

DEPLOYMENT GUIDE

Implementing Microsoft Server DNS Logging and Diagnostics with Reporting and Analytics

Table of Contents

Introduction	2
Feature Overview	2
Data Flow for Grid Support of Microsoft DNS and DHCP Servers	4
Requirements	4
Deployment Summary	4
Deployment Instructions	4
Enable Analytics on the Microsoft Server.....	4
Add Microsoft DNS and DHCP servers to the Grid.....	8
Enable receiving of report data from Microsoft server.....	11
Viewing Reports.....	12
Troubleshooting.....	13

Introduction

The Infoblox DDI solution now supports data from Microsoft DNS and DHCP services and integrates this data into the reporting and analytics platform thus providing a single view into all DDI (DNS, DHCP and IP Address Management) services.

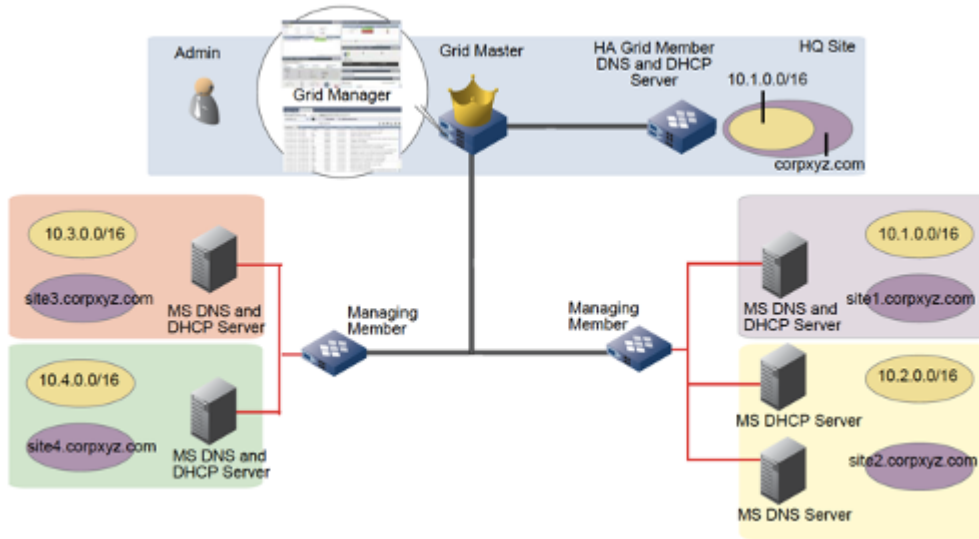
This deployment guide explains how to enable and provision Microsoft DNS and DHCP logging, to integrate with the Infoblox Reporting and Analytics platform.

Feature Overview

- Supports existing DNS/DHCP/IPAM reports to include the data from Microsoft DNS and DHCP servers along with Infoblox appliance data.
- Synchronizes Microsoft 'DNS Analytic events' logged for DNS queries and DNS responses in 'Event Viewer' for preparing DNS reports data.
- DHCP/IPAM reports data is prepared based upon existing Microsoft DHCP object synchronization.
- Leverages Microsoft server managing Grid member's reporting configurations and service to prepare the data as a forwarder and send to the reporting member (indexer).
- Uploads the collected data files to Data Connector VM to support DCVM reports with Microsoft DNS data.
- The following DHCP Reports are supported with Microsoft data:
 - DHCP Lease History
 - DHCP Message Rate Trend
 - DHCP Top Lease Clients
 - DHCPv4 Usage Trend
 - DHCPv4 Usage Statistics
 - DHCPv4 Range Utilization Trend
 - DHCPv4 Top Utilized Networks
- The following IPAM reports are supported with Microsoft data:
 - IPAMv4 Network Usage Statistics
 - IPAMv4 Network Usage Trend

- IPAMv4 Top Utilized Networks
- The following DNS reports are supported with Microsoft data:
 - DDNS Update Rate Trend
 - DNS Top Requested Domain Names
 - DNS Query Rate by Query Type
 - DNS Top Clients
 - DNS Query Rate by Member
 - DNS Daily Peak Hour Query Rate by Member
 - DNS Top Clients per Domain
 - DNS Top NXDOMAIN-NOERROR (no data)
 - DNS Top SERVFAIL Errors Sent
 - DNS Top Timed-Out Recursive Queries
 - DNS Query Trend Per IP Block Group
 - DNS Domains Queried by Client
 - DNS Domain Query Trend
 - Top DNS Clients by Query Type
 - DNS Top Clients Querying MX Records

