Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Enabling and Configuring Infoblox Secure Dynamic Update

Contents

Introduction

DDNS (Dynamic DNS) is a method by which DNS data (A, TXT, AAAA, and PTR records etc.) is updated by sources such as DHCP servers and other systems that support DDNS updates. This Deployment Guide details a quick setup on a newly introduced feature, Secure Dynamic Update in NIOS 7.3, which uses GSS-TSIG (Generic Security Service Algorithm for Secret Key Transaction) to authenticate DDNS updates from clients.

In addition, Infoblox Secure Dynamic Update provides more granular access controls for restricting which DDNS clients can be updated. This document addresses the security around DNS updates coming from DDNS clients directly to NIOS DNS servers.

Prerequisites

The following are prerequisites for Secure Dynamic Update:

- Functional 7.3 Infoblox Grid™ with a Grid Master
- Active Grid and DNS license
- At least one NIOS appliance acting as a Primary DNS server
- Functional Microsoft Active Directory Domain Controller

Overview

Prior to the 7.3 release, NIOS did not have granular access control to restrict which GSS-TSIG authenticated DNS clients could make direct DNS updates. The initial GSS-TSIG implementation was intended to support zone transfers between Microsoft and Infoblox servers and assumed that the peer DNS server was secure. As a result, clients configured to do GSS-TSIG direct updates were allowed to update any record in a zone for which it was authenticated. Moreover, previous releases relied on the DHCP server to perform Secure Dynamic Updates on behalf of unauthenticated clients via DHCID TXT records. Any client configured with a valid ACL doing direct unauthenticated updates could update the entire zone.

Infoblox Secure Dynamic Update improves security around DDNS by providing the following capabilities:

- Protecting specific records so that DDNS clients cannot update them
- Specifying a list of fully-qualified domain name (FQDN) patterns that will prevent DDNS updates to any matching FQDN patterns
- For authenticated updates, tracking the GSS-TSIG principal of the client that created the record
- Preventing DDNS updates to records created by a different GSS-TSIG principal

Best Practices

Follow these best practices when deploying Secure Dynamic Update:

- Turn on Principal name tracking immediately after deploying this feature in order to start collecting principals of DDNS clients.
- To protect static records, use static record protection.
- To protect dynamic records created via unauthenticated updates, use protected record flag
- To protect dynamic records created via GSS-TSIG authenticated updates, use principal protection

Enabling DDNS Update

By default, DDNS updates are blocked by NIOS DNS servers. NIOS provides the following options to allow specific DDNS clients to update DNS records:

- Unauthenticated dynamic DNS updates
- GSS-TSIG authenticated dynamic DNS updates
- Combination of both unauthenticated and GSS-TSIG authenticated dynamic DNS updates

Unauthenticated Dynamic DNS Updates

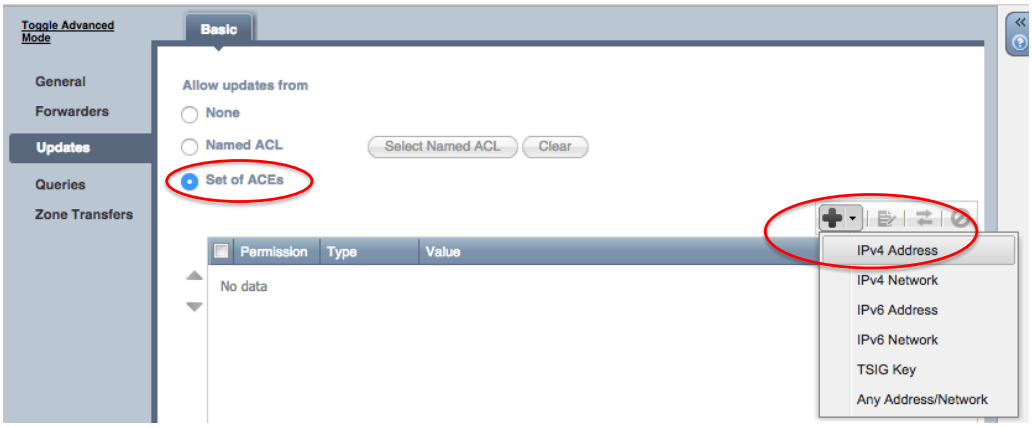
This option does not involve any GSS-TSIG authentication. By default the Allow updates from option is set to None, which means that no one can dynamically update DNS records until access is specifically configured.

Other options available to grant access are:

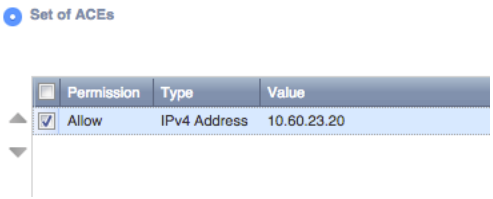
- Access list
- Client IPv4/v6 addresses
- Client IPv4/v6 networks
- TSIG keys
- Any address/network

In this example, a specific client with the IP address 10.60.23.20 is allowed to update DNS records by going to Data Management > DNS > Grid DNS Properties > Updates > Basic.

