DEPLOYMENT GUIDE

Implementing Microsoft Server DNS Logging and Diagnostics with Reporting and Analytics

Table of Contents

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.

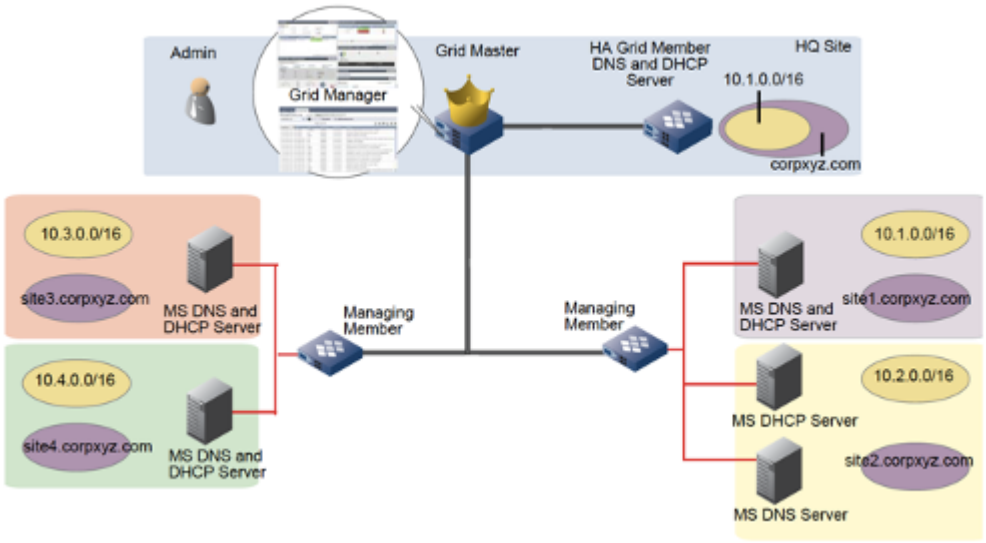
This deployment guide explains how to enable and provision Microsoft DNS and DHCP logging, to integrate with the Infoblox Reporting and Analytics platform.

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

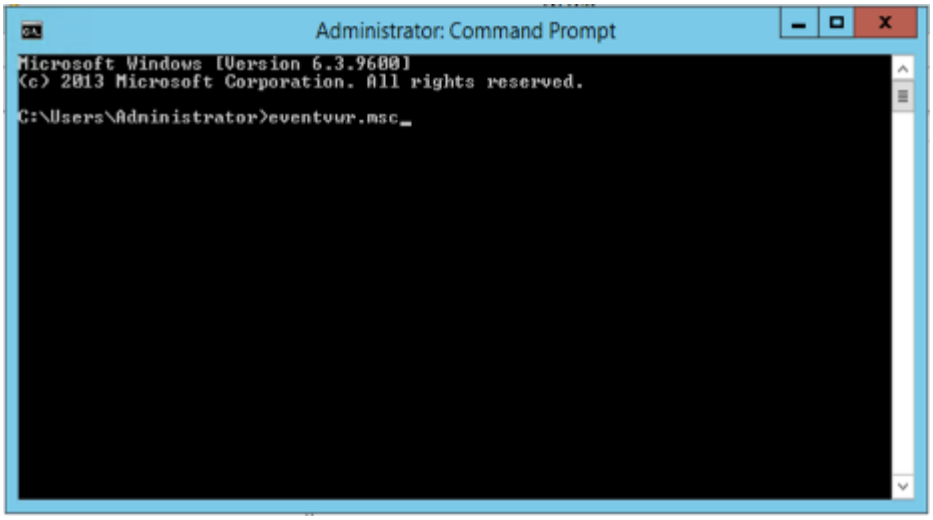
Deployment Summary

- 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).

