Infoblox

Deployment Guide

NIOS SNMP and Syslog Deployment Guide

Table of Contents

Introduction

In this document, we cover the required steps to set up Syslog and SNMP monitoring, as well as to enable email and SNMP alerts. Monitoring DDI services and getting SNMP alerts allow you to provide continuous and reliable DDI. DDI provides core services in your network so it is important to ensure the health of your environment as uptime of DDI is directly tied to uptime of your applications and services.

Syslog

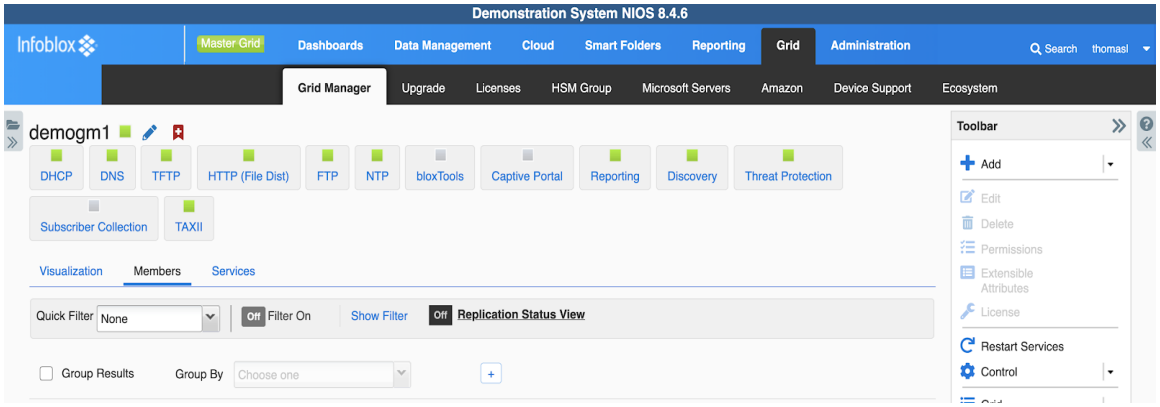
This section covers how to configure Infoblox syslog settings.

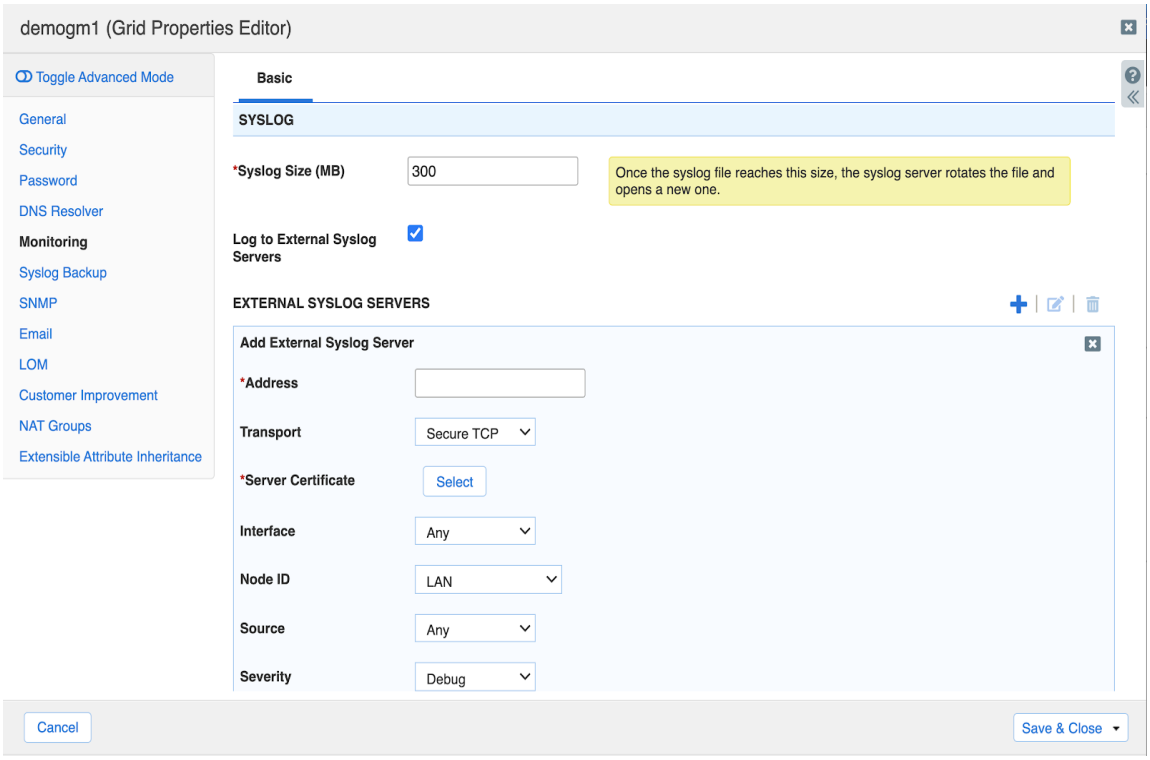
Configuration

Syslog configuration can be done Grid wide and/or customized at the Grid member level. When you edit the Syslog settings at the member level, you have the option to inherit the Syslog grid wide settings or override those grid wide settings

You can access the Grid wide settings under:

1. **Grid** > **Grid Manager** > **Members**.
2. Click **Grid Properties** > **Edit** in the right-hand **Toolbar**.
3. Select the **Monitoring** tab.





To send syslog data to an external Syslog server, check the box "**Log to External Syslog Servers**".

Once enabled, complete the steps for adding information of your external syslog server:

Click the **+** icon of the **External Syslog Servers** table and enter the following information in the new row:

— **Address**: The IPv4 or IPv6 address of the syslog server.

— **Transport**: The protocol supported by your syslog server. Secure TCP is the default

— **Interface**: Select the interface to be used for the connection to the syslog server.

- **Any**: The appliance chooses any port that is available for sending syslog messages. The server will use its routing table, including any static routes you have added, to determine the interface to be used.

— **Node ID**: Specify the host or node identification string used to identify the appliance from which syslog messages are originated. This string appears in the header message of the syslog packet.

— **Source**: From the drop-down list, select **Any** to send messages

— **Severity**: Choose a severity filter from the drop-down list. When you choose a severity level, Grid members send messages for that severity level plus all messages for all severity levels above it.

— **Port**: Enter the destination port number. The default is 514 for TCP and UDP. For Secure TCP, the default port is 6514.

— **Logging Category**: Select one of the following logging categories:

- **Send all**: Select this to log all syslog messages. This is the default.
- **Send selected categories**: Select this to configure logging categories from the list of available logging categories.

Note: The syslog categories you specify here are different from the logging categories specified in the Logging tab in the *Grid DNS Properties* or *Member DNS Properties* editor. The external server preserves contents of the selected categories even when the selection is changed from **Send all** to **Send selected categories** and vice versa.

— **Copy Audit Log Messages to Syslog**: Select this for the Grid member to include audit log messages among the messages it sends to the syslog server. For many security compliance audits this setting needs to be enabled.