1. Under Allow updates from, select Set of ACEs > + > IPv4 Address.



2. Add 10.60.23.20 in the Value column.



3. Click Save & Close and Restart.

With access provided to the specific client above, not only can it update its own DNS resource record but, any record (static or dynamic) on the Grid. This was the NIOS behavior in releases prior to 7.3.

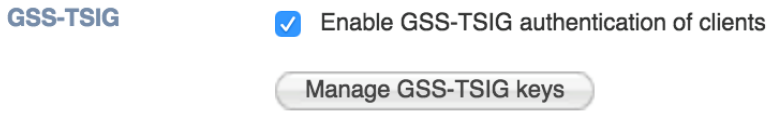
With Secure Dynamic Update, users can specify layers of security to restrict DDNS clients from updating specific DNS records on the Grid.

GSS-TSIG Authenticated DNS Updates

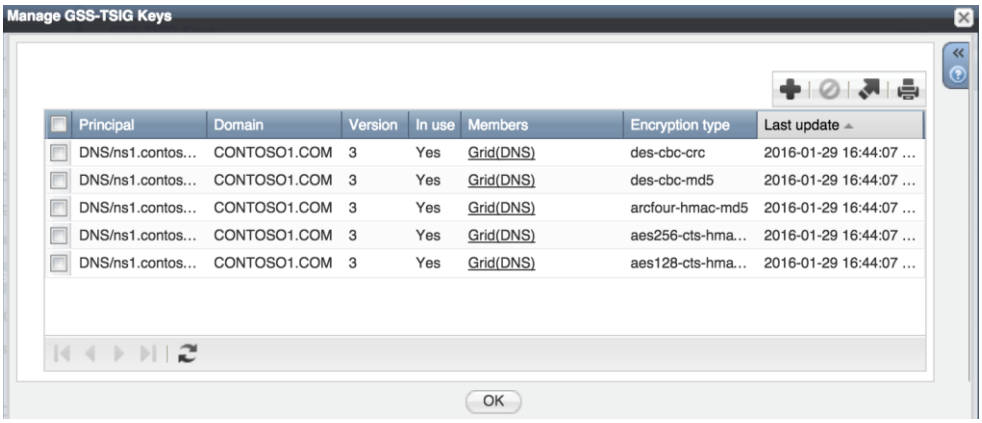
This option allows DDNS update access to clients using GSS-TSIG keys for authentication. Before enabling GSS-TSIG authenticated updates on the Grid, a keytab file needs to be generated from a Microsoft AD domain controller. The procedure is to generate keytab file is provided in NIOS Administration Guide. Once the keytab file is generated, it should be stored in a place where the Infoblox Grid can easily access it,

To enable GSS-TSIG signed updates:

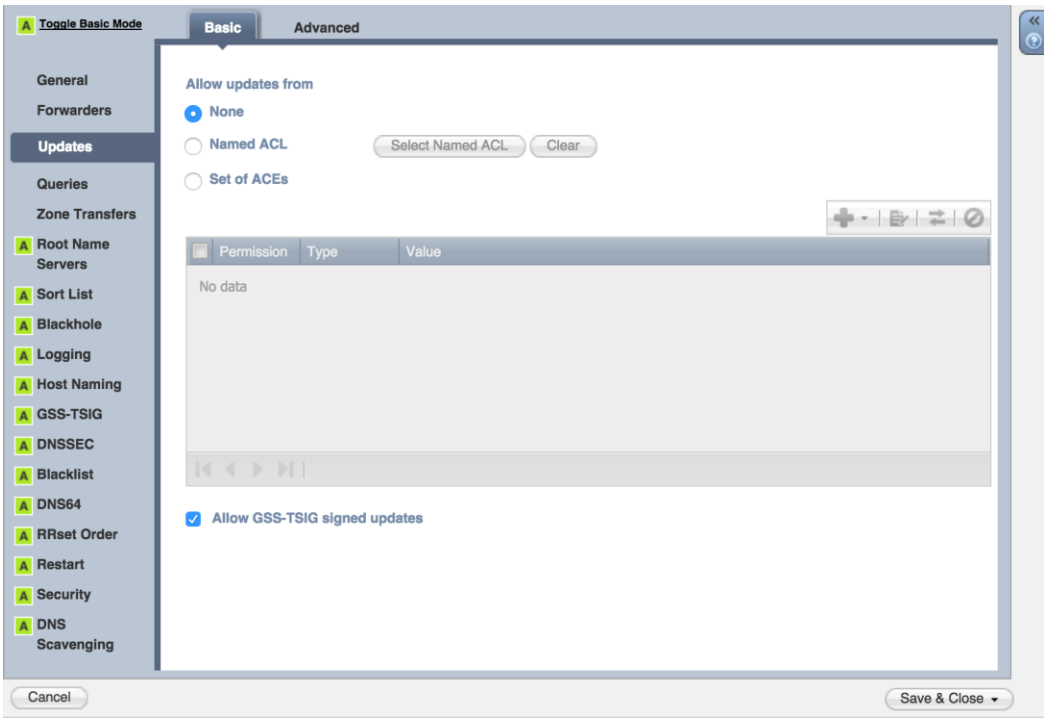
1. Go to Grid DNS Properties and under Toggle Advance Mode, click the GSS-TSIG tab.
2. Select Enable GSS-TSIG Authentication of clients.