Data Flow for Grid Support of Microsoft DNS and DHCP Servers



Requirements

The following items are required for Microsoft DNS and DHCP server support:

- Infoblox NIOS version 8.2.1 or later.
- Infoblox Microsoft management license for every member that will service Microsoft DNS and DHCP servers.
- Infoblox Reporting Server.
- Supported [Microsoft Windows Versions](#)

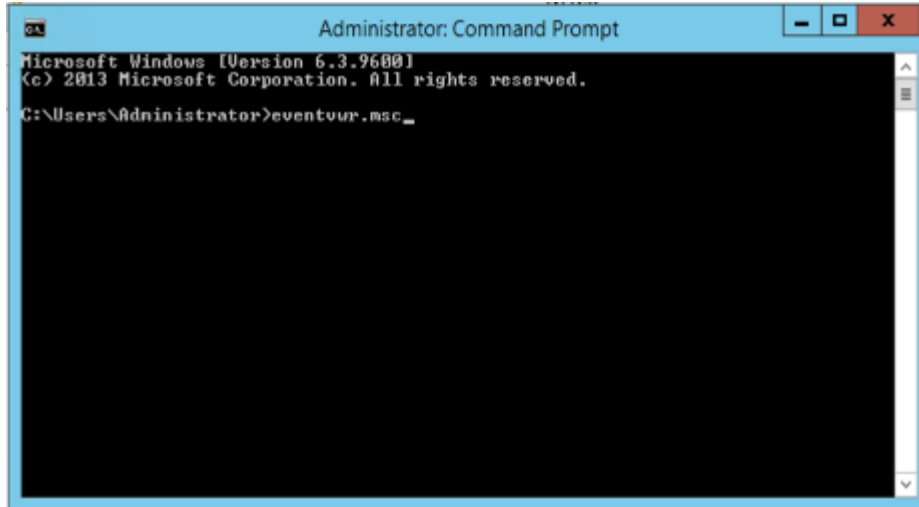
Deployment Summary

- Enable enhanced DNS logging and diagnostics.
- Install Microsoft management license on each member performing MS synchronization services.
- Add Microsoft DNS and DHCP servers to the Grid Member(s).