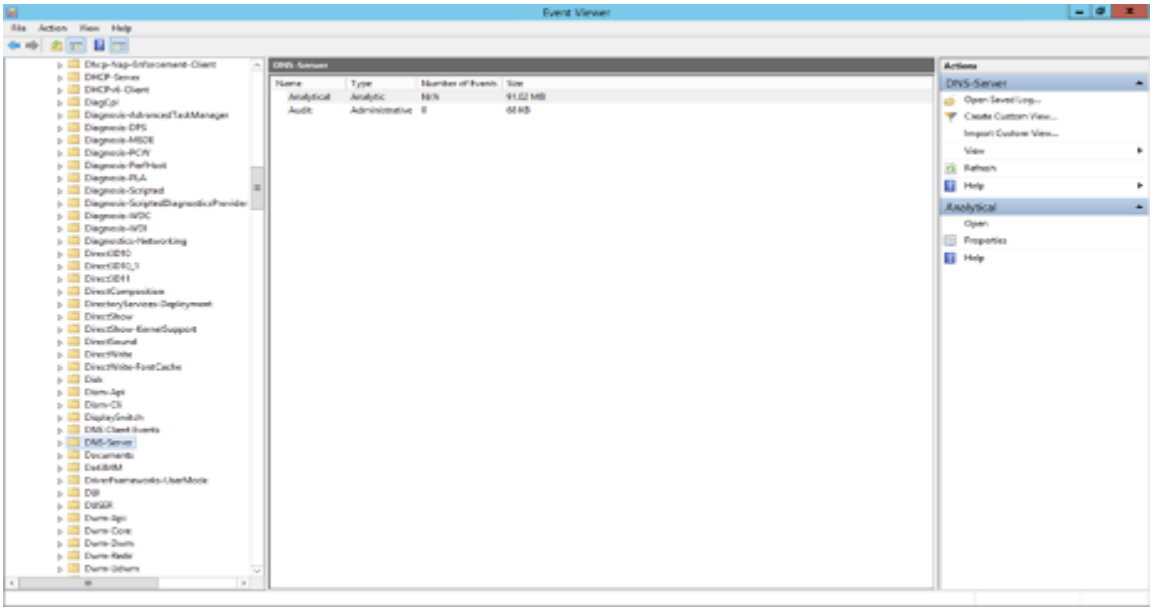
Deployment Instructions

Enable Analytics on the Microsoft Server

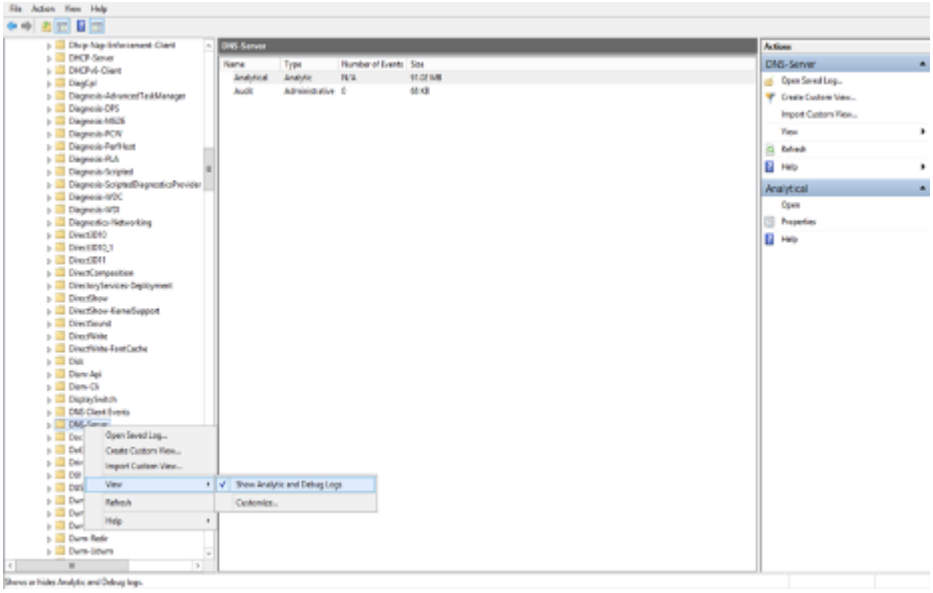
1. Log onto the Microsoft Server.
2. From an elevated command prompt, type `eventvwr.msc` to start the event viewer.



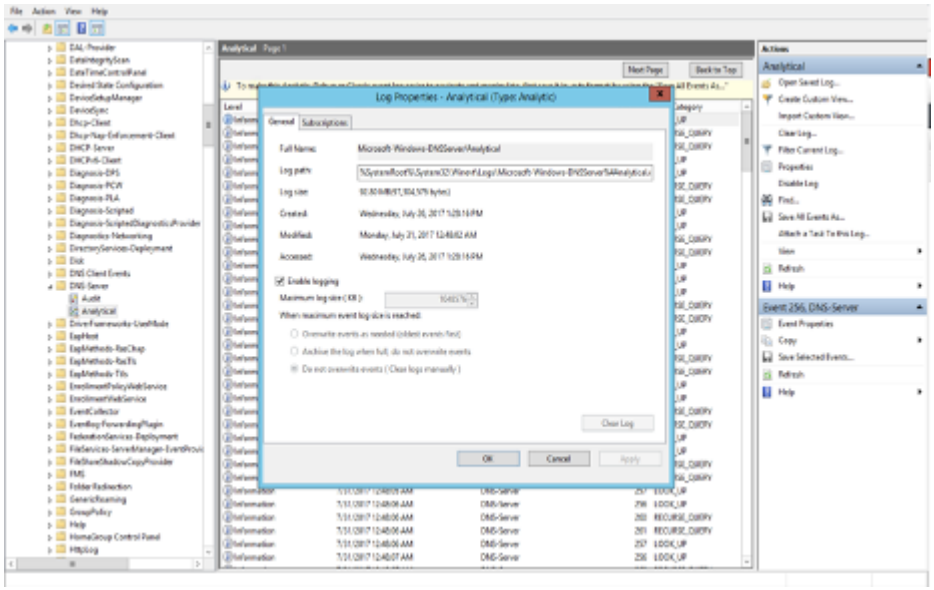
3. In the event viewer, navigate to **Applications and Services Logs → DNS-Server**. *Note: This entry will not appear if the Microsoft 2012 R2 server is not up-to-date on patches.*



