Infoblox
CONTROL YOUR NETWORK

DEPLOYMENT GUIDE

Configuring and Enabling GSS-TSIG on NIOS

Contents

Introduction

GSS-TSIG (Generic Security Service Algorithm –Transaction Signature) is used to authenticate DDNS (Dynamic Domain Name System) updates. It is an extension of TSIG authentication that uses the Kerberos v5 authentication system. There are a set of client/server negotiations to establish a “security context” and makes use of a Kerberos server (Microsoft AD domain controller) that functions as the KDC (Kerberos Key Distribution Center). The KDC provides session tickets and temporary session keys to users and computers within an Active Directory Domain. An Infoblox NIOS (Network Identity Operating System) appliance is configured to accept GSS-TSIG signed DDNS updates from multiple clients in a realm or multiple clients that belong to different AD domains in which each domain has a unique GSS-TSIG key. Infoblox appliances acting as DHCP Servers can also update DNS records when zones are managed on AD Domain Controllers via DDNS updates secured through using GSS-TSIG.

Prerequisites

The following are prerequisites for GSS-TSIG support for secure dynamic DNS updates:

- Functional 7.3 Infoblox Grid with a Grid Master (although GSS-TSIG support is available in prior releases the NIOS 7.3 release adds service principal name tracking).
- At least one Grid member with an active DNS license installed and the DNS service enabled.
- At least one NIOS appliance acting as an authoritative DNS Server (Primary).
- Microsoft Domain Controller to generate a keytab file.
- The time must be in sync between Microsoft Domain Controller and NIOS DNS appliance with NTP enabled.
- A Microsoft DNS server with an authoritative zone for the domain and domain controllers which have been registered in the domain using this DNS server
- A Windows client which is a member of the domain and is using the Infoblox server for DNS services

Limitations

Following general limitations apply:

- A NIOS appliance serving DHCP can send GSS-TSIG authenticated DDNS updates to an external DNS Server (such as an AD Domain Controller or another Infoblox Grid) or a NIOS appliance serving DNS can accept GSS-TSIG authenticated updates from DHCP clients and servers. These two features are not supported at the same time.

Best Practice

The following best practices will make deployment easier:

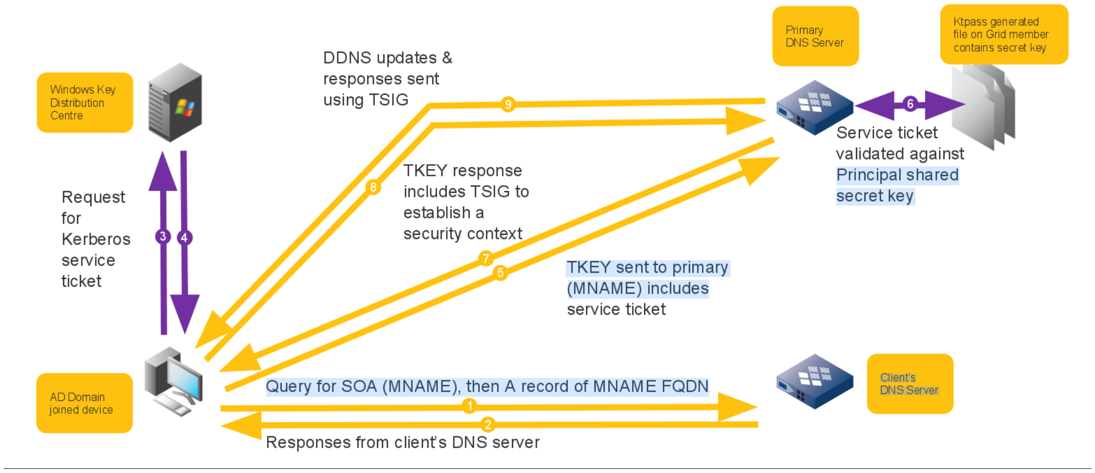
- Set the Active Directory user account for the NIOS DNS server to have a never expiring password and disable the ability of user to change the password. Otherwise the keytab file must be updated every time the password expires and DDNS updates will fail until this is done. Instead, use your company’s process for changing passwords in service type accounts.
- The keytab file contains highly sensitive data for the NIOS appliance account. Ensure that you store and transport its contents securely.

DDNS Update Process

- The DDNS client sends a DNS request to locate a domain controller and logs in to the domain controller.
- The DDNS client automatically sends a DNS query for the Kerberos Server.
- The NIOS appliance replies with the name of the Kerberos server.
- The DDNS client automatically logs in to the Kerberos server.
- The Kerberos server sends the client a TGT (ticket-granting ticket).
- Using the TGT, the AD member requests a service ticket for the DNS server.
- The Kerberos server replies with a service ticket for that server.

- The client sends an unauthenticated DDNS update, which is refused by the DNS server.
- The DDNS client sends the DNS server a TKEY (transaction key) request:
  - A transaction key record establishes shared secret keys for use with TSIG resource record.
  - The request includes the service ticket. The service ticket includes the appliance’s principal and proposed TSIG key, along with other items such as ticket lifetime and a timestamp.
  - The DNS server responds with a DNS server-signed TSIG.
  - The DDNS client and NIOS appliance now have established a security context.
- The DDNS client sends an authenticated DDNS update.
- The DNS server authenticates the DDNS update and processes it.
- The DNS server sends a GSS-TSIG-authenticated response to the AD member, confirming the update.

DDNS Update Process Using GSS-TSIG


Windows Key Distribution Centre
DDNS updates & responses sent using TSIG
Primary DNS Server
Ktpass generated file on Grid member contains secret key
9
6
Service ticket validated against Principal shared secret key
8
TKEY response includes TSIG to establish a security context
Request for Kerberos service ticket
3
4
7
5
TKEY sent to primary (MNAME) includes service ticket
AD Domain joined device
Query for SOA (MNAME), then A record of MNAME FQDN
1
2
Client's DNS Server
Responses from client's DNS server

Enabling NIOS DNS Server to Receive GSS-TSIG Updates

A NIOS appliance is configured to support Active Directory and accept secure DDNS updates from clients using GSS-TSIG. It requires certain steps as given below:

1. Add a user account in Active Directory for the NIOS DNS Server.
2. Generate a keytab file on the AD Domain Controller using the newly created user account.
3. Import the keytab file to the Infoblox Grid.
4. Create a forward-mapping zone in NIOS and import the zone data from the AD domain controller.
5. Enable GSS-TSIG updates.

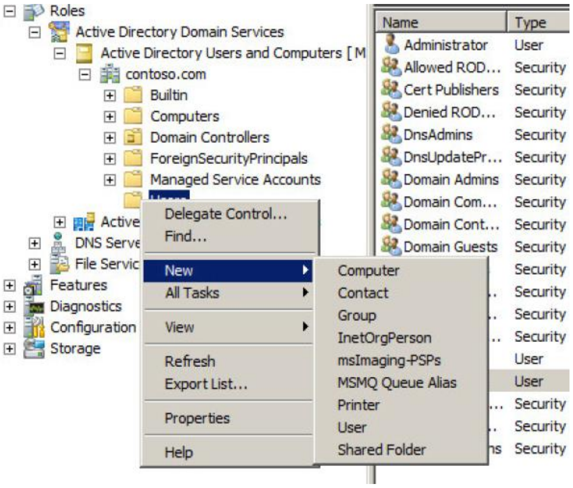
Creating an AD user account

In our example, we create a user account named ns in Active Directory that matches with the host name of the NIOS appliance in the **contoso.com** domain. This account will be used to generate the keytab file which will be exported to NIOS.

