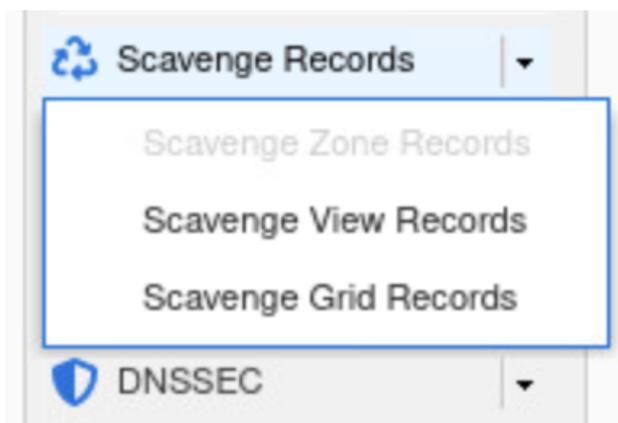
Cancel
OK

In summary, NIOS provides broad scheduling options for an automated DNS scavenging process.

Manually Scavenging Stale Records

The DNS scavenging process can also be run manually on an as-needed basis. Manual scavenging can be performed on Grid, View, and Zone. “Grid scavenging” is performed on all views and all zones within those views. View Scavenging is for all zones in a particular view and Zone scavenging is for a particular zone.

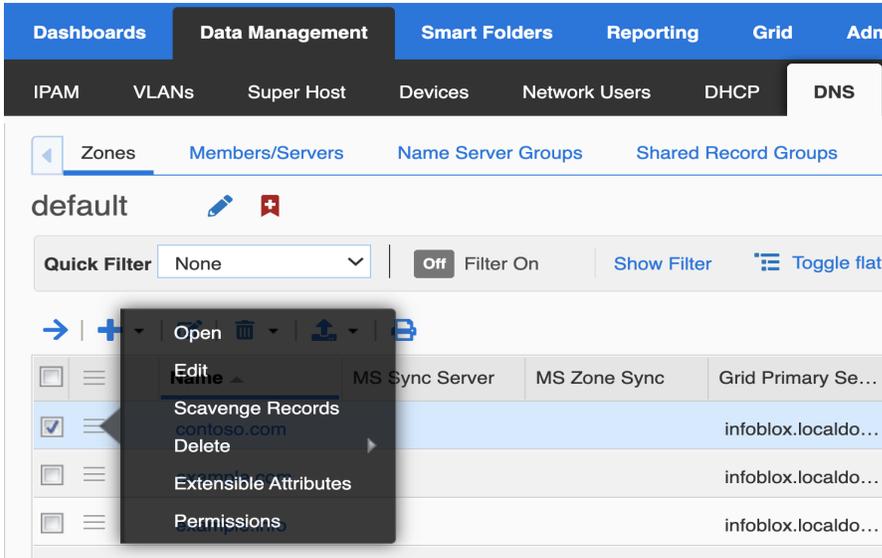
1. Go to **Data Management** → **DNS** → **Zones**.
2. Under the toolbar on the right-hand side, click on the **Scavenge Records** drop-down menu.