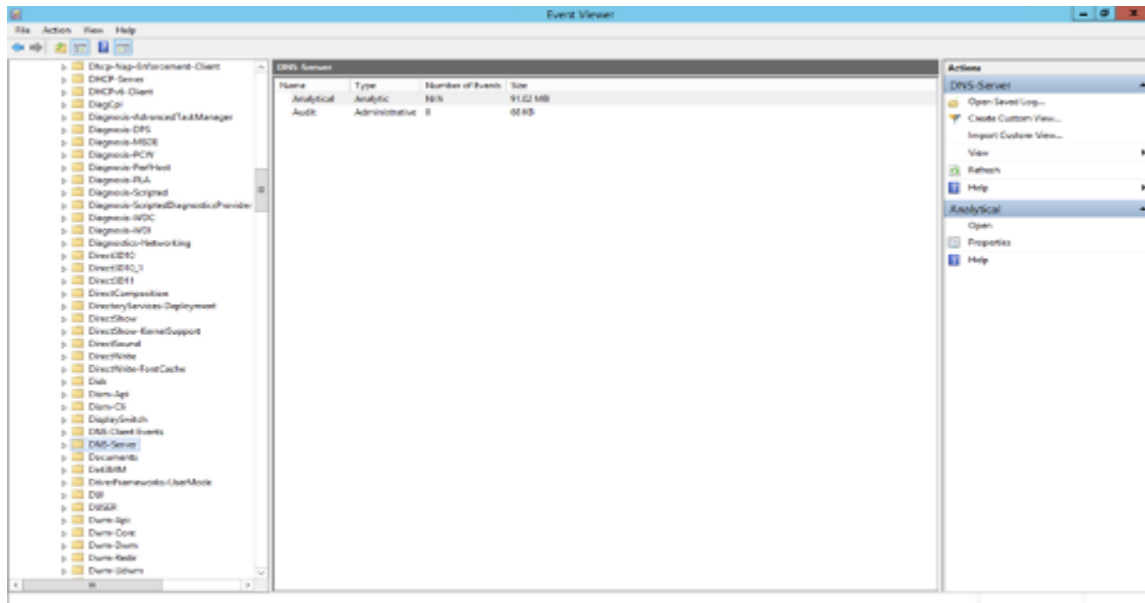
Deployment Instructions

Enable Analytics on the Microsoft Server

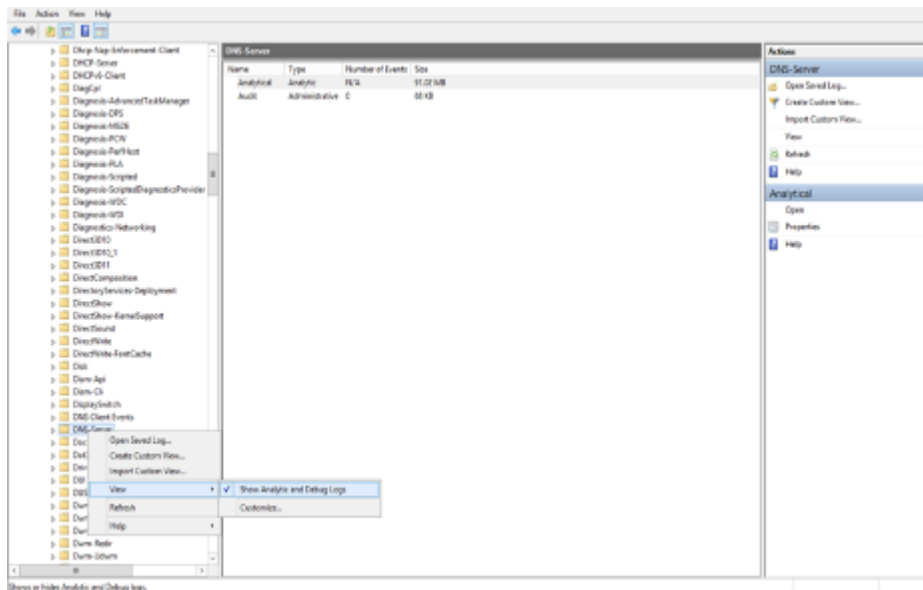
1. Log onto the Microsoft Server.
2. From an elevated command prompt, type `eventvwr.msc` to start the event viewer.



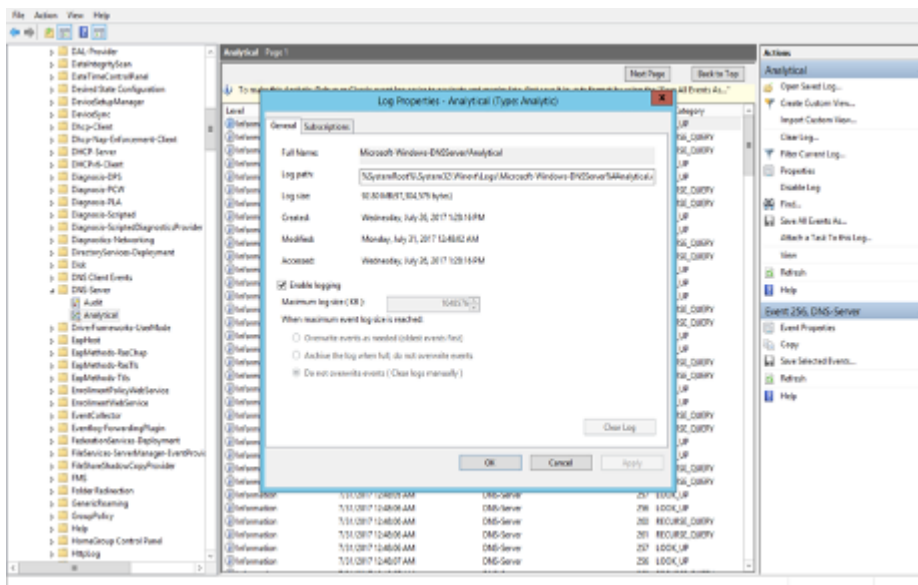
3. In the event viewer, navigate to **Applications and Services Logs** → **DNS-Server**. *Note: This entry will not appear if the Microsoft 2012 R2 server is not up-to-date on patches.*