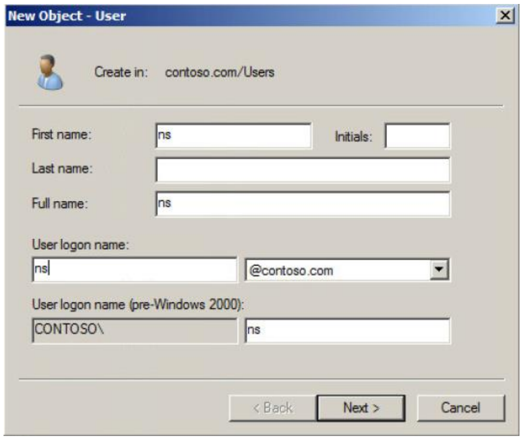
Login to a Microsoft Domain Controller using an account with account creation privileges in Active Directory.

1. Open the Active Directory Users and Computers Snap-in in the Server Manager

   Right-click the Users OU, click **New** and click **User.**



2. Type the user information. In our example the login name is **ns** and is part of **contoso.com** domain. Click **Next.**



New Object - User

Create in: contoso.com/Users

First name: ns Initials:

Last name:

Full name: ns

User logon name:

ns @contoso.com

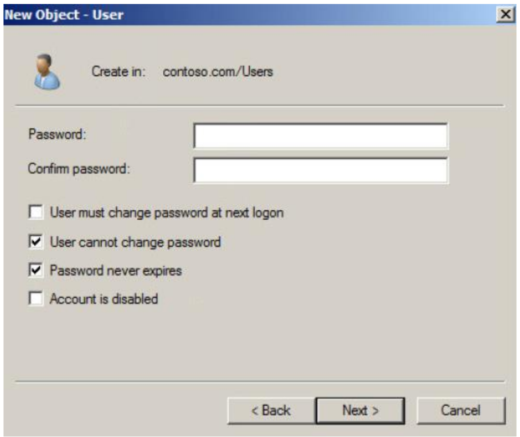
User logon name (pre-Windows 2000):

CONTOSO\ ns

< Back Next > Cancel

Note: The name you enter in the User logon name field is the name that is later used to export the keytab file. This is also the principal name. It's better to use the hostname of the appliance for which the keytab file is to be generated. In our example, the NIOS DNS appliance name is ns.contoso.com

3. Enter the password and enable the options “User cannot change password” and “Password never expires”. Click **Next.**



New Object - User

Create in: contoso.com/Users

Password:

Confirm password:

☐ User must change password at next logon

☑ User cannot change password

☑ Password never expires

☐ Account is disabled

< Back Next > Cancel

4. Click **Finish.**

Generating the Keytab File

In our example, we are using Microsoft 2008 R2 Server as a Domain Controller and this server is going to be used as the Kerberos Key Distribution Center. The PowerShell commands used to generate the keytab files may vary between different versions of Microsoft servers. For other versions, please refer to the NIOS Admin Guide.

The keytab file can be generated using the Ktpass tool. The version of the Ktpass tool must match the Windows version of the domain controller. Windows 2012/R2 domain controllers allow generating a keytab file with multiple keys for one principal. The Infoblox DNS server accepts GSS-TSIG updates from clients that provide a Kerberos ticket for any of the keys in its configured keytab. To generate the keytab file using the Ktpass tool, execute the following command in a command prompt:

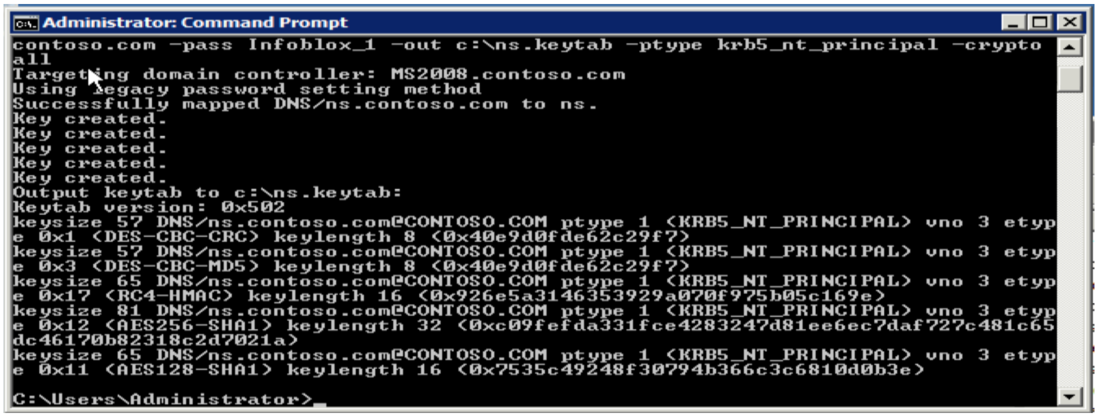
ktpass -princ DNS/FQDN_instance@REALM -mapuser AD_username -pass password -out filename.keytab -ptype krb5_nt_principal -crypto encryption all

Using our example where the NIOS DNS server is named **ns.contoso.com** and its corresponding AD user is **ns@contoso.com**, the command is as follows:

ktpass –princ DNS/ns.contoso.com@CONTOSO.COM -mapuser ns@contoso.com -pass Infoblox_1 –out c:\ns.keytab –ptype krb5_nt_principal –crypto all

where:

- princ = Kerberos principal.
- DNS = Service name in uppercase format.
- ns.contoso.com = Instance in FQDN format; this is the same as the DNS name of the NIOS appliance.
- CONTOSO.COM = The Kerberos realm in uppercase; this must be the same as the AD domain name.
- mapuser = Maps the Kerberos principal name to the AD user account .
- ns@contoso.com = The AD user name for the NIOS appliance.
- pass = The AD user account password — Infoblox_1 = The password of the user account for the NIOS appliance.
- out = Exports the keytab file — c:\ns1.keytab = The name and location of the keytab file.
- ptype = Sets the principal type. This must be krb5_nt_principal.
- crypto = Specifies the encryption type. All = specifies that all encryption types can be used



