LOGZILLA DOCUMENTATION

Infoblox

LogZilla App Store application: Infoblox

LogZilla App Store · Generated May 3, 2026 · logzilla.ai/docs/logzilla-appstore/infoblox

Overview

Infoblox NIOS (Network Identity Operating System) is a platform for automating DNS, DHCP, and IP Address Management (IPAM). NIOS appliances generate syslog messages across multiple services including DNS resolution, DHCP leasing, administrative audit trails, and Advanced DNS Protection (ADP) threat events.

App Function

- Parse Infoblox DNS query/response logs and extract client IP, domain, record type, and response code
- Parse DNS RPZ (Response Policy Zone) events in CEF format for DNS firewall monitoring
- Parse DNS dynamic update security events
- Parse DHCP lease events (DISCOVER, OFFER, REQUEST, ACK, RELEASE) with Infoblox-specific extensions (TransID, lease-duration, uid)
- Parse audit logs for authentication tracking and configuration change monitoring
- Parse ADP threat protection events in CEF format
- Classify all events with standard Event Class/Type taxonomy and MITRE ATT&CK mappings
- Provide dashboards for DNS, DHCP, security, and audit monitoring
- Alert on zone transfers, DNS failures, RPZ blocks, ADP threats, authentication failures, and unauthorized DNS updates

Vendor Documentation

- Using a Syslog Server - NIOS 9.0 (https://docs.infoblox.com/space/nios90/280403148)
- Capturing DNS Queries and Responses (https://docs.infoblox.com/display/NAG8/Capturing+DNS+Queries+and+Responses)
- Setting DNS Logging Categories (https://infoblox-docs.atlassian.net/wiki/spaces/nios90/pages/1381139017/Setting+DNS+Logging+Categories)
- Monitoring through Syslog - NIOS 9.0 (https://docs.infoblox.com/space/nios90/280275770)

LogZilla Configuration

Infoblox NIOS uses standard daemon names (`named`, `dhcpd`, `ntpd`, `httpd`) that collide with stock Linux systems, and emits a non-standard syslog header. A dedicated LogZilla port is required so Infoblox traffic can be identified and parsed separately from OS logs.

Navigate to **Settings → System Settings → Application Ports**
Set **Syslog Infoblox Port** to a dedicated port (e.g., `5525`)
Click **Save**
Both TCP and UDP listeners are enabled on the configured port.

Device Configuration

Configure the Infoblox appliance to send all syslog messages to the dedicated port configured above:

Log in to the Infoblox Grid Manager
Navigate to **Grid > Grid Manager > Members**
Select the member and click **Edit**
Under **Monitoring > Syslog**, add the LogZilla server IP with the dedicated port
Under **Monitoring > Syslog**, select **Send All** for log categories (or select specific categories: DNS queries, DNS responses, DHCP, RPZ)
Enable **Copy Audit Log Messages to Syslog** in Grid Properties for audit event forwarding
Click **Save** to apply the configuration

Verification

Generate a DNS query or trigger a DHCP lease, then verify events appear in LogZilla with the `Vendor` tag set to `Infoblox`.

Incoming Log Format

Infoblox syslog header

Every NIOS message begins with a non-standard header that includes the grid member FQDN and grid member IP:

```
<timestamp> <syslog_host> <grid_fqdn> <grid_ip> <program>[<pid>]: <body>
```

The grid FQDN is extracted as the `IB Grid Member` tag for per-node filtering. Standard RFC3164 (no grid FQDN/IP) is also accepted for NIOS builds that don't emit the extended header.

Per-service body formats

Infoblox NIOS generates multiple body formats depending on the service:

Standard BIND named client query log

```
client @<pointer> <SrcIP>#<port> (<query>): view <N>: query: <query> IN <qtype> <flags>
(<resolver_ip>)
```

Infoblox DNS Query Logging (optional feature)

```
infoblox-responses: <timestamp> client <SrcIP>#<port>: <protocol>: query: <query> IN <qtype>
response: <rcode> <flags> [<answer_data>]
```

DHCP (ISC DHCP, lease and operational output)

```
DHCPACK on <IP> to <MAC> (<hostname>) via <interface> relay <relay_ip> lease-duration <seconds> [uid
<client_id>]
Option 82: received a DISCOVER DHCP packet from relay-agent <IP> with a circuit-id of "<id>", ...
bind update on <IP> from DHCP_Failover(<peer>) rejected: <reason>
failover peer DHCP_Failover(<peer>): <N> leases added to send queue from pool <ptr> <subnet>
```