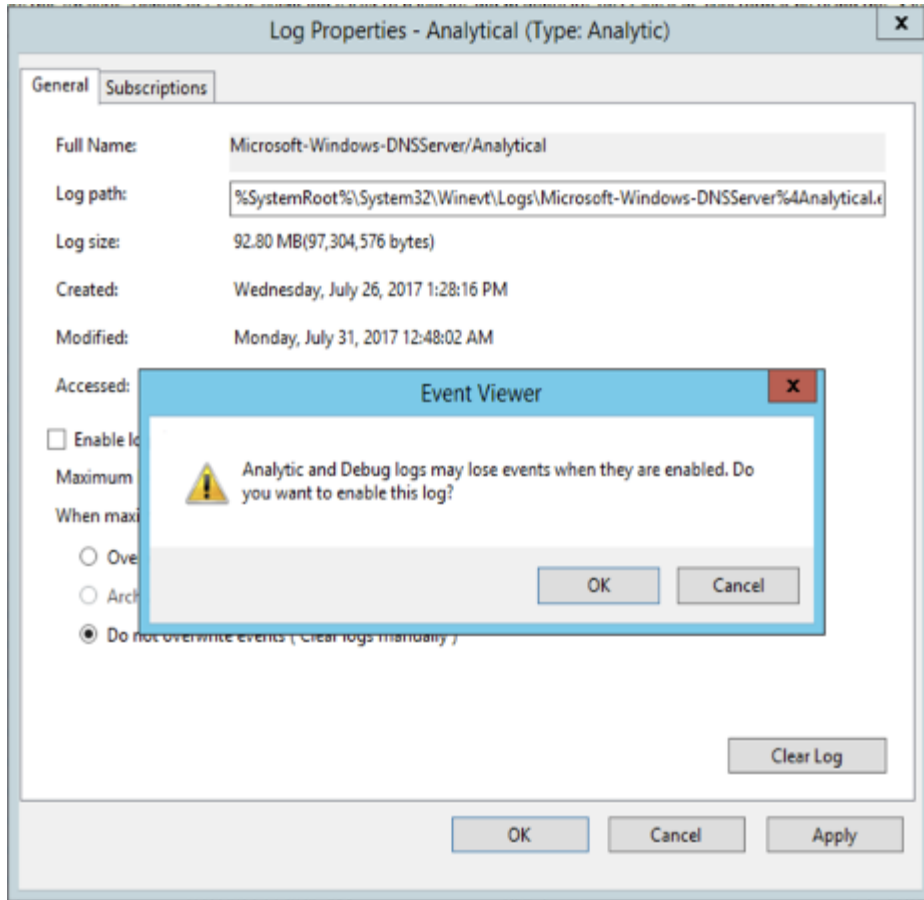
- Right click on **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**. The Analytical log will be displayed.



- Right Click on **Analytical** and then click on **Properties**.



- In the screen above, under When maximum event log size is reached, choose **Do not overwrite events (Clear logs manually)**, select the **Enable logging** checkbox, and click **OK** when you are asked if you want to enable this log. *Note: This step is documented in the Microsoft website.*



Add Microsoft DNS and DHCP servers to the Grid

Note: This section is optional if you have already added your Microsoft servers to the Grid Master. If you have already added Microsoft servers to your grid, then skip to the next section.

1. Navigate **Grid** → **Microsoft Servers** → **Toolbar** → **Add Microsoft Servers**. Enter the domain/username and password. Select the managing member by clicking on the **Select Member** button. Select the **Network View** and **DNS View** to synchronize. Click **Next**. Note: The screenshot below is just an example. Refer to the NIOS Administrator's Guide on setting the proper Microsoft server credentials.

Add Microsoft Server(s) Wizard > Step 1 of 3

GENERAL SETTINGS

Credentials to connect to the Microsoft server(s)

*Domain\username administrator

Password

Managing Member

None demogm1.infoblox.com

Select Member

*Minimum synchronization interval 2 minutes

*Synchronize data into Network View Company 1

*Synchronize DNS data into DNS View default

Logging level Normal

Logging output destination Microsoft Log

Inherited from Grid demogm1

Override

Comment

Cancel Previous Next Save & Close

2. Set the credentials for connecting to DNS and DHCP services and set the **Manage DNS and DHCP services in** to Read/Write or Read Only. Click **Next**.

Add Microsoft Server(s) Wizard > Step 2 of 5

Select your across-server settings for DNS and DHCP Services

Use general credentials (from first page of wizard)

Credentials to connect to DNS and DHCP Services

Domain\username

Password

Use general synchronization interval (from first page of wizard)

*Minimum synchronization interval minutes

Manage DNS and DHCP services in

Cancel Previous Next Save & Close

3. Set the credentials for connecting to Active Directory and set the **Manage Active Directory sites** in to Read/Write or Read Only. Click **Next**.