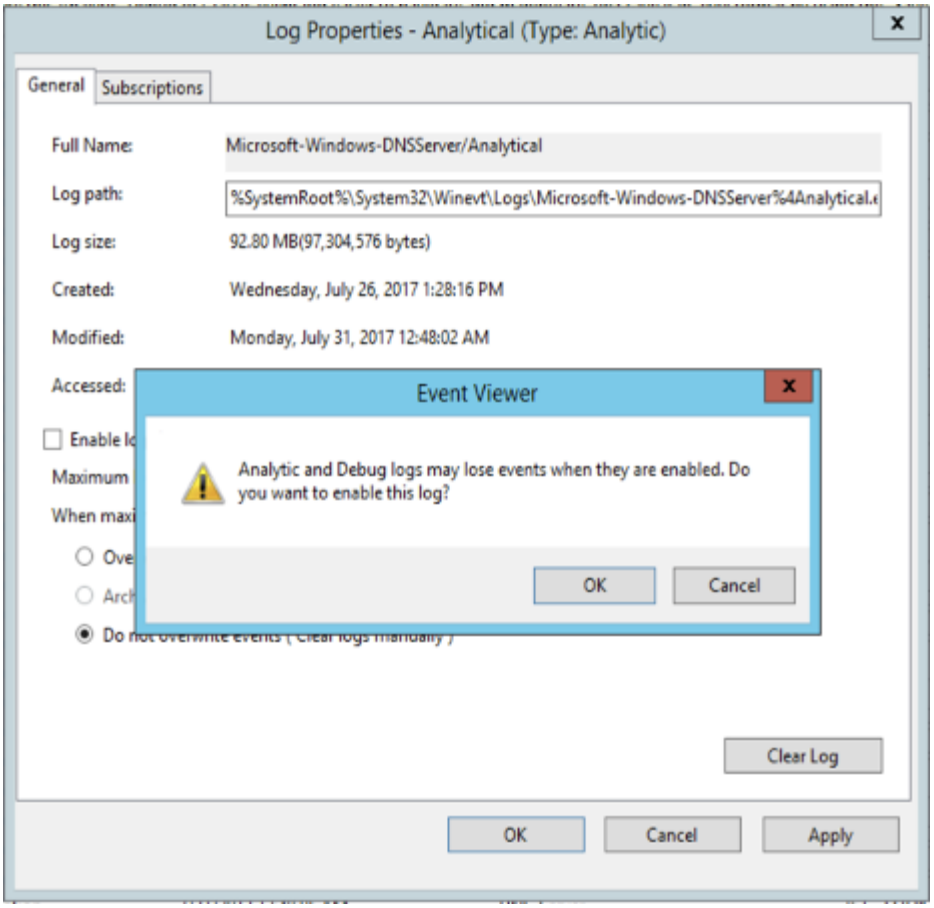
4. Right click on **DNS-Server**, point to **View**, and then click **Show Analytic and Debug Logs**. The Analytical log will be displayed.



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



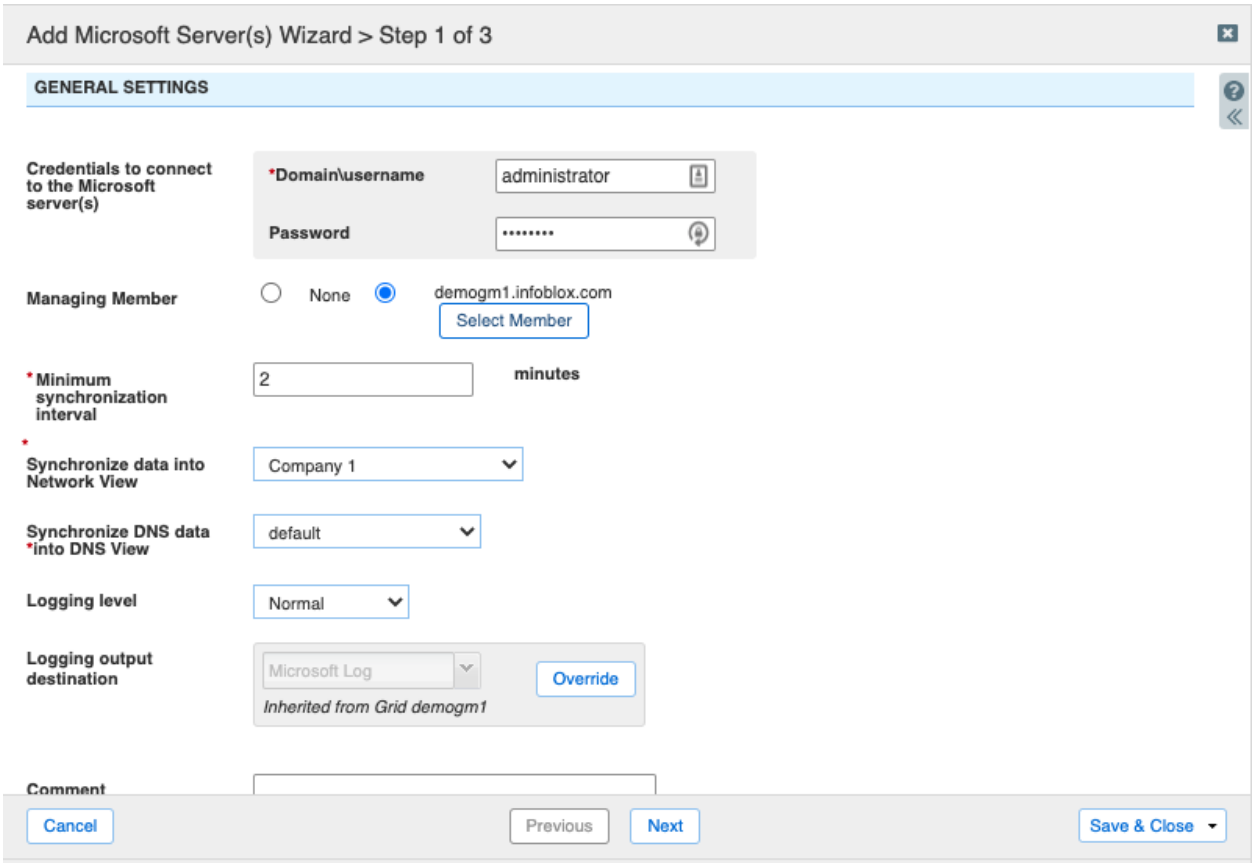
6. In the screen above, under When maximum event log size is reached, choose **Do not overwrite events (Clear logs manually)**, select the **Enable logging checkbox**, and click **OK** when you are asked if you want to enable this log. *Note: This step is documented in the Microsoft website.*