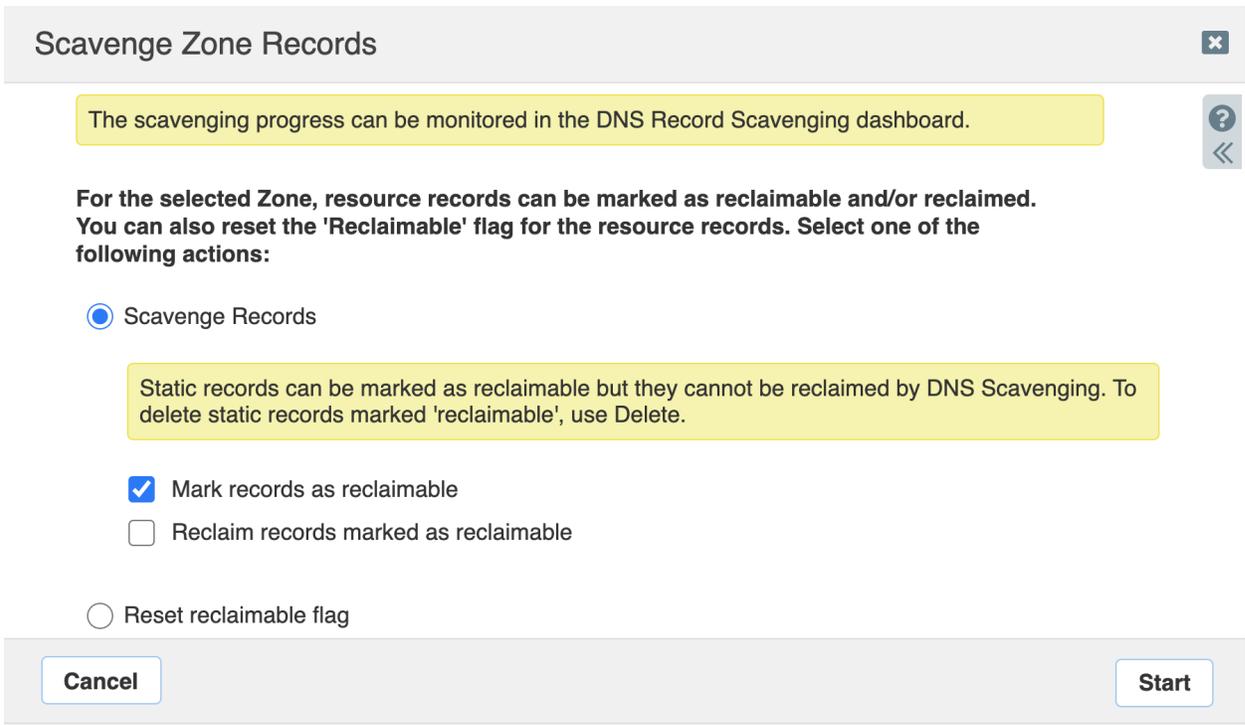
Note: If no zone is selected or the user is not in a zone, the Scavenge Zone Records option is grayed out.

In this example, scavenging will be run manually on a DNS zone named contoso.com.

1. Click on the hamburger icon next to the zone contoso.com in the **Data Management** → **DNS** → **Zones** tab and click **Scavenge Records**.



The Scavenge Zone Records screen provides options.



2. To scavenge stale records, select Scavenge Records, and then choose any of the following:
 - To flag only stale records, select option Mark records as reclaimable
 - To delete dynamic records that were previously flagged, select Reclaim records marked as reclaimable.
 - To flag and delete all records, select both options.
3. In this example, the first option is selected. Click Start to detect and flag stale records.
4. To view stale records flagged by NIOS, go to the particular zone the scavenging process was run on. In this example it is contoso.com zone. Inside the zone two records flagged as Reclaimable, and the Reclaimable column shows a value of Yes for these records.

