Implementing and securing a resilient network services infrastructure
Implementing a resilient network services infrastructure

Kier Prior-Williams
Calleva Networks
kpw@callevanetworks.com
Agenda

• The need for resilience
• DNS resilience
  • Challenges and Solutions
• DHCP resilience
  • Challenges and Solutions
• The benefits of integrated IPAM, DNS, DHCP
• Summary
• Q&A
The need for resilience

• Without core network services (DNS & DHCP)
  • Users can't access the network/internet
  • Email not working
  • Apps not working
• Stuff breaks! Users are on the phone to support (unless it's VoIP!)
• Resilient DNS/DHCP services can eliminate potential network downtime
DNS resilience
Existing DNS environment?

- May have lots of Microsoft DNS...
  - AD integrated
  - DNS running on all your DC’s
- It probably works more by accident than by design...
  - There are likely to be inconsistencies
- Patch Tuesday forces a monthly reboot?
Existing DNS environment?

- Hybrid deployment...
  - Both Linux and Microsoft DNS servers
- Keeping BIND updated can be a challenge
  - Security vulnerabilities
  - How do you patch?
- Do you integrate BIND and AD?
  - Or run completely separate environments?
DNS support & resilience

- Can you count on a vendor for support?
- Have you configured any kind of resilience?
  - VIPs or Windows/Linux Cluster
  - RAID 1 to combat HDD failure?
  - Dual PSU?
- Are you doing any monitoring and alerting?
DNS deployment considerations

• **Internal DNS:**
  • Clients configured to talk to 2 or more servers
  • Local survivability needed? Local DNS service vs Centralised service

• **External DNS:**
  • Separation of services:
    • Authoritative (offsite secondary, geographic diversity)
    • Recursive (but no open recursive!)
DNS High Availability

• Shared VIP across multiple DNS servers
  • Commonly use Router Redundancy Protocols

• Benefits:
  • Lose one node and another node provides service
  • No downtime during upgrades/maintenance

• Considerations:
  • Must be on same layer 2 network
  • Number of HA pairs
DNS High-availability

Step 1: Server 1 failed
VIP1 is automatically reallocated to server 2

Step 2: Server 1 reinstatement
VIP1 is automatically reallocated to server 1

SCALABILITY
Add new server 3 with shared VIP2
DNS Anycast

- Allows multiple, geographically diverse DNS servers to advertise the same IP address
  - Looks like multiple routes to the same server
- A user’s query is routed to their nearest DNS server
- If that server dies, queries get routed to the next nearest instance
DNS Anycast – benefits

- Increased Reliability/Availability. Lose several DNS servers and we've still got service
- Improved performance
- Load balancing
- Resilience against DDoS attacks (localised impact of the attack)
- Simplified Client Configuration
- Internet Root servers use it – so it can’t be bad
DNS Anycast – considerations

- Consistent data on DNS servers
- Rollout is not a trivial task
- Need a good relationship with the network guy (better still - you are the network guy)
- Troubleshooting
Load balancers (hardware)

• Use a load balancing appliance in front of a DNS server farm
• Load balancer will distribute queries and monitor DNS servers
• Good:
  • Existing infrastructure may support this
  • No DNS outage when a server fails or during maintenance
Load balancers

• Considerations:
  • Additional technology now in the data flow
  • Consistent data on DNS servers
  • May complicate troubleshooting
  • Different teams likely to be involved - finger pointing
  • Expense of new kit if there isn’t enough capacity in existing load balancer appliances
Other DNS considerations

- Standard DNS security: version updates (DNS binary & OS), ACLs, data flows
- DNSSEC: Data integrity - validate the origin and integrity of DNS data
- DNS Firewall (RPZ-based) – block access to Malware sites at the DNS level
- DDoS mitigation service
DHCP resilience
Existing DHCP environment?

