DEPLOYMENT GUIDE

BloxOne™ Threat Defense Data Connector

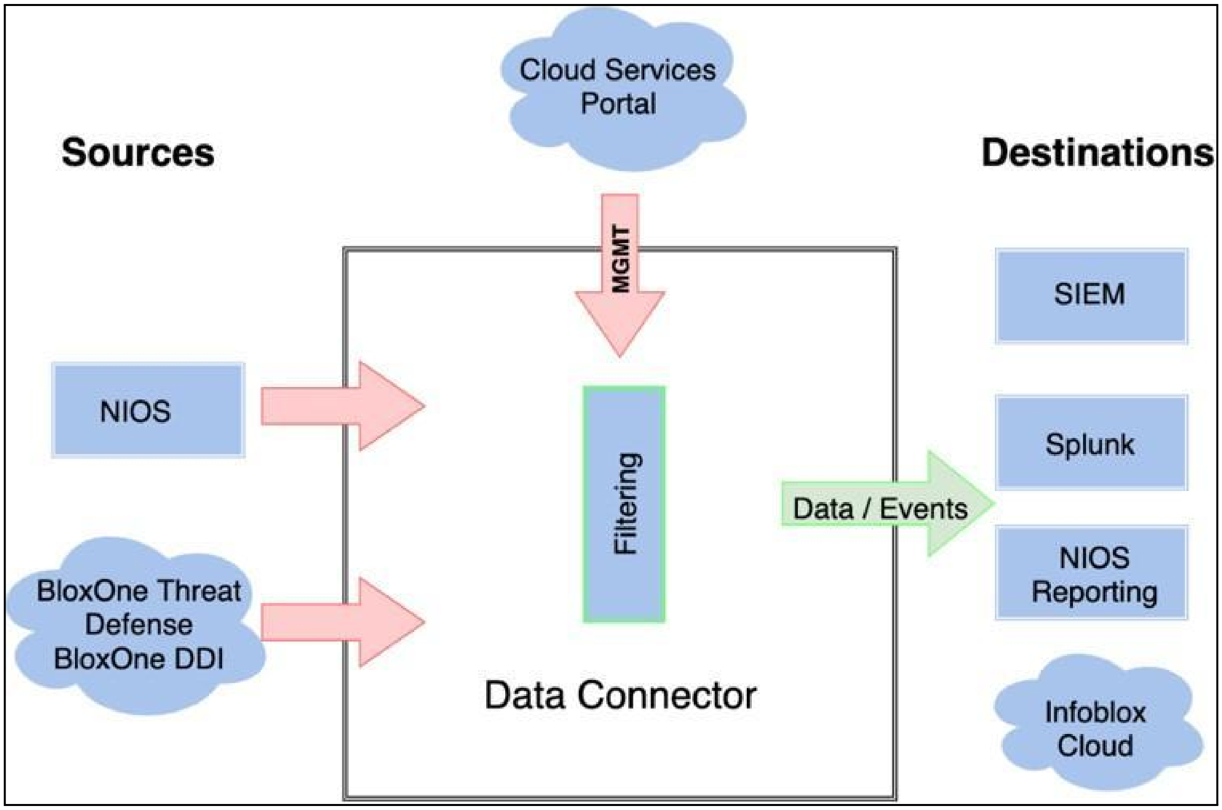
Table of Contents

Overview

The Infoblox cloud managed Data Connector (DC) is a utility designed to collect DNS query and response data and security logs and transfer the data to defined destinations such as the BloxOne Threat Defense Cloud, Infoblox NIOS reporting server, and syslog servers such as a SIEM (Security Information and Event Manager).

The Data Connector's filtered source data is based on user criteria (thus reducing data quantity) and converts the data to a format that can be securely transferred and easily consumed by supported destinations. The Data Connector acts as a central point for data collection across your devices, which reduces the impact of data exchange and improves your Grid performance If NIOS Grid is configured as a source.

The following illustration describes the basic concept of the data collection process, which includes collecting supported data from NIOS or BloxOne Threat Defense Cloud, filtering and storing the data, and sending the data to the supported destinations.



Prerequisites

BloxOne Host

The Data Connector requires a BloxOne host to be tethered with. Prior to following steps in this guide you will need to deploy a host that meets minimum requirements, including a 750 GB disk. For details on requirements and deployment options, refer to BloxOne documentation.

Licensing

One of the following licenses/subscriptions is required to use Data Connector:

- BloxOne Threat Defense Advanced
- BloxOne Threat Defense Business – Cloud
- BloxOne Threat Defense Business – On Premise
- Security Ecosystem Business

System Requirements and Port Usage

BloxOne host with necessary ports opened for inbound and outbound access depending on services used as well as minimum system requirements (here).

Syslog Requirements

Ensure that the following are configured for a secure transport for forwarding data to a syslog destination:

You may configure a syslog tool to secure TCP communication using TLS. This is mandatory for encrypted communication.

Configure server certificates so that the Data Connector can forward DNS queries and responses to the configured syslog tool. *Note that the server certificates must be self-signed or signed by CA authorities. You can retrieve these from your syslog tools. For more information, refer to the respective syslog tool documentation.*

Generate and install a self-signed certificate

A self-signed certificate is not the only option available however it will be useful for quickly getting started. This self signed certificate will be used further in NIOS Grid Manager and while configuring the Source in Data Connector in the cloud services portal. The pem file will be used in Data Connector **Source Configuration** for RPZ logs. In order to generate and install a self-signed certificate perform the following:

1. Create CA certificates by performing the following command:

```
openssl req - ×509 sha256 - days 365 nodes newkey rsa:2048
subj "/C=IN/ST=KA/L=Bglr/0=Infoblox/OU=Cloud/CN=*"
keyout rootCA.key -out rootA.crt
```

2. Create a key and a certificate signing request:

```
openssl reg batch -new -newkey rsa: 2048 nodes -kevout server.key
out rpz.csr -subj " /C=IN/ST=KA/L=Bglr /0=Infoblox /OU=SAAS /CN=*"
```

3. Create a server certificate by signing it with the CA:

```
openssl x509 -req -in rpz.csr -CA rootCA.crt -CAkey rootCA.key
-CAcreateserial -out server.crt
```

4. Create a new .pem file by copying the server.crt and server.key file contents. Use this new .pem file as a certificate for RPZ logs in the GUI.

```
cat server.crt server.key > rpz.pem
```

5. Use the **rootCA.cert** in the **NIOS** to configure **Secure TCP** and the **rpz.pem** in the source for **Traffic Flow** configuration under Data Connector.

Known Limitations

- You can only assign one destination for every traffic flow you create (see sections “Adding Traffic Flows” and “Adding destinations” for more information on traffic flows and destinations).

Best Practices

For the successful deployment of a Data Connector consider the following best practices:

- If you need to change the IP address of the host after the configuration, you must restart the system for the change to take effect.
- For the Data Connector service to function properly in OVA deployments on ESXi servers, ensure that you specify the NTP server during deployment. If you do not specify the NTP server, ensure that you open the UDP 123 port for time synchronization with the Ubuntu NTP servers.
- If you need to re-deploy a Data Connector service as a container on the same host, you must manually clean up the /Infoblox directory on the host before re-deploying Data Connector.
- Infoblox recommends that customers should use the list of publicly used IP's found on the Data Connector Admin guide to determine the needed access to the internet.
- Before you deploy the Data Connector, ensure that the host that you intend to attach the Data Connector service to meets the minimum system requirements, and has access to the appropriate ports and IPs as specified in the prerequisites section of this guide.
- If the Data Connector is transferring IPAM data from NIOS, to,, enable the NIOS Object Change Tracking feature to reduce the quantity of data transferred. When you enable this feature, the appliance tracks the changes that are made to NIOS objects and periodically synchronizes changed objects.
- The Data Connector VM has two hard disk drives. Hard Disk 2 is used for data storage, and you may substitute it for a larger drive to expand the data storage space

Workflow

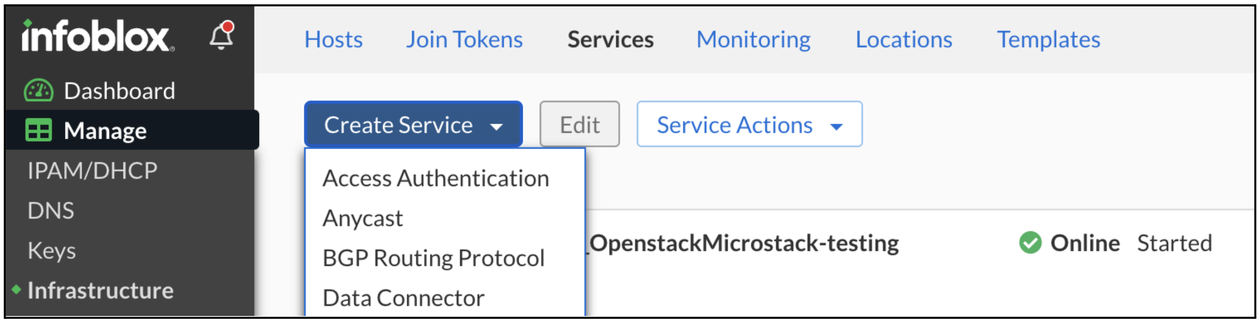
1. Deploy BloxOne host (not covered in this guide).
2. **Navigate** to CSP and **enable** the Data Connector service.
3. Configure Data Connector **Sources**.
4. Configure Data Connector **Destinations**.
5. Configure Data Connector **ETL** (Extract, Transform, Load) filters.
6. Configure Data Connector **Traffic Flows**.