Log Properties - Analytical (Type: Analytic)
General
Subscriptions
Full Name:
Microsoft-Windows-DNSServer/Analytical
Log path:
%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-DNSServer%4Analytical.e
Log size:
92.80 MB(97,304,576 bytes)
Created:
Wednesday, July 26, 2017 1:28:16 PM
Modified:
Monday, July 31, 2017 12:48:02 AM
Accessed:
Event Viewer
Analytic and Debug logs may lose events when they are enabled. Do you want to enable this log?
OK
Cancel
Maximum
When maxi
Clear Log
OK
Cancel
Apply

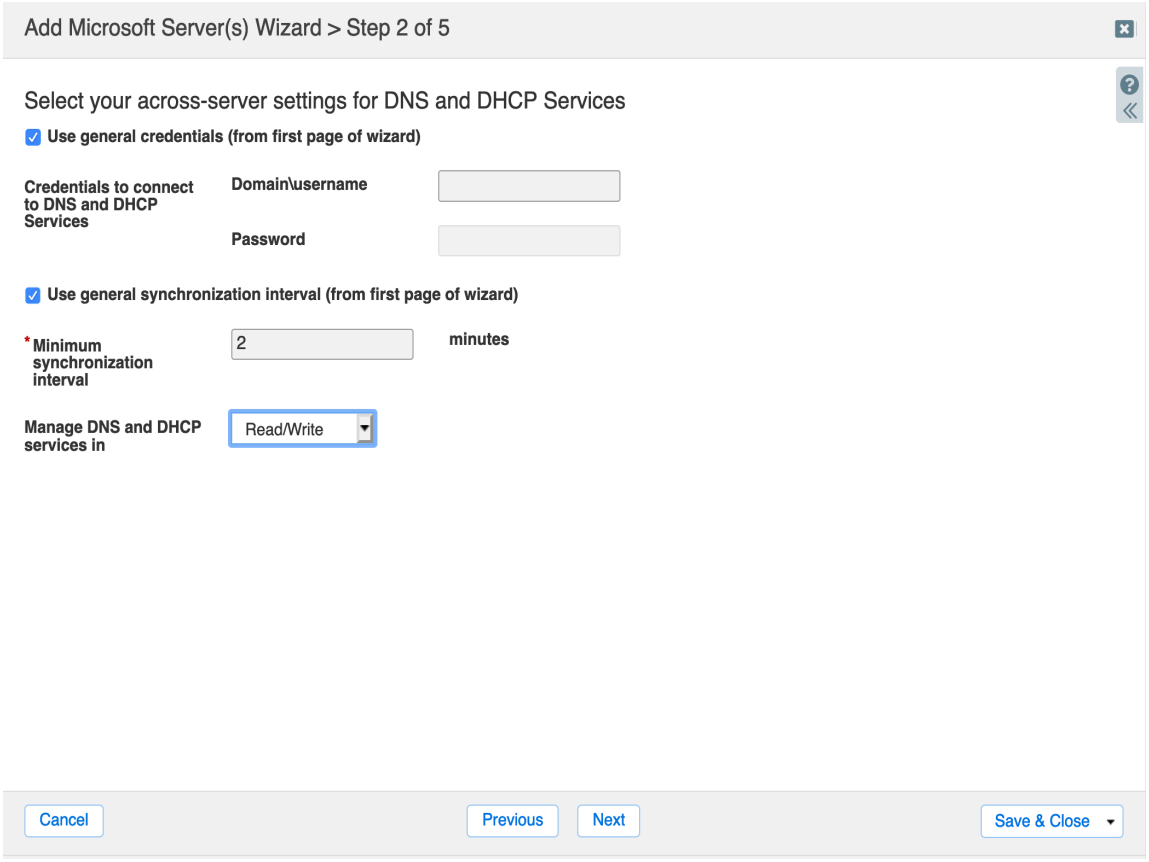
Add Microsoft DNS and DHCP servers to the Grid

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.