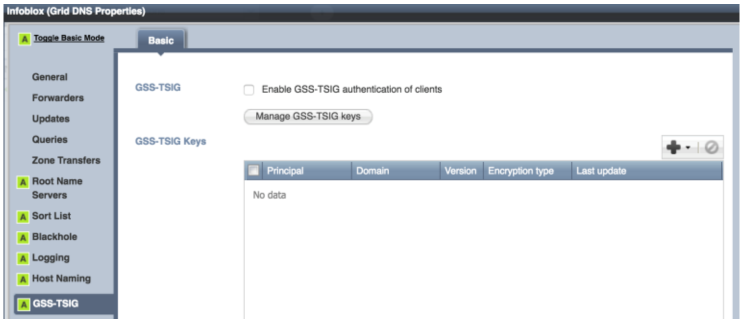
```
contoso.com -pass Infoblox_1 -out c:\ns.keytab -ptype krb5_nt_principal -crypto
all
Targeting domain controller: MS2008.contoso.com
Using legacy password setting method
Successfully mapped DNS/ns.contoso.com to ns.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:\ns.keytab:
Keytab version: 0x502
keysize 57 DNS/ns.contoso.com@CONTOSO.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etyp
e 0x1 (DES-CBC-CRC) keylength 8 (0x40e9d0fde62c29f7)
keysize 57 DNS/ns.contoso.com@CONTOSO.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etyp
e 0x3 (DES-CBC-MD5) keylength 8 (0x40e9d0fde62c29f7)
keysize 65 DNS/ns.contoso.com@CONTOSO.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etyp
e 0x17 (RC4-HMAC) keylength 16 (0x926e5a3146353929a070f975b05c169e)
keysize 81 DNS/ns.contoso.com@CONTOSO.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etyp
e 0x12 (AES256-SHA1) keylength 32 (0xc09fefda331fce4283247d81ee6ec7daf727c481c65
dc46170b82318c2d7021a)
keysize 65 DNS/ns.contoso.com@CONTOSO.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etyp
e 0x11 (AES128-SHA1) keylength 16 (0x7535c49248f30794b366c3c6810d0b3e)

C:\Users\Administrator>_
```

Importing the Keytab file and Enable GSS-TSIG on NIOS Appliance

In the previous section, we have shown how to generate a keytab file from an AD Domain Controller. The keytab file now needs to be imported into the NIOS DNS appliance to support GSS-TSIG authenticated DDNS updates. This keytab file needs to be in a location accessible from the NIOS GUI so that it can be uploaded to the NIOS appliance. In our example, we are applying this to the entire Grid. To import the keytab file, do the following:

1. Go to **Data Management** > **DNS** > **Grid DNS Properties**
2. Click **Toggle Advanced mode**

3. Click **GSS-TSIG** tab

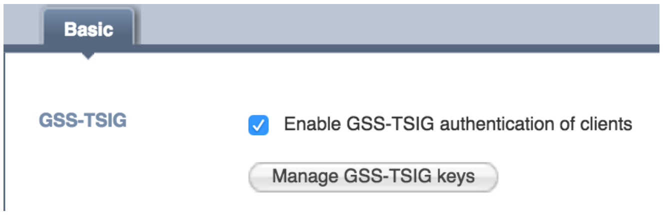


GSS-TSIG ☐ Enable GSS-TSIG authentication of clients

GSS-TSIG Keys

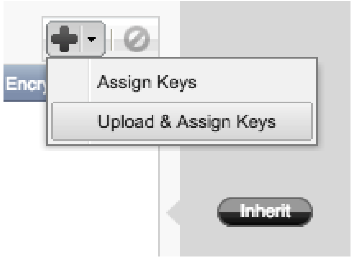
☐	Principal	Domain	Version	Encryption type	Last update
No data					

4. Select option **Enable GSS-TSIG authentication of clients**

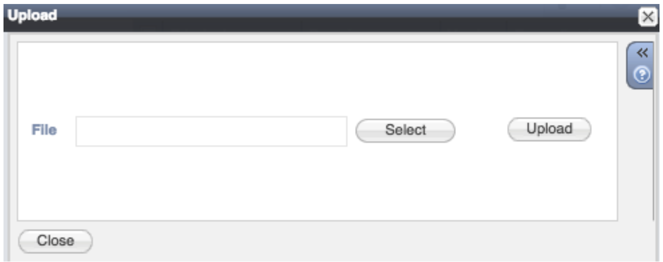


GSS-TSIG ☑ Enable GSS-TSIG authentication of clients

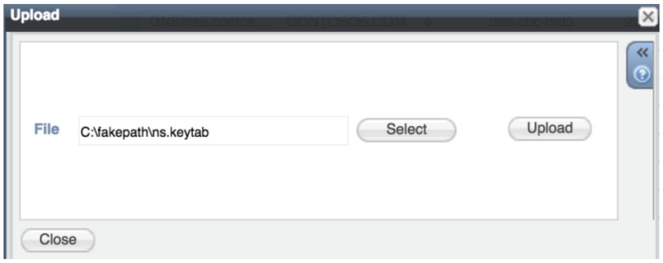
5. Click **+** drop down menu



6. Click **Upload and Assign Keys**

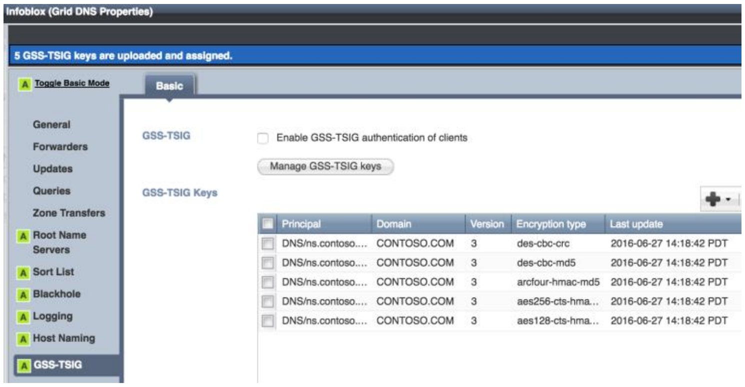


7. Click **Select** to select the keytab file **ns.keytab**



File C:\fakepath\ns.keytab

8. Click **Upload**



5 GSS-TSIG keys are uploaded and assigned.

GSS-TSIG □ Enable GSS-TSIG authentication of clients

GSS-TSIG Keys

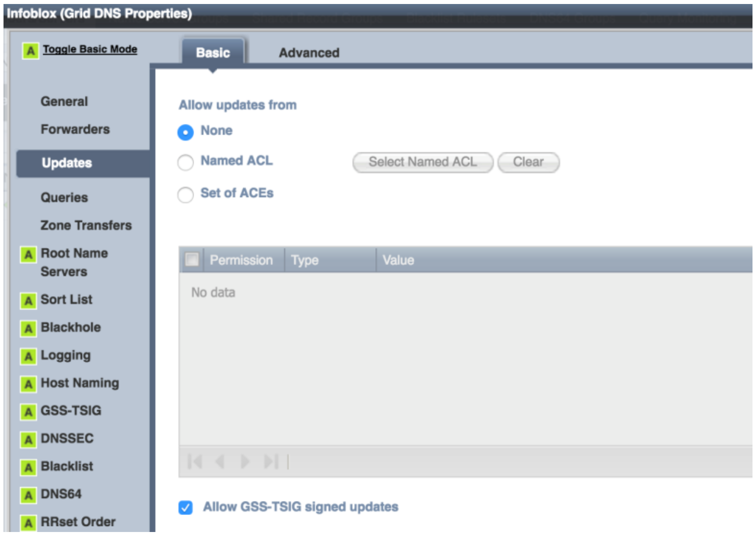
Principal	Domain	Version	Encryption type	Last update
DNS/ns.contoso....	CONTOSO.COM	3	des-cbc-crc	2016-06-27 14:18:42 PDT
DNS/ns.contoso....	CONTOSO.COM	3	des-cbc-md5	2016-06-27 14:18:42 PDT
DNS/ns.contoso....	CONTOSO.COM	3	arcfour-hmac-md5	2016-06-27 14:18:42 PDT
DNS/ns.contoso....	CONTOSO.COM	3	aes256-cts-hma...	2016-06-27 14:18:42 PDT
DNS/ns.contoso....	CONTOSO.COM	3	aes128-cts-hma...	2016-06-27 14:18:42 PDT