Logging Categories

The following categories are available to select from when forwarding Syslog Messages:

- Threat Protection
  - These are the ADP events as well as ruleset update events
- Active Directory Authentication
  - Events based on authentication against Microsoft Active Directory
- Common Authentication
  - Authentication against all configured forms
- LDAP Authentication
  - Authentication against LDAP systems
- Non-system Authentication
  - Any non-local authentication events
- RADIUS Authentication
  - Authentication against RADIUS systems
- TACACS Authentication
  - Authentication against TACACS systems
- UI API Authentication
  - Any form of authentication tied to API logins
- Cloud API
  - Cloud API events including discovery, synchronization and automation events
- DHCP Process
  - Events based on the DHCP process status
- DNS Client
  - Events based on client DNS behavior
- DNS Config

    - Events related to config loads and changes for BIND
- DNS Database
    - Events related to the DNS dataset, this includes multi master updates and DDNS processing
- DNSSEC
    - Events related to key rollover, signing and validation
- DNS General
    - Events that do not fall under the other DNS specific categories
- DNS Lame Servers
    - Events pertaining to lame DNS server, these are unresponsive or misconfigured servers outside of your control
- DNS Networks
    - Events related to DNS scavenging
- DNS Notifies
    - DNS notify logs, incoming notifies for secondary zones, outgoing notifies when primary
- DNS Queries
    - DNS query logging events, will show each query a client makes
- DNS Query Rewrites
    - Events are logged if query rewrites are taking place
- DNS Resolver
    - DNS resolver events which include cache utilization
- DNS Responses
    - Events similar to DNS queries, this logs the responses to each query
- DNS RPZ
    - RPZ log events including client hits of RPZ
- DNS Scavenging
    - Events on the automated scavenging
- DNS Security
    - Events on NXDOMAIN, SERVFAIL and BIND Rate Limiting tracking
- DNS Unbound
    - Any Unbound logs when the unbound engine is active
- DNS Updates
    - DDNS update events
- DNS Update Security
    - Updates to rulesets
- Zone Transfer In
    - Incoming zone transfer events
- Zone Transfer Out
    - Outgoing zone transfers
- DTC Health Monitors
    - DTC health monitor events
- DTC Load Balancing
    - Load balancing service and data events

- FTP Process
    - Logging on the ftp process
- MS AD Users
    - Logging on the MS AD user integration
- MS Connect Status
    - Events related to MS connection status
- MS DHCP Clear Lease
    - Events related to Microsoft sync and clearing DHCP leases
- MS DHCP Lease
    - Events related to Microsoft sync and handing out DHCP leases
- MS DHCP Server
    - Events related to Microsoft sync the DHCP server status
- MS DNS Server
    - Events related to Microsoft sync the DNS server status
- MS DNS Zone
    - Events related to Microsoft sync the DNS zones changes
- MS Sites
    - Events related to Microsoft sync the Sites and Services synchronization
- Non-categorized
    - All others
- NTP
    - NTP process and status logging
- Outbound API
- TFTP Process
    - TFTP service logs

After selecting logging categories above, click on TEST button to test connectivity to the syslog server and/or click on the ADD button to add the external syslog server entry.

Click Save and Close.

Syslog server configuration

For the purpose of this deployment we have set up an external syslog server on an Ubuntu system with rsyslog.

On this system the following steps are taken to allow us to accept logging:

- Modify rsyslog.conf to accept external connections
- Setup syslog rolling once the file size reaches 150MB

Before you forward to your external server you only see localhost entries:

```
May  2 15:54:47 localhost systemd[1]: Stopping System Logging Service...
May  2 15:54:47 localhost systemd[1]: Stopped System Logging Service.
May  2 15:54:47 localhost rsyslogd-2222: command 'KLogPermitNonKernelFacility' is currently not permitted - did you already set
 it via a RainerScript command (v6+ config)? [v8.16.0 try http://www.rsyslog.com/e/2222 ]
May  2 15:54:47 localhost rsyslogd: rsyslogd's groupid changed to 109
May  2 15:54:47 localhost rsyslogd: rsyslogd's userid changed to 104
May  2 15:54:47 localhost systemd[1]: Starting System Logging Service...
May  2 15:54:47 localhost systemd[1]: Started System Logging Service.
```

After making the listed changes you will see the log messages from your grid members:

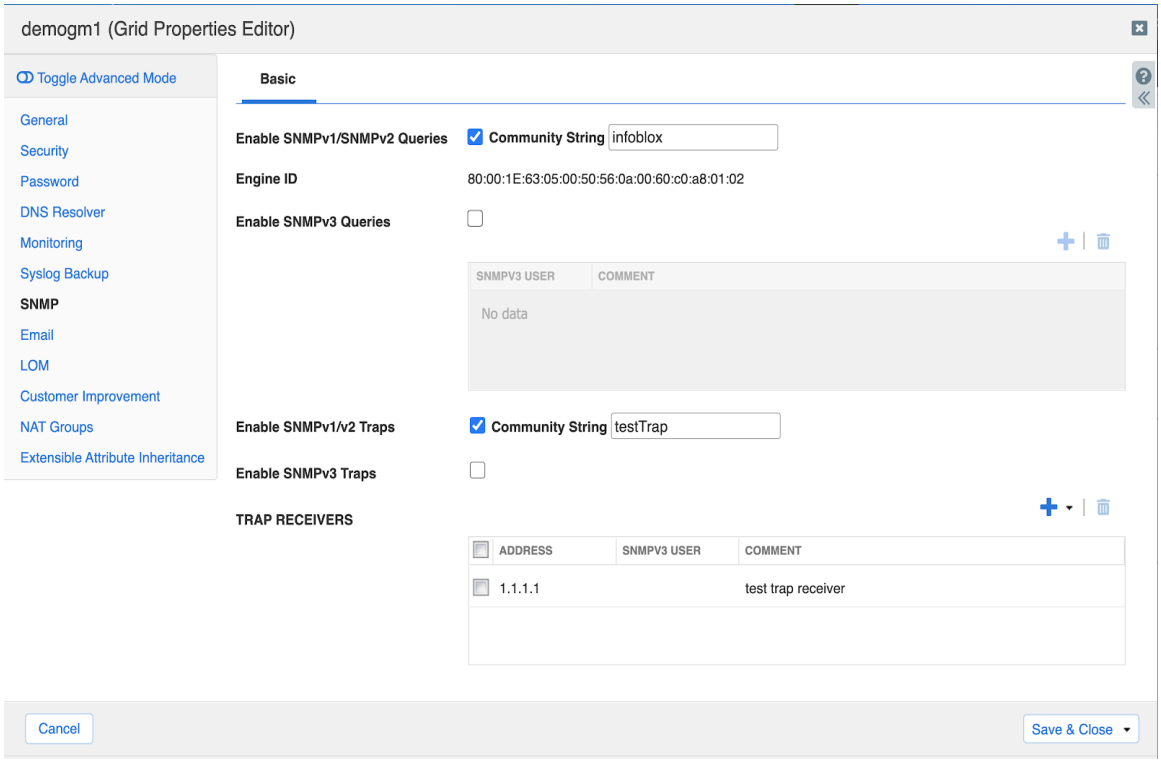
```
May  2 16:28:12 10.61.1.153 named[22482]: Recursion cache view "_default": size = 70216, hits = 2, misses = 7
May  2 16:28:12 10.61.1.153 named[22482]: Recursion client quota: used/max/soft-limit/s-over/hard-limit/h-over/low-pri = 0/2/0/
0/1000/0/0
May  2 16:28:14 10.61.1.63 netauto_core[508]: netautoctl: Smart Subnet Ping Sweep is not running correctly, attempting to start
May  2 16:28:14 10.61.1.63 netauto_core[508]: netautoctl: Smart Subnet Ping Sweep started correctly
```

Configuring SNMP

SNMP configuration can be done at the Grid and/or member level. You have the options to inherit the grid wide settings or override Grid settings at a member level.