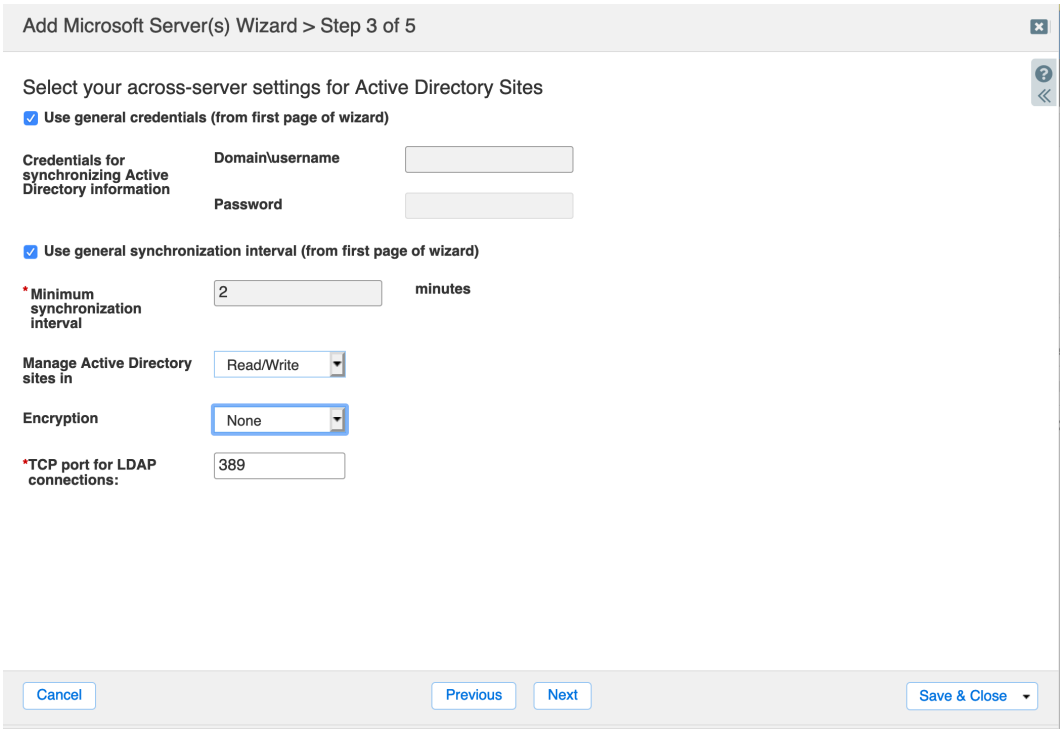
1. Navigate **Grid** → **Microsoft Servers** → **Toolbar** → **Add Microsoft Servers**. Enter the domain/username and password. Select the managing member by clicking on the **Select Member** button. Select the **Network View** and **DNS View** to synchronize. Click **Next**. *Note: The screenshot below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



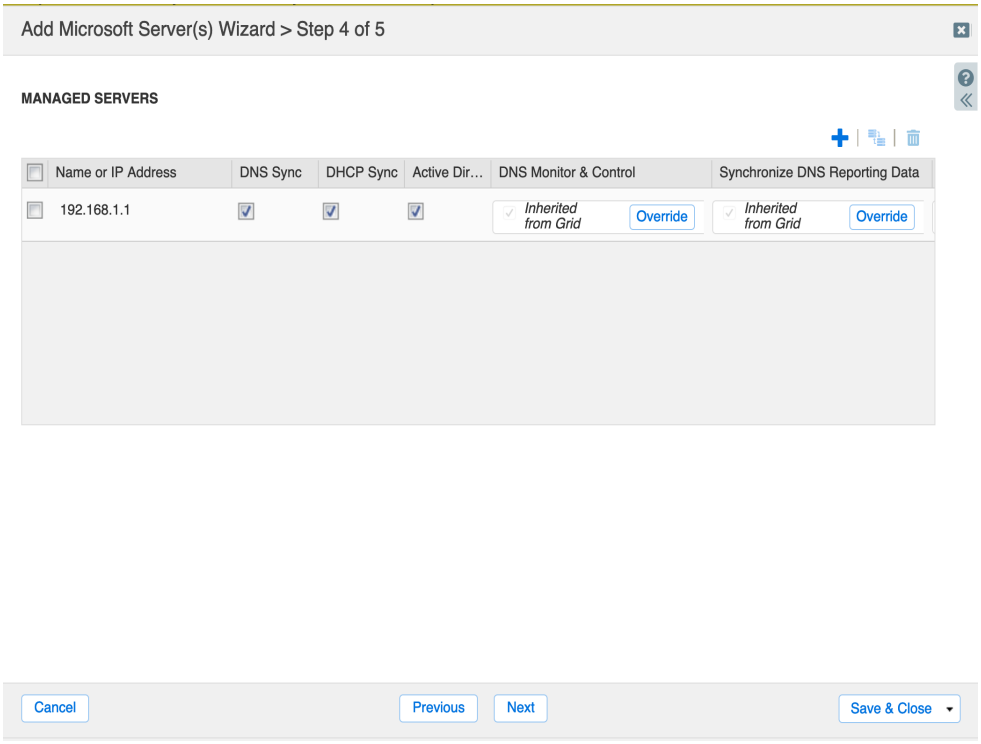
2. Set the credentials for connecting to DNS and DHCP services and set the **Manage DNS and DHCP services in** to Read/Write or Read Only. Click **Next**.