9. Click **Save & Close**
10. Click **Restart**

Accepting GSS-TSIG Updates

A Grid, specific members, or zones can be configured to accept GSS-TSIG signed updates from the DDNS clients. In our example, we are setting it at the Grid level by doing the following:

1. Go to the **Data Management** > **DNS** > **Grid DNS Properties** > **Updates** tab
2. Enable the option **Allow GSS-TSIG signed updates**



Allow updates from

● None

○ Named ACL

○ Set of ACEs

Permission	Type	Value
No data		

☑ Allow GSS-TSIG signed updates

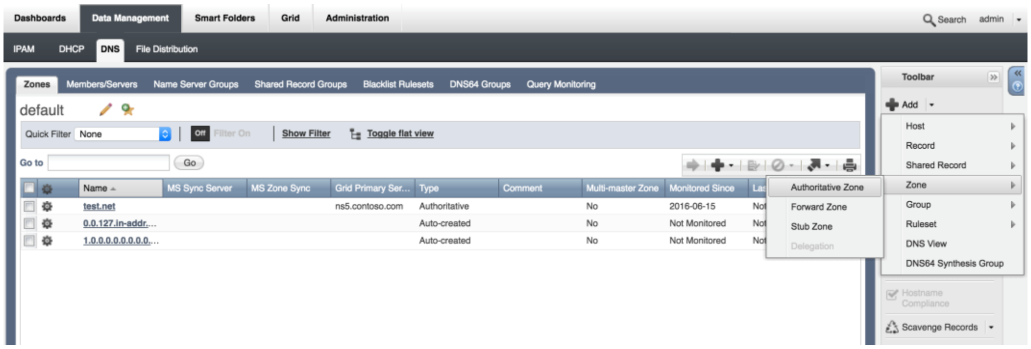
3. Click **Save & Close**
4. Click **Restart**

Create Zone and Import Zone Data from Domain Controller

Create a forward-mapping zone and import the zone data from the AD domain controller. The zone name must match between the AD Domain controller and the NIOS DNS appliance. Make sure that zone transfers from the AD domain controller to the NIOS appliance are allowed.

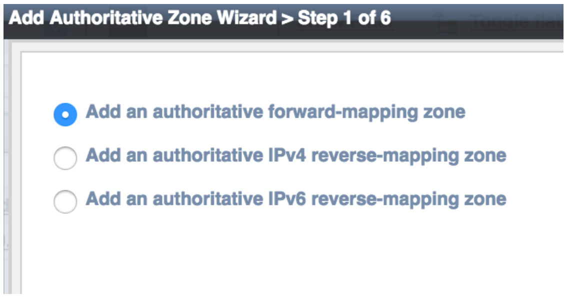
In our example, we are going to create a forward mapping zone named **contoso.com**:

1. Go to **Data Management** > **DNS** > **Zones** > **Add** > **Zone** > **Authoritative Zone**



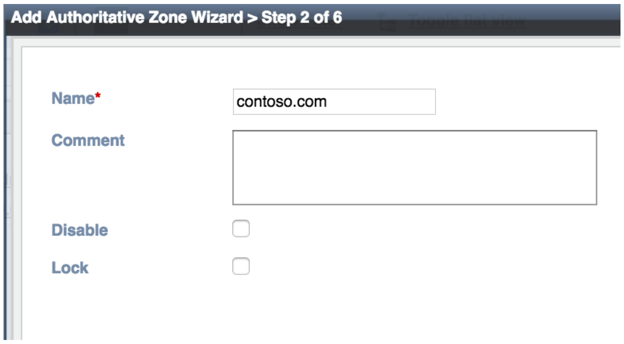
Name	MS Sync Server	MS Zone Sync	Grid Primary Ser...	Type	Comment	Multi-master Zone	Monitored Since	Las
test.net			ns5.contoso.com	Authoritative		No	2016-06-15	Not
0.0.127.in-addr....				Auto-created		No	Not Monitored	Not
1.0.0.0.0.0.0.0....				Auto-created		No	Not Monitored	Not

2. Select option **Add an authoritative forward-mapping zone**



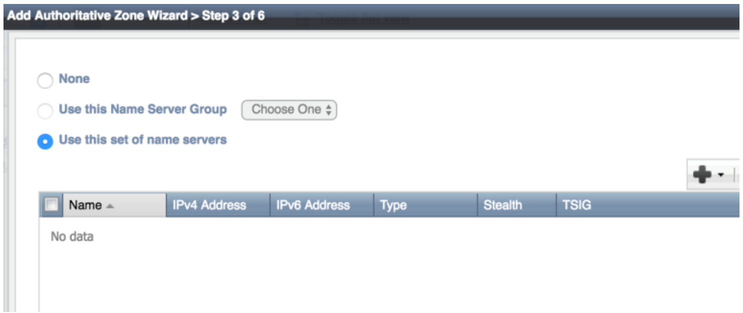
● Add an authoritative forward-mapping zone
○ Add an authoritative IPv4 reverse-mapping zone
○ Add an authoritative IPv6 reverse-mapping zone

3. Click **Next**
4. Type **contoso.com** in the **Name** field



Name*	contoso.com
Comment	
Disable	□
Lock	□

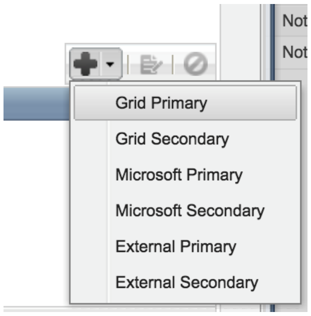
5. Click **Next**
6. Select option **Use this set of name servers** (In our example we are not using a Name Server Group, though it can be used.)