You can access the Grid wide settings under:

1. **Grid** > **Grid Manager** > **Members.**
2. Click **Grid Properties** > **Edit** in the right-hand toolbar.
3. Select the **SNMP** tab.



- **Enable SNMPv1/SNMPv2 Queries**: Select this to accept SNMPv1 and SNMPv2 queries from management systems.
- **Enable SNMPv3 Queries**: Select this to accept SNMPv3 queries from management systems.
- Enter the SNMPv3 username(s).

— **Community String**: Enter a text string that the management system must send together with its queries to the appliance.

- **Enable SNMPv1/SNMPv2 Traps**: Select this to enable the appliance to send traps to specified management systems.

— **Community String**: Enter a text string that the NIOS appliance sends to the management system together with its traps. Note that this community string must match exactly what you enter in the management system.

- **Trap Receivers**: Click + and select **SNMPv1/SNMPv2**. In the Address field, enter the IPv4 or IPv6 address of the SNMP management system where the traps will be sent to. Multiple receivers can be added.

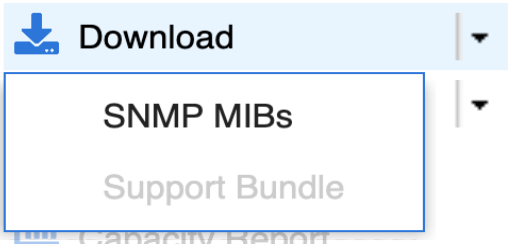
SNMP System Information: You can enter values for the following managed objects in MIB-II, the standard MIB defined in RFC 1213. Management systems that are allowed to send queries to the appliance can query these values..

- **sysContact**: Enter the name of the contact person for the appliance.
- **sysLocation**: Enter the physical location of the appliance.
- **sysName**: Enter the fully qualified domain name of the appliance.
- **sysDescr**: Enter useful information about the appliance, such as the software version it is running.

4. Click **Save & Close**.

MIB

You can obtain the Infoblox SNMP MIB details by clicking the **Downloads** button under **Toolbar**.



For further documentation on the structure of the MIB objects and which OID's you can query, refer to the Administrators Guide for your version of NIOS.

Testing and Troubleshooting

External SNMP configuration

In our example, we used a Ubuntu system with snmpd and snmptrapd configured.

Configure the community strings of the Ubuntu host to match the Infoblox grid member so one can query it.

Test this by executing the following command on the shell:

```
"snmpget -v 2c -c public $memberIP .1.3.6.1.4.1.2021.10.1.5.2
```

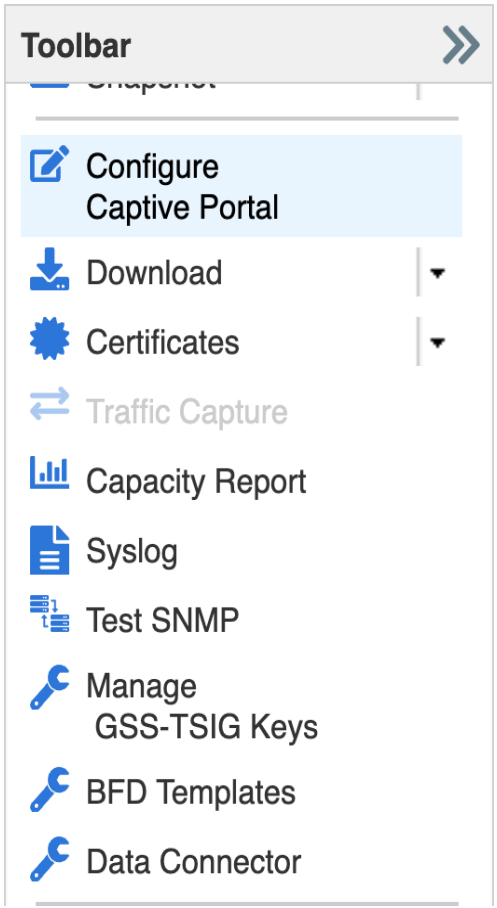
"-v 2c" specifies we are using SNMPv2
"-c public" means the configured community string is set to "public"
"$memberIP" should be replaced with the IP of the member you are querying
".1.3.6.1.4.1.2021.10.1.5.2" The number at the end is the OID we are querying, in this case it is the system load information.

If you want to get a look at all available data from the grid member through SNMP you can also use snmpwalk. Please note that if you have a large dataset of zones and networks this can be a lot of data.

```
"snmpwalk -v 2c -c public $memberIP"
```

You should see a full snmpwalk output which gives you all the data that can be queried by SNMP..

After you configured SNMP traps on the appliance, you can click **Test SNMP** from the Toolbar to test your SNMP configuration. The appliance sends a "**test trap**" string to the trap receiver. In our example it will arrive to Ubuntu VM as shown below.



The following example demonstrates a test trap being successfully received on the Ubuntu system:

```
May  3 10:15:12 localhost snmptrapd[21881]: internal1.nios [UDP: [10.61.1.153]:54077->[10.61.2.128]:162]: T
rap , DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (75350000) 8 days, 17:18:20.00, SNMPv2-MIB::snmpTrap
OID.0 = OID: SNMPv2-MIB::snmpTrapOID, SNMPv2-MIB::sysName.0 = STRING: 'Test trap'
```

You also have the ability to trigger specific traps from the servers CLI. While logged in to the CLI of the grid member, enter maintenance mode by entering the command:

```
set maintenancemode
```

This enables the ability to execute the `set snmptrap` command used for testing specific SNMP traps. For more details on how to run the set snmptrap command, please see the NIOS CLI document.

