



DNS Discovery

June 2011

In This Article

- Overview
- Implementation
- Limitations

A supplemental discovery mechanism has been included with Netaphor SiteAudit™ 4.4 to allow discovery of printers by DNS name. The following information describes this new feature, how to use it, and its limitations.

Overview

The DNS discovery feature is a supplemental discovery technique implemented in SiteAudit to allow for scanning DNS names instead of IP addresses during the discovery phase. Previously, discovery was based on IP addresses only. The DNS discovery feature was added to facilitate those customers who want to either replace or augment the discovery scan range of IP hosts based on DNS names.

Implementation

The implementation has no visible UI. It relies on the existence of a single, specifically named text file: *SiteAuditDnsDiscoveredHosts.txt*. This file is referred to as the DNS hosts file.

This file must be created and placed into the same application folder as the configuration files used to adjust parameters related to monitoring, discovery etc. This folder is *C:\ProgramData\Netaphor\SiteAudit* or its equivalent on your system.

The file can contain multiple entries, one per line, each entry representing either a dotted-decimal IPv4 address, or a FQDN as specified by DNS (Domain Name Service) rules.

A line is defined as a sequence of characters followed by a line feed ("`\n`"), a carriage return ("`\r`"), or a carriage return immediately followed by a line feed ("`\r\n`").

DNS names are case-insensitive.

Entries may be additionally separated by blank lines for legibility. No other provisions such as commenting out a line or allowing multiple hosts to be specified on a single line are provided.

At the end of a discovery cycle, if the DNS hosts file is present, it is read line-by-line, and each host that successfully resolves to an IPv4 address is scanned for the presence of a

printer or a WMI printer host. The discovery cycle reports progress as it does for other discovery events.

If a host entry is malformed or cannot be resolved to an IPv4 address, it is skipped. An error message is entered into the Netaphor event log.

Limitations

This section describes the limitations of DNS Discovery

1. SiteAudit operates on IPv4 addresses. This mechanism does not change any operational aspects of SiteAudit on that basis.
2. While the scanning and discovery of IP addresses specified in the DNS hosts is under progress, the DNS hosts file is unavailable for editing. If editing is required at the time, the discovery process has to be stopped while the changes are made. Currently the only way to accomplish this by stopping the SiteAudit monitoring service.
3. Once a discovery cycle completes, no further attempts will be made to re-parse the file until the next discovery cycle, which by default is seven days later. Should a host change its IP address, SiteAudit will not monitor it unless the change is such that the new address was also being monitored by SiteAudit previously.
4. Should there be a need to monitor for host IP addresses more frequently, the only mechanism available to the user is to stop monitoring and restart it.
5. All other mechanisms of SiteAudit Discovery remain effective unless specifically disabled in the Discovery configuration. This means that should a host change its address in between two discovery cycles, while it will not be monitored by re-parsing the DNS hosts file, SiteAudit will automatically re-associate the correct printer with the IP address.
6. To disable this feature the DNS hosts file must be removed or renamed.

Example

The following is an example of *SiteAuditDnsDiscoveredHosts.txt*. This example contains three entries, one per line. The sample includes two DNS names and one IPv4 address. SiteAudit will attempt to resolve the DNS names and discover/monitor all three printers.

```
PRT299  
RIBEYE  
10.0.0.85
```