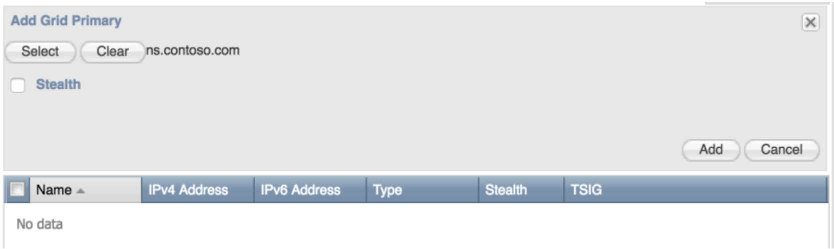
○ None
○ Use this Name Server Group
● Use this set of name servers

Name	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
No data					

7. Click **+** drop down and select **Grid Primary**



8. Click **Select** button from **Add Grid Primary** section (it will automatically select the DNS server in a standalone/single server Grid). In our example, it is **ns.contoso.com**.



Add Grid Primary

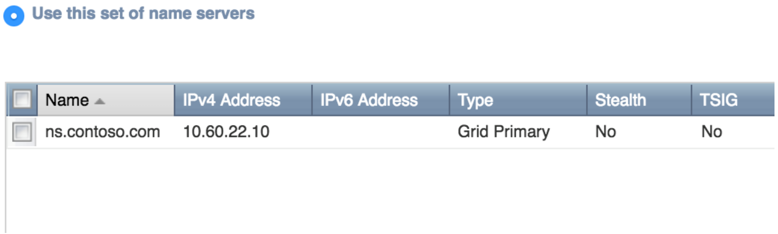
Select Clear ns.contoso.com

□ Stealth

Add Cancel

□	Name ▲	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
No data						

9. Click **Add**



● Use this set of name servers

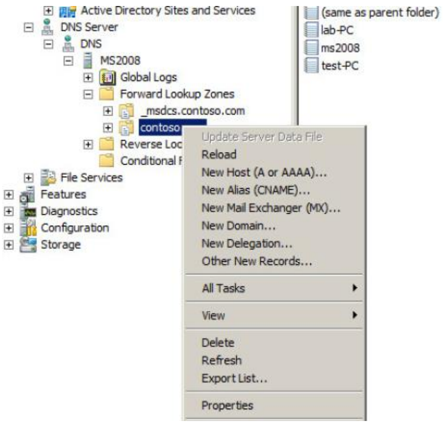
□	Name ▲	IPv4 Address	IPv6 Address	Type	Stealth	TSIG
□	ns.contoso.com	10.60.22.10		Grid Primary	No	No

10. Click **Save & Close**
11. Click **Restart**

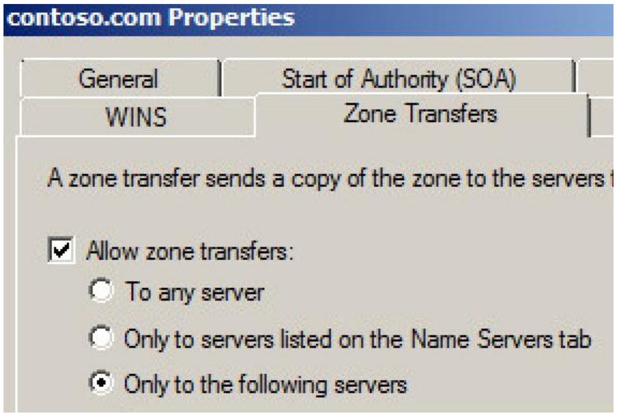
Once the zone **contoso.com** is created, we are going to enable zone transfer on the Microsoft Domain controller so that NIOS DNS appliance can import zone data from the domain controller.

To do so, login to the Microsoft Domain Controller with appropriate privileges:

1. Open **Server Manager**, Right click on **contoso.com** zone under DNS Server and click **Properties**



2. Select the **Zone Transfers** tab and select **Allow zone transfers.** In our example, we are opting for the more secure option of **Only to the following servers**.



contoso.com Properties

A zone transfer sends a copy of the zone to the servers t

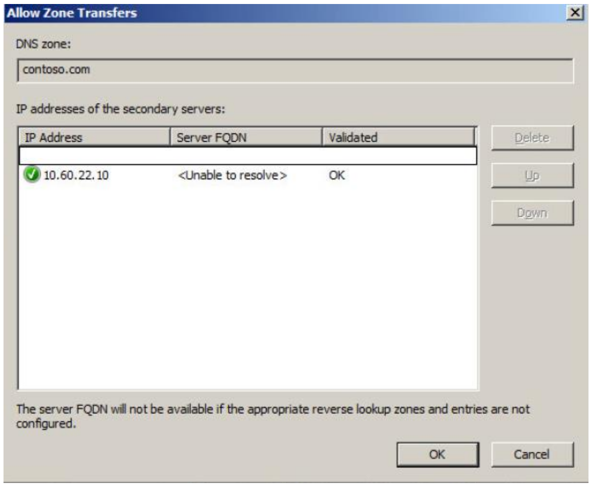
☑ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

3. Click **Edit** and type the IP address of the NIOS DNS appliance. In our example, it is **10.60.22.10.**



Allow Zone Transfers

DNS zone:

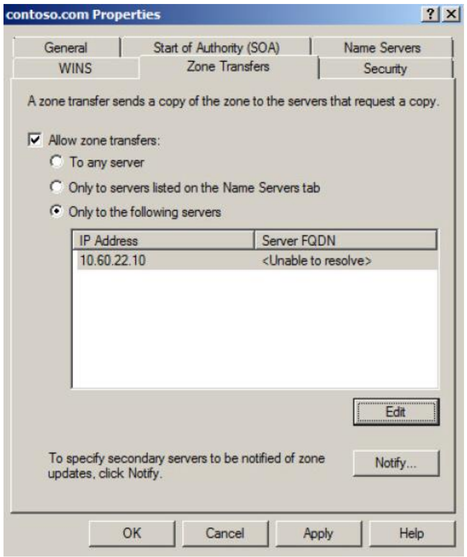
contoso.com

IP addresses of the secondary servers:

IP Address	Server FQDN	Validated
10.60.22.10	<Unable to resolve>	OK

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

4. Click **OK**



contoso.com Properties

A zone transfer sends a copy of the zone to the servers that request a copy.

☑ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

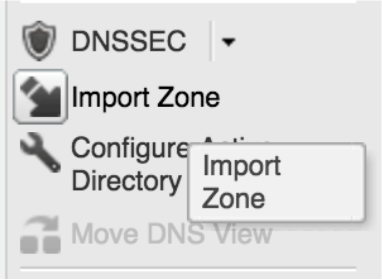
IP Address	Server FQDN
10.60.22.10	<Unable to resolve>

To specify secondary servers to be notified of zone updates, click Notify.

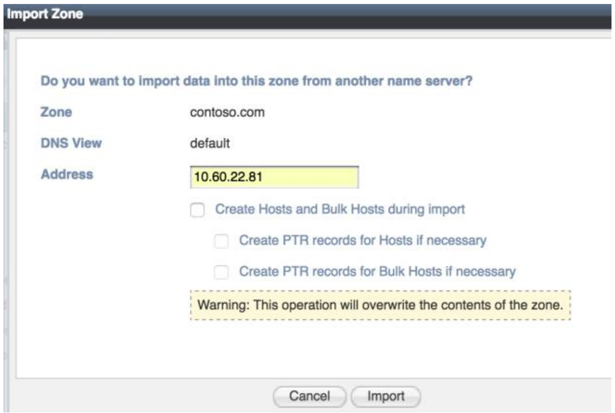
5. Click **OK**

Once zone transfers are allowed on the Microsoft domain controller, we are going to import the **contoso.com** zone data into the NIOS DNS appliance by doing the following:

1. Go to **Data Management** > **DNS** > **Zones**
2. Select the **contoso.com** zone
3. Click **Import Zone** from the **Toolbar**



4. Type the Microsoft Domain controller's IP address in **Address** field. In our example, it is **10.60.22.81**.



Import Zone

Do you want to import data into this zone from another name server?