Enable Data Connector Services

This allows the data connector to work on the host. **Do note that the DNS Forwarding Proxy and the Cloud Connector at the same time**.

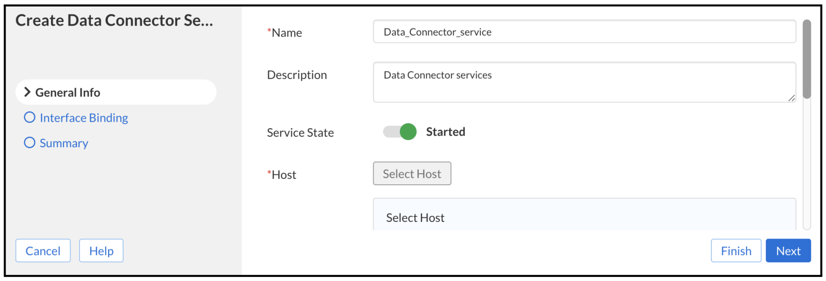
1. Log in to the Cloud Services Portal.

2. Under **Services** tab, click **Create Service** and select **Data Connector**.



3. On the **Create Data Connector Services** enter the following:

   - **Name**: Name for the Data Connector service
   - **(Optional) Description**: If required, input a description.
   - **Service State**: Toggle the switch to enable/disable the service state.
   - **Host**: Select the Host on which the Data Connector service should be running and associated with.



*Name: Data_Connector_service

Description: Data Connector services

Service State: Started

*Host: Select Host

Select Host

4. Click **Finish** and click **Save & Close**.

Configuring Sources

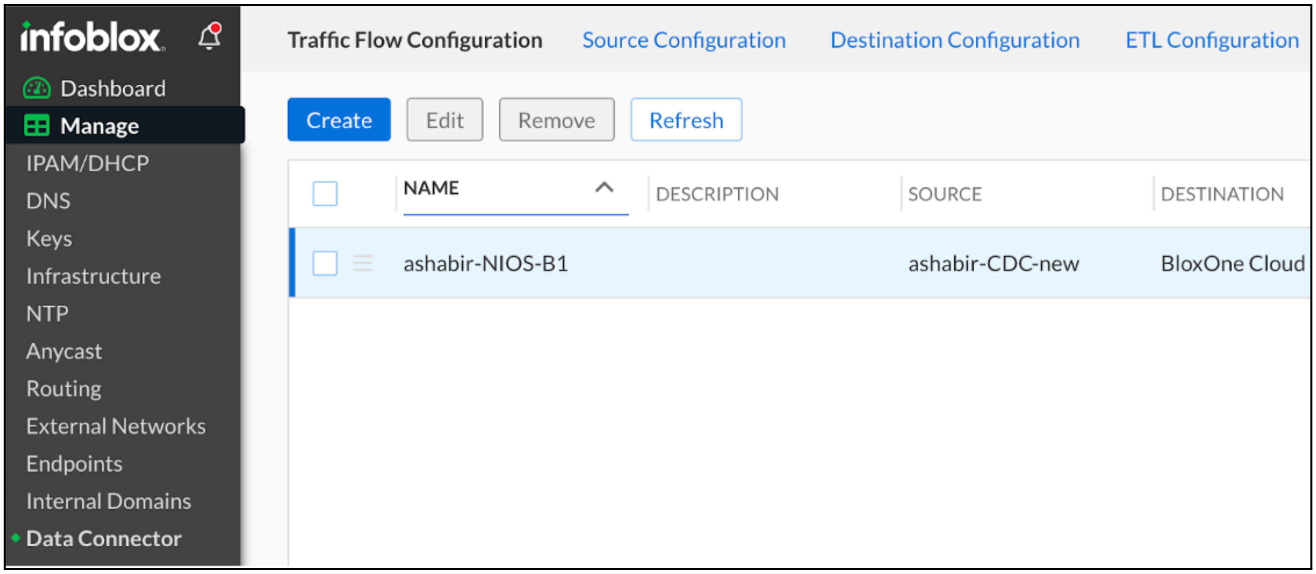
For Data Connector to collect corresponding data and security logs and for traffic flows to function properly, you must set up your sources correctly. Do note that the BloxOne Cloud source is created by default and can't be modified or deleted.

Adding NIOS as a Source

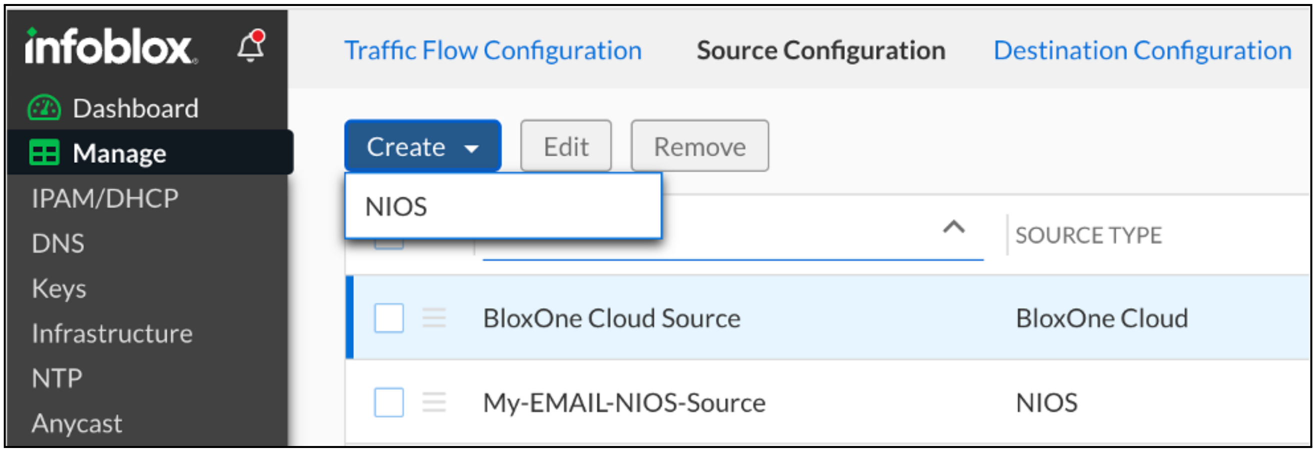
To add NIOS sources for the Data Connector traffic flows, perform the following steps:

1. Log in to the Cloud Services Portal.

2. Click **Manage** → **Data Connector.**



NAME	DESCRIPTION	SOURCE	DESTINATION
ashabir-NIOS-B1		ashabir-CDC-new	BloxOne Cloud



	SOURCE TYPE
BloxOne Cloud Source	BloxOne Cloud
My-EMAIL-NIOS-Source	NIOS

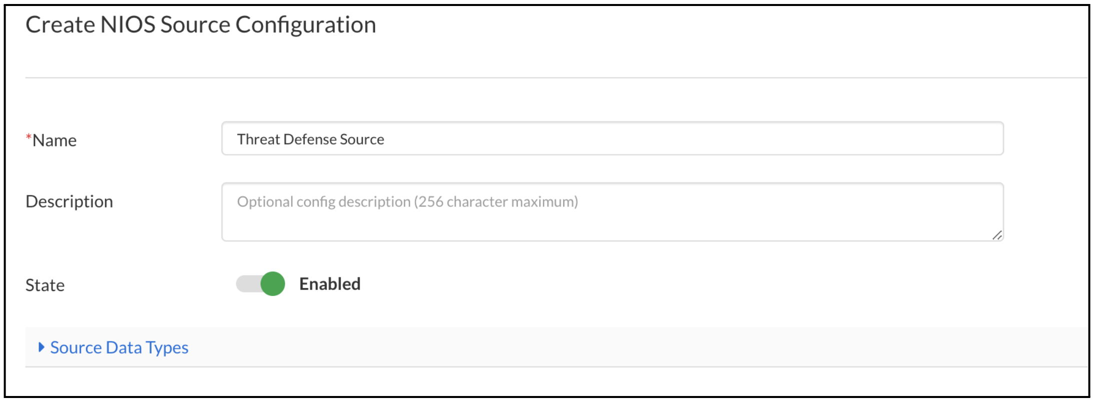
3. Select the **Source Configuration** tab, and then click **Create** and from the Create drop-down list select **NIOS**.

4. In the **Create NIOS Source Configuration** wizard, complete the following:

   ○ **Name**: Enter the name of the source. Select a name that best describes the source, so that you can distinguish this from other sources.

   ○ **Description**: Enter the description of the source. The field length is 256 characters.

