infoblox. | VendorN
DDI Security and Automation

DEPLOYMENT GUIDE

INFOBLOX NIOS & VENDORN VISION DEPLOYMENT GUIDE

TABLE OF CONTENT

OVERVIEW

Infoblox NIOS and VendorN Vision work together in providing organizations with long-term access to enterprise DNS log history, providing a current unparalleled view into your DNS data and context. Once aggregated, your DNS data can then be fed into your SIEM or SOAR platforms to enhance security operations and improve effectiveness. The VendorN Vision platform drives value from DNS data in a host of ways:

Discover New Connections

Vision has been designed with a “what has changed” philosophy, so new data can be easily identified using simple filtering and sorting.

Prioritize Data

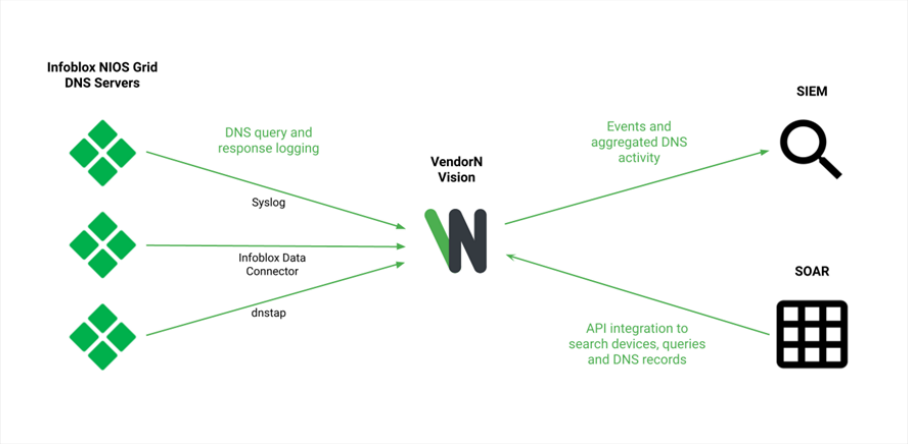
Groups can be created for critical networks and devices so that DNS data and events can be quickly identified and prioritized.

Navigate History

Instantly and easily understand which devices have performed which queries and which records these queries have resolved to.

HOW IT WORKS

Vision receives DNS query and response logs from Infoblox NIOS Grid DNS servers. It aggregates and stores this data while also optionally sending events and aggregated DNS data to an organization’s SIEM. An organization can also use its SOAR and other systems to query the Vision API to access DNS activity history data. When sending data to Vision, NIOS has a comprehensive suite of features which can be used, these are Syslog, the Infoblox data connector and DNSTAP:



The CONFIGURATION section contains a sub-section documenting how each of these methods are configured in the Infoblox NIOS platform.