Add Microsoft Server(s) Wizard > Step 3 of 5

Select your across-server settings for Active Directory Sites

Use general credentials (from first page of wizard)

Credentials for synchronizing Active Directory information

Domain/username

Password

Use general synchronization interval (from first page of wizard)

* Minimum synchronization interval minutes

Manage Active Directory sites in

Encryption

*TCP port for LDAP connections:

Cancel Previous Next Save & Close

4. Add the servers with either the FQDN or IP address and select the services to be synchronized with the Grid Member. Click **Save & Close**.

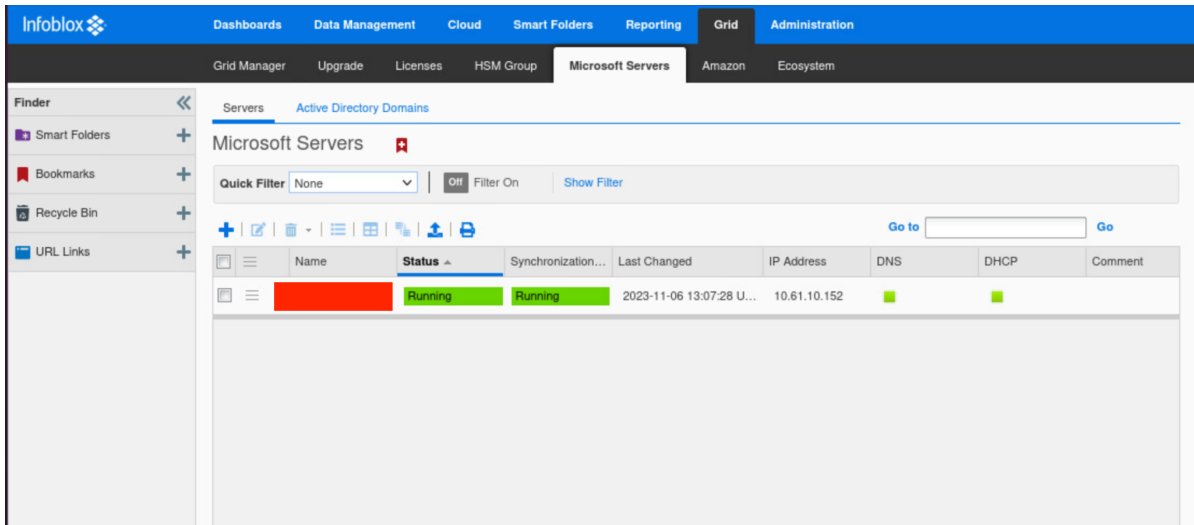
Add Microsoft Server(s) Wizard > Step 4 of 5

MANAGED SERVERS

Name or IP Address	DNS Sync	DHCP Sync	Active Dir...	DNS Monitor & Control	Synchronize DNS Reporting Data
<input type="checkbox"/> 192.168.1.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Inherited from Grid Override	<input checked="" type="checkbox"/> Inherited from Grid Override