contoso.com Authoritative Zone

Records Subzones

Quick Filter: None | Filter On | Show Filter | Toggle flat view

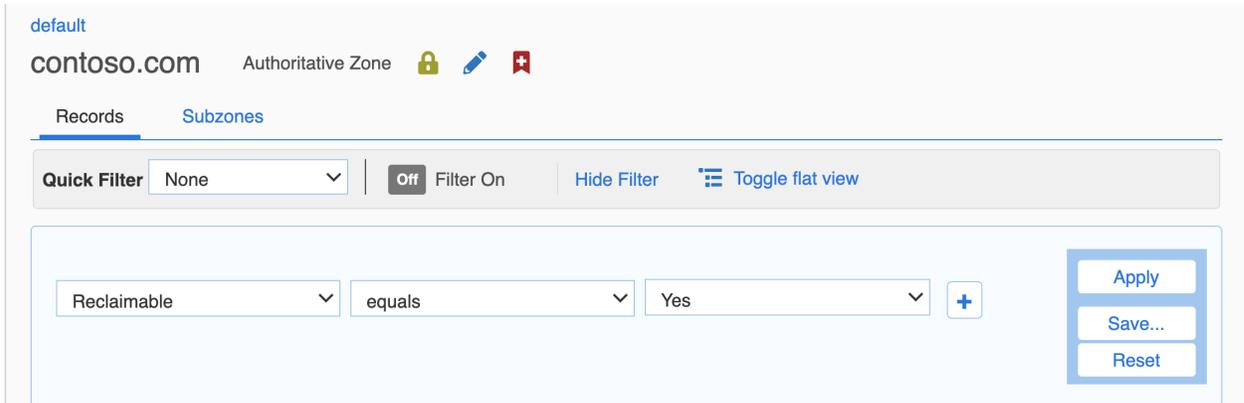
Go to: [] Go

Name	Type	Data	Reclaimable	Created Timestamp	Record Source
www	A Record	10.60.24.5	Yes	2015-12-17 14:39:37 PST	Static
tme-pm-pc	A Record	10.60.24.102	Yes	2015-12-29 12:39:28 PST	Dynamic

Manually Deleting Reclaimable Records

To delete reclaimable records, first find marked records. Using a NIOS quick filter is a way to easily accomplish this. In this example, find all reclaimable records in the contoso.com zone and delete them all in one action.

1. Click **Show Filter** to bring up filter options.
 - From the choose filter drop-down menu, select **Reclaimable**.
 - From the choose operator drop-down menu, select **equals**, and select **Yes** as shown in the figure below.



2. Click **Apply** to see all reclaimable records.

Note: Static records can be scavenged only by deleting them manually.

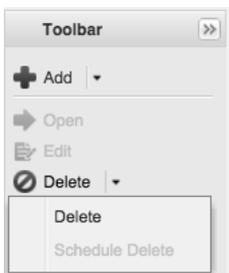
Go to Go

<input type="checkbox"/>	Name	Type	Data	Protected	Reclaimable
<input type="checkbox"/>	win-dhcp	A Record	10.60.24.12	No	Yes
<input type="checkbox"/>	tme-pm-pc	A Record	10.60.24.102	No	Yes
<input type="checkbox"/>	pc-4-tmes	A Record	10.60.24.104	No	Yes
<input type="checkbox"/>	lab-pc	A Record	10.60.24.103	No	Yes

3. Select all records by checking the topmost checkbox.

<input checked="" type="checkbox"/>	Name	Type	Data	Protected	Reclaimable
<input checked="" type="checkbox"/>	win-dhcp	A Record	10.60.24.12	No	Yes
<input checked="" type="checkbox"/>	tme-pm-pc	A Record	10.60.24.102	No	Yes
<input checked="" type="checkbox"/>	pc-4-tmes	A Record	10.60.24.104	No	Yes
<input checked="" type="checkbox"/>	lab-pc	A Record	10.60.24.103	No	Yes

4. Click **Delete** in the Toolbar to delete all selected records at once.



Reset Reclaimable Flag

Infoblox NIOS provides the ability to clear the reclaimable flag on stale records. This is extremely useful if an administrator wants to perform a new scavenging analysis starting with a clean slate. The reclaimable flag can be cleared at a Grid, view, or zone level.

1. To clear reclaimable flags on records in a zone, click on the gear icon next to a zone. In this example it is contoso.com under **Data Management** → **DNS** → **Zones** and click **Scavenge Records**

Scavenge Zone Records

The scavenging progress can be monitored in the DNS Record Scavenging dashboard.

For the selected Zone, resource records can be marked as reclaimable and/or reclaimed. You can also reset the 'Reclaimable' flag for the resource records. Select one of the following actions:

Scavenge Records

Static records can be marked as reclaimable but they cannot be reclaimed by DNS Scavenging. To delete static records marked 'reclaimable', use Delete.

Mark records as reclaimable
 Reclaim records marked as reclaimable

Reset reclaimable flag

Cancel **Start**

2. Select the **Reset reclaimable flag** option and click **Start**.

Disabling Scavenging on Individual Resource Records

Infoblox NIOS provides protection for individual resource records to exclude them from being scavenged. The option is to disable scavenging for these records. Disabling scavenging for a record only prevents the record from being deleted, but the record can still be marked as reclaimable for the purpose of analysis.