3. Click Manage GSS-TSIG keys to invoke a file upload wizard. To upload the keytab file to the Grid, click the plus icon (+), and click Save & Close



4. Click Updates in Grid DNS properties.



5. Select Allow GSS-TSIG signed updates.
6. Click Save & Close and Restart.

NOTE: Allow GSS-TSIG signed updates can be overridden at the zone level.

Tracking GSS-TSIG Principals

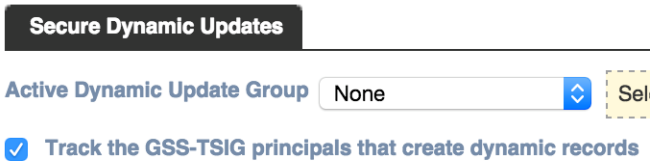
If the DDNS updates are performed by an authenticated GSS-TSIG principal, then the principal name can be tracked. Note that tracking alone does not make the DNS record secure as anyone with access to update zones can add or delete DNS record with a particular principal. It is useful when the need is to know who made the last DDNS update by looking at the principal in the Principal column in a particular zone.

Tracking also allows the security enforcement, as updates cannot be prevented without knowing the principal. The option of tracking the principal can be set at the Grid level and overridden at view and zone levels. In this example, the principal is being tracked at a Grid level.

1. Go to Data Management > DNS > Grid DNS Properties.

   NOTE: Make sure that toggle Advanced mode is on.

2. Go to the Updates tab > Advanced.
3. Select Track the GSS-TSIG principals who create dynamic records.



4. Click Save & Close and Restart.

   Once the option is enabled, the principals for GSS-TSIG based updates will be listed in the Principal column in a zone as shown below, after the next GSS-TSIG authenticated DDNS updates.

DDNS Update Restrictions

NIOS provides several mechanisms to restrict which DDNS clients can update which records. All of these mechanisms apply only to DDNS clients *after the DDNS clients have passed the effective ACL for the zone*. By default system records cannot be modified by DDNS updates; only dynamic (created using DDNS update) or static records can be modified. Once DDNS update restrictions are in place then certain records are protected and cannot be modified through DDNS updates.

The following restrictions are available to protect DNS records from being modified using DDNS updates.

Static Record Restriction

This mechanism protects static records and they are treated as restricted. Any DDNS update that attempts to modify an RRset containing a static record is denied. The denial is then logged to the syslog with cause. This option is configurable at the Grid, view or zone level.

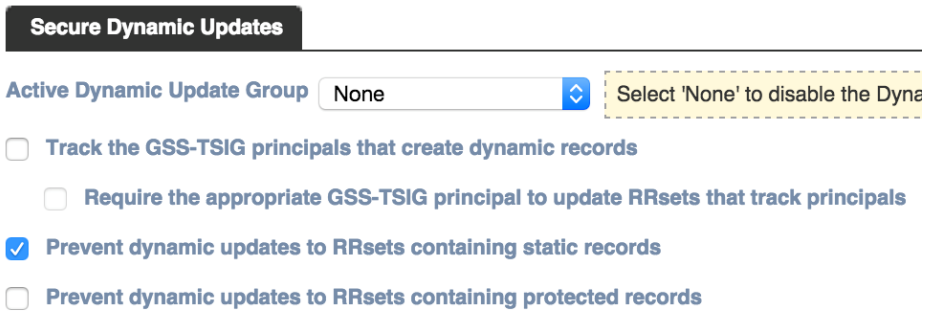
In this example, it is set at Grid level so that it applies to all views within the Grid and all zones within those views.

1. Go to Data Management > DNS > Grid DNS Properties.

   NOTE: Make sure that toggle Advanced mode is on.

2. Go to Updates > Advanced.

3. Select Prevent dynamic updates to RRsets containing static records.



4. Click Save & Close and Restart.

The following ERROR log message is logged in syslog when the DDSN update to a static DNS record is refused with static records protection turned on:

ERROR	named[18563]	Add error: .com.contoso1.static[_default] (data="<none>", source="<none>", DDNS principal="centos/centos.contoso1.com@CONTOSO1.COM"): static record

Protected Record Restriction

This option protects records and any DDNS update that attempts to modify an RRset containing a protected record is denied. The option is available at Grid, view and zone levels. The protected flag can be set for both static and dynamic records.