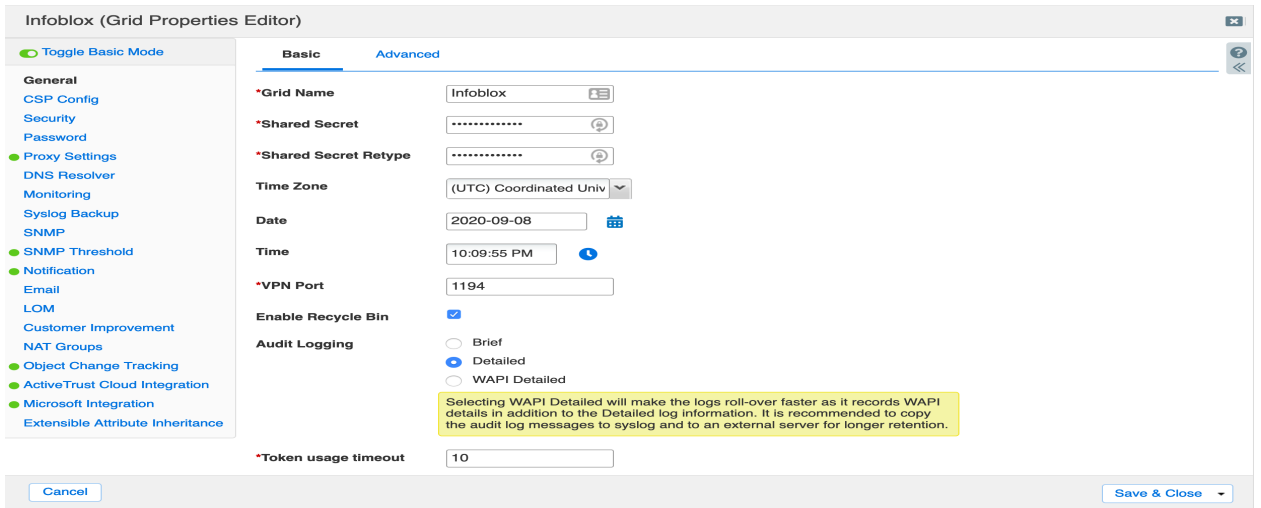
Cancel Previous Next Save & Close

- After about 5 minutes of synchronizing the data between the Grid Master, you should see the following:

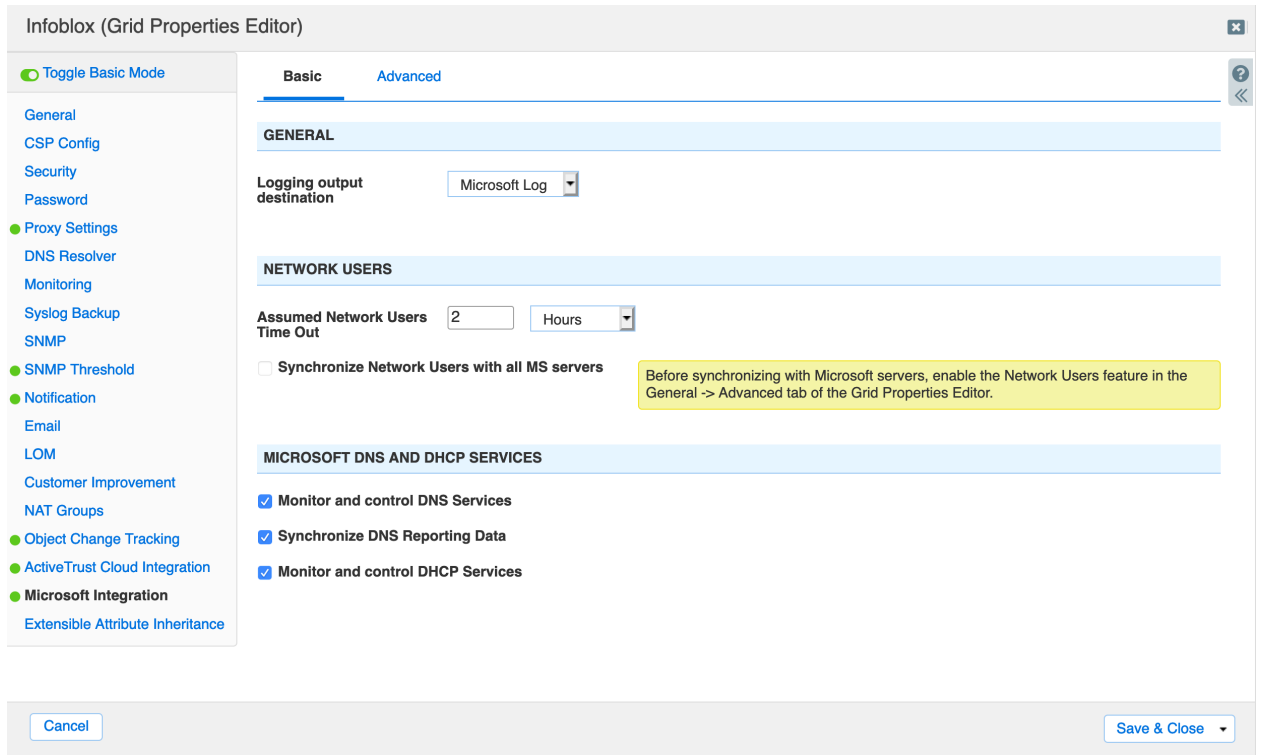


Enable receiving of report data from Microsoft server

- Navigate to Grid → Grid Manager → Toolbar → Grid Properties → Edit.



2. Toggle **Advanced Mode** and then click on **Microsoft Integration**. Click on **Synchronize DNS Reporting Data**. Click **Save & Close**.