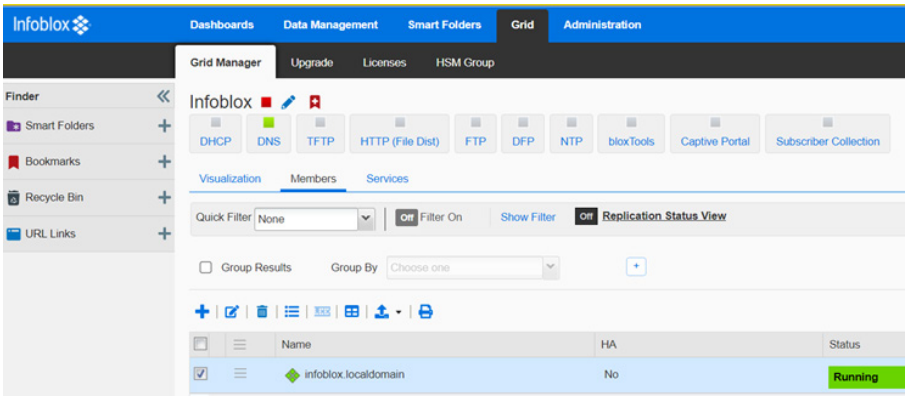
CONFIGURATION

SYSLOG

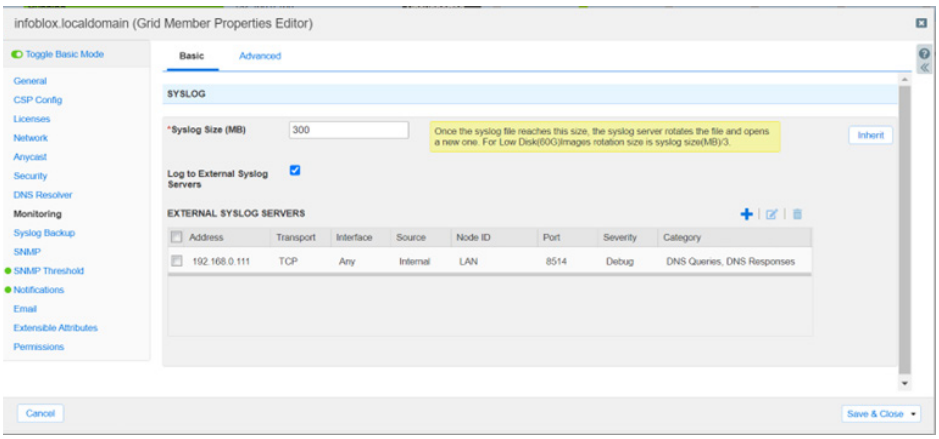
With the Syslog method, NIOS Grid DNS servers are configured to forward their Syslogs to a Vision Sensor. Note: Query and response logging must be enabled on the DNS servers.

To configure the Syslog method in Infoblox NIOS use the following steps:

1. Once the Infoblox NIOS user interface has been accessed, navigate to the Grid / Grid Manager / Members page:

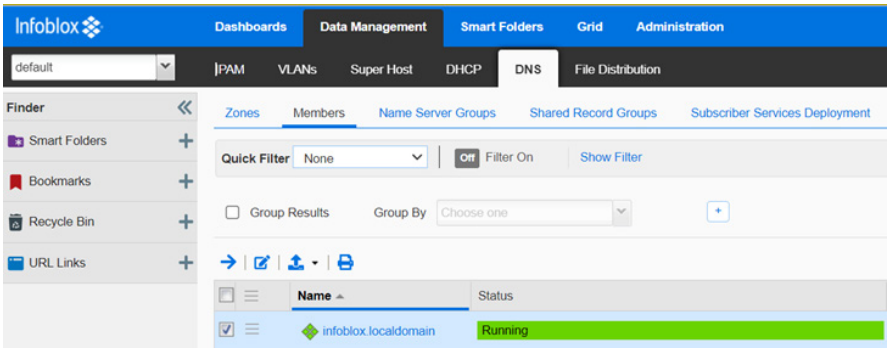


2. Select a member and click the “edit” button displayed in the table toolbar to edit the member properties:

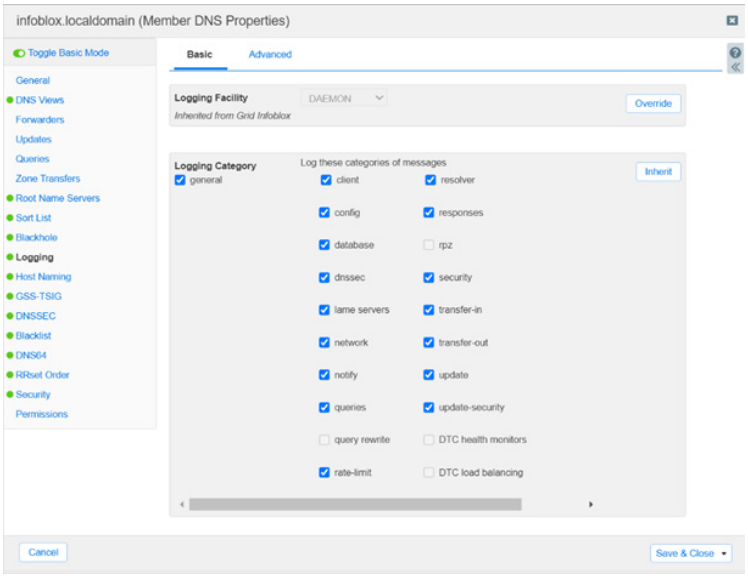


3. Under the Monitoring / Basic tab make the following changes and save and close the dialog:
   a. Check the “Log to External Syslog Servers” checkbox.
   b. Add a Vision Sensor under the “EXTERNAL SYSLOG SERVERS” table, ensuring TCP port 8514 is specified and ensure “Category” is set to “DNS Queries” and “DNS Responses”.

