Using Unbound DNS Resolution

You now have the ability to switch between BIND or Unbound resolvers on IB-4030-10GE appliances. Following are a couple scenarios for which you may consider using Unbound DNS resolution:

- To maintain optimum query performance in networks that have lower CHR (Cache Hit Ratio). For more information about CHR, see DNS Statistics for Cache Acceleration.
- To temporarily switch from BIND to Unbound when you encounter an unresolved vulnerability in BIND. Upon resolution of the vulnerability, you can switch back to BIND. For information about how to switch from BIND to Unbound and vice versa, see Configuring DNS Resolver Type.

To use Unbound DNS, you must install the Dual Engine DNS license (in addition to the DNS Cache Acceleration license) on your IB-4030-10GE appliance. Contact your Infoblox representative to obtain these licenses. For information about how to install licenses, refer to the Infoblox NIOS Administrator Guide.

Note: When the Dual Engine DNS license (either temporary or permanent) expires, you will not be able to change the resolver type from Unbound to BIND. You must install a permanent license or extend the current license in order to change the resolver type.

When you use Unbound as the DNS resolver, the appliance acts as a recursive-only name server. Before you use Unbound DNS resolution, ensure that you understand some of the limitations and ramifications. For more information, see Best Practices for Configuring Unbound DNS.

Best Practices for Configuring Unbound DNS

Following are some guidelines for consideration before you use Unbound as the DNS resolver:

- When you configure your IB-4030-10GE to use Unbound DNS, it acts as a recursive-only name server and some of the NIOS features are not supported. For a list of unsupported features, see Unsupported NIOS Features for Unbound DNS.
- In general, for all unsupported NIOS features for Unbound DNS, their corresponding functions and tabs do not appear in Grid Manager. However, this might not hold true in a Grid when Unbound is configured for only one member and there are other members not configured for Unbound. In this case, you might still be able to see some of the unsupported tabs and functions through Grid Manager.
- Unbound DNS supports only the default DNS view; it does not support other user-defined DNS views that are supported by BIND. When you switch from BIND to Unbound, the appliance falls back to the default DNS view configuration.
- You must restart DNS service each time you switch between Unbound and BIND in order for the configuration to take effect. Switching between Unbound and BIND might cause some service interruptions.
- Query results could be different when using BIND versus Unbound. For example, when you query the auto created zone "0.0.127.in-addr.arpa,"

  BIND:
  
  ;; ANSWER SECTION:
  0.0.127.in-addr.arpa. 3600 IN SOA cluster. please_set_email.absolutely.nowhere. 2 10800 3600 604800 3600

  UNBOUND:
  
  ;; AUTHORITY SECTION:
  127.in-addr.arpa. 10800 IN SOA localhost. nobody.invalid. 1 3600 1200 604800 10800

  For more information about Unbound specifications and how it works, refer to the Unbound documentation at https://www.unbound.net/documentation/index.html.

- There might be a few known general issues when configuring Unbound DNS resolution. Refer to the latest version of the NIOS 7.2.x release notes to review these issues.

Configuring DNS Resolver Type

To use Unbound as the DNS resolver:

1. Ensure that you have the Dual Engine DNS license installed on the appliance.
2. From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.
3. In the Member DNS Properties editor, click Toggle Advanced Mode.
4. When the additional tabs appear, click the General tab -> Advanced tab.
5. In the DNS Resolver Type section, select Unbound. To use the standard DNS resolution, select BIND. Note that when you switch between Unbound and BIND, the appliance preserves all relevant configurations.
6. Save the configuration and click Restart to restart DNS service.

Note: You must restart DNS service for the configuration to take effect.

Unbound DNS Logging
Logging is available when you select Unbound as the DNS resolver. However, the format and severity levels are different than that of the standard DNS logging. You can select the severity level for Unbound DNS logging, but you cannot configure logging facilities and categories—these functions will not be displayed in Grid Manager.