3. By default, the analytics logs from the Microsoft server are synchronized from Microsoft event logs every 15 seconds. You can change the DNS synchronization interval to any time between 1 second to 3600 seconds.

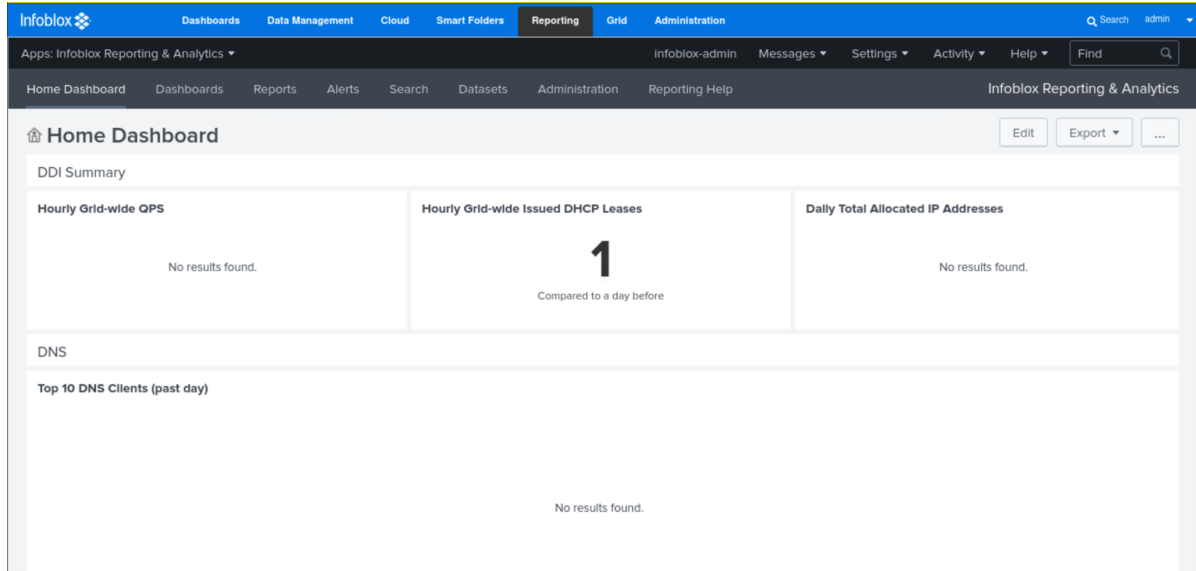
```

Infoblox > set ms_dns_reports_sync_interval
Synopsis:
  set ms_dns_reports_sync_interval <MSSERVERIP> <seconds>
Description:
  Set the MS Sync interval to new value in seconds.
  By default analytics logs for DNS is synced from MS eventlogs every 15 seconds.
  Note: DNS sync Interval must be between 1 and 3600.
Usage:
  set ms_dns_reports_sync_interval 10.102.30.2 25
Infoblox >

```

Viewing Reports

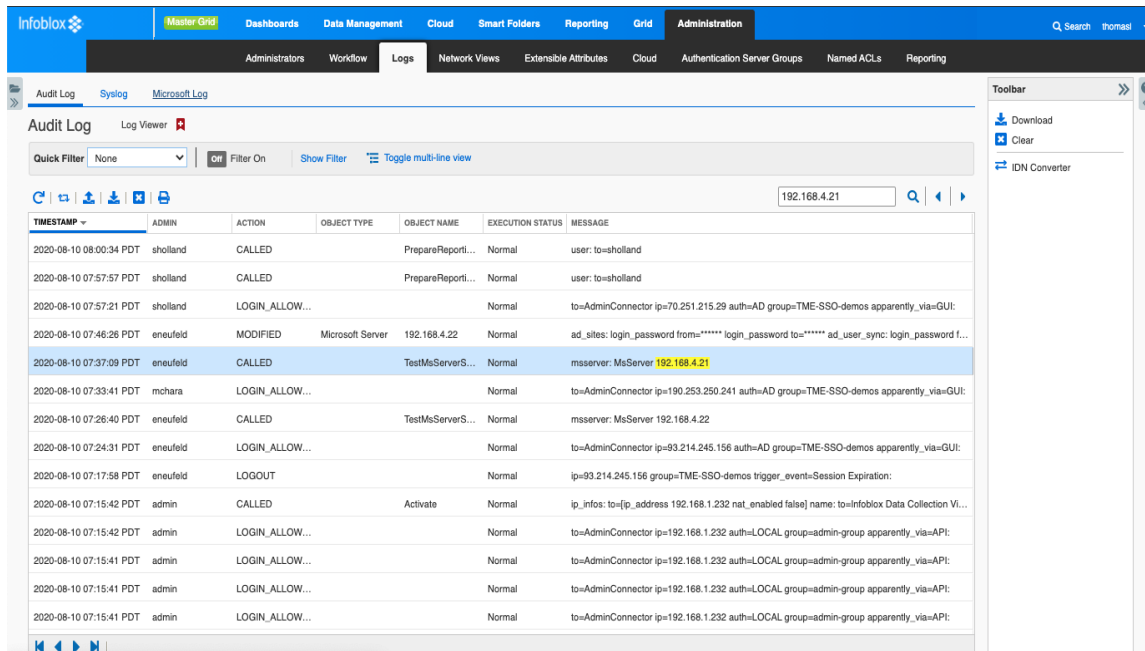
1. Navigate to the **Reporting** tab and pick one or more of the supported reports. Take note of the Microsoft server drop down menu for filtering purposes.