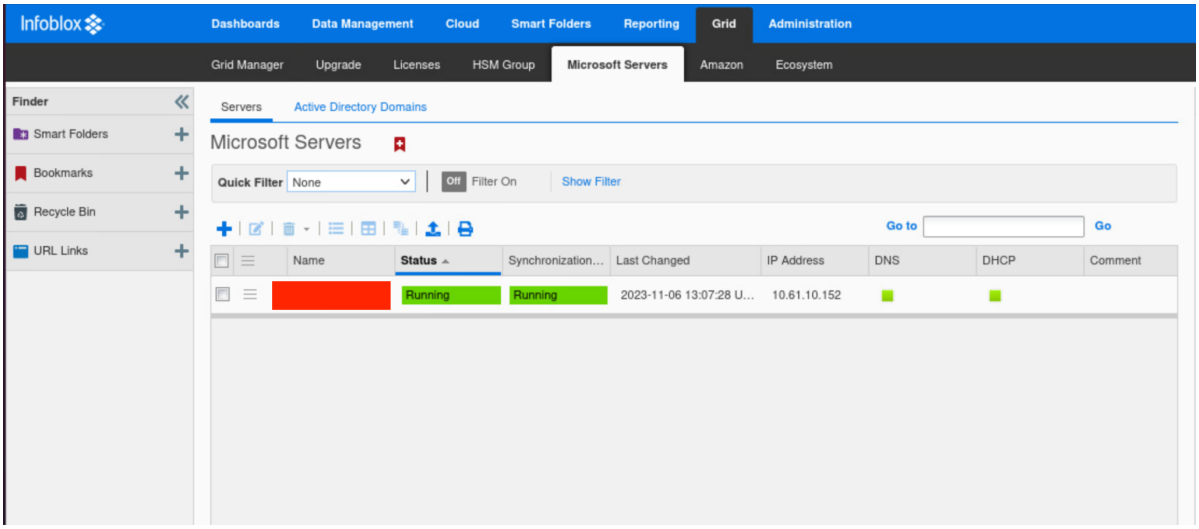
3. Set the credentials for connecting to Active Directory and set the **Manage Active Directory sites in** to Read/Write or Read Only. Click **Next**.



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**.