In this example, scavenging is disabled for the A record web.contoso.com by editing its properties in the DNS Scavenging tab,

web.contoso.com (A Record)

Basic

- Disable scavenging for this record

Record was created	2020-12-30 18:02:21 PST
Record was last queried	
Record is in reclaimable state	No

Cancel Save & Close

Using Multiple Matching Rules in a Scavenging Policy

This section describes some use cases to delete stale DNS records, which helps users create a scavenging policy using multiple matching rules. Scavenging specifics are determined by users based on their specific networking environment.

Static Records Not Queried in a Year

An administrator needs to clean up a DNS database by removing all those static records that have not been queried for more than a year. You can set matching rules for this in NIOS, as shown below.

Enable record scavenging

Match of the following rules: Reset

<input type="text" value="Record Source"/>	<input type="text" value="equals"/>	<input type="text" value="Static"/>	<input type="button" value="-"/>	<input type="button" value="+"/>	<input type="button" value="▶"/>	<input type="button" value="◀"/>
<input type="text" value="Last Queried Time"/>	<input type="text" value="is greater than"/>	<input type="text" value="52"/>	<input type="text" value="week(s)"/>	<input type="button" value="-"/>	<input type="button" value="+"/>	<input type="button" value="▶"/>

Dynamic Records Created More Than a Month Ago

An administrator needs to clean up a DNS database by removing all those dynamic records that were created more than 30 days ago. You can set matching rules for this in NIOS, as shown below.

Enable record scavenging

The screenshot shows a configuration window for DNS scavenging. At the top, it says "Match all of the following rules:" with a "Reset" button. Below this, there are two rows of rules. The first row has "Record Source" set to "Dynamic" with the operator "equals". The second row has "Creation Time" set to "30" "day(s)" with the operator "is greater than". There are navigation icons (minus, plus, right arrow, left arrow) between the two rows.

Simulate Microsoft DNS Scavenging Behavior

This use case provides the same scavenging behavior as is available on Microsoft DNS servers. You can set up matching rules to accomplish Microsoft DNS scavenging behavior, as shown below.

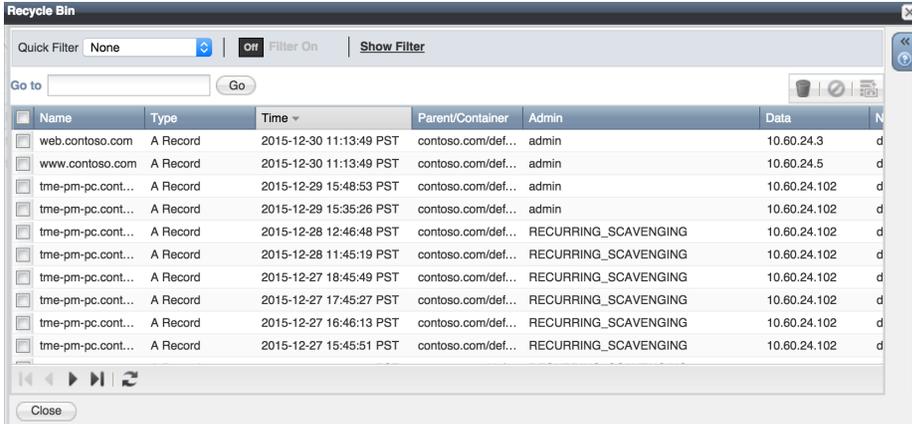
Enable record scavenging

The screenshot shows a configuration window for DNS scavenging. At the top, it says "Match all of the following rules:" with a "Reset" button. Below this, there are two rows of rules. The first row has "Record Source" set to "Dynamic" with the operator "equals". The second row has "Creation Time" set to "7" "day(s)" with the operator "is greater than". There are navigation icons (minus, plus, right arrow, left arrow) between the two rows.