• Linux and/or Microsoft?
  • Is failover deployed?
    • Failover is not split-scopes!
• Many devices dependent upon DHCP
  • VoIP Phones, wireless clients, desktops etc.
• Support/management/monitoring
• How do you document IP allocations?
Management headaches

• Microsoft DNS/DHCP use separate MMC consoles
  • And you have to know which server to connect to
  • Limited granular access control
• Linux is primarily command line driven
• IPAM normally done elsewhere
  • e.g. In a spreadsheet
DHCP – Single server

• Individual server(s) doing DHCP
• Server dies
  • No-one can get a new IP
  • Clients with a lease okay up to expiry time
• How long to restore the configuration?
• Lost some or all of the IP lease information
• Clients may have to change IP address
DHCP split-scope

- Multiple, independent DHCP servers
- Typically known as “80/20 split”
- DHCP servers are independent of each other
- If you lose the 80% server, does the 20% server have the capacity to handle all clients
- A client will have to change its IP address when getting a lease from the "other" server
DHCP failover

- DHCP protocol level redundancy
- Two DHCP servers in a “relationship”
  - Doesn’t have to be a monogamous relationship!
- Share a common pool of DHCP addresses
- Synchronise lease information
- Consideration:
  - As an admin, you need to know how the failover behaves if you do lose a DHCP server
DHCP failover benefits

- **Benefits:**
  - Resiliency – if one server is down, the other still provides service
  - No risk of duplicate IP addresses
  - Load-balancing – Active/Active
  - Geographically separate locations - different subnets
DHCP One-to-one failover
DHCP Star Failover
IPAM / DDI
What is IPAM

- IPAM is a management process that involves documenting IP subnets and addresses
- IPAM benefits:
  - Centralised view of an IP plan
  - Avoid service disruption - duplicate IPs
  - Capacity planning for future growth
  - Granular role based delegation
  - Auditing
How does DDI fit in?

• Integrating IPAM with DNS and DHCP

• Enables:
  • Backups and Disaster Recovery process for DNS/DHCP configuration and IPAM data
  • Move away from traditional "server-by-server" management to an architecture-based administration
  • Simplify provisioning of IP/DHCP/DNS
    • Do it once
Introducing a DDI solution

- IP address plan management
- Integrated network services engines: DNS-DHCP-NTP-TFTP
- Multi-vendor DNS & DHCP services management
  - Microsoft – ISC – Cisco – SOLIDServer™
- Active IP address tracking with IPLocator module
- Unified system management
  - Integrated zero admin database
  - Hardened OS with embedded stateful firewall
  - Simplified upgrades, backups and disaster recovery
Multi-vendor/heterogeneous support

Centralised DDI Management and backup
Active mode

Data Center A

Centralised DDI Management and backup
Recovery mode

Data Center B

Data centre 1

Data centre 2

SOLIDserver
DNS-DHCP-NTP-TFTP
High Availability

Existing DNS DHCP architecture management

Cisco IOS

Open source DNS DHCP

Microsoft DNS DHCP

Microsoft Certified Partner
SMART Architectures™: DNS-DHCP Architecture Management

SmartArchitecture™ are Templates of DNS or DHCP architectures

Each slot has a predefined role in the SmartArchitecture™

Each DNS server is inserted in the appropriate slot

Automated configurations of all servers according to their role in the SmartArchitecture™

Ex: Master-Slave
SMART Architectures™: Architecture Management

- Smart Architecture™ Library

**DHCP**
- DHCP Single
- DHCP Failover One to One
- DHCP Split Scope
- DHCP Star Failover

**DNS**
- DNS Single
- DNS Master-Slave
- DNS Multi-Master
- DNS Stealth
- DNS Slave
- Hidden DNS Master
SMART Architectures™: Move to Architecture Management

- Reduce Complexity: Manage Architectures rather than servers
- Automate your Deployment and Management

DHCP Star Failover

DNS Master-Slave

DNS Multi-Master

Global Architecture Management

DHCP Split Scope

DNS Stealth
User defined home pages

Customised Bookmarks
Customised Alerts
Customised Quick wizard
Customised Quick searches
Customised Top lists

User-defined pies and graphs based on Metadata
Intuitive full function UI

- Unified IPAM DNS DHCP view
- Display of user defined metadata
- IP address template for server object
- User-defined wizards with metadata
DDI Reconciliation

- Active IP address tracking with IPLocator
  - Identify IP/MAC address connections on the network
  - Identify associated switch and switch port

![Diagram showing IP address connection tracking and associated switch and port information.]
Summary

• The need for resilient network services
• Deploying resilient DNS services
• Deploying resilient DHCP services
• Benefits of an integrated DNS, DHCP, IPAM solution
Thank You

Kier Prior-Williams
kpw@callevanetworks.com
www.callevanetworks.com
@CallevaNerworks