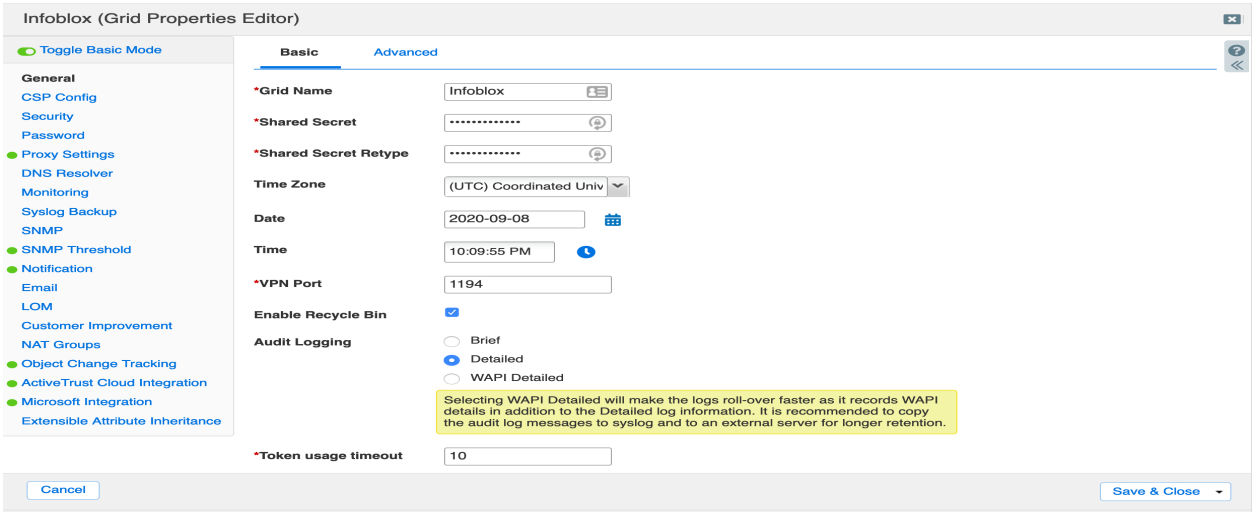


5. After about 5 minutes of synchronizing the data between the Grid Master, you should see the following:

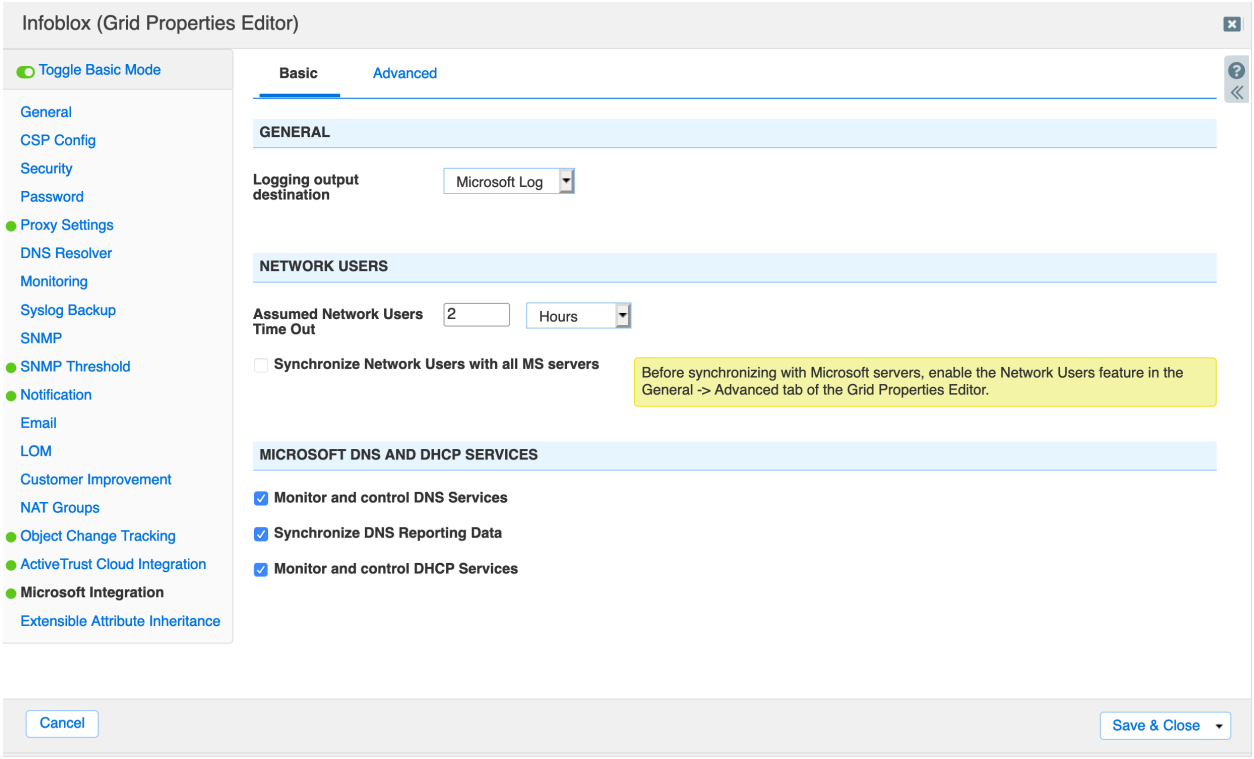


Enable receiving of report data from Microsoft server

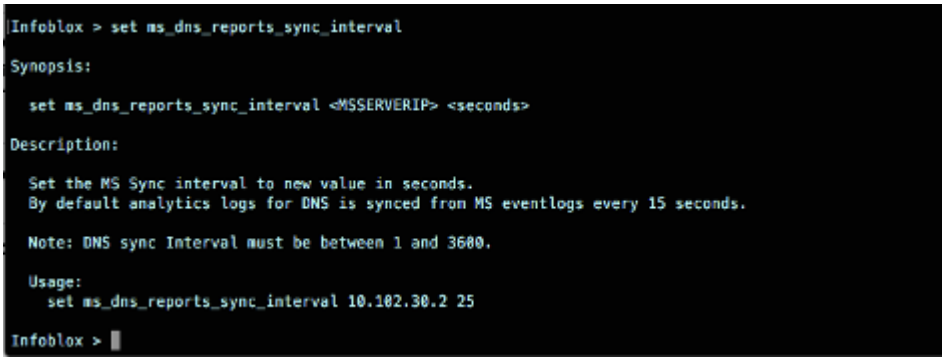
1. Navigate to **Grid → Grid Manager → Toolbar → Grid Properties → Edit**.



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

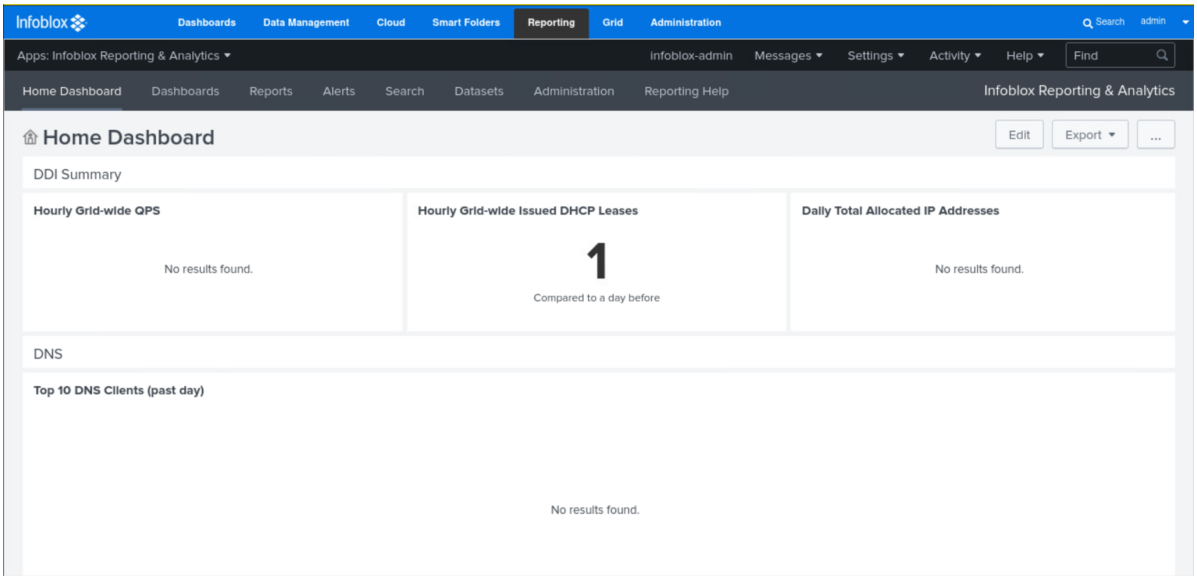


3. By default, the analytics logs from the Microsoft server are synchronized from Microsoft event logs every 15 seconds. You can change the DNS synchronization interval to any time between 1 second to 3600 seconds.



