About DNS Integrity Check for Authoritative Zones

In certain DNS domain hijacking scenarios, hijackers alter the DNS data of a domain after gaining control of it. They consequently redirect users to a fraudulent site, instead of the legitimate site, on the Internet. To protect your authoritative DNS server against this type of DNS domain hijacking, you can configure the appliance to periodically monitor DNS data for top-level or parent authoritative zones. Based on your configuration, the appliance periodically checks DNS data in the NS RRsets for these zones and compares the data with that in the appliance database. It then reports data discrepancies through SNMP traps and logs related events in the syslog. You can also monitor the status of DNS data discrepancies, if any, through the DNS Integrity Check widget on the Task Dashboard. The severity in data discrepancies can help identify possible domain hijacking.

DNS integrity check is supported on all Infoblox appliances, including Advanced Appliances used primarily for Infoblox. For information about Infoblox, see About Infoblox Advanced DNS Protection. You can configure DNS integrity check for any selected authoritative zones, but you cannot configure it at the Grid, member, or DNS view level. When you enable this feature, the appliance queries the NS RRsets and glue records for the top-level authoritative zones and compare the data with that in the appliance database. It does not query data for sub zones or delegated zones in the Grid.

Configuring DNS Integrity Check

To configure the appliance to check NS and glue records for a top-level or parent authoritative domain, complete the following:

1. From the Data Management tab, select the DNS tab -> Zones tab -> top-level authoritative zone that you want to monitor, and then click the Edit icon from the Toolbar. Note that you can configure this feature only at the zone level. You can also configure zones that have the same name in different DNS views.

   **Note:** Once you configure a zone for DNS integrity check, you will not be able to add a parent zone above this zone. You must disable DNS integrity check for this zone before you can add the parent zone.

2. In the Authoritative Zone editor, toggle to the Advanced Mode, select the DNS Integrity Check tab -> Basic tab and complete the following:
   - **Enable:** Select this check box to enable the DNS integrity check feature.
   - **Member:** Click Select Member to select the Grid member you want to use for DNS integrity check. When you select a member, ensure that the member is configured to send and receive DNS queries and responses from Grid primaries (including stealth primaries) for the zone being monitored. Note that queries generated by DNS integrity check for the first reachable internal Grid primary (including a stealth primary) are logged in relevant DNS reports. For information about reports, see Infoblox Reporting and Analytics.
   - **Check Frequency:** Enter how often the appliance monitors DNS data for the authoritative zone. Select the time unit from the drop down list. The appliance periodically queries DNS data for the top-level zone based on the time interval you configure here. The default value is one hour, and the minimum configurable value is 15 minutes.
   - **Enable Verbose Logging:** Select this to enable detailed logging of events related to DNS integrity check.

   When you select this option, the appliance logs additional information in the syslog when DNS data discrepancies are detected. It also logs a message when no data discrepancies are found during a DNS data check. When you clear this check box, the appliance logs standard information in the syslog and does not log an event when no data discrepancies are found during a DNS integrity check. This is disabled by default. For information about the syslog, see Viewing the Syslog.

3. Save the configuration.

Monitoring DNS Data Discrepancies for Authoritative Zones

When the appliance detects DNS data discrepancies between the authoritative and delegated zones, it reports the discrepancies through SNMP traps and email notifications, if configured. For more information, see Setting SNMP and Email Notifications. The appliance classifies data discrepancies by severity, as follows:

- **Critical:** Data in the NS RRsets for the authoritative and delegate zones are completely out of synchronization.
- **Severe:** Some data in the NS RRset between the authoritative and delegate zones overlaps and some data is different.
- **Warning:** The NS RRset for the authoritative zone is a subset of the NS RRset for the delegate zone. It is possible that incorrect IP addresses have been entered at the registrar.
- **Informational:** The NS RRset for the delegate zone is a subset of the NS RRset for the authoritative zone.
   - This could indicate a possible delay in domain registration.
- **Normal:** There are no DNS data discrepancies between the NS RRsets for the authoritative and delegated zones.
- **None:** No DNS discrepancies data has been collected or DNS integrity check has not been performed.

When different Grid primaries report different severity levels for the same data check, the appliance reports the most severe discrepancy level. When different Grid primaries report the same severity for the data check, the appliance reports only the first check.

You can use the following methods to monitor DNS data discrepancies for selected authoritative zones:

- Viewing syslog events, as described in Viewing the Syslog.
- Monitoring DNS data discrepancy status through the DNS Integrity Check dashboard widget, as described in DNS Integrity Check.
- Receiving SNMP traps and email notifications, as described in Setting SNMP and Email Notifications.