Audit (httpd)

```
<ISO8601_timestamp> [<username>]: <Action> [<object_type> <object_name>]: <details> apparently_via=
<method>
```

ADP Threat Protection (CEF)

```
adp: CEF:0|Infoblox|NIOS Threat|<version>|<rule_id>|<rule_name>|<severity>|src=<IP> spt=<port> dst=
<IP> dpt=53 act="<action>" cat="<category>" fqdn=<domain>
```

DNS RPZ (CEF)

```
CEF:0|Infoblox|NIOS|<version>|<trigger_type>|<action>|<severity>|app=DNS dst=<IP> src=<IP> spt=<port>
view=<view> qtype=<type> msg="rpz <trigger> <action> rewrite <domain>"
```

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Infoblox	Vendor name
Product	NIOS	Product name
Event Class	Network, Security, Auth, Config	Cross-vendor classification
Event Type	Lease, Threat, Session, Configuration	Event subtype
MitreId	T1071.004	MITRE ATT&CK technique ID
MITRE Tactic	Command and Control	MITRE ATT&CK tactic
SrcIP	10.1.2.50	Source IP address (HC)
DstIP	10.10.10.1	Destination IP address (HC)

Tag Name	Example	Description
SrcMAC	00:00:5e:00:53:02	DHCP client MAC address (HC)
Query	www.example.com	DNS query domain name (HC)
Domain	malware.example.com	Domain from RPZ/ADP events (HC)
User	admin	Audit username (HC)
Action	Login_Allowed, DROP, denied	Action taken
Interface	eth2	DHCP relay interface (NIOS appliance side)
IB Grid Member	grid1.example.net	Grid member FQDN from the non-RFC header
IB Query Type	A, TXT, AXFR	DNS record type
IB Response	NOERROR, NXDOMAIN	DNS response code (infoblox-responses only)
IB DNS View	1, 3, _default	BIND view that served the query
IB DHCP Type	DHCPACK, DHCPREQUEST	DHCP message type
IB DHCP Subtype	Option 82, Failover, Pool Balancing	Non-lease dhcpd output classification
IB DHCP Hostname	DESKTOP-01	Client-reported hostname
IB DHCP Relay	10.0.0.1	DHCP relay-agent IP
IB DHCP Circuit ID	00:04:00:d2:23:73	Option 82 circuit-id value
IB DNS Zone	10.in-addr.arpa	DNS zone (update-security)
IB Audit Object	Network, AuthZone	Audit object type
IB Audit Via	GUI, API	Audit access method
IB RPZ Trigger	RPZ-QNAME, RPZ-IP	RPZ trigger type

Tag Name	Example	Description
IB Threat Category	DNS Tunneling	ADP threat category
IB Threat Rule	DNS HTTPS record	ADP rule name

High-Cardinality (HC) Tags

- SrcIP
- DstIP
- SrcMAC
- Query
- Domain
- User

Log Examples

Each example shows the complete raw syslog payload including the Infoblox non-RFC header.

DNS BIND client query (stock NIOS output)

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 named[5678]: client @0xdeadbeef0001
10.0.0.50#52638 (www.example.com): view 3: query: www.example.com IN A + (10.0.0.70)
```

DNS AXFR zone transfer (security event — T1595)

```
Apr 17 16:00:00 10.0.0.100 grid1.example.net 10.0.0.70 named[5678]: client @0xdeadbeef0003
203.0.113.5#12345 (example.com): view 1: query: example.com IN AXFR + (10.0.0.70)
```

DNS Query Logging feature response

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 named[5678]: infoblox-responses: 17-Apr-2026
15:22:36.339 client 192.0.2.10#57398: UDP: query: api.example.com IN A response: NOERROR +
```

DNS RPZ block (CEF)

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 named[5678]: CEF:0|Infoblox|NIOS|9.0.6|RPZ-QNAME|NXDOMAIN|7|app=DNS dst=198.51.100.1 src=192.0.2.10 spt=52240 view=_default qtype=A msg="rpz QNAME NXDOMAIN rewrite malware.example.com [A] via malware.example.com.rpz1.example.net"
```

DNS update denied

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 named[5678]: update-security: client @0xdeadbeef0004 192.0.2.10#60753: update '10.in-addr.arpa/IN' denied
```