   ○ **State**: Use the slider to enable or disable the source configuration. *Note that the source configuration is in effect only when you enable it. If you disable the source configuration, you will not be able to select this source when you create a traffic flow.*

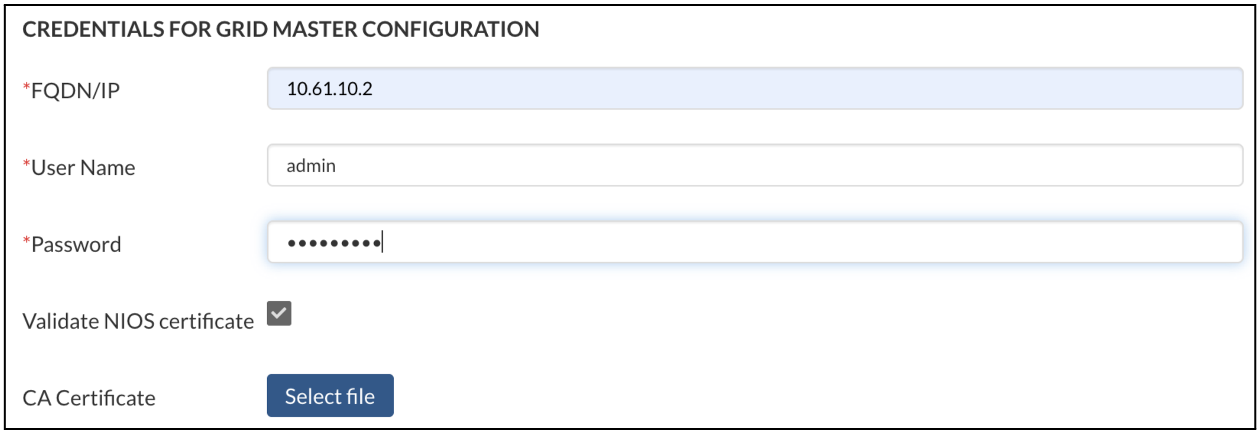


Create NIOS Source Configuration

*Name	Threat Defense Source
Description	Optional config description (256 character maximum)
State	Enabled

- ○ **Expand** the Source Data Type section and select the source data you want the Data Connector to collect from this source.
- ○ In the **CREDENTIALS FOR GRID MASTER CONFIGURATION** section, complete the following:
  - ■ **FQDN/IP**: Enter the FQDN or the IP address of the source.
  - ■ **User Name**: Enter the user name for the source credentials. The Data Connector uses this entry to access the source appliance.
  - ■ **Password**: Enter the password for the source credentials. The Data Connector uses this entry to access the source appliance.
  - ■ **Insecure Mode**: This is selected by default if you do not upload a CA certificate. When this checkbox is selected, Data Connector uses basic authentication using the user name and password you entered. However, if you do not upload a CA certificate, your certificate will not be validated.

5. **CA Certificate**: Click Select file to upload the CA-signed certificate for the NIOS appliance. When you upload a valid CA certificate, Data Connector uses the basic authentication using the credentials, plus the certificate you uploaded to secure the connection.

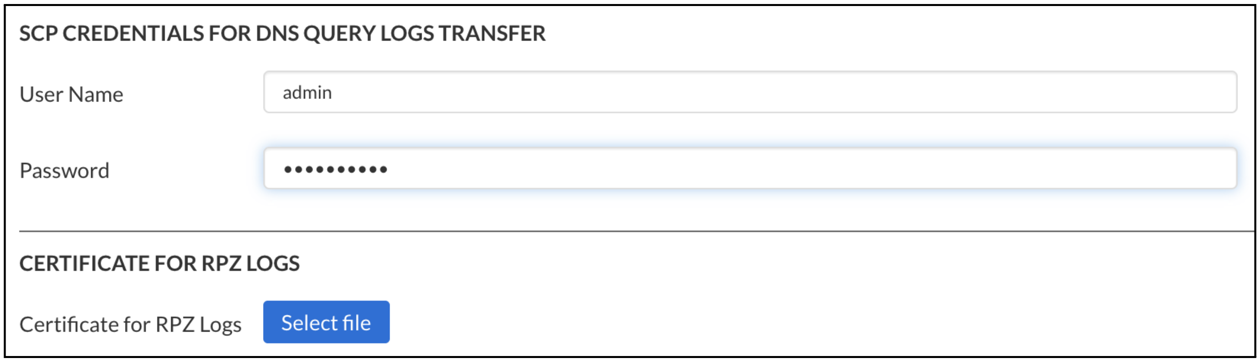


CREDENTIALS FOR GRID MASTER CONFIGURATION

*FQDN/IP	10.61.10.2
*User Name	admin
*Password	•••••••••
Validate NIOS certificate	☑
CA Certificate	Select file

- To allow query and response log data transfer, you must allow access for the Data Connector to collect this data through SCP. In the SCP CREDENTIALS FOR DNS QUERY LOGS TRANSFER section, complete the following:
    - **User Name**: Enter the user name used to access the SCP server. The Data Connector uses SCP to communicate with the source.
    - **Password**: Enter the password for the SCP server.

6. If you select RPZ Logs as the source data type, you must upload the security certificate for the Data Connector to access the RPZ logs. In the CERTIFICATE FOR RPZ LOGS section, complete the following:
    - **Certificate** for RPZ Logs: Click **Select** file and navigate to the RPZ certificate to upload. This is the self signed certificate (.pem file) that we created earlier.



SCP CREDENTIALS FOR DNS QUERY LOGS TRANSFER

User Name: admin

Password: •••••••••••

CERTIFICATE FOR RPZ LOGS

Certificate for RPZ Logs: Select file

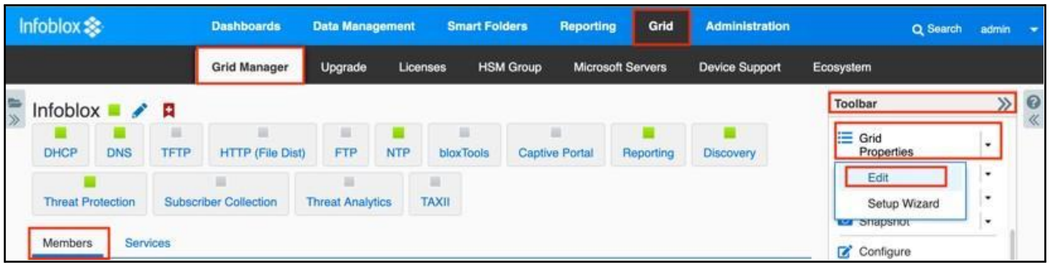
Configuring NIOS to communicate with Data Connector

Before capturing DNS query and response data from the Infoblox Grid, the Infoblox Grid must be configured to allow the Data Connector to collect DNS data from the respective Grid members. Additionally, the Data Connector must be configured to send the data to designated destinations. This section walks you through these procedures:

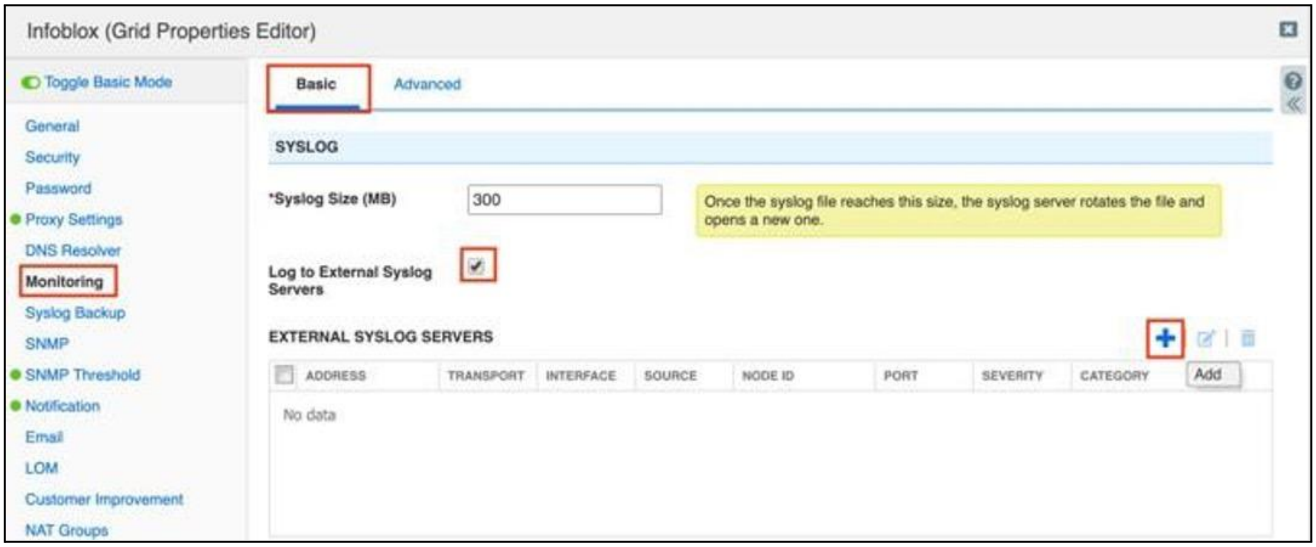
DNS Firewall (RPZ) logs

1. Log in to the Grid Master.

2. Navigate to **Grid** → **Grid Manager** → **Members** → Expand the **Toolbar** → **Grid Properties** → **Edit**.



3. In the **Grid Properties** editor select **Monitoring**. Under the **Basic** tab select the Log to External Syslog Servers check box, click the **Add** icon.