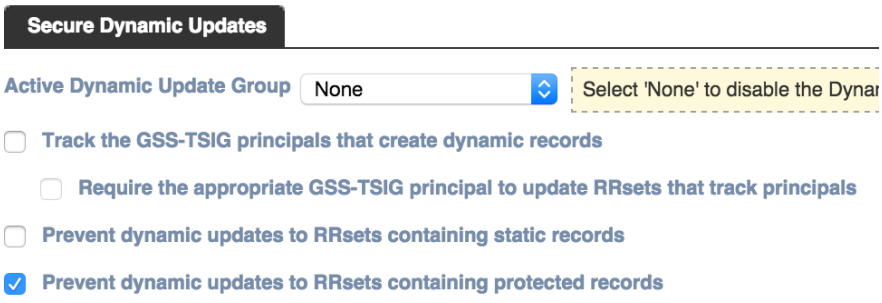
In this example it will be set at the Grid level so that it applies to all views within the Grid and all zones within those views.

1. Go to Data Management > DNS > Grid DNS Properties.

   NOTE: Make sure that toggle Advanced mode is on.

2. Go to Updates > Advanced.

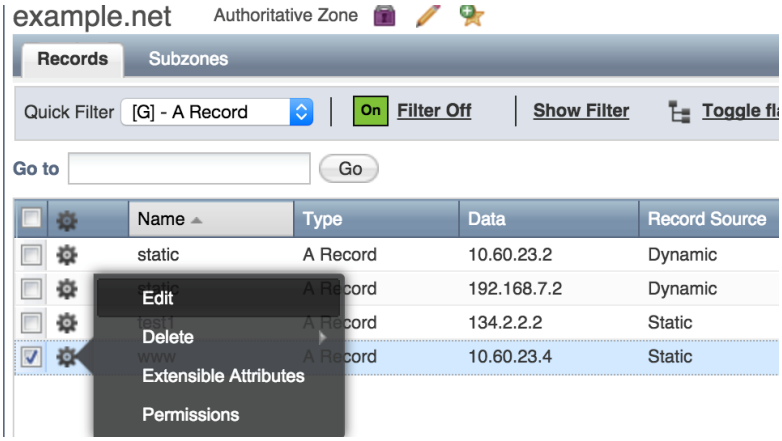
   Select Prevent dynamic updates to RRsets containing protected records.



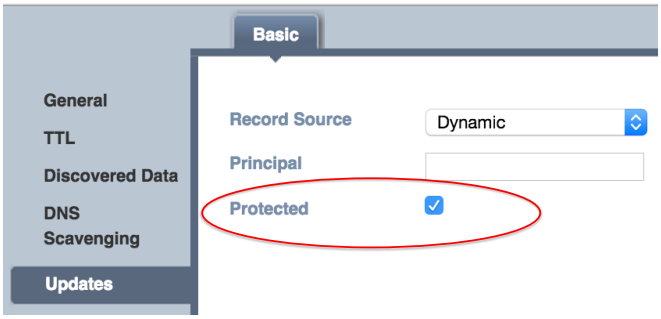
3. Click Save & Close > Restart.

   In the next step, the protected flag needs to be enabled on records that are to be protected from dynamic updates. Edit the properties of the specific dynamic record. In this example, the protected flag is enabled for a specific record www.example.net.

4. Inside the zone containing the record to be protected, in this example zone example.net, click on the gear icon next to the record www.example.net and click Edit.



5. Click the Updates tab and select Protected.



The following ERROR log message is logged in syslog when a DDNS update is refused because the record is protected:

Level	Server	Message
ERROR	named[9700]	Add error: .net.example.www[_default] (data="10.60.23.4", source="bind_a"): protected record

FQDN Pattern-based Restriction

With this protection enabled, any DDNS update to an FQDN that matches any of the configured patterns is denied. The denial is then logged to the syslog with cause. The patterns are exactly the same as those used by Infoblox DNS Traffic Control, including wildcard matching.

A pattern matches an FQDN if the entire FQDN matches. A pattern may include mixed case. The patterns are compared against DNS names in a case-sensitive manner. The table below shows how pattern matching is done.