Zone: contoso.com

DNS View: default

Address: 10.60.22.81

□ Create Hosts and Bulk Hosts during import

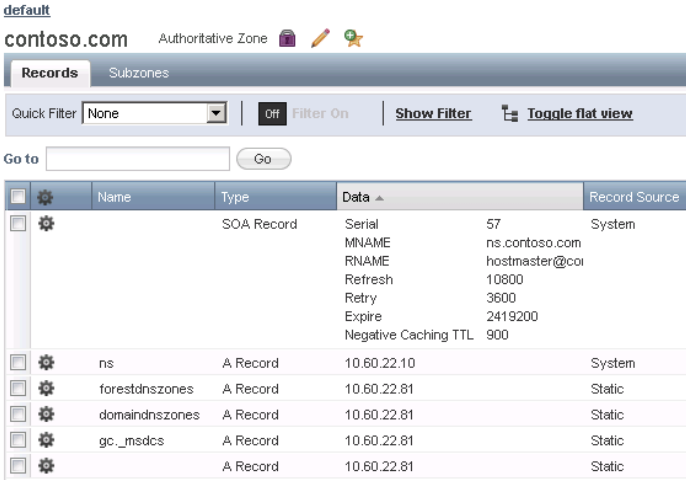
□ Create PTR records for Hosts if necessary

□ Create PTR records for Bulk Hosts if necessary

Warning: This operation will overwrite the contents of the zone.

5. Click **Import**
6. Click **Restart**

After the restart, the imported data can be seen in the zone.



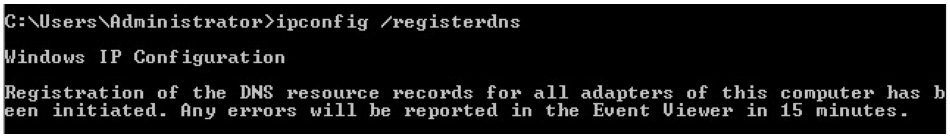
□		Name	Type	Data		Record Source
□			SOA Record	Serial MNAME RNAME Refresh Retry Expire Negative Caching TTL	57 ns.contoso.com hostmaster@coı 10800 3600 2419200 900	System
□		ns	A Record	10.60.22.10		System
□		forestdnszones	A Record	10.60.22.81		Static
□		domaindnszones	A Record	10.60.22.81		Static
□		gc._msdcs	A Record	10.60.22.81		Static
□			A Record	10.60.22.81		Static

Generate GSS-TSIG authenticated update

You can now test a GSS-TSIG authenticated DDNS update from a client. In our example, we are using a Windows 7 client named “test-pc” that is a member of the **contoso.com** domain. To generate the GSS-TSIG based authenticated DDNS update, do the following:

From the Windows client, issue the following command at the command prompt:

1. ipconfig /registerdns

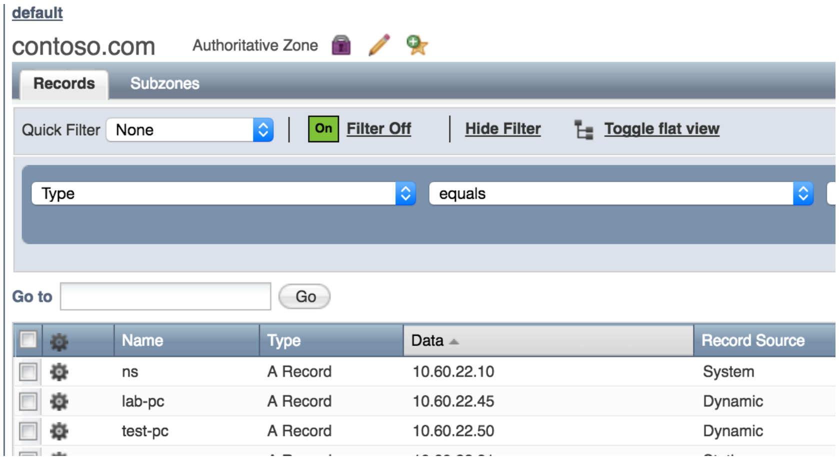


```
C:\Users\Administrator>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has b
een initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

Note: The NIOS DNS appliance must be used by the Windows client for all DNS queries. In our case it is **10.60.22.10**. Also note that Windows clients typically send an unsecure update followed by a secure (GSS-TSIG) update, this can be changed by Windows Group Policy so that clients only perform secure updates.

To verify if the GSS-TSIG authenticated DDNS update is successful:

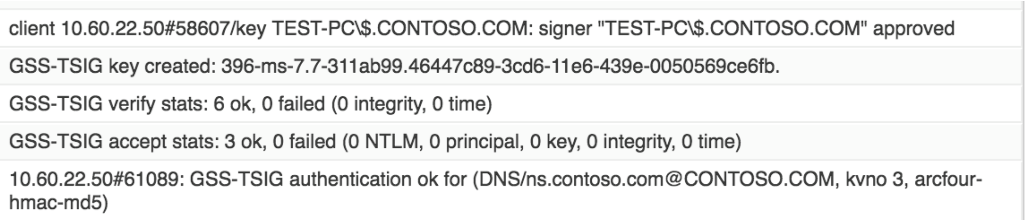
1. Go to zone **contoso.com** under **Data Management** > **DNS** > **Zones**
2. Verify if a Dynamic record has been created for the client. In our example, the two DDNS clients registered their DNS records as lab-pc and test-pc.



Name	Type	Data	Record Source
ns	A Record	10.60.22.10	System
lab-pc	A Record	10.60.22.45	Dynamic
test-pc	A Record	10.60.22.50	Dynamic

For troubleshooting purposes, you can view the syslog for the DDNS transactions.

1. Navigate to **Administration** > **Logs** > **Syslog**
2. Enable toggle multi-line view.
3. Below shows a sample DDNS transaction.