*Syslog Size (MB): 300

Once the syslog file reaches this size, the syslog server rotates the file and opens a new one.

Log to External Syslog Servers ☑

□	ADDRESS	TRANSPORT	INTERFACE	SOURCE	NODE ID	PORT	SEVERITY	CATEGORY
No data								

4. When adding the External Syslog Server endpoint make sure to specify the **IP address** of the Host that the Data Connector is associated with, and select Secure TCP or TCP as the Transport option. When selecting Secure TCP, upload the **server.crt** certificate file created earlier.

5. **Restart** services if requested.

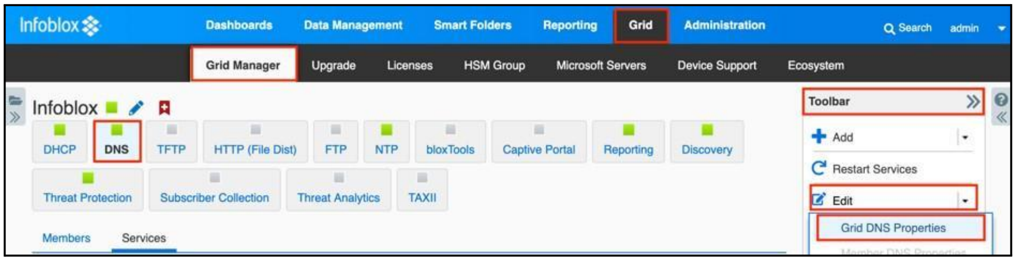
DNS Query/Response logs

1. Edit **Grid DNS Properties**.

2. Navigate to **Grid** → **Grid Manager** → **DNS** → Expand the **Toolbar** → **Edit** → **Grid DNS Properties.**

3. Navigate to **Data Management** → **DNS** → **Members** → **Toolbar** → **Grid DNS Properties.**

4. In the Grid DNS Properties or Member DNS Properties editor, click **Toggle** Advanced Mode and select **Logging** → **Advanced** tab.



5. Under **Data Connection for all DNS Queries/Responses** to a Domain, complete the following:

    - Select the **Capture DNS Queries** check box to start capturing DNS queries. This enables the feature set for configuration. When you enable this option at the member level, the appliance captures DNS queries for the selected members only.
    - Select the **Capture DNS Responses** check box to start capturing DNS responses. This enables the feature set for configuration. When you enable this option at the member level, the appliance captures DNS responses for the selected members only.

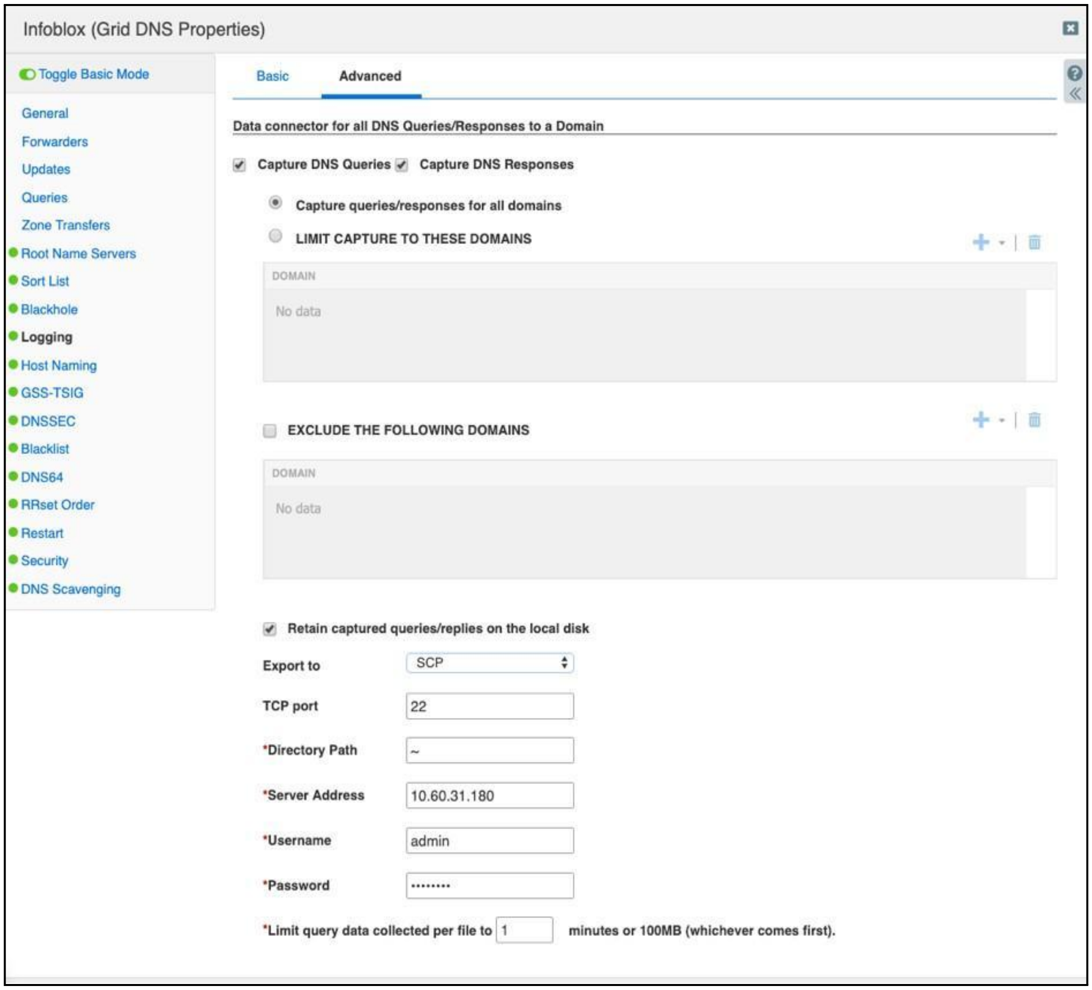
Note: Make sure that only the Query or Response is selected. If needing both the query and the response data then the response should be selected as it contains both the query and the response.

- Select **Capture queries/responses for all domains** to capture queries and responses to all domains and zones.
- Select **Limit capture to these domains** to capture DNS queries and responses to domains and zones one at a time.
- Specify **domains** for DNS capture operations in the Domain table by clicking the **Add** icon and choosing **Add Domain or Bulk Add Domains** from the menu.
- Retain captured queries on the local disk: **Select** this check box to save the DNS queries on the appliance.
- **Export** to: From the drop-down list, select **SCP** to back up the DNS queries on the Data Connector and None to save queries only on the appliance. To save the captured DNS queries on both the appliance and the Data Connector, select the **Retain captured queries on the local disk** check box and **SCP** from the Export to drop-down list. To define the destination for capture files, perform the following:

When you select **SCP** from the **Export to** drop-down list, complete the following:

- In the **Directory Path** field, enter the directory to which the capture file will be saved on the server.Use the ~ symbol for the Data Connector.
- In the **Server Address** field, enter the IP address of the BloxOne host that the Data Connector is associated with.
- Enter the **Username** and **Password** values that were input in the CSP when creating the NIOS source.
- Limit query data collected per file to minutes or 100MB (whichever comes first).

Note, this option limits the collection of query data per capture file. A capture file for logging DNS queries and responses is rolled over based on the configured time limit or when the file reaches 100 MB in size, whichever is sooner. The default time limit is 10 minutes. You can enter a value from 1 to 10.