Pattern	FQDN	Match?	Comment
a.b.c	a.b.c.	yes	exact
a.b.c	a.b.c.d.	no	incomplete
a.b.c	a.a.b.c.	no	incomplete
*.com	foo.com.	yes	wildcard match
*.com	www.*.com.	no	wildcards don't span labels
www?bar.com	www.bar.com.	no	wildcards don't match labels
www.*.com	www.foo.com.	yes	wildcard match
www.*.com	www.foo.bar.com.	no	wildcards don't span labels
www.FOO.com	www.foo.com.	yes	match ignores case
???.foo.com	ftp.foo.com.	yes	wildcard match
???.foo.com	mail.foo.com.	no	incomplete
???.*.com	www.foo.com.	yes	multiple wildcards
?*?*?.foo.com	www.foo.com.	yes	star may be empty
*****.foo.com	www.foo.com.	yes	multi-star same as star
a\032b.foo.com	a b.foo.com.	yes	exact match
a\032b.foo.com	a\032b.foo.com.	yes	exact match
a\032b.foo.com	a\\032b.foo.com.	no	incomplete
a*c.foo.com	abcabc.foo.com.	yes	wildcards are greedy

The option is available at the Grid level, with an override possible at the view and zone levels.

In this example, it is set at the Grid level so that it is applicable to all views within the Grid and all zones within those views.

1. Go to Data Management > DNS > Grid DNS Properties.

   NOTE: The toggle Advanced mode is on.

2. Go to Updates > Advanced.
3. Select Prevent dynamic updates to FQDNs matching these patterns and click + every time a new FQDN pattern needs to be entered. In this example four Domain name patterns are added.

The following INFO log message is logged once a DDNS update is rejected due to FQDN pattern matching.

INFO	named[21678]	client 10.60.23.20#55620/key centos.centos.contoso1.com.CONTOSO1.COM: updating zone 'foo.org/IN': updating 'www.foo.org' rejected by pattern '*.*.org' (REFUSED)

GSS-TSIG Principal Restriction

With the “Require the appropriate GSS-TSIG principal” option on, NIOS will not allow anyone without the matching principal to update the DDNS record. This means that the DDNS client who created the Dynamic record is the only one that can modify it since it’s the only one with the correct principal.

The option is available at the Grid level, and can be overridden at the view and zone levels.

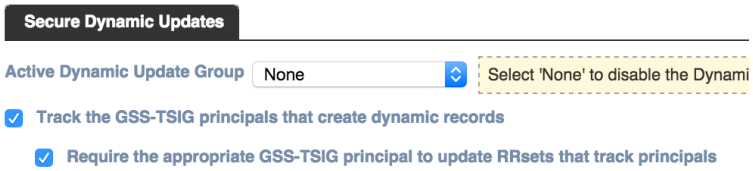
In this example, the option is set at the Grid level.

Go to Data Management > DNS > Grid DNS Properties

NOTE: Make sure that toggle Advanced mode is on.

1. Go to Updates > Advanced.

   Select Require the appropriate GSS-TSIG principal to update RRsets that track principals. The option is available under the previously selected option to track principals Track the GSS-TSIG principals who create dynamic records.



2. Click Save & Close and Restart.

The following ERROR log message is logged in syslog when someone tries to update a dynamic record without the correct principal:

ERROR	named[1942]	Delete error: .com.contoso1.lab-pc[_default] (data="10.60.23.150", source="bind_a", DDNS principal="centos/centos.contoso1.com@CONTOSO1.COM", RR principal="LAB-PC$@CONTOSO1.COM"): secure record

The error shows that a client with principal centos/centos.contoso1.com@CONTOSO1.COM is trying to update a dynamic DNS record with tracked principal of LAB-PC@CONTOSO1.COM. Unless the two principals are both allowed to update each other’s DNS records with the use of a dynamic update group, NIOS considers them a mismatch and denies the DDNS update. Dynamic update groups are discussed in the next section.

Dynamic Update Groups, Clusters, and Principals

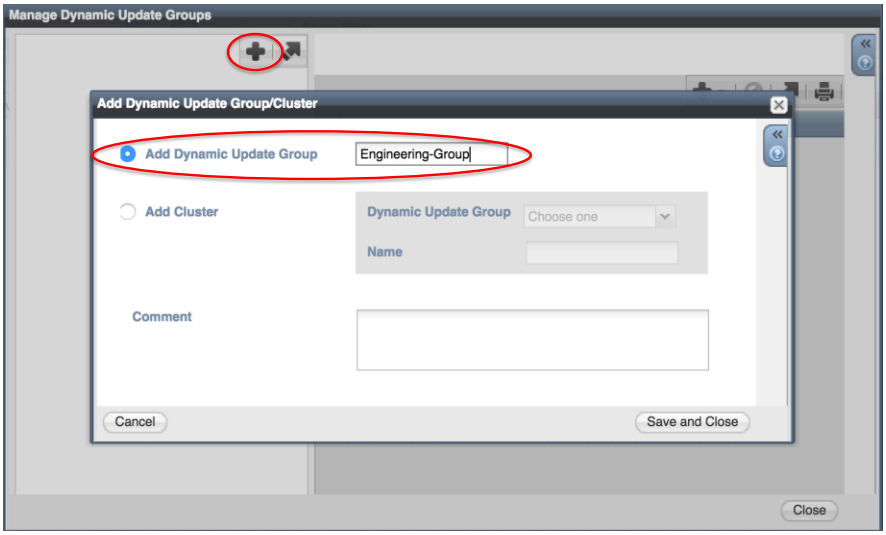
In some use cases, DDNS clients need to update each other’s DNS dynamic records. When these clients have different principals, the only way they can update each other’s records is via a dynamic update group.