4. Next, navigate to the Data Management / DNS / Members page:



5. Select a member and click the “edit” button displayed in the table toolbar to edit the member DNS properties:



6. Under the Logging / Basic tab make the following changes and then save and close the dialog:
   a. Check the “queries” checkbox.
   b. Check the “responses” checkbox.
7. Once saved, a service restart of the DNS server will be required for the changes to take effect.

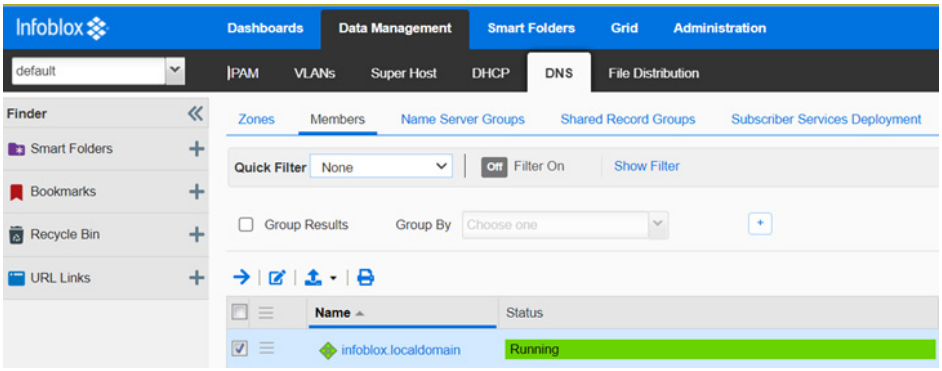
Following this, NIOS Grid DNS servers will log query and response messages to their local Syslog which is then forwarded to the Vision Sensor in real-time.

INFOBLOX DATA CONNECTOR

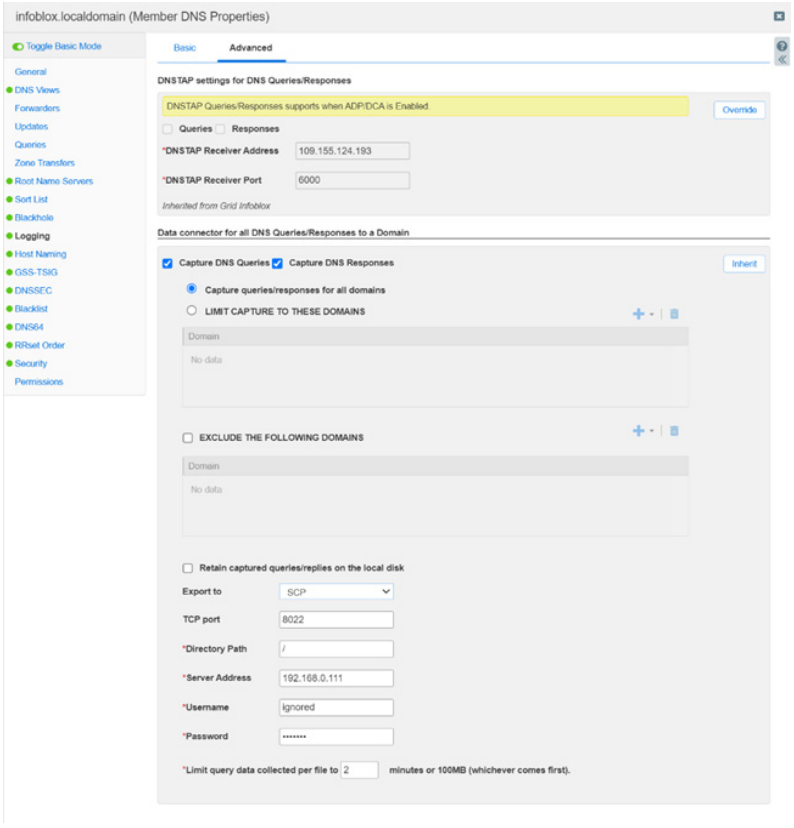
With the Infoblox Data Connector method, NIOS Grid DNS servers are configured to periodically send files to a Vision Sensor which contain similar query and response messages to the Syslog method but using SCP.