Infoblox (Grid DNS Properties)

Data connector for all DNS Queries/Responses to a Domain

☑ Capture DNS Queries ☑ Capture DNS Responses

● Capture queries/responses for all domains

○ LIMIT CAPTURE TO THESE DOMAINS

DOMAIN
No data

□ EXCLUDE THE FOLLOWING DOMAINS

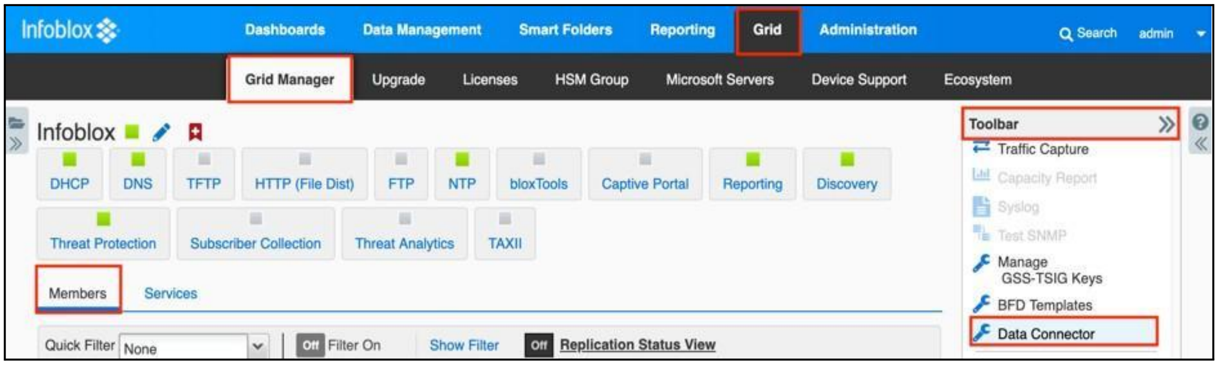
DOMAIN
No data

☑ Retain captured queries/replies on the local disk

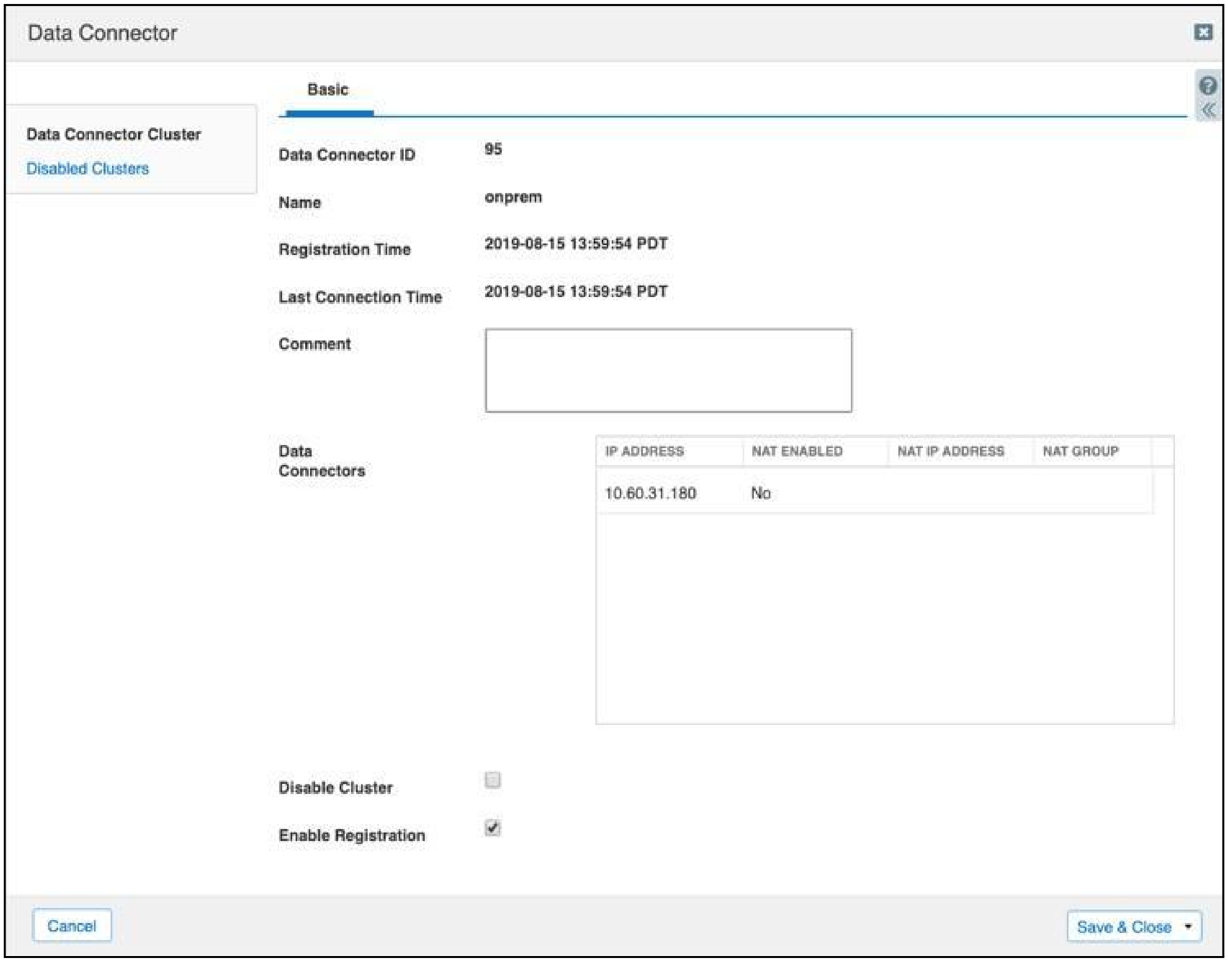
Export to	SCP
TCP port	22
*Directory Path	~
*Server Address	10.60.31.180
*Username	admin
*Password	••••••••

*Limit query data collected per file to 1 minutes or 100MB (whichever comes first).

6. **Save** the configuration.
7. **Restart** services if requested.
8. Navigate to **Grid** → **Grid Manager** → **Members** and click **Data Connector** from the Toolbar.



9. In the **Data Connector** editor, you can view the details of the registered Data Connector VM in the Data Connector Cluster tab.



Data Connector ID 95

Name onprem

Registration Time 2019-08-15 13:59:54 PDT

Last Connection Time 2019-08-15 13:59:54 PDT

Comment

Data Connectors

IP ADDRESS	NAT ENABLED	NAT IP ADDRESS	NAT GROUP
10.60.31.180	No		

Disable Cluster ☐

Enable Registration ☑

10. The appliance displays the following information in the Data Connector VMs editor:

    ○ **Cluster Unique ID**: The unique ID of the Data Connector VM.
    ○ **Name**: The name of the Data Connector VM
    ○ **Registration Time**: The timestamp when the Data Connector VM was initially registered with the Infoblox Grid.
    ○ **Last Activation Time**: The timestamp when the Data Connector last contacted the Infoblox Grid.
    ○ **Comment**: Displays additional information about the Data Connector.
    ○ **VMs in Cluster**: Displays the following information:
    ○ **VM IP Address**: Displays the IP address of the Data Connector VM.
    ○ **NAT Enabled**: Not supported in this release.
    ○ **NAT IP Address**: Not supported in this release.
    ○ **NAT Group**: Not supported in this release.
    ○ **Disable Cluster**: Indicates whether this Data Connector VM should be deleted and moved to the list of deleted clusters so you can allow another Data Connector VM to register with the Grid.

IPAM Meta data pooling

1. Navigate to **Grid** → **Grid Manager** → **Members** → **Toolbar** → **Grid Properties** → **Edit**.

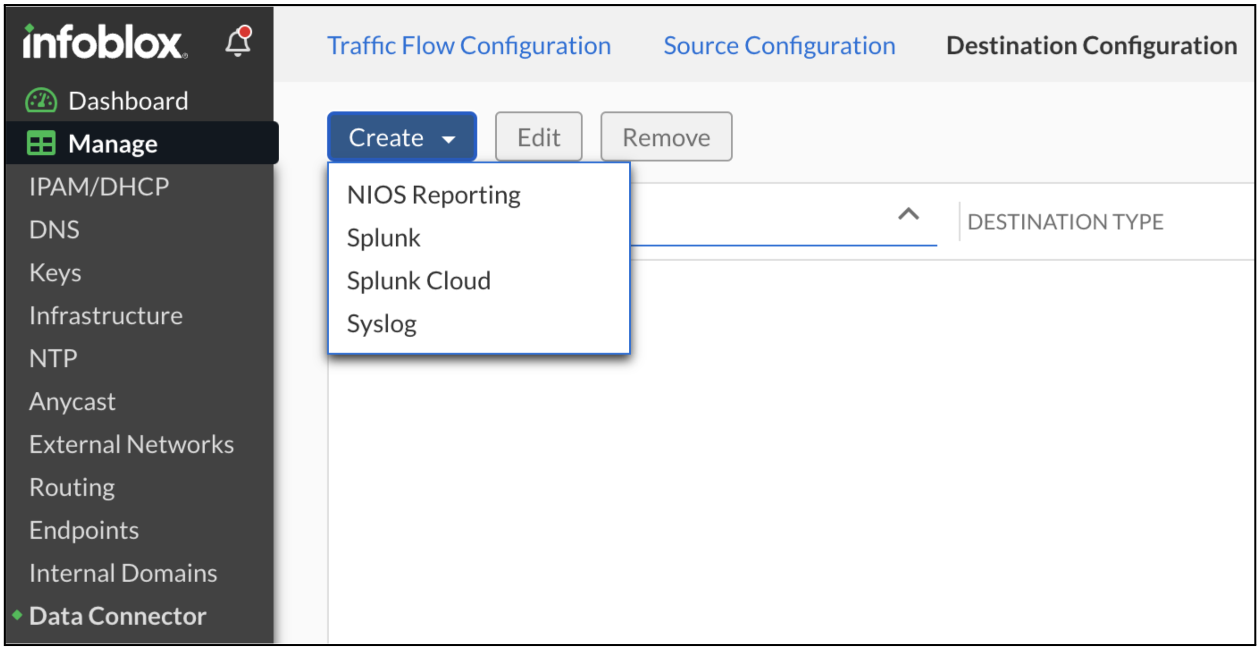
2. Check the **Enable Object Change Tracking** and set the appropriate Maximum time to track deleted objects and the Maximum number of deleted objects that will be tracked according to your needed requirements

Adding Destinations

To add destination for the Data Connector traffic flows, perform the following steps:

1. Log in to the Cloud Services Portal.

2. Click **Manage** → **Data Connector** → **Destination Configuration** tab and click **Create**.



3. From the Create drop-down list, select one of the following:

   - **NIOS Reporting:** To set the NIOS Reporting server as the destination.
   - **Splunk:** To set Splunk as the destination.
   - **Syslog:** To select one of the supported syslog file types to the destination.