Recycle Bin

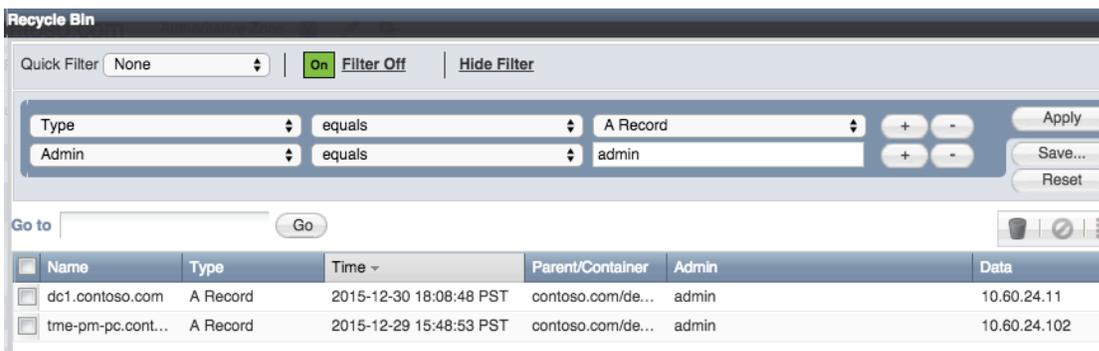
Deleted stale DNS resource records end up in the Recycle bin. Users can view all deleted records in the Recycle Bin with their type, zone, and data and see whether the deletion was through a recurring scavenging process or deleted manually by a user. Users can either completely empty the stale entries or recover deleted records if required.

1. Click Show All under Recycle Bin to display the Recycle Bin window.



A new powerful feature introduced in NIOS 7.3 is the use of quick filters in the Recycle Bin. Different criteria can be used to search for deleted entries in Recycle Bin and records recovered if needed. For example, if a user wants to recover A records deleted by a user named admin, a user can build a quick filter as follows.

1. Click **Show Filter** and
 - From the Choose Filter drop-down menu, select **Type**.
 - From the Choose Operator drop-down menu, select **equals**.
 - In the value field, select **A record**.
2. Click the plus (+) sign to add a second filter and
 - In the Choose Filter drop-down menu, select **Admin**.
 - In the Choose Operator drop-down menu, select **equals**.
 - In value field, type **admin**.
3. Click **Apply**.



Dashboard Widget

A new dashboard widget in NIOS 7.3 named DNS Record Scavenging shows the status and results of the scavenging process. It displays information about current and previous scavenging tasks, which includes the time the task ran and finished, number of records scavenged, and level of hierarchy the task ran at, i.e. Grid, view or zone. The refresh interval can be set as desired in seconds.

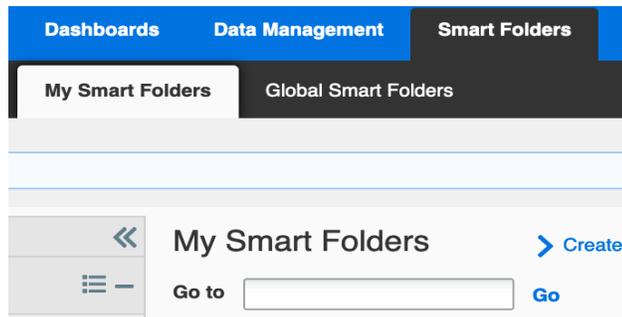
DNS Record Scavenging	
Current Scavenging Activity	Last Scavenging Activity
Status:	Completed
Start:	2021-03-12 17:46:27 PST
End:	2021-03-12 17:46:28 PST
User:	admin
Selected Object:	Zone: example.com
Action:	Mark as reclaimable
Processed Records:	2
Reclaimable Records:	0
Reclaimed Records:	0

Refresh Off Last updated: 2021-03-12 17:46:43 PST

Smart Folders

With DNS Scavenging, a new smart folder is introduced called Reclaimable. It is the one place where an IT administrator can take a peek at all reclaimable addresses in all applicable zones hosted by the Grid.

1. Go to **Smart Folders** → **My Smart Folders** → **Create**.



2. Give the Smart Folder a name, for example Reclaimable Records.
3. Click **Save**
4. Select **Yes** and click **Apply**.

Name **Reclaimable Records** Save

Comment

Reclaimable equals Yes + Apply

Group Results Group By +

Go to Go ↩ 📄 🔍 🔒 🔄 🖨

<input type="checkbox"/>	Name ▲	Comment	Type	Site
<input type="checkbox"/>	lab-pc.contoso1.com		A Record	
<input type="checkbox"/>	test1.example.net		A Record	
<input type="checkbox"/>	www.example.net		A Record	



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