Sending notifications

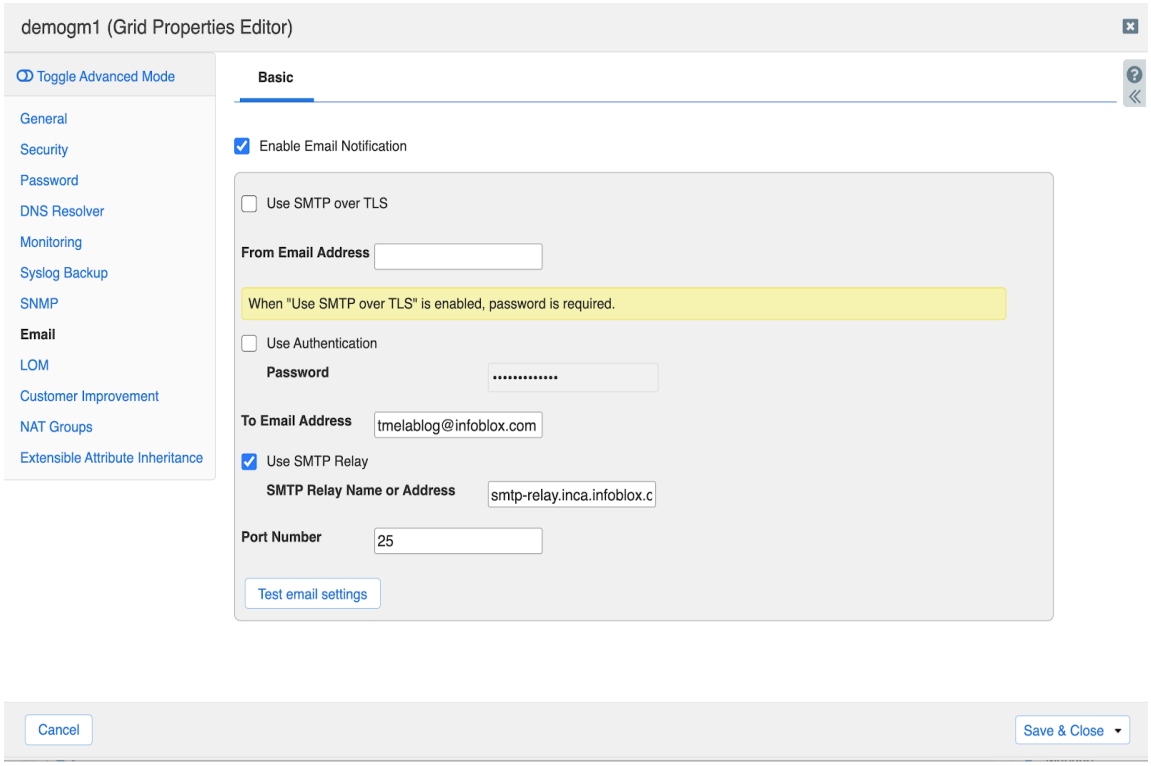
Enable email notifications (Grid)

This section explains how to configure / enable email notifications from the Grid and Reporting server. Note that from the Grid you cannot use a SMTP relay with authentication.

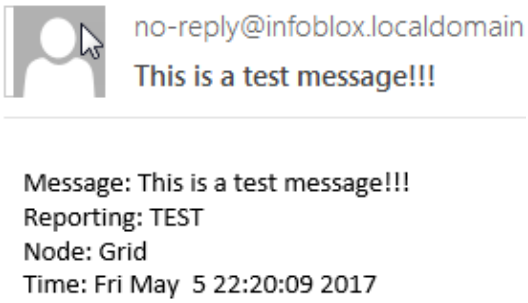
The preferred way is to implement an internal email server to receive email notifications from the Grid.

To configure email notifications from the Grid:

1. Go to **Grid** > **Grid Manager** > **Members**.
2. Click **Grid Properties** > **Edit** from the **Toolbar**
3. **Grid** > **Grid Properties** > **Email**



4. Check "**Enable Email Notification**" and enter the **"TO"** email address.
    a. If required, enable the **Use SMTP Relay** and enter the name or IP address of the relay server to be used.
5. Click to the "**Test email settings**" to send a test email message.
6. Verify that the test email was received. The sender will be no-reply@<servername>, where <servername> is the name configured for your Infoblox server.



7. Click Save and Close.

Enable email notifications (Splunk)

To configure email notifications from Reporting Server:

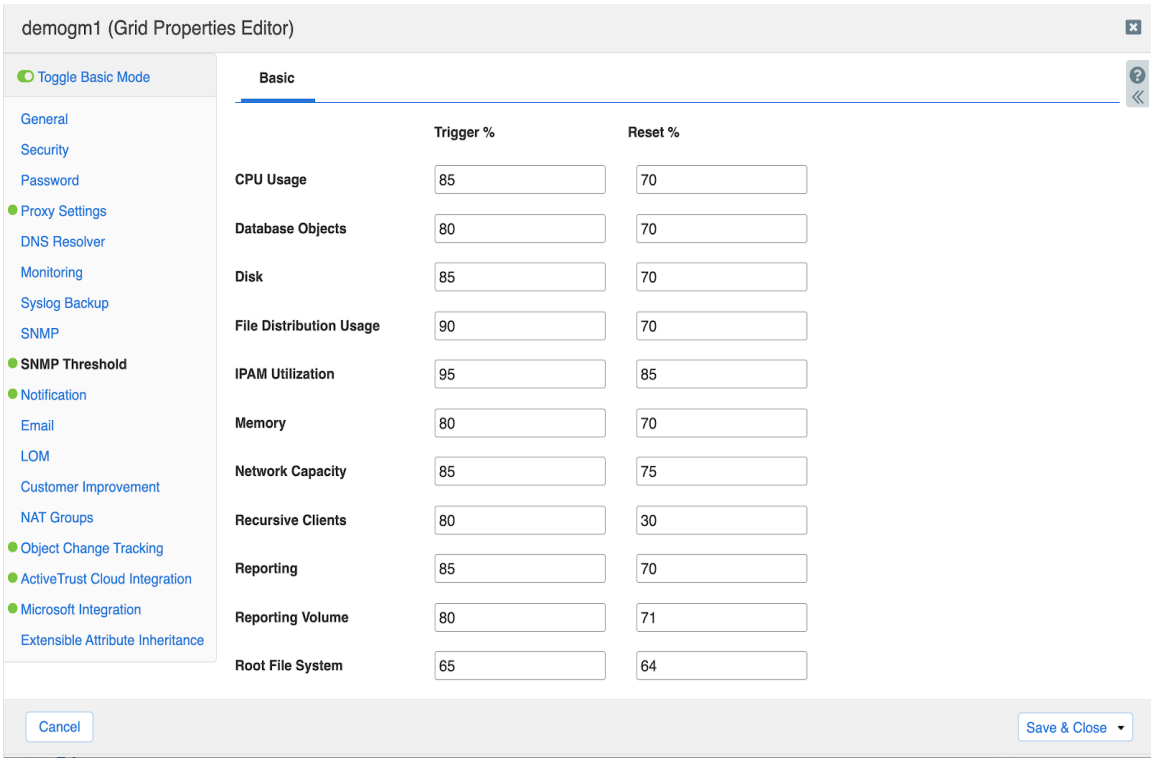
1. Go to **Reporting** > **Settings** > **Server Settings**.
2. Click **Email settings**

Enter the email server and any authentication details for it. Fill out the link hostname field with your Grid Master's hostname or IP.
A minimal mail server installation guide can be found in the annex section.