4. Depending on your selection, complete the following steps in the **Create Source Configuration** wizard:

NIOS Reporting

- **Name**: Enter the name of the destination. Select a name that best describes the destination and helps you distinguish this from other destinations.

- **Description**: Enter the description of the destination. The field length is 256 characters.

- **State**: Use the slider to enable or disable the destination configuration. Note that the destination configuration is in effect only when you enable it. If you disable the destination configuration, you will not be able to select this destination when you create a traffic flow.

- In the NIOS GRID MASTER DETAILS section, complete the following:

  - **FQDN/IP**: Enter the FQDN or the IP address of the Grid Master.
  - **Reporting Appliance Address**: The IP address of the NIOS Reporting server.
  - **User Name**: Enter the user name for the Grid Master. The Data Connector uses this entry to access the appliance.
  - **Password**: Enter the password for the Grid Master. The Data Connector uses this entry to access the appliance.

Splunk

- **Name**: Enter the name of the destination. Select a name that best describes the destination and helps you distinguish this from other destinations.

- **Description**: Enter the description of the destination. The field length is 256 characters.

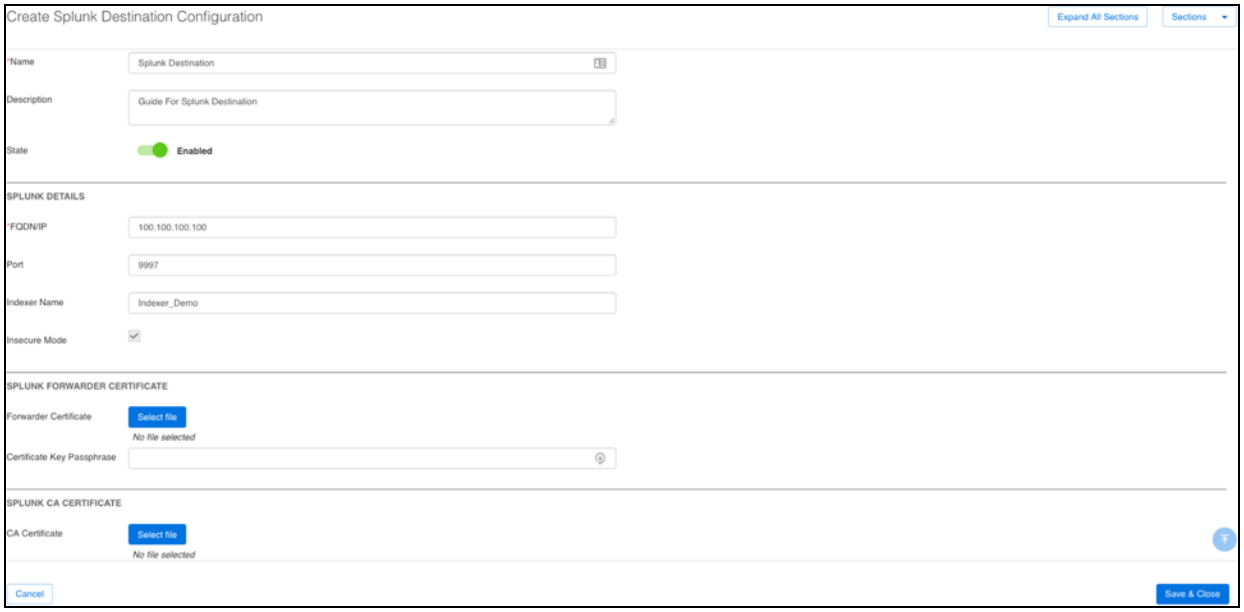
- **State**: Use the slider to enable or disable the destination configuration. Note that the destination configuration is in effect only when you enable it. If you disable the destination configuration, you will not be able to select this destination when you create a traffic flow.

- In the **SPLUNK DETAILS** section, complete the following:

  - **FQDN/IP**: Enter the FQDN or the IP address of the Splunk indexer to which you want the Data Connector to send data.
  - **Port**: Enter the port number (between 1 and 65536) to reach the Splunk indexer.
  - **Indexer Name**: The name of the Splunk index.
  - **Insecure Mode**: Selected by default to use a secure transport (TLS) for the data. Otherwise, complete the following sections to upload certificates for secure transport
  - In the **SPLUNK FORWARDING CERTIFICATE** section, complete the following:
    - **Forwarder Certificate**: Click Select file to upload the forwarder certificate on the Splunk forwarder. You need to first generate a certificate request in ".PEM" format. This certificate request must be signed by the third-party Certification Authority for you to get a forwarder certificate.

    - **Certificate Key Passphrase**: Enter the key passphrase for the certificate.

- In the **SPLUNK CA CERTIFICATE** section, complete the following:



Create Splunk Destination Configuration

*Name	Splunk Destination
Description	Guide For Splunk Destination
State	Enabled

SPLUNK DETAILS

*FQDN/IP	100.100.100.100
Port	9997
Indexer Name	Indexer_Demo
Insecure Mode	☑

SPLUNK FORWARDER CERTIFICATE

Forwarder Certificate	Select file *No file selected*
Certificate Key Passphrase	

SPLUNK CA CERTIFICATE

CA Certificate	Select file *No file selected*

- **CA Certificate**: Click Select file to upload the CA signed certificate on the Splunk indexer.

Syslog

- **Name**: Enter the name of the destination. Select a name that best describes the destination and helps you distinguish this from other destinations.

- **Description**: Enter the description of the destination. The field length is 256 characters.

- **State**: Use the slider to enable or disable the destination configuration. Note that the destination configuration is in effect only when you enable it. If you disable the destination configuration, you will not be able to select this destination when you create a traffic flow.

- **Format**: From the drop-down list, select the Syslog format type you want to configure as the destination.

- In the **SYSLOG DETAILS** section, complete the following:

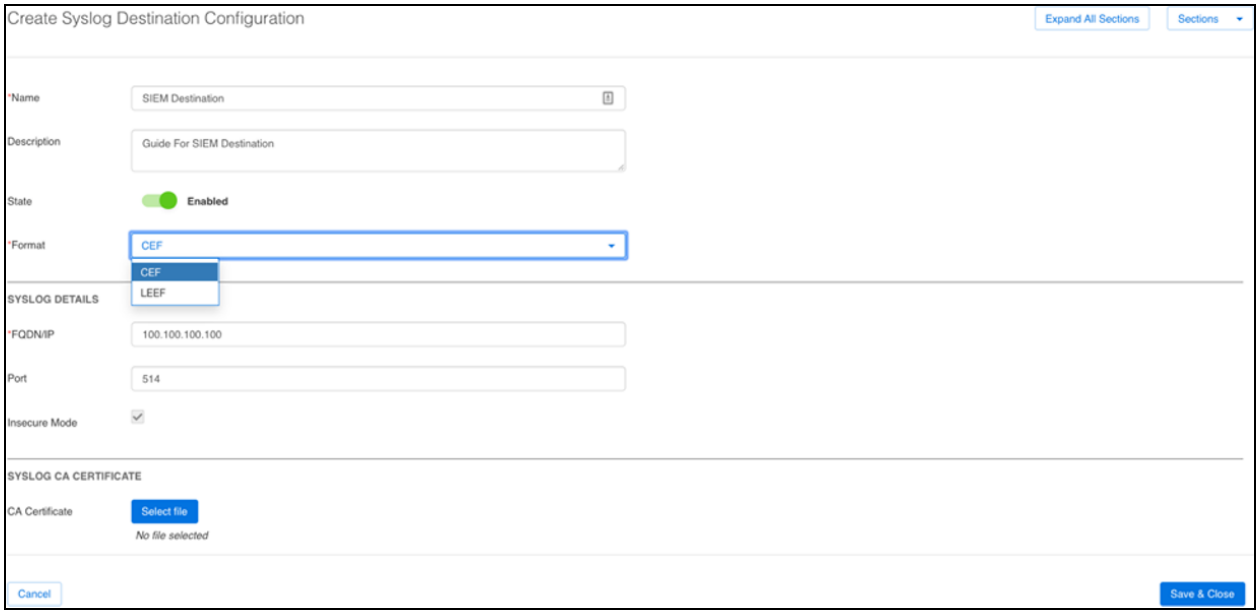
  - **FQDN/IP**: Enter the FQDN or the IP address of the syslog tool to which you want the Data Connector to send data.

  - **Port**: Enter the port number (between 1 and 65536) to reach the syslog tool.

