

DNSSEC in Windows Server

DNS Server changes

- Provide DNSSEC support in the DNS server
 - Changes should allow federal agencies to comply with SC-20 and SC-21 security controls proposed in NIST 800-53.
 - DNS servers support signed DNS records and return the signatures in response to queries (SC-20)
 - DNS servers support recursive resolvers that authenticate and check integrity of secure records (SC-21)

DNS Server changes

- Highlights
 - Implement core RFCs 4033, 4034, 4035
 - Support for RRSIG, NSEC, DNSKEY, DS
 - Tool for signing DNS zone files.
 - Enable verification of chain of trust
 - Authentication and Integrity check of records
 - Enable support for trust anchors
 - Policy to return only secure records to clients.
 - Other policies under consideration.

Our plans

- Planning currently in progress
- Beta: middle of 2007
- RTM: late 2007 or early 2008
 - General availability by first service pack of Longhorn Server.