Defining SNMP Thresholds

You can access the Grid wide settings under:

1. Go to **Grid** > **Grid Manager** > **Members**.
2. Click **Grid Properties** > **Edit** from the **Toolbar**
3. Click **Toggle Advanced Mode** if not already enabled.
4. Click **SNMP Threshold**



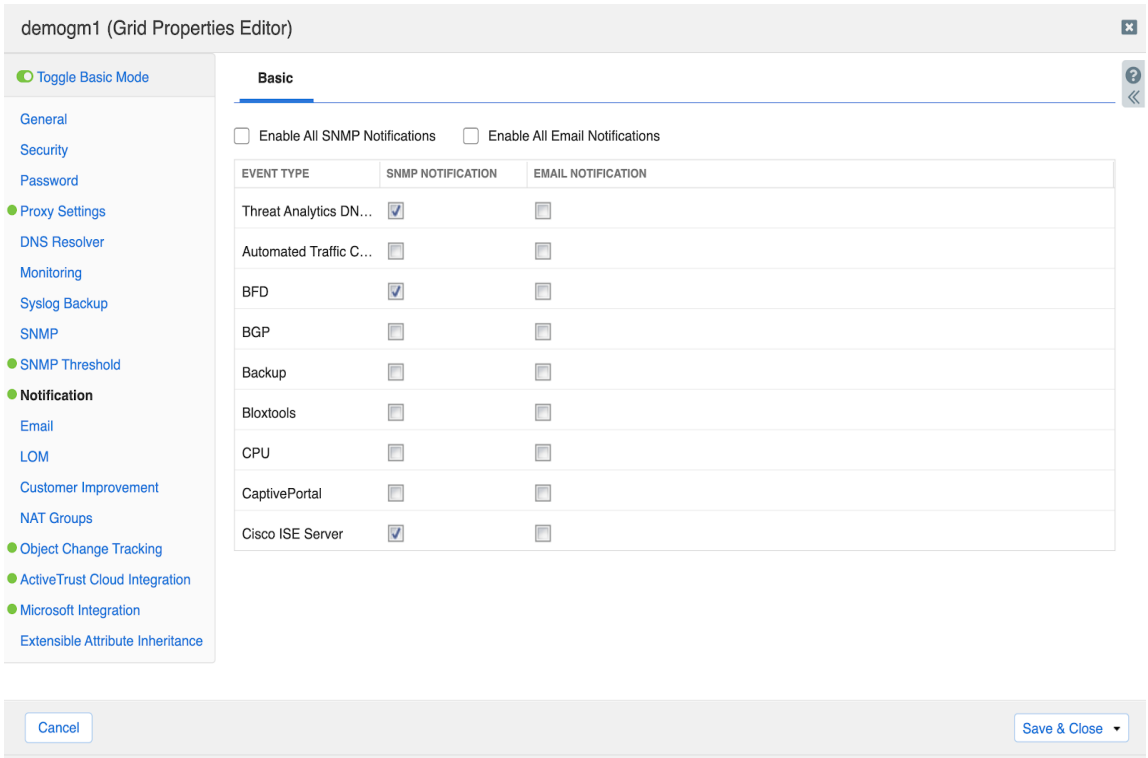
When enabled, SNMP thresholds are used to define triggers for when an appliance sends SNMP traps and email notifications. When any allocated usage exceeds the trigger value, the member sends the applicable SNMP trap and email notification to the designated destination, and the status icon for that usage turns red. When usage drops to the Reset value, the status color goes back to normal and turns green.

Notifications

The settings under this tab determine which notifications are also sent as an SNMP trap and which are sent as an email notification.

You can access the Grid wide settings under:

1. Go to **Grid** > **Grid Manager** > **Members**.
2. Click “**Grid Properties**” > **Edit under** in the right-hand **Toolbar.**
3. Click **Toggle Advanced Mode** if not already enabled.
4. Select the **Notifications** tab.



Monitoring configuration

The following section details the different service, errors and values to monitor depending on which services are running on the appliance.

DNS

DNS Service

Description

Detect if the DNS service is down or if any troubles are detected.

Implementation

DNS event type must be enabled as a notification category in the Grid properties or on a member level.

DNS Service Health Check

Description

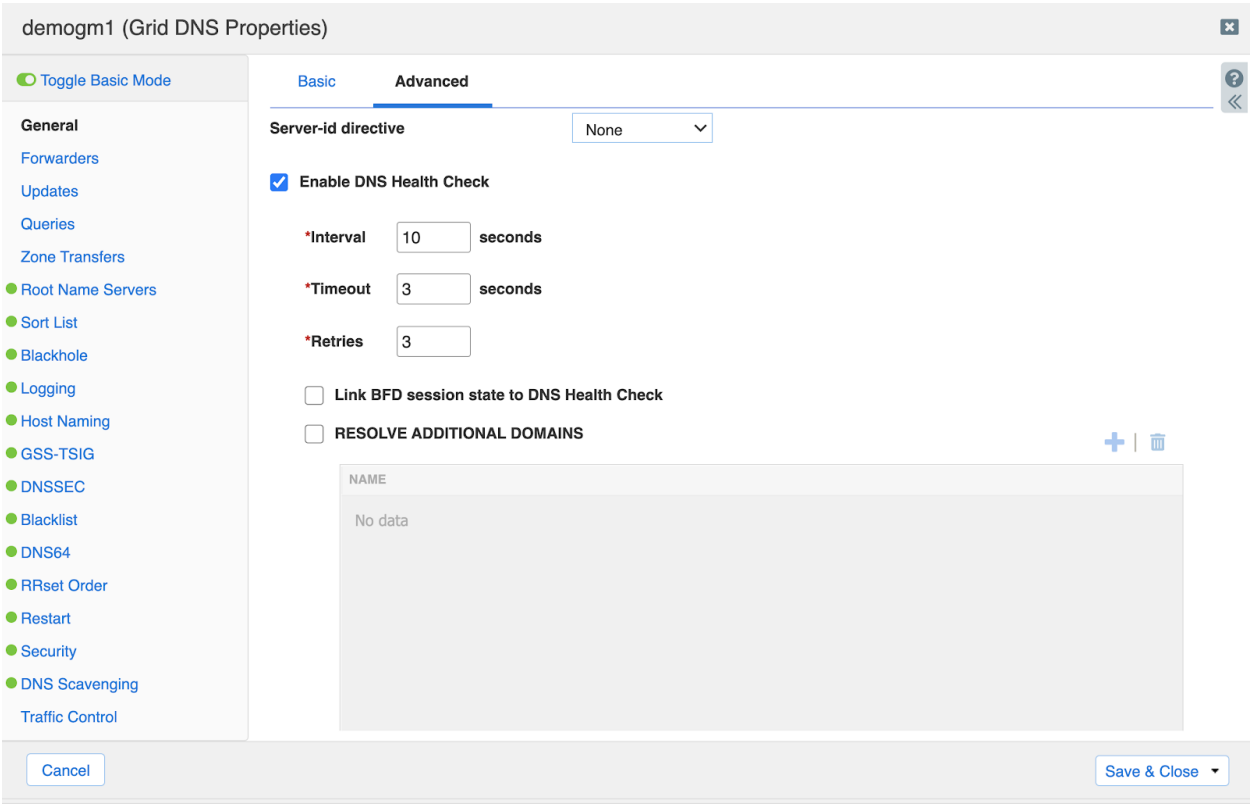
Detect if a DNS health check failed has been raised in the syslog messages.
It indicates that the DNS resolution is out of order despite the DNS service running.
This can happen when the member is overload and / or under attack.

Implementation

DNS health check must be enabled:

1. **Data management > DNS > Members/Servers**

2. Click **Grid DNS properties** in the **toolbar**
3. Click **Toggle Advanced Mode** if not already enabled.
4. Go to **Advanced** tab under **General**
5. Enable “**DNS Health Check**”
6. Click **Save & Close**.



Note: **DNS** event type must be enabled as a notification category in the Grid properties or in the member level.

