National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-81r1 Checklist Items and Microsoft Windows Server 2008 R2

Date created: 05/11/2008
Last modified: 11/09/2009

This document is intended to be a companion piece to NIST Special Publication 800-81r1. NIST SP 800-81r1 contains the text and descriptions of the checklist items listed below, but does not contain full descriptions of other DNS implementations. This supplement is intended to help administrators of these other DNS implementations to meet the checklist items in the Special Publication. Some checklist items in SP 800-81r1 do not apply to DNS server configuration but instead address general content management or network architecture recommendations. These checklist items are listed in the table below, but only for completeness, as they do not directly apply to the configuration or operation of a MS Windows Server 2008 R2 DNS deployment.

This supplement is not meant to be a guide on DNSSEC deployment on a MS Windows Server 2008 R2 system. Microsoft has developed guides for deployment and administrators should look there for documentation and how-to guidance. URL's to relevant Microsoft TechNet articles are included in the Notes section below for example commands and more information.

In the table below –
Checklist Item: Refers to the numbered checklist items in the text of NIST SP 800-81r1.
Applicable: Yes if the checklist item applies to the operation of a MS Windows system. No otherwise.
Compliance: Yes if the MS Windows system contains a feature or option that meets the checklist item. No otherwise.
Feature used: The specific feature or configuration option used to meet the checklist item.
Notes: Any other information about the feature or option. Or more information as to why the checklist item is not relevant or why compliance was not met.

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
1 (Section 7.4)	No	N/A		http://go.microsoft.com/fwlink/?LinkID-166512
2 (Section 7.4)	Yes	Yes	Microsoft TechNet website.	
3 (Section 7.4)	Yes	No		Microsoft servers respond to BIND version queries.
4 (Section 7.4)	No	N/A		Depends on the organization's network infrastructure.
5 (Section 7.4)	Yes	Yes	DNS Snap-in in MMC	http://technet.microsoft.com/en-us/library/ee649273%28WS.10%29.aspx
6	Yes	No (see	Listing forwarders in the DNS Snap-	http://technet.microsoft.com/en-

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
(Section 7.4)		Note)	In for MMC	us/library/cc754941.aspx
7 (Section 8.3)	Yes	No (see Note)	DNS Snap-In for MMC	No ACL for Windows Server, but can direct some queries to a forwarder (see Notes for Checklist Item 5 & 6).
8 (Section 8.3)	Yes	Yes (see Note)	GSS-TSIG	GSS-API is approved for use within the USG.
9 (Section 8.3)	Yes	No (See Note)	GSS-TSIG	Microsoft Win Server 2008 does not use TSIG to protect zone transfers. For secure dynamic update: http://technet.microsoft.com/en-us/library/cc753751.aspx
10 (Section 8.3)	Yes	Yes	GSS-TSIG	
11 (Section 8.3)	No	N/A	Handled by GSS-API	
12 (Section 8.3)	Yes	No	Handled by GSS-API lower level	Microsoft Win Server 2008 does not use TSIG to protect zone transfers. For secure dynamic update: http://technet.microsoft.com/en-us/library/cc753751.aspx
13 (Section 8.3)	Yes	Yes	Handled by OS.	The DNS server and all files can only be accessed by users with Administrator's privileges.
14 (Section 8.3)	Yes	Yes (See Note)	Handled via GSS-API	For secure dynamic update: http://technet.microsoft.com/en-us/library/cc753751.aspx
15 (Section 9.10)	Yes	Yes	Default behavior if DNSSEC signed zone loaded.	
16 (Section 9.10)	Yes	Yes	Handled by OS	All appropriate files can have access restricted to only those with Administrator's privileges. To export a key: http://technet.microsoft.com/en-us/library/ee649161%28WS.10%29.aspx
17 (Section 9.10)	Yes	Yes (See Note)	`DnsCmd` utility and the `/GenKey` option	Generate Keys: http://technet.microsoft.com/en-us/library/ee649204%28WS.10%29.aspx Sign zone file: http://technet.microsoft.com/en-us/library/ee649286%28WS.10

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
				%29.aspx
18 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
19 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
20 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
21 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
22 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
23 (Section 10.5)	No	N/A		Depends on DNS administrator's configuration choices.
24 (Section 10.5)	Yes	Yes	`DnsCmd /OfflineSign` command option for setting the validity period	http://technet.microsoft.com/en-us/library/ee649286%28WS.10%29.aspx
25 (Section 10.5)	Yes	Yes	`DnsCmd /OfflineSign` command option for setting the validity period	http://technet.microsoft.com/en-us/library/ee649286%28WS.10%29.aspx
26 (Section 10.5)	Yes	No	Microsoft Server 2008 R2 cannot generate or server NSEC3 signed zones.	NSEC3 not required for the protocol.
27 (Section 10.5)	Yes	No	Microsoft Server 2008 R2 cannot generate or server NSEC3 signed zones.	NSEC3 not required for the protocol.
28 (Section 11.4)	Yes	Yes	`DnsCmd` Tool to generate keys and sign zones.	http://technet.microsoft.com/en-us/library/ee649227%28WS.10%29.aspx
29 (Section 11.4)	Yes	Yes (see Note)	`DnsCmd` Tool to generate keys and sign zones.	http://technet.microsoft.com/en-us/library/ee649203%28WS.10%29.aspx
30 (Section 11.4)	Yes	Yes (see Note)	`DnsCmd` Tool to generate keys and sign zones.	http://technet.microsoft.com/en-us/library/ee649203%28WS.10%29.aspx
31 (Section 11.4)	No	N/A		Organization's DNS admin responsible for contact information
32 (Section 11.4)	No	N/A		Organization's DNS admin responsible for contact information
33 (Section 11.4)	Yes	Yes	`DnsCmd` Tool to generate keys and sign zones.	http://technet.microsoft.com/en-us/library/ee649228%28WS.10%29.aspx

Checklist Item (Section)	Applicable	Compliance	Feature used	Notes
34 (Section 11.4)	Yes	Yes	`DnsCmd` Tool to generate keys and sign zones.	Zone administrator should make sure the SOA serial number is incremented before re-signing the zone file.