Troubleshooting

If the reports are not showing any data from the Microsoft servers, you can look at the Audit log or Microsoft log.

1. To see the Audit log, navigate to **Administration** → **Logs** → **Audit Log**. Look for entries that pertain to the IP address of the Microsoft server.



2. To see the Microsoft log, navigate to **Administration** → **Logs** → **Microsoft Log**.

The screenshot displays the Infoblox Administration console. The top navigation bar includes 'Master Grid', 'Dashboards', 'Data Management', 'Cloud', 'Smart Folders', 'Reporting', 'Grid', and 'Administration'. The 'Administration' menu is expanded to show 'Administrators', 'Workflow', 'Logs', 'Network Views', 'Extensible Attributes', 'Cloud', 'Authentication Server Groups', 'Named ACLs', and 'Reporting'. The 'Logs' section is active, showing 'Microsoft Log' for the server 'dc1.ad.infobloxdemo.c'. A note states: 'Note: Logs for some Microsoft servers may be found on the Syslog tab'. The log viewer includes a 'Quick Filter' set to 'None', a 'Filter On' button, and a 'Toggle multi-line view' option. The log entries are as follows:

TIMESTAMP	SOURCE	LEVEL	OBJECT TYPE	OBJECT NAME	MESSAGE
2020-09-08 15:37:30 PDT	Sync status	INFO	ADDRESS	192.168.4.21	Opened RPC interface <MS-SCMR> as user 'ad'niosadmin'
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Summary of operations on NIOS:Microsoft (added, updated, deleted, ignored): records (0/0, 0/0, 0/0, 0/0), zone prop...
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Committing synchronization.
2020-09-08 15:37:06 PDT	Sync DNS zone	ERROR	FQDN	adtest	Operation 'add' on record 'm2.infoblox.com.' in DNS zone 'adtest' ignored: DNS record already exists.
2020-09-08 15:37:06 PDT	Sync DNS zone	ERROR	FQDN	adtest	Operation 'add' on record '@' in DNS zone 'adtest' ignored: DNS record already exists.
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Opened RPC interface <MS-DNSP> as user 'ad'niosadmin'
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	NIOS added nameserver association @ (name= dname=m2.infoblox.com address=2001:db8:a42:cafe:100::4).
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Restricting synchronization to zone properties and nameservers due to identical SOA serial number (8).
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Opened RPC interface <MS-DNSP> as user 'ad'niosadmin'
2020-09-08 15:37:06 PDT	Sync DNS zone	INFO	FQDN	adtest	Starting synchronization.
2020-09-08 15:37:06 PDT	Sync DNS zone	ERROR	FQDN	adtest	Pending operation 1016312 has failed: Duplicate object in list
2020-09-08 15:37:00 PDT	Sync status	INFO	ADDRESS	192.168.4.21	Opened RPC interface <MS-SCMR> as user 'ad'niosadmin'
2020-09-08 15:36:30 PDT	Sync status	INFO	ADDRESS	192.168.4.21	Opened RPC interface <MS-SCMR> as user 'ad'niosadmin'
2020-09-08 15:36:06 PDT	Sync Network U...	INFO	ADDRESS	192.168.4.21	Committing synchronization.



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