DNS Internet Resolution Check

Description

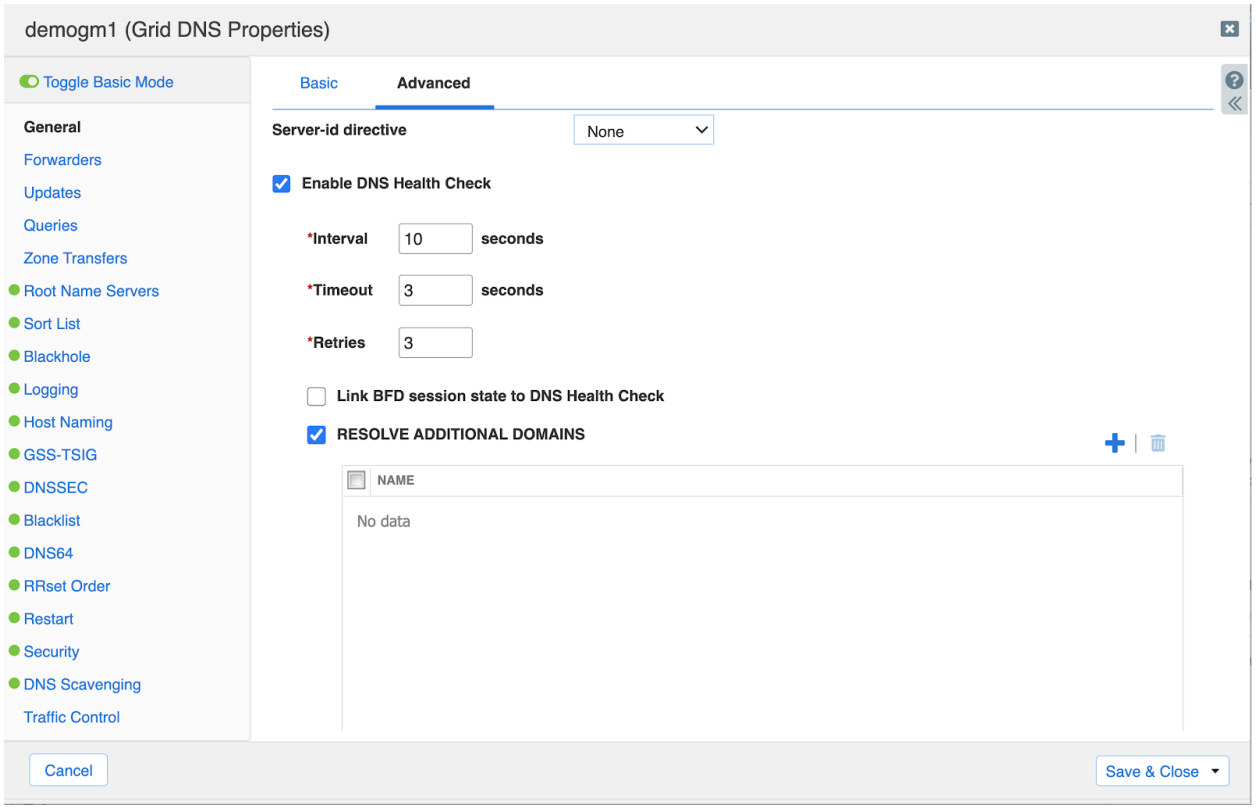
Detect whether a public domain resolution is working or not. This is only relevant for DNS members which have a recursive/forwarding role for public domain. (your caching resolvers.)

Implementation

DNS health check must be enabled:

1. **Data management > DNS > Members/Servers**
2. Click **Grid DNS properties** in the **toolbar**
3. Click **Toggle Advanced Mode** if not already enabled.
4. Go to **Advanced** tab under **General**
5. Enable “DNS Health Check”
6. Enable "Resolve Additional Domains" and add a public domain to the list (for example infoblox.com). Currently up to 16 domains can be specified

7. Click Save & Close.



Note: **DNS** event type must be enabled as a notification category in the Grid properties or on the member level

DNS Integrity Check

Description

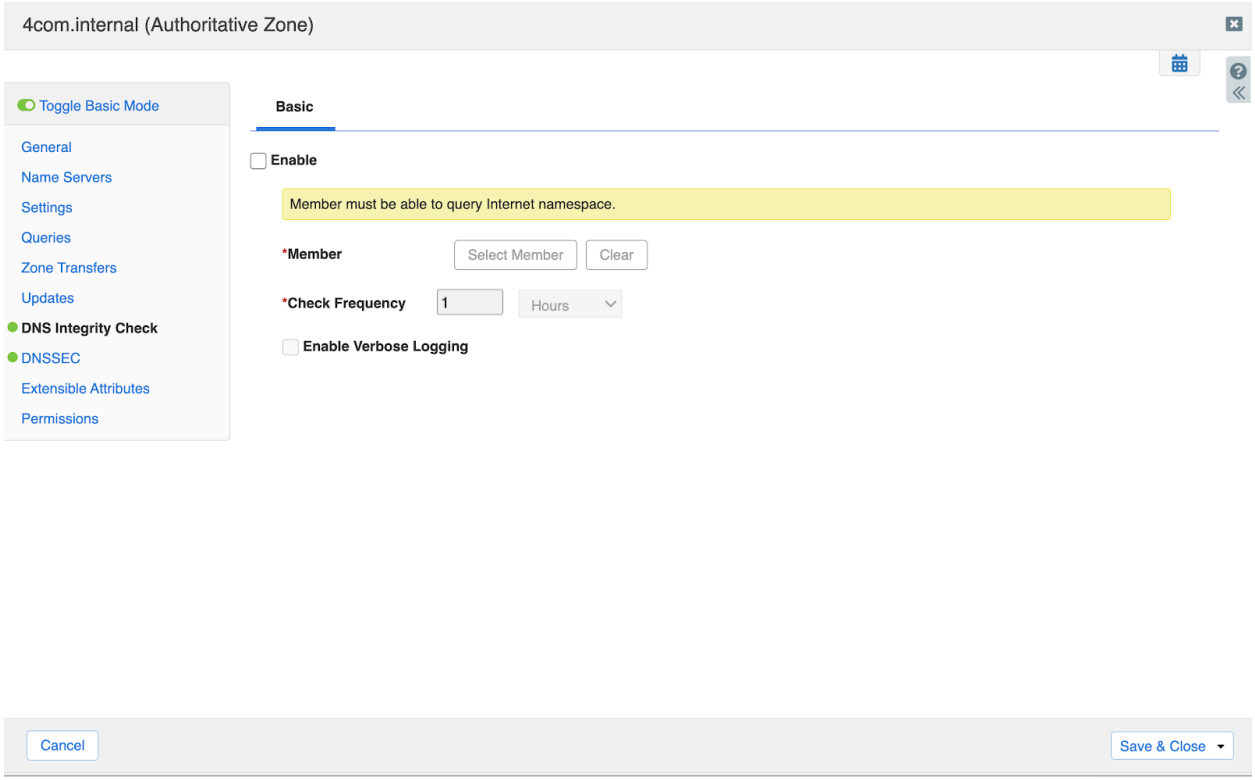
Check whether the authority servers declaration for a public zone are the same from DNS Internet NS and Infoblox database. If not, this could indicate the domain is being a hijacked or simply not renewed in time. This is only relevant for DNS members which hosts your public zones.

Implementation

DNS Integrity Check must be enabled for all public zones you want to monitor.

1. Navigate to **Data management > DNS > Zones**
2. Select the desired DNS view if applicable.
3. Select the zone you want to edit and click on **Edit**
4. Click **Toggle Advanced Mode** if not already enabled.
5. Go to the **DNS integrity** tab
6. Check the **Enable** box
7. **Select the member** to run the check from (this member should be allowed to query public domains)
8. Set the frequency

9. Click **Save & Close**.



"DNS Integrity Check / Connection" event type must be enabled as a notification category in the Grid properties or in the member level.