  - **Insecure Mode**: Selected by default to use a secure transport (TLS) for the data. Otherwise, complete the following sections to upload certificates for secure transport.

- In the **SYSLOG CA CERTIFICATE** section, complete the following:

  - **CA Certificate**: Click Select file to locate the CA certificate from the syslog tool and upload it.



*Name: SIEM Destination
Description: Guide For SIEM Destination
State: Enabled
*Format: CEF

SYSLOG DETAILS
*FQDN/IP: 100.100.100.100
Port: 514
Insecure Mode: ☑

SYSLOG CA CERTIFICATE
CA Certificate: *No file selected*

BloxOne Cloud Destination

- By default, BloxOne Cloud Destination is pre-configured as the destination. No configuration is required on your part.

ETL Filters

ETL (Extract, Transform, Load) filters are used to exclude specific information, and the unfiltered data will be transferred to the configured destinations. Organizations can set up ETL configurations using regex for Grid member names as well as IP/Network, or FQDN's which will apply the ETL configurations to the traffic flow configurations.

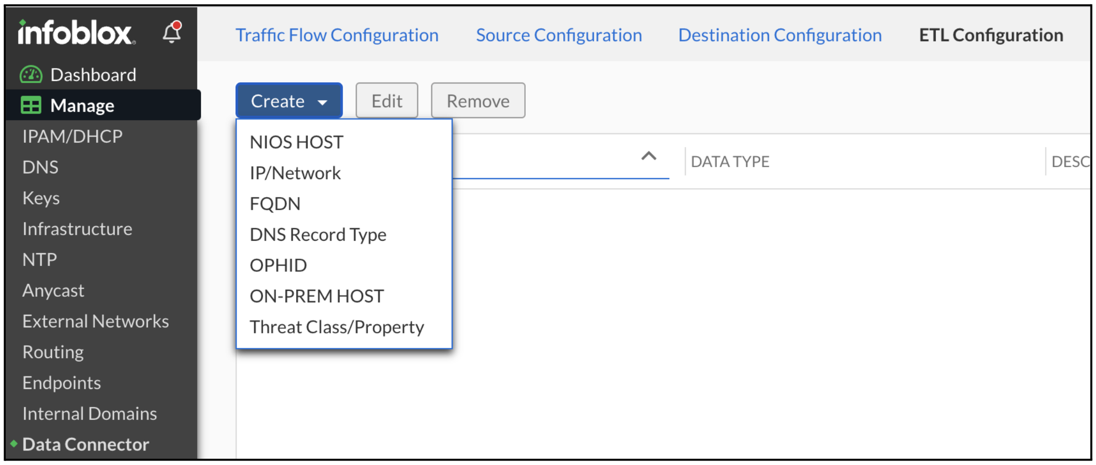
Adding ETL Configuration

To create data filters for your source data, perform the following steps:

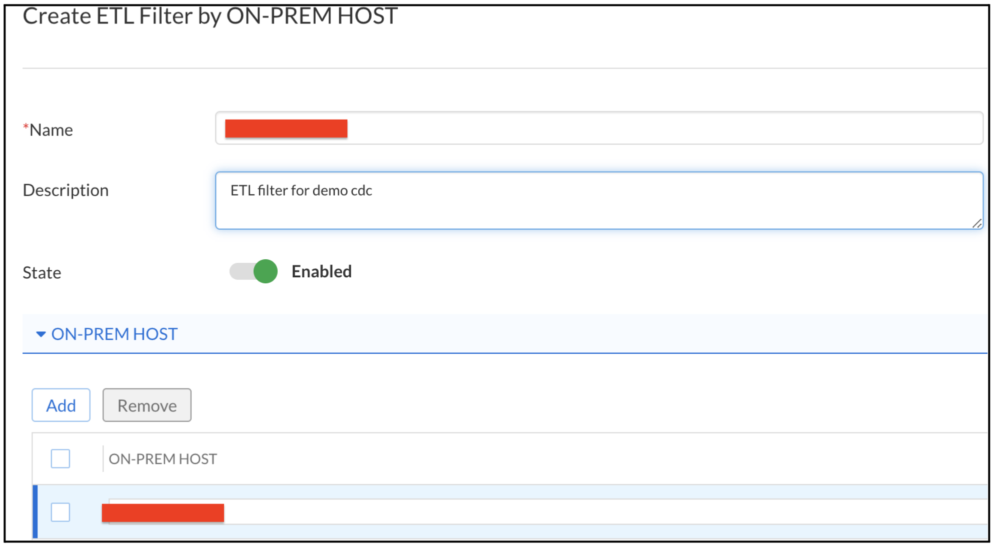
- Navigate to **Manage** → **Data Connector** → **ETL Configuration** tab and click **Create.**

- From the **Create** drop-down list, select the filtering criterion for the ETL configuration. You can select one of the following:
    - NIOS HOST
    - IP/Network
    - FQDN
    - DNS Record type
    - OPHID

- ON-PREM-HOST
- Threat Class/Property



- Depending on your selection, complete the following steps in the Create ETL Filter wizard and then click **Save & Close**:
    - **Name**: Enter the name of the ETL configuration. Select a name that best describes the filter.
    - **Description**: Enter the description of the ETL configuration. The field length is 256 characters.
    - **State**: Use the slider to enable or disable the ETL configuration. Note that the ETL configuration is in effect only when you enable it. If you disable the configuration, the ETL filter is not in effect even if you have applied the ETL configuration to a traffic flow configuration.
    - Expand the **NIOS HOST**, **IP/Network**, or **FQDN** section, then click **Add** to the applicable parameters.



*Name [redacted]

Description: ETL filter for demo cdc

State: Enabled

[redacted]

        - **IP/Network**: The IP/Network filter applies to DNS query/response events, IP metadata, and RPZ events. You can specify the query source IP address when the event is a query and the destination IP address when the event is a response. You can specify the client_ip filter in the following format in CIDR block e.g. 10.10.0.1/15, 2001:cdba:9abc:5678::/64, etc.

        - **FQDN**: The FQDN filter applies to DNS query/response events and RPZ events. A query filter is a combination of valid FQDN and wildcards.

Note the following about wildcards:

- You can specify a wildcard either on the left or on the right side of the domain name.

- A rule can have either 0, 1, or 2 wildcards.

- If a rule has 2 wildcards, they have to be on the opposite ends of the FQDN.

- A wildcard on the left side must be followed by a dot (.), except for the '?' wildcard.

- A wildcard on the right side must be preceded by a dot (.) except for the '?' wildcard.

List of supported wildcards

Wildcard	Description	Example
*	Applicable for zero or more domain name labels. It can be specified only on the left side of the domain name.	*.foo.com
#	Applicable for one or more domain name labels. It can be specified only on the left side of the domain name.	#.foo.com
?	For exactly one domain name label. It can be specified either on the left or right side of the domain name.	?.foo.com ? ?. corp.?.

Viewing ETL Configuration

To view all the ETL configurations, perform the following step:

1. Navigate to **Manage** → **Data Connector** → **ETL Configuration** tab and the Cloud Services Portal displays the following for all the ETL configurations:

    - **Name**: The name of the ETL configuration.

    - **Data Type**: The filter criterion for the ETL process.

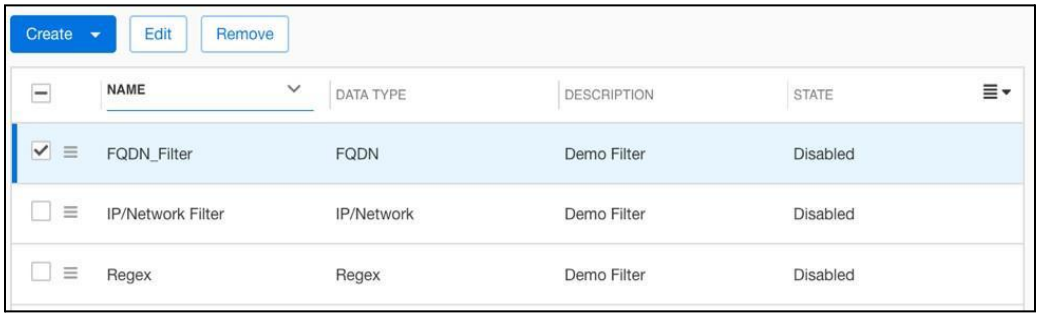
- **Description**: The information about the ETL configuration.

- **State**: Describes whether the configuration is Enabled or Disabled.

Deleting ETL Configurations

To remove an ETL configuration, complete the perform following steps:

2. Navigate to **Manage** → **Data Connector** → **ETL Configuration** tab and select the ETL configuration you want to remove, and then click **Remove**.