To configure the Infoblox Data Connector method in Infoblox NIOS use the following steps:

1. Once the Infoblox NIOS user interface has been accessed, navigate to the Data Management / DNS / Members page:



2. Select a member and click the “edit” button displayed in the table toolbar to edit the member DNS properties:



3. Under the Logging / Advanced tab, make the following changes and then save and close the dialog:
    a. Check the “Capture DNS Queries” checkbox.
    b. Check the “Capture DNS Responses” checkbox.
    c. Check the “Capture queries/responses for all domains” radio button.
    d. Uncheck the “Retain captured queries/replies to the local disk” checkbox.
    e. Set “Export to” to “SCP”.
    f. Set “TCP port” to “8022”.
    g. Set “Directory Path” to “/”.
    h. Set “Server Address” to be the Vision Sensors IP address.
    i. Set “Username” and “Password” to “ignored” – the Vision Sensor will refuse connections from devices it has not been configured with, the username and password specified is ignored by the sensor.
4. Once saved, a service restart of the DNS server will be required for the changes to take effect.

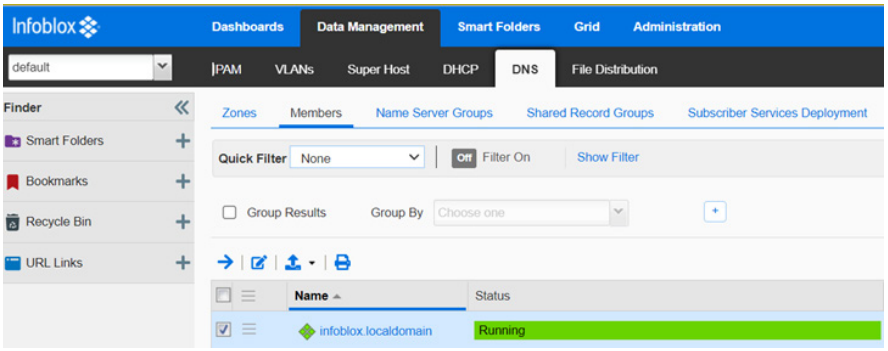
Following this, NIOS Grid DNS servers will log query and response messages to a local file which is then forwarded to a Vision Sensor periodically.

DNSTAP

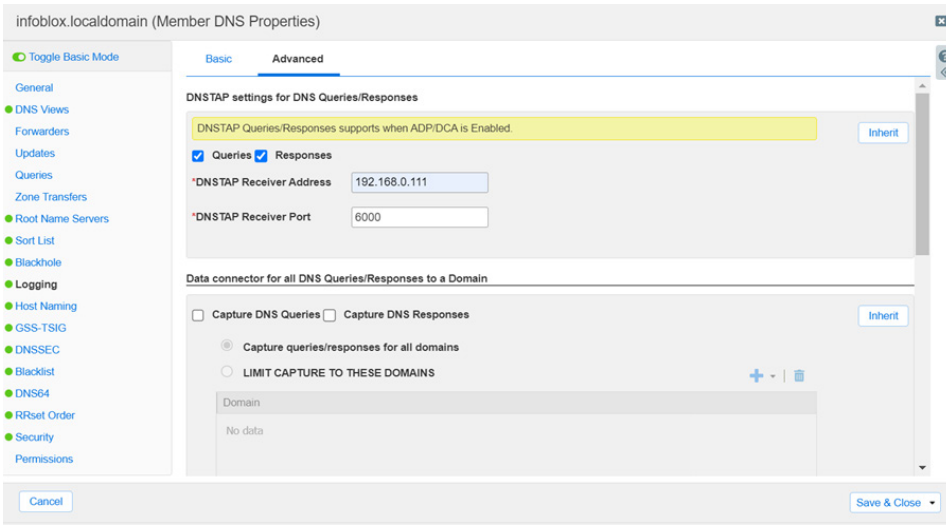
With the dnstap method, NIOS Grid DNS Servers are configured to forward DNS queries and responses to a Vision Sensor using the dnstap protocol.

To configure the dnstap method in Infoblox NIOS, take the following steps:

1. Once the Infoblox NIOS user interface has been accessed navigate to the Data Management / DNS / Members page:



2. Select a member and click the “edit” button displayed in the table toolbar to edit the member DNS properties:



3. Under the Logging / Advanced tab make the following changes and then save and close the dialog:
    a. Check the “Queries” checkbox.
    b. Check the “Responses” checkbox.
    c. Set “DNSTAP Receiver Address” to the Vision Sensors IP address.
    d. Set “DNSTAP Receiver Port” to “6000”.
4. Once saved, a service restart of the DNS server will be required for the changes to take effect.

Following this, NIOS Grid DNS servers will send DNS query and response messages to a Vision Sensor in real-time.

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

Version: 20240322v1