To configure the severity level for Unbound DNS logging:

1. From the Data Management tab, select the DNS tab -> Members tab -> member check box -> Edit icon.
2. In the Member DNS Properties editor, click Toggle Advanced Mode.
3. When the additional tabs appear, click the Logging tab -> Basic tab.
4. From the Logging Severity drop-down list, select one of the following:
   - Cache Misses: Logs client identification for missed caches.
   - Algorithm: Logs information at the algorithm level.
   - Query: Logs information at the query level.
   - Detailed Operations: Logs detailed information for operations.
   - Errors Only: Logs errors only.

   **Note:** The default is Detailed Operations. Infoblox highly recommends that you keep the default setting or select Errors Only. Selecting other options might result in large log files, which could possibly affect your system performance.

5. Save the configuration and click Restart to restart DNS service.

### Unsupported NIOS Features for Unbound DNS

When you configure your appliance to use Unbound as the DNS resolver, the IB-4030-10GE acts as a recursive-only name server and some of the NIOS features are not supported. As a result, corresponding tabs and functions for these features do not appear in Grid Manager when Unbound DNS is configured. Table 4 lists NIOS features that are not supported for Unbound DNS.

**Note:** In the default DNS view, certain unsupported features are displayed in Grid Manager and you can configure these features for members that are not using Unbound DNS resolution.

<table>
<thead>
<tr>
<th>Unsupported features</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authoritative name server and all related functions</td>
<td>Unsupported features include but are not limited to DNS64, AAAA filtering, DDNS updates, notify source and delay, slave mode, wildcard, bulk hosts, IP blocks/IP block groups, and DNS zone transfers. Unbound DNS supports forward and stub zones.</td>
</tr>
</tbody>
</table>
| Security related features                        | Some security related features are not supported. They include the following: DNS blackhole lists, DNS blacklist rulesets, GSS-TSIG, enabling and disabling accept-expired-signature for DNSSEC (other aspects of DNSSEC are supported, such as trust anchors and negative trust anchors), NXDOMAIN mitigation/RRL (Response Rate Limiting), recursive client limits, recursive client SNMP traps, and Infoblox DNS Firewall (RPZ).

   **Note:** The TSIG Key menu item remains in the Queries and Recursive Queries tables even though it is not supported for Unbound DNS.

| UDP source port configuration                     | Port configuration and network settings are automatically switched between Unbound DNS and standard DNS when you change the DNS resolution configuration. |
| DNS requests through a single TCP session         | This is not supported for Unbound DNS even though this option might appear in the Member Security Properties editor of the Grid Manager when Unbound is configured for the member. |
| DNS views                                         | User-defined DNS views are not supported. Unbound DNS supports only the default DNS view. |
| Logging                                           | DNS query logging and DNS response logging are not supported. Logging format and severity levels for Unbound DNS are different than that of the standard DNS. For more information, see Unbound DNS Logging. |
| Reporting                                         | The DNS Replies Trend report is the only supported report for Unbound DNS. Also, the DNS Response Latency Trend report periodically queries against the DNS server to determine latency and is not affected by Unbound DNS. All other reports that do not support Unbound are still available and include data from members running standard DNS. However, they do not collect data from members using Unbound DNS. For information about reports for IB-4030-10GE, see Reports for IB-4030 and IB-4030-10GE. |
| RRset order                                       | This is not supported. For information about this feature, see Preserving the RRset Order for Cached DNS Responses. |
| Sort list                                         | This is not supported. For information about this feature, see Defining Sort List for Cached DNS Responses. |
| HSM group status and traps                        | Although HSM groups are not supported, the HSM event type remains visible in the Notifications tab of the Grid Member Properties editor. |
The following DNS enhancements are not supported: DNS query capture, disabling EDNS0 (Extension Mechanism for DNS), DNS Traffic Control, HA mode transition optimizations, and DNS fault tolerant caching.

### Configuring Hostname and Server ID Options for Unbound DNS

Unbound DNS supports the configuration of hostname bind directive and server-id directive options, which enables the appliance to return the hostname of the answering DNS name server in response to queries from clients in a DNS anycast configured environment. For information about how to configure the hostname bind directive and server-id directive options, refer to the **Configuring Hostname and Server ID Options** section in the Infoblox NIOS Administrator Guide.

**Note:** Even though you can configure both hostname bind directive and server-id directive options, Unbound DNS ignores the hostname bind directive setting and considers only the server-id directive setting.