```
client 10.60.22.50#58607/key TEST-PC\$.CONTOSO.COM: signer "TEST-PC\$.CONTOSO.COM" approved
GSS-TSIG key created: 396-ms-7.7-311ab99.46447c89-3cd6-11e6-439e-0050569ce6fb.
GSS-TSIG verify stats: 6 ok, 0 failed (0 integrity, 0 time)
GSS-TSIG accept stats: 3 ok, 0 failed (0 NTLM, 0 principal, 0 key, 0 integrity, 0 time)
10.60.22.50#61089: GSS-TSIG authentication ok for (DNS/ns.contoso.com@CONTOSO.COM, kvno 3, arcfour-
hmac-md5)
```

Enabling NIOS DHCP Server to send DDNS Updates through GSS-TSIG

A NIOS DHCP appliance can be configured to send DDNS updates using GSS-TSIG authentication, on behalf of its DHCP clients, to Microsoft DNS Servers as follows:

1. Add a user account in Active Directory for the NIOS DHCP Server.
2. Generate a keytab file on the AD Domain Controller using the newly created user account.
3. Import the keytab file to the Infoblox Grid.
4. Configure DDNS updates

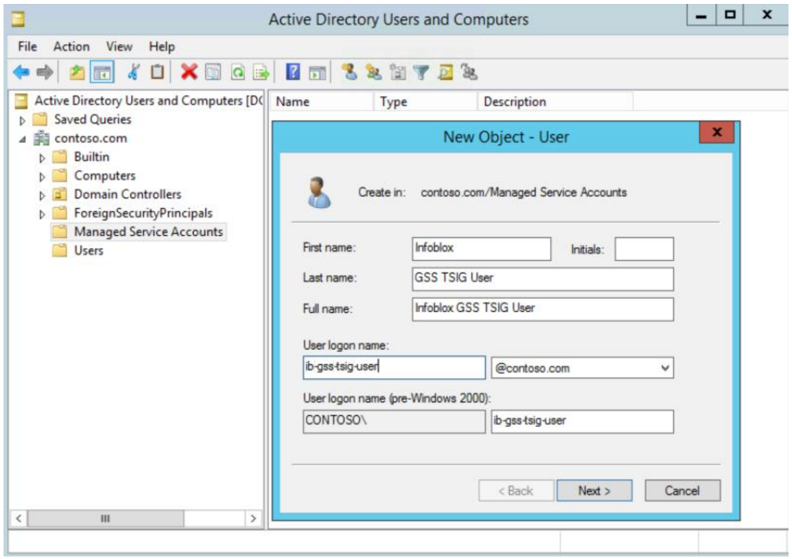
Creating an AD user account

In our example, we create a user account named ib-gss-tsig-user in Active Directory. This account will be used to generate the keytab file, which will be exported to NIOS.

Login to a Microsoft Domain Controller using an account with account creation privileges in Active Directory.

1. Open the **Active Directory Users and Computers** Snap-in in the Server Manager

   Right-click the **Managed Service Accounts** OU, click **New** and **User.** Type the user information



Create in: contoso.com/Managed Service Accounts

First name: Infoblox Initials:

Last name: GSS TSIG User

Full name: Infoblox GSS TSIG User

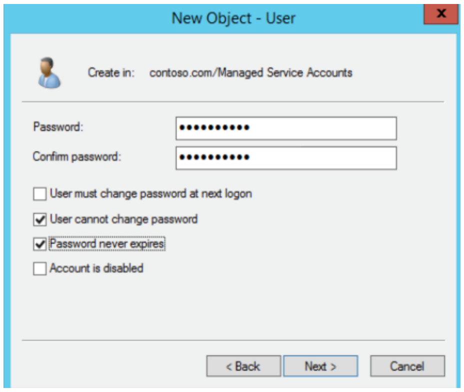
User logon name: ib-gss-tsig-user @contoso.com

User logon name (pre-Windows 2000): CONTOSO\ ib-gss-tsig-user

Note: The name you enter in the User logon name field is the name that is later used to export the keytab file. This is also the principal name.

2. Click **Next.**

3. Enter the password and enable the options “User cannot change password” and “Password never expires”. Click **Next,**



Create in: contoso.com/Managed Service Accounts

Password: ••••••••••

Confirm password: ••••••••••

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

4. Click **Finish**
5. The newly created AD user account should be member of group **DnsUpdateProxy** or an account that allows it to update records that have potentially been added by another DHCP server, such as the **DNS Admins.**

Generating the Keytab File

Once the user account has been created the Keytab file can be generated using the Windows ktpass utility.

Note that any changes to the user account, such as changing the password, mean that the Keytab file needs to be regenerated. The following is a format of the command to generate keytab file. The case sensitivity is important.

```
ktpass -princ ib-gss-tsig-user@CONTOSO.COM -mapuser ib-gss-tsig-user@CONTOSO.COM -pass **** -out ib-gss-tsig-user.tab -ptype krb5_nt_principal -crypto AES256-SHA1
```

In our example we used the command to generate keytab as follows,

```
C:\Users\administrator>ktpass -princ ib-gss-tsig-user@CONTOSO.COM -mapuser ib

-gss-tsig-user@CONTOSO.COM -pass !infobl0x -out ib-gss-tsig-user.tab -ptype k

rb5_nt_principal -crypto AES256-SHA1

Targeting domain controller: dc-01.contoso.com

Using legacy password setting method

Failed to set property 'servicePrincipalName' to 'ib-gss-tsig-user' on Dn 'CN=In

foblox GSS TSIG User,CN=Managed Service Accounts,DC=contoso,DC=com': 0x13.

WARNING: Unable to set SPN mapping data.

If ib-gss-tsig-user already has an SPN mapping installed for ib-gss-tsig-user, t

his is no cause for concern.

Key created.

Output keytab to ib-gss-tsig-user.tab:

Keytab version: 0x502

keysize 81 ib-gss-tsig-user@contoso.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 ety