DNS Zone Transfer

Description

Detect if a zone transfer from an external DNS primary server has failed.
This is really useful to avoid discrepancies between the DNS master of a zone and the DNS slave servers.
Remember also that after the expiration time is reached, the DNS slave server will not respond to the queries for the secondary zone anymore.

Implementation

This alert requires the reporting member or an external syslog server (like Splunk).
Syslog data must be sent from the Infoblox DNS members to the reporting server. In order to do so enable the **Syslog** category under the reporting index settings.

In reporting, this alert can be scheduled to run at any interval. However, the setting for this interval depends on the expiration time of your zones. You should alert before the expiration time and allow for some time to address the issue.

The following search command will provide you with the failed zone transfer events:

```
index=ib_syslog err transfer of failed
```

DNS RFC 1918

Description

Detect whether a private IP address is configured in a DNS response. This must be resolved by creating all the IPv4 private reverse-mapping zone (cf RFC 1918)

Implementation

This alert requires the reporting member or an external syslog server (like Splunk).
Syslog data must be sent from the Infoblox members to the reporting server. In order to do so enable the **Syslog** category under the reporting index settings.

In reporting, this alert can be scheduled to run at any interval.

Example:
each day / look for RFC 1918 events in the last 24h.
The following search command will provide you with the events when the private IP address is configured in the DNS response:

```
index=ib_syslog rfc 1918 response from internet
```

DNS Cache Response time

Description

Measure the DNS response time for a resource record that is already in the cache. This is typically around 1ms and should not be more than 5-10ms. If it is longer than 10ms it could be a component in your network that is introducing extra latency or there is a routing problem. This is relevant for all members which operate as caching DNS servers and have to retrieve a record from another DNS server (forward and stub zones, delegations).

Implementation

This check should be executed regularly by an external monitoring system.
You can monitor the response time with the dig command:

```
dig monitor.mydomain.intra | grep -i "query time"
;; Query time: 1 msec
```

Note that you have to define an existing resource record for your test and set the cache timers higher than your test schedule frequency to ensure you monitor a DNS response time for a cached entry.

DNS Response time uncached

Description

Measure the DNS response time for a resource record not in the cache. This is relevant for all members and in particular caching DNS servers which have to retrieve a record to another DNS server (forward and stub zones, delegations).

Implementation

This check should be executed regularly by an external monitoring system.
You can monitor the response time with the dig command:

```
dig monitor.mydomain.intra | grep -i "query time"
;; Query time: 1 msec
```

Note that you have to define an existing resource record for your test and set the cache timers **Lower** than your test schedule frequency to ensure you monitor a DNS response time for an uncached entry.

DTC (DNS Traffic Control)

DTC Monitor

Description

Check whether a health monitor check to a server has failed (http(s), icmp, tcp...).

Implementation

This alert requires the reporting member or an external syslog server (like Splunk).
Syslog data must be sent from the Infoblox members to the Reporting member. In order to do so enable the **Syslog** category under the reporting index settings.
DTC health monitors logging must be enabled as a DNS logging category

In reporting, this alert can be scheduled to run at any interval.
(depending of your health monitor interval time check)

Below the alert search:

```
index=ib_syslog monitor status is offline
```

Splunk alerts

Create an alert

How to create an alert from Splunk and send it by mail. This is not a complete overview of all Splunk capabilities. Please visit the Splunk website for more detailed product documentation.

A Splunk alert is typically based on a "keyword" search. The first step is to know what the log content will be.

We will configure an alert example for a failed transfer zone from an external master DNS server.
If we search the log, we can see a log message like:

```
“transfer of 'zt.intra/IN' from 192.168.1.60#53: failed to connect:
connection refused”
```

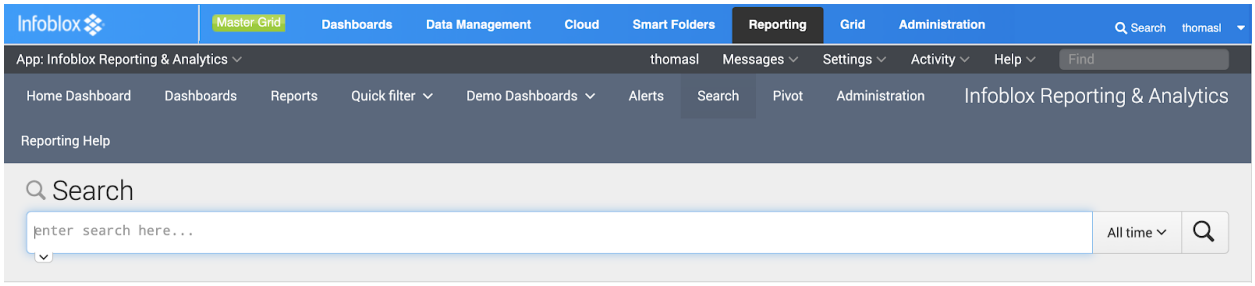
OR

```
“transfer of 'fresh-domain.surbl.rpz.infoblox.local/IN' from
54.69.93.185#53: failed while receiving responses: REFUSED"”
```

We have to observe what will be the common word when there are some issues with a zone transfer and be sure that both alerts will be caught. Here the keywords should be " transfer of" and "failed"

Once we've identified the keywords to catch the relevant log entry, we have to create the alert:

Go to **Reporting** > **Search** and enter the keywords “transfer of” and “failed”



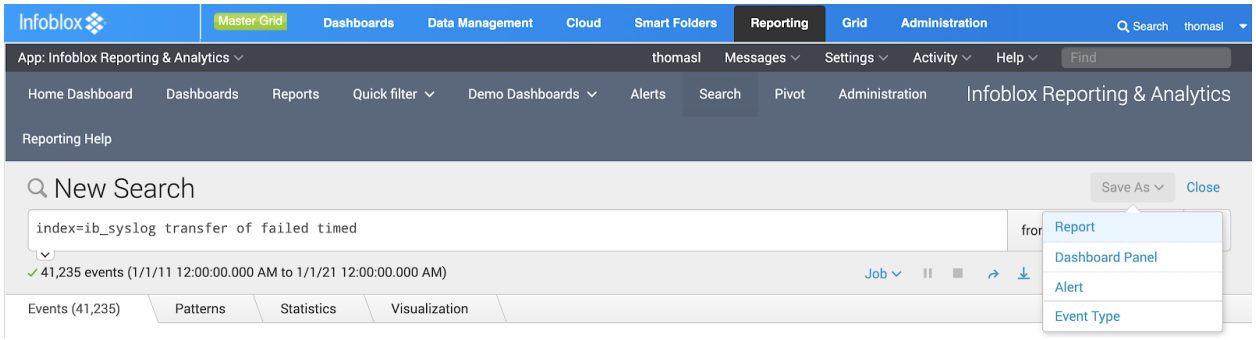
You should see some messages that match you search:

As you can see, there is a field called "index=ib_syslog" which indicates the log category this index belongs to (here ib_syslog)
When you perform a search without specifying the index category, Splunk searches all the logs in all the categories. This takes more system resources and can take a very long time when your system deals with a lot of data.