DHCPACK (lease completion)

```
Apr 17 15:22:27 10.0.0.100 grid1.example.net 10.0.0.70 dhcpd[1234]: DHCPACK on 10.1.1.63 to 00:00:5e:00:53:02 (client1) via eth3 relay 10.1.1.1 lease-duration 600 (RENEW) uid 01:00:00:5e:00:53:02
```

DHCPDISCOVER (no IP yet)

```
Apr 17 15:22:25 10.0.0.100 grid1.example.net 10.0.0.70 dhcpd[1234]: DHCPDISCOVER from 00:00:5e:00:53:03 (HP-Printer) via 10.1.1.1 TransID 7b860000 uid 01:00:00:5e:00:53:03
```

Option 82 relay metadata

```
Apr 17 15:22:25 10.0.0.100 grid1.example.net 10.0.0.70 dhcpd[1234]: Option 82: received a DISCOVER DHCP packet from relay-agent 10.1.1.1 with a circuit-id of "00:04:00:d2:23:73", a link-selection of "10.1.1.0", a server-id-override of "10.1.1.1" for 10.1.1.254 (00:00:5e:00:53:07) lease time is 600 seconds. (NEW)
```

DHCP failover (HA event)

```
Apr 17 15:52:39 10.0.0.100 grid1.example.net 10.0.0.70 dhcpd[1234]: failover peer DHCP_Failover(1234567890p): 5 leases added to send queue from pool 000000000000 10.1.0.0/16
```

Audit login allowed

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 httpd[1234]: 2022-03-21 08:53:51.087Z
[admin1]: Login_Allowed - - to=AdminConnector ip=192.0.2.10 auth=LOCAL group=admin-group
apparently_via=API
```

Audit configuration change

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 httpd[1234]: 2022-03-18 12:40:05.241Z
[admin1]: Modified MemberDhcp infoblox.localdomain: Changed enable_service:False->True
```

ADP threat detection (CEF)

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 threat-protect-log[1234]: adp:
CEF:0|Infoblox|NIOS Threat|9.0.6|130502880|DNS HTTPS record|4|src=203.0.113.50 spt=43120
dst=198.51.100.1 dpt=53 act="DROP" cat="DNS Message Types" nat=0 nfpt=0 nlpt=0
fqdn=suspicious.example.com hit_count=1
```

NTP synchronization

```
Apr 17 15:22:36 10.0.0.100 grid1.example.net 10.0.0.70 ntpd[1234]: synchronized to 192.0.2.1, stratum
2
```

MITRE ATT&CK Mapping

Query Type / Event	MITRE ID	Tactic	Description
NULL query	T1071.004	Command and Control	DNS tunneling via NULL records
AXFR query	T1595	Reconnaissance	Zone transfer enumeration
IXFR query	T1595	Reconnaissance	Incremental zone transfer
ANY query	T1595	Reconnaissance	Zone enumeration / amplification
RPZ block	T1071.004	Command and Control	DNS firewall policy match

Query Type / Event	MITRE ID	Tactic	Description
ADP threat	T1071.004	Command and Control	Advanced DNS Protection detection

TXT queries are intentionally **not** flagged as threats. TXT is the dominant legitimate qtype (SPF/DKIM/DMARC, ACME challenges, Microsoft 365 domain verification) so a flat qtype tag would drown real threats in false positives. TXT tunneling detection belongs in a dedicated trigger using query length, entropy, and subdomain depth, not on qtype alone.

Dashboards

The app includes one dashboard:

- **Infoblox: NIOS Overview** — Event counts by class, EPS rate, top source IPs, DNS query/response trends, DHCP message types, audit actions, and a live event stream

Triggers

Trigger	Description
`Infoblox: MITRE ATT&CK Threat Detected`	Catch-all for MITRE-tagged events
`Infoblox: Zone Transfer`	AXFR/IXFR queries (zone enumeration)
`Infoblox: DNS SERVFAIL`	DNS resolution failures
`Infoblox: DNS REFUSED`	Access control or policy issues
`Infoblox: ADP Threat Blocked`	ADP threat protection DROP actions
`Infoblox: RPZ Block`	DNS firewall blocked a query
`Infoblox: Authentication Failure`	Login denied in audit logs
`Infoblox: DNS Update Denied`	Unauthorized dynamic DNS update