DNS Traffic Management and DNS data mining

Making Windows DNS Server Cloud Ready
~Kumar Ashutosh, Microsoft
Windows DNS Server

- Widely deployed in enterprises
- Fair presence in the DNS resolver space
- Standards compliant and interoperable
- Secure and scalable
Needs of DNS server in cloud

- Policy based traffic management
- Audit and billing mechanism for DNS service
- The DNS data mine and analytics
- Security and High availability
Policy based Traffic Management

- DNS Policy is **Windows DNS Server** construct that allows DNS administrators to control the DNS Query processing in order to achieve:
  - Global Traffic Management,
  - Application Load Balancing,
  - Intelligent DNS responses based on communication protocol (IPV4 or V6) or transport protocol (UDP and TCP),
  - Applying tenant specific filters for black holing, parental control etc.
  - Split-Brain DNS Deployment
    ... and much more
Anatomy of a policy

Criteria
Any combination of Client Subnet, Server Interface IP, FQDN, Internet protocol (IPV4/V6), Transport Protocol (UDP/TCP), Time Of Day, Query Type

Action
If policy matches what action to take: ALLOW, DENY, IGNORE

Content
If Action is allow, what data to respond with and in what ratio.
Capabilities

- Traffic Management
  - Location aware responses

- High Availability
  - Improve availability of critical applications by failover policies

- Load Balancing
  - Application Load Balancing based on the performance of host

- Time of day
  - Time of day based policies

- Filters
  - Split Brain DNS
  - Black Hole and Filters
DNS Audit Trail

What changed?
- Zone
- Server
- Record

Who changed?
- DC admin
- Tenant admin

When?
- For Reporting
- Audit Trails
- diagnostics
DNS Data mine

Data collection → Data Preparation → Pattern discovery → Actionable Information
DNS Data mine: Data Collection

- Collect data from every DNS server
- Centralized system for collection
- Real time collection with minimal performance impact
- Kinds of Data collected:
  - All DNS transactions
    - Queries/responses
    - XFR
    - Dynamic updates
  - Server state
    - Health indicators
    - Performance counters
DNS Data mine : Data Preparation

- Cleaning the data
- Data transformation
  - Creating relational databases for different purposes
  - Related calculations – like amplification factor, frequency etc.
  - Collation of data across the server farm
- Correlation of data
  - Across multiple servers
  - Between single user
  - Relationship with state of the server.
- Rolling over with knowledge transfer.
DNS Data mine: Pattern Discovery

- Domain name analysis,
- Amplification analysis
- User behaviour analysis
- Client subnet analysis
- Security analysis
DNS Data mine: Actionable Information

- User behaviour analytics
- Load model
- DDoS detection
Thank You