Viewing Reports

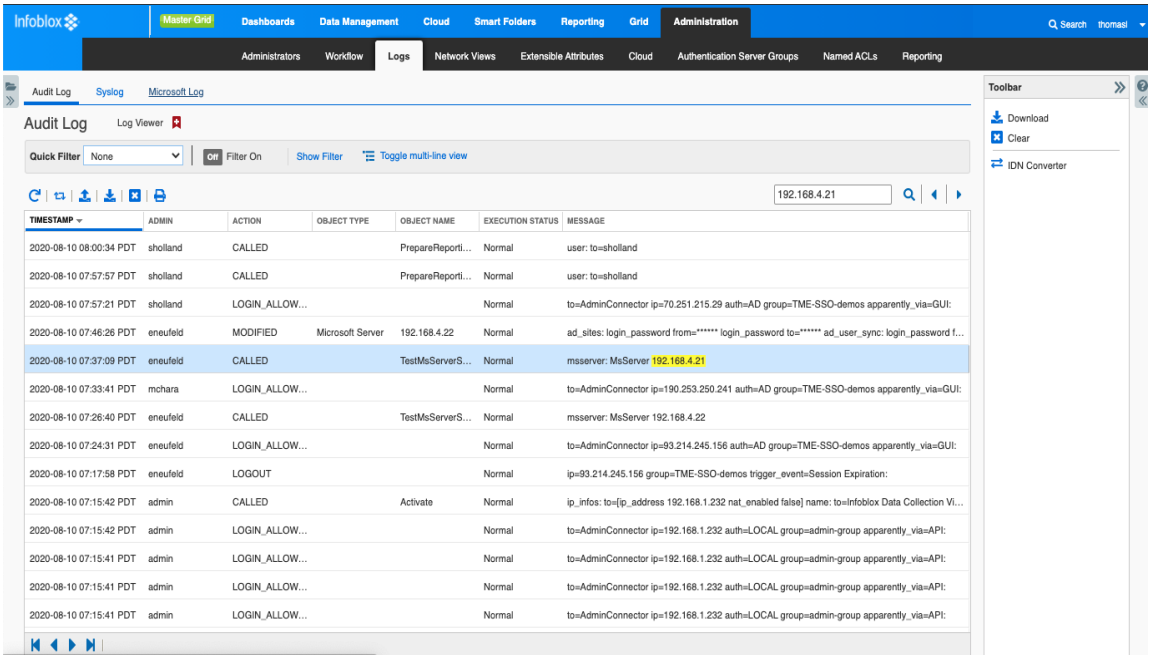
1. Navigate to the **Reporting tab** and pick one or more of the supported reports. Take note of the Microsoft server drop down menu for filtering purposes.



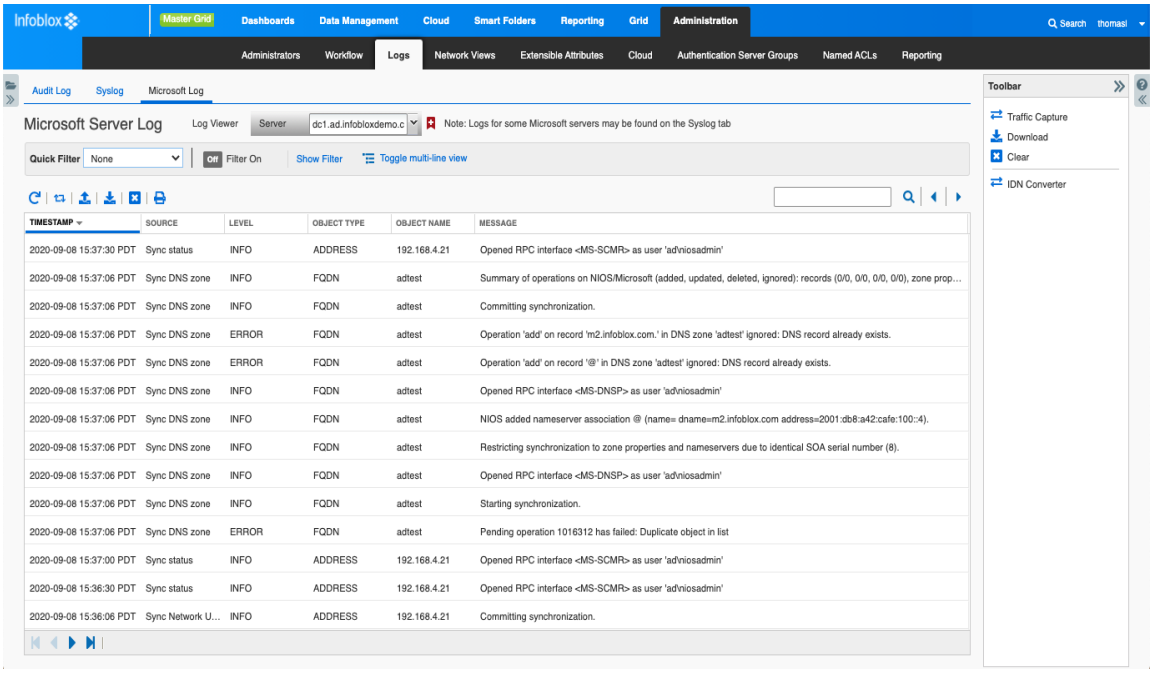
Troubleshooting

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**.



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