In NIOS, users create dynamic update groups, which can contain one or more clusters. Each of these clusters can contain multiple principal names. The principal names in a cluster must be unique. The principals can appear in multiple clusters. The primary use case is a DHCP failover associations.

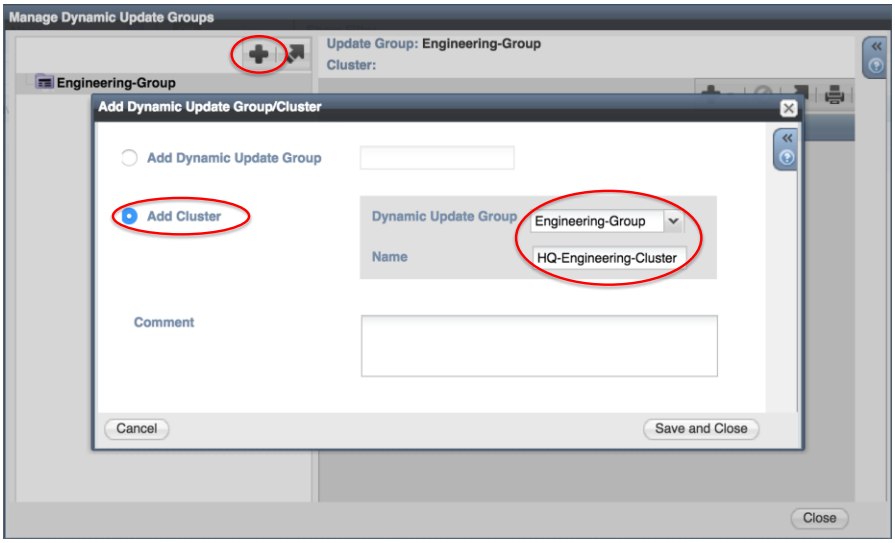
Once a cluster group is configured with clusters containing principals, an option is configured to select the active cluster group. This option is at the Grid level with overrides available at view and zone levels. If one is selected, then restricting updates to secure records will consider any principals in the same cluster in the group to be equivalent.

In this example, a cluster group called Engineering-Group is configured, with two clusters named HQ-engineering-cluster and BO-engineering-cluster. The principals will then be added to individual clusters for equivalency.

1. Go to Data Management > DNS > Manage Dynamic Update Groups > **+.**
2. In the field Add Dynamic Update Group, type a name for the group. In this example, Engineering-Group.

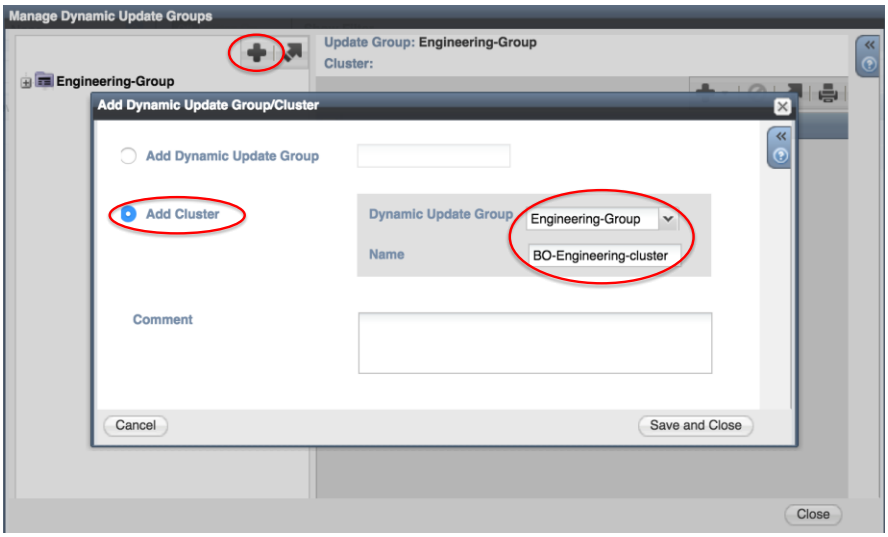


3. Click Save & Close.
4. Once the new group is added, click same + icon one more time and select the Add Cluster option.
5. Click the drop-down menu Dynamic Update Group and choose the previously created group Engineering-Group.
6. Type HQ-Engineering-Cluster in the Name field as the name of the cluster.



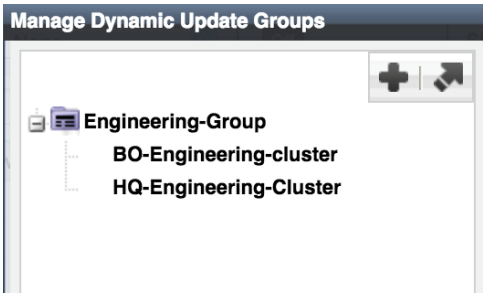
7. Click Save & Close.