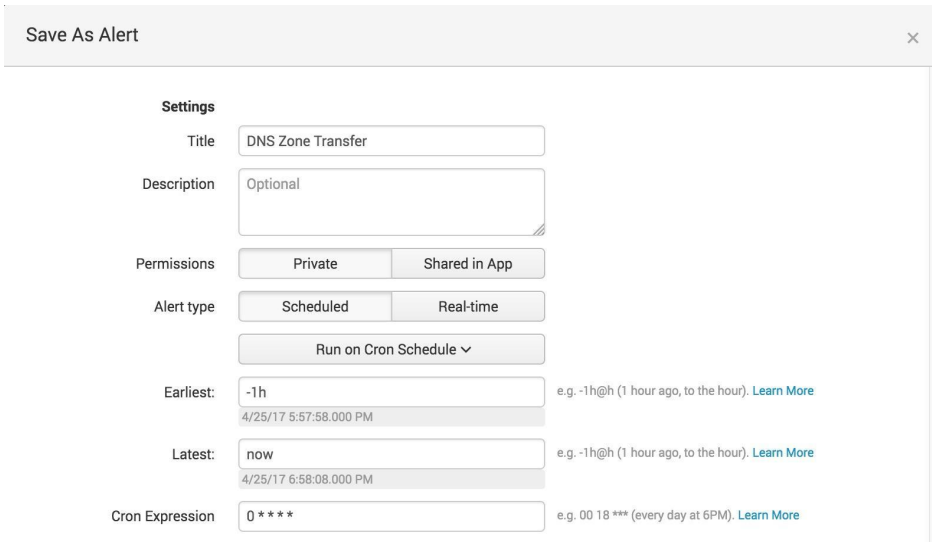
Specify the index category to improve the search performance with the search below:

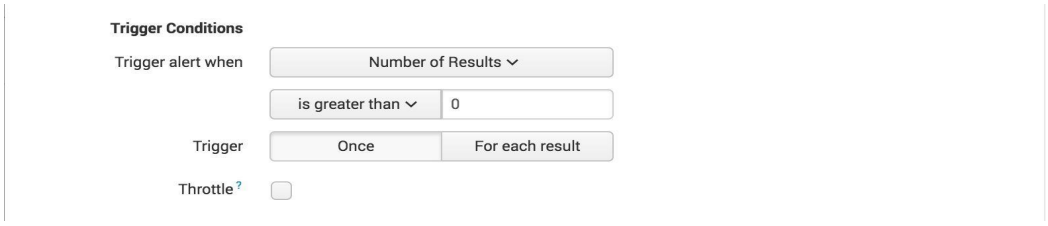
```
index=ib_syslog transfer of failed
```

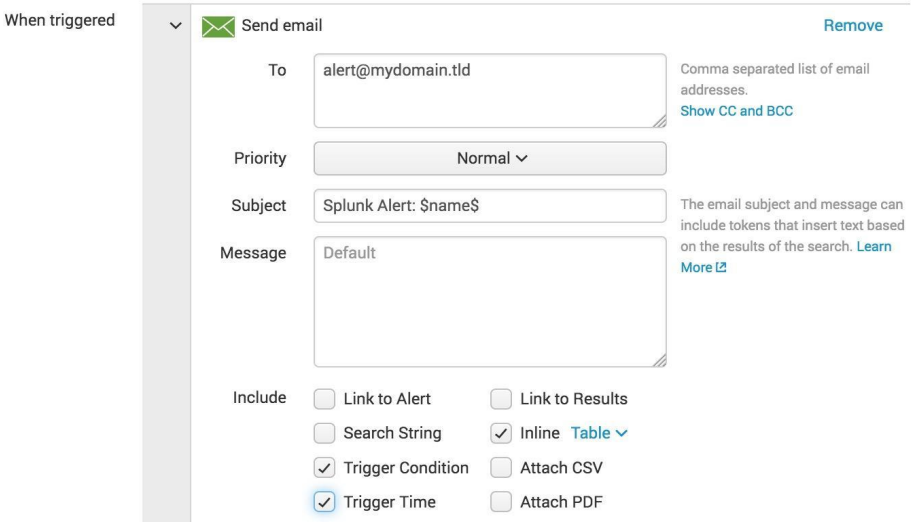
Once you have created your search and validate the match, you have to save it as an alert.



Configure the alert settings:







Splunk will analyze all the log entries one hour earlier than each time the search is run. If the search starts at 4:00, Splunk will analyze all logs between 3:00 and 4:00.
Earliest: -1h
Latest: now

If there is at least one log entry caught by the search, Splunk will apply the trigger actions. In this case Splunk will send an email and add this event to triggered alerts.

Scheduled or real-time alert?

The big advantage of a real-time alert means that you will receive the alert as soon an issue is detected . However, you have to take into account that a real-time alert will consume a lot or system resources. The reporting engine must analyze each log line received and compare with all real time search alerts. Because real-time alerts require additional system resources, Infoblox suggests administrators use them judiciously. For example, the failed zone transfer alert does not require immediate action in most environments. However if there is a zone for which requires frequent changes, differences between the primary DNS server and the secondary DNS server is going to be problematic, then setting the real-time alert would be appropriate. Currently Infoblox supports 5 real time alerts.

Additional Documentation

- NIOS Admin Guide
    - Chapter 37 “Monitoring the Appliance”
        - Monitoring Services
        - Using a Syslog Server
        - Monitoring Tools
    - Chapter 39 Monitoring with SNMP
- NIOS CLI Guide
- DNS Log Message Reference
- DHCP Log Message Reference

Annex

How to quickly install a mail server to receive mail alert notification

These are quick steps to install for a full mail server with Postfix and Dovecot on an Ubuntu Linux distribution.

To install postfix: "`sudo apt-get install postfix`"
Choose "Internet Site" option
Set the next parameter to default
Add the home directory for users where the mails will be store
Edit the "`/etc/postfix/main.cf`" and add:
home_mailbox = Maildir/

In the same file, add the domain for your mailbox to the conf line "mydestination"

Then restart the Postfix service issue: `sudo /etc/init.d/postfix restart`

To add a mailbox, just add a user with the name for which you want an email address:
`adduser user`
Test if the mailbox receives the mail for your mail address
`“sudo apt-get install mailutils”`

Then send a test email:

```
echo "mail content" | mail -s "This is the mail object"
user@mydomain.tld
```

If you go to "/homer/username/Maildir/new, you should see the file which is the mail you just sent.

Install Dovecot to retrieve the mails with your client mail: "`apt-get install dovecot-pop3d`" to use POP mail protocol or "`dovecot-imapd`" to use IMAP mail protocol.

Edit the "`/etc/dovecot/conf.d/10-auth.conf`" and uncomment the "`disable_plaintext_auth = yes`" line
On the same line **replace yes by no**. Then restart the service "`sudo /etc/init.d/dovecot restart`"
Specify to dovecot the directory where the mails are. Edit "`/etc/dovecot/conf.d/10-mail.conf`" and set the mail_location value like below

```
mail_location = maildir:~/Maildir
```

Restart the service "`sudo /etc/init.d/dovecot restart`"

Don't forget to create your MX / A Record to locate your mail server:

YourDomain	MX	10	YourServerName

YourServerName A @IP

Configure your mail client with the information you provided.

Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com