pe 0x12 (AES256-SHA1) keylength 32 (0x685effa0c1119b5e0c1e2b89560433d20b1ae8b80d

32f45668389a8712dd131b)
```

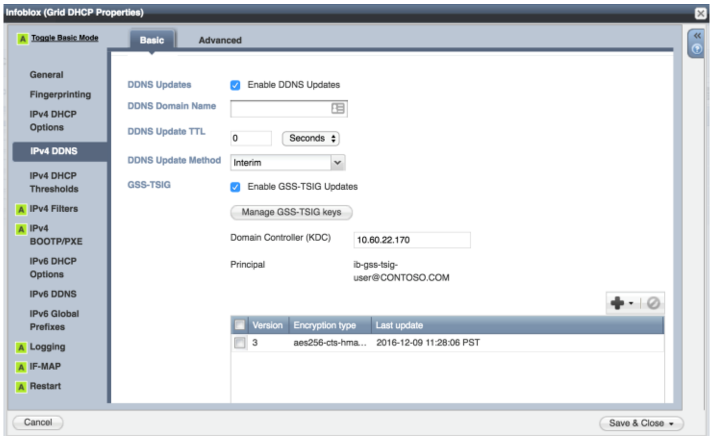
Once the keytab file is generated, please refer to the previous section "**Importing the keytab file and Enable GSS-TSIG on NIOS Appliance"** to import the keytab file in NIOS.

Configure DDNS Updates

Once the keytab file is generated and imported, the DDNS updates are configured in **Grid DHCP Properties** and in a separate control option called **Configure DDNS** under **Toolbar**.

1. Go to **Data Management** > **DHCP** > **Networks** and under Toolbar, click **Grid DHCP Properties** > **IPv4 DDNS**

2. Check option **Enable DDNS Updates**
3. Check option **Enable GSS-TSIG Updates**
4. Write the IP Address of Windows AD Server in **Domain Controller (KDC)** field, in our example **10.60.22.170**
5. Click **+** > **Assign Keys** (If keytab file already uploaded) or Click **Upload & Assign Keys** if keytab is still to be uploaded and select the keytab file
6. Click **Save & Close**



DDNS Updates ☑ Enable DDNS Updates

DDNS Domain Name

DDNS Update TTL 0 Seconds

DDNS Update Method Interim

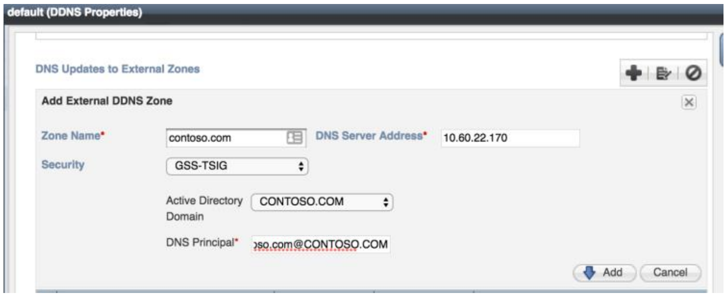
GSS-TSIG ☑ Enable GSS-TSIG Updates

Domain Controller (KDC) 10.60.22.170

Principal ib-gss-tsig-user@CONTOSO.COM

□	Version	Encryption type	Last update
□	3	aes256-cts-hma...	2016-12-09 11:28:06 PST

7. Click **Configure DDNS** in **Toolbar**
8. In Section **DNS Updates to External Zones**, Click **+**, fill zone name in **Zone Name** field, in our example it is **contoso.com**
9. Type **DNS Server Address**
10. Select **Security** as **GSS-TSIG** from drop down menu
11. Select **AD Domain** as it is on the DNS Server to be updated using DDNS
12. Type DNS Principal, in our example is DNS/dc-1.contoso.com@CONTOSO.COM
13. Click **Add**



Zone Name* contoso.com

DNS Server Address* 10.60.22.170

Security GSS-TSIG

Active Directory Domain CONTOSO.COM

DNS Principal*)so.com@CONTOSO.COM

14. Click **Save & Close**

Test the Configuration

Test the configuration to see if a TGT can be obtained. The following is output from the "`show dhcp_gss_tsig config`" command to test the configuration:

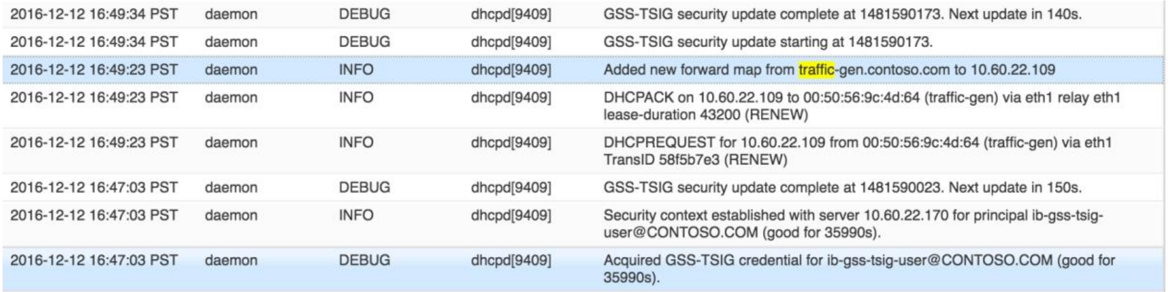
```
Infoblox > show dhcp_gss_tsig config

System time: Wed Dec 8 14:07:55 UTC 2016
```

```
DHCP GSS-TSIG configuration for this member:
  KDC address              10.60.22.170
  KDC IP                   10.60.22.170
  Member principal         ib-gss-tsig-user@CONTOSO.COM
  Member domain            CONTOSO.COM
  GSS-TSIG                 enabled
  DDNS updates             enabled
  DHCP service             enabled

Test KDC using member configuration? (y or n): y
Requesting TGT for ib-gss-tsig-user@CONTOSO.COM from KDC 10.60.22.170...
Successfully obtained test TGT.

Credentials cache: FILE:/tmp/krb5_cache.3815
        Principal: ib-gss-tsig-user@CONTOSO.COM
    Cache version: 4

Server: krbtgt/CONTOSO.COM@CONTOSO.COM
Client: ib-gss-tsig-user@CONTOSO.COM
Ticket etype: aes256-cts-hmac-sha1-96, kvno 2
Ticket length: 1118
Auth time:  Dec  8 14:07:59 2016
End time:   Dec  9 00:07:59 2016
Ticket flags: initial, pre-authenticated
Addresses: addressless

Successful test. Test TGT destroyed.

This member is configured to update the following zones:
  contoso.com on 10.60.22.170 as DNS/dc-1.contoso.com@CONTOSO.COM

Test configured zones? (y or n): y
```

```
Next zone is contoso.com on 10.60.22.170.

Test this zone? (y or n): y

Testing external zone contoso.com on NS 10.60.22.170...

DNS principal is DNS/dc-1.contoso.com@CONTOSO.COM.

Derived FQDN is dc-1.contoso.com.

FQDN resolves to nameserver IP.

SOA for contoso.com has MNAME dc-1.contoso.com.

Nameserver is authoritative for zone.

Zone contoso.com appears valid.
```

Syslog messages

In syslog the following log messages, as shown in the screenshot below, confirm DDNS updates are being forwarded to the Microsoft DNS Server.



2016-12-12 16:49:34 PST	daemon	DEBUG	dhcpd[9409]	GSS-TSIG security update complete at 1481590173. Next update in 140s.
2016-12-12 16:49:34 PST	daemon	DEBUG	dhcpd[9409]	GSS-TSIG security update starting at 1481590173.
2016-12-12 16:49:23 PST	daemon	INFO	dhcpd[9409]	Added new forward map from traffic-gen.contoso.com to 10.60.22.109
2016-12-12 16:49:23 PST	daemon	INFO	dhcpd[9409]	DHCPACK on 10.60.22.109 to 00:50:56:9c:4d:64 (traffic-gen) via eth1 relay eth1 lease-duration 43200 (RENEW)
2016-12-12 16:49:23 PST	daemon	INFO	dhcpd[9409]	DHCPREQUEST for 10.60.22.109 from 00:50:56:9c:4d:64 (traffic-gen) via eth1 TransID 58f5b7e3 (RENEW)
2016-12-12 16:47:03 PST	daemon	DEBUG	dhcpd[9409]	GSS-TSIG security update complete at 1481590023. Next update in 150s.
2016-12-12 16:47:03 PST	daemon	INFO	dhcpd[9409]	Security context established with server 10.60.22.170 for principal ib-gss-tsig-user@CONTOSO.COM (good for 35990s).
2016-12-12 16:47:03 PST	daemon	DEBUG	dhcpd[9409]	Acquired GSS-TSIG credential for ib-gss-tsig-user@CONTOSO.COM (good for 35990s).