8. Repeat the step above to add another cluster named BO-engineering-cluster under the same group called Engineering-Group.



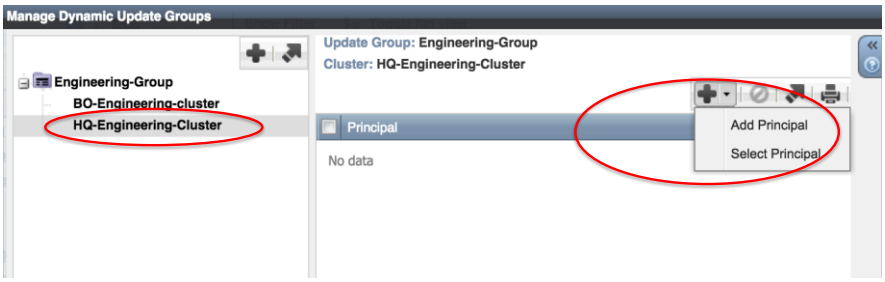
9. Click Save & Close.

   Once two clusters are added to the dynamic group, the clusters will appear under the group as follows,

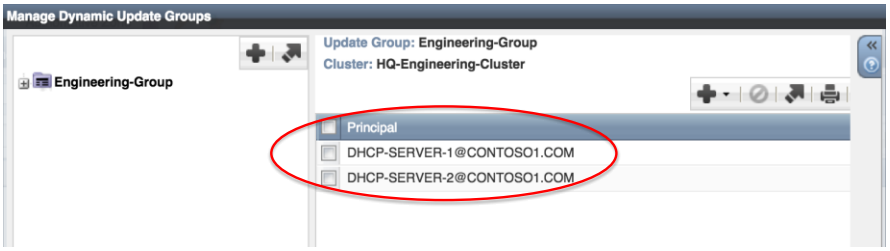


Next, principals that are to update each other's records must be added to the same cluster.

1. Click on one of the clusters. In this example, the cluster named HQ-Engineering-Cluster.
2. To add the principals, click Add Principal or Select Principal options on the + drop -down menu,



   The Add Principal option lets a user add a principal manually. Two principals are added manually to make them equal.

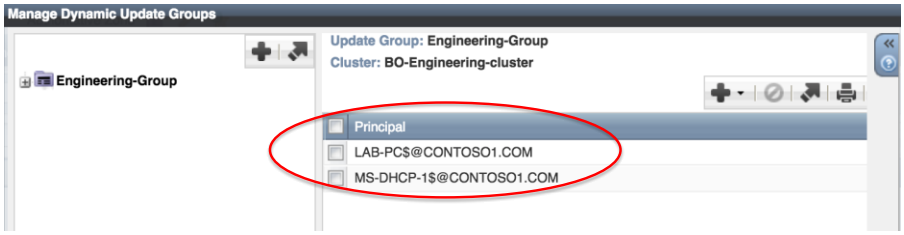


The clients with principals DHCP-SERVER-1@CONTOSO1.COM and DHCP-SERVER-2@CONTOSO1.COM can now update each other's created records in addition to records they created.

Next the Select Principal option is used to add principals that are already being tracked by NIOS to cluster named BO-Engineering-Cluster.

When the Select Principal option is selected on the + drop-down menu, tracked principals are displayed in a list format.

In this example, two principals are selected from the lists named LAB-PC@CONTOSO1.COM and MS-DHCP-1@CONTOSO1.COM, so that both can update each other's created dynamic records in addition to records they created.



NOTE: Principals can only update each other's records when they are part of the same cluster. Principals from two clusters cannot do so even if they are part of the same dynamic group.

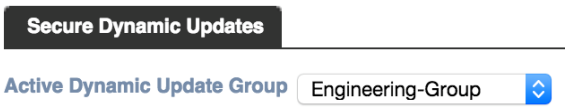
Once groups are created with clusters and principals added to the clusters, the next step is to make the dynamic group active so that it can be part of NIOS running configuration. Dynamic groups can be made active for the Grid, with an override possible at view and zone levels.

In this example, the dynamic group Engineering-Group will be made part of the running configuration at the Grid level in Data Management > DNS > Grid DNS Properties.

1. Go to Updates > Advanced.

   NOTE: Make sure that toggle Advanced mode is on.

2. Select Engineering-Group from the Active Dynamic Update Group drop-down menu.



3. Click Save & Close and Restart.

Smart Folders

With Secure Dynamic Update come a few smart folders to help administrators view consolidated data for protected records and principals being tracked. These smart folders can be created using available filters named Protected, Principals, and Record Source.