	NAME	DATA TYPE	DESCRIPTION	STATE
☑	FQDN_Filter	FQDN	Demo Filter	Disabled
□	IP/Network Filter	IP/Network	Demo Filter	Disabled
□	Regex	Regex	Demo Filter	Disabled

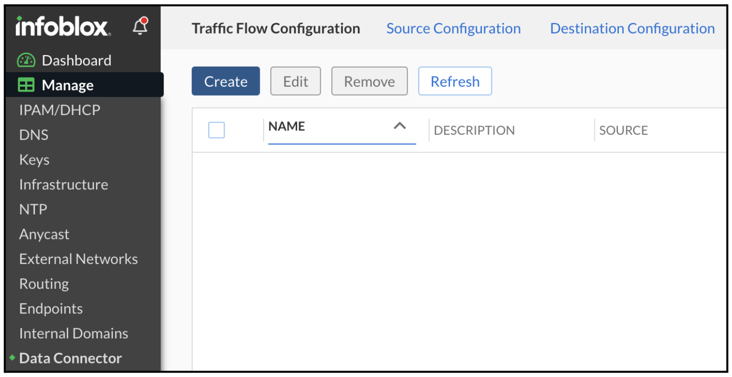
Configuring Traffic Flows

A traffic flow must be configured for the Data Connector to send and receive data. The Data Connector collects data from the defined source and sends that data to the selected destination in the format chosen.

Adding Traffic Flows

To add a new traffic flow for the Data Connector, perform the following steps:

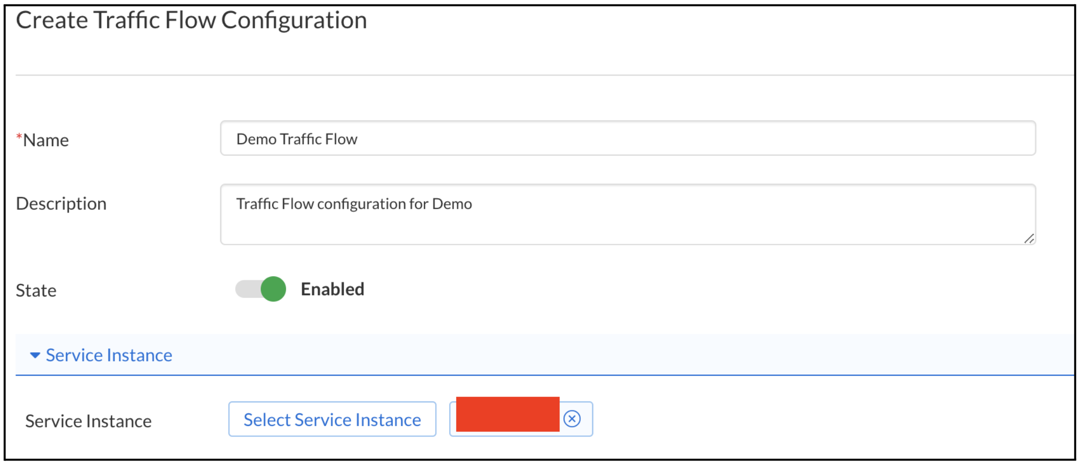
1. Navigate to **Manage** → **Data Connector** → **Traffic Flow Configuration** tab and click **Create**.



2. In the **Create Traffic Flow** Configuration wizard, complete the following:

   - **Name**: Enter a name for this traffic flow configuration.

- **Description**: Enter a description for this configuration to distinguish this Data Connector from other hosts. The maximum length is 256 characters
- **State**: Use the slider to enable or disable this configuration. When the configuration is disabled, no traffic flow happens based on the configuration. You can enable the configuration when you want the Data Connector to start the traffic flow.
- **Service Instance**: Expand this section and select the Data Connector from the BloxOne host list. You must first set up and configure Data Connectors before they appear in this list.



Create Traffic Flow Configuration

*Name: Demo Traffic Flow

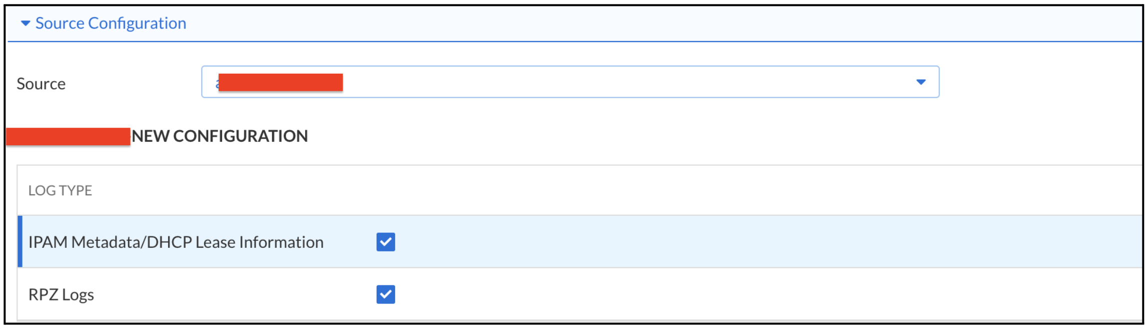
Description: Traffic Flow configuration for Demo

State: Enabled

▾ Service Instance

Service Instance: Select Service Instance [redacted] ⊗

3. Under **SELECT CONFIGURATION**, expand the Source Configuration section, and complete the following:
   - **Source Configuration**: Select the source from which the Data Connector collects. Ensure that you select the correct source for this traffic flow, depending on the source type that you select below.



▾ Source Configuration

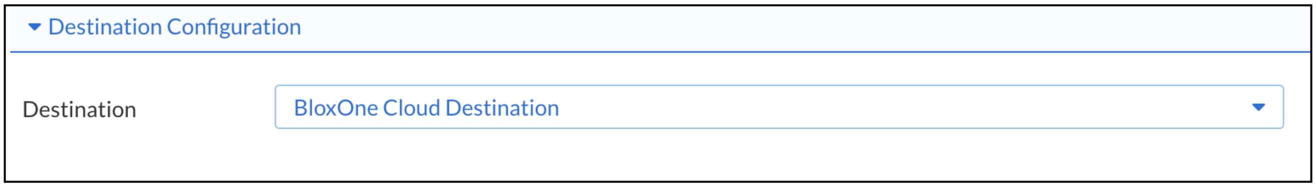
Source: [redacted] ▾

[redacted] NEW CONFIGURATION

LOG TYPE	
IPAM Metadata/DHCP Lease Information	☑
RPZ Logs	☑

   - **Log Type**: Select the type of data you want the Data Connector to collect/receive from the source and pass to a destination. Depending on the source that you have selected and the destination for this traffic flow, the source type varies. For information about the source data type that the Data Connector supports for NIOS and BloxOne Threat Defense Cloud, see the Supported Traffic Flow table in this topic.

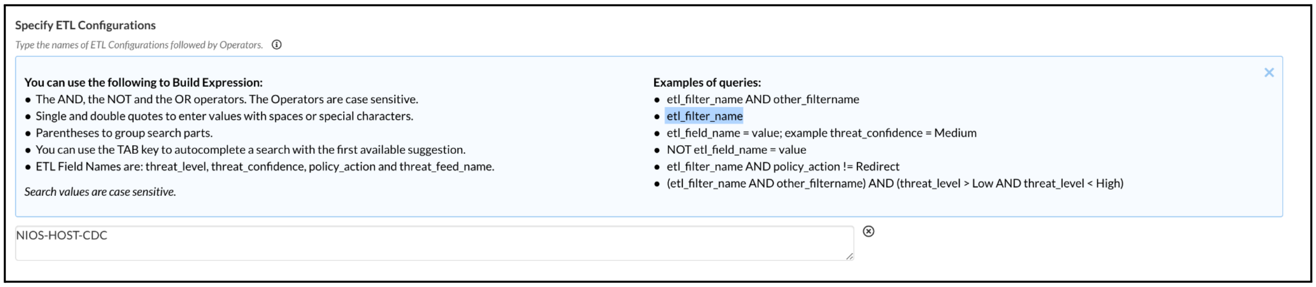
- **Destination Configuration**: Select the corresponding destination that you want the Data Connector to send the source data to. Note that you can send certain data to specific destinations, depending on the supported traffic flow. If you select a different source type or destination, the traffic flow becomes invalid.



Destination Configuration

Destination: BloxOne Cloud Destination

- **ETL Configuration:** In the Filter Expressions field, you can enter one or more ETL configurations. If using more than one configuration, use operators to build the expression. Click the circled **i** icon to open up a panel describing all permitted build expressions along with a list of query examples. For more information, see Performing Filter Search Queries.



Specify ETL Configurations

Type the names of ETL Configurations followed by Operators.

You can use the following to Build Expression:

- The AND, the NOT and the OR operators. The Operators are case sensitive.
- Single and double quotes to enter values with spaces or special characters.
- Parentheses to group search parts.
- You can use the TAB key to autocomplete a search with the first available suggestion.
- ETL Field Names are: threat_level, threat_confidence, policy_action and threat_feed_name.

Search values are case sensitive.

Examples of queries:

- etl_filter_name AND other_filtername
- etl_filter_name
- etl_field_name = value; example threat_confidence = Medium
- NOT etl_field_name = value
- etl_filter_name AND policy_action != Redirect
- (etl_filter_name AND other_filtername) AND (threat_level > Low AND threat_level < High)

NIOS-HOST-CDC

4. Click **Save & Close**.

Supported Traffic Flows

The traffic flows, their data types and the destinations supported can be found here.

infoblox.

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