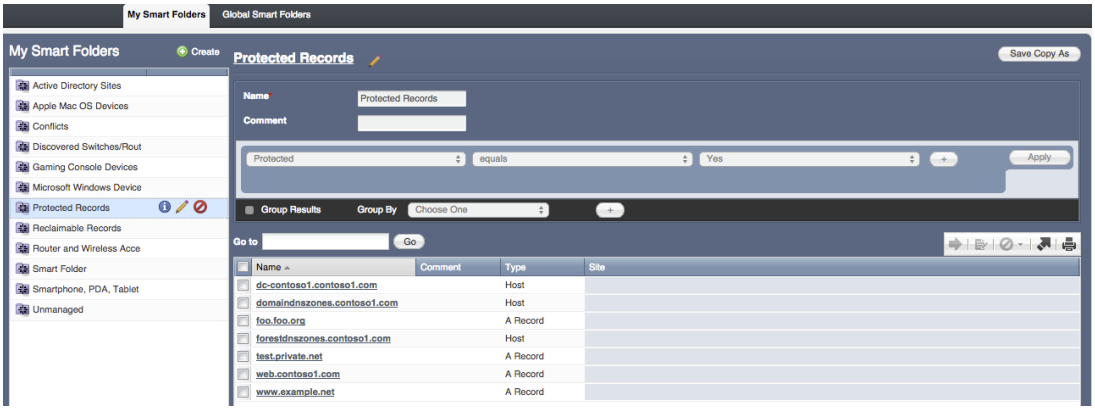
Protected

A Protected filter is available to create a smart folder that pulls all protected records in the Grid from all zones and views based on the search criteria for the protected flag.

1. Go to Smart Folder > My Smart Folders (or Global Smart Folder).

   NOTE: My Smart Folders are available only to a specific user who created them. Global Smart Folders are available to all users in the Grid.

2. Click Create.
3. Give a name to the smart folder, for example Protected Records in the Name field. (The Comment field is optional.)
4. From the drop-down menu Choose Filter, select Protected.
5. The Choose Operator drop-down menu is automatically set to equals. Select Yes.
6. Click Apply and Save.



Principal

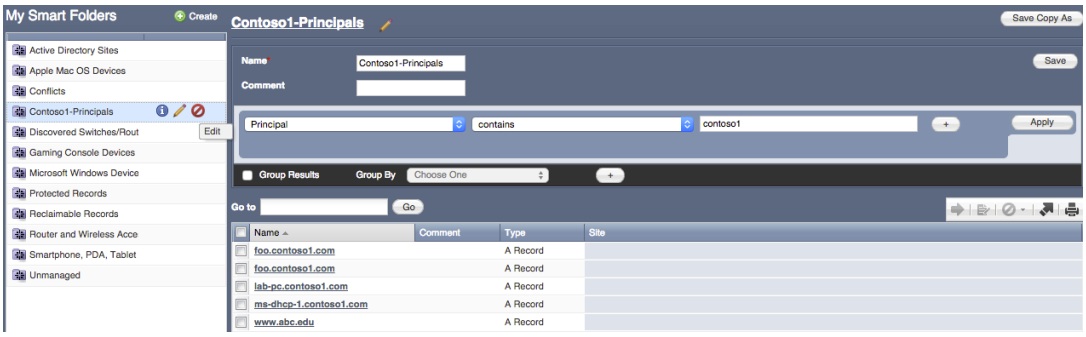
The Principal filter is available to create a smart folder that pulls records based on principal names in the Grid.

1. Go to Smart Folder > My Smart Folders (or Global Smart Folder).

   NOTE: My Smart Folders are available only to the specific user who creates them. Global Smart Folders are available to all users in the Grid.

2. Click Create.
3. Give a name to the smart folder. For example to see principals for a specific Microsoft Active Directory, use Kerberos realm as part of the smart folder name. In this case the name is Contoso1-Principals, where Contoso1 is the realm and an active directory on the Microsoft domain controller. The Comment field is optional.
4. Select Principal from Choose Filter drop-down menu.
5. Use the operator that best matches your search on the Choose Operator drop-down menu. In this example select contains, and then type the word for the search to be based on. In this example we used the Kerberos realm name contoso1.

6. Click Apply and Save.



Record Source

The Record Source filter is available to search and view records based on their type i.e. Dynamic, Static, or System.

1. Go to Smart Folder > My Smart Folders (or Global Smart Folder).

   NOTE: My Smart Folders are available only to the specific user who creates them. Global Smart Folders are available to all users in the Grid.

2. Click Create.
3. Give a name to the smart folder. For dynamic records, use something that tells you what type of records are in these smart folder. In this example, a smart folder for dynamic records is created with the name Dynamic Records. The Comment field is optional.
4. Select Record Source from the Choose Filter drop-down menu.
5. The Choose Operator drop-down menu is automatically set to equals. In the value field drop-down menu, select Dynamic.
6. Click Apply and Save.