Key3 Media Group PRESENTS NETWORLD+INTEROP

Directory and Active Directory Overview

Daniel Blum

Senior Vice President, Research Director

Dblum@tbg.com

September 12, 2001

Directory Overview

Words to live by

> “In theory there is no difference between theory and practice. In practice there is.”
>
> Yogi Berra

Directory Overview

In theory, Active Directory will . . .

- Relieve the headaches associated with managing NT Server domains, reducing TCO
  - A more scalable naming context that eliminates the complexity of point-to-point trust relationships
  - Delegated administration
  - Centralized systems management functions for operating systems and applications
  - Integrated security management model, including both Kerberos and public key infrastructure (PKI)
- Support Microsoft's e-business initiatives

Directory Overview

In practice, Active Directory will . . .

- Solve some existing problems, introduce new ones
  - AD is better than NT 4 domains and should make Windows 2000 clients and servers cheaper to own and manage over the long term
  - But getting there will be expensive and difficult for large organizations; requires intensive planning up front
  - Earlier marketing oversimplified deployment issues
  - Active Directory is a “1.0” product and isn’t perfect
  - While clearly suited to the NOS administration role, AD isn’t as well-suited for other directory roles, so it won’t solve all of your directory problems

Active Directory in Context

Active Directory’s roles

- Win2K Server: Highly integrated, standards support, but monolithic due to focus on NOS market drivers
- In theory, AD can be THE enterprise and e-business directory
- In practice, AD is primarily a NOS admin directory
  - Reflects Microsoft’s focus on improving Windows client and server management
  - Tightly integrated environment yields many benefits in the NOS environment
  - But tight integration makes AD inflexible in other roles
  - Limitations can make deployment, management a challenge in any role

Active Directory in Context

The NOS role: Upsides

- Upside: Massive improvement over NT domains
  - LDAP, Kerberos, DNS, DHCP, delegated administration, policy-based resource management, separates user & machine identities, roaming…
- Downsides: Numerous gotchas
  - Single schema per forest, cannot remove items
  - Full-mesh replication within domains (no partitions)
  - Expensive to replicate global catalog, multivalued attributes
  - Weak change management tools for rename, merge
  - Hard to deploy 1 enterprise-wide forest w/few domains
  - No inheritance across domains in a forest
  - Management tools lack drag and drop GUI functions

Active Directory in Context

Bottom line assessment

- Some, but not all AD gotchas will improve with Windows .NET server next year
  - Change management, Global Catalog, inter-forest trusts
- So, for most organizations, it’s not a question of “if”, but a question of “when and in what roles”
  - Microsoft’s dominant position in the server OS and messaging markets ensures that some customers upgrade willingly, others because they have to
  - Most will use AD in the NOS role, but many will instead use best of breed directories in enterprise or e-business roles

Active Directory in Context

Migration: What to watch out for

- Expect the expected (in ANY directory migration, not just AD)
  - Distributed nets w/low bandwidth links, branch offices
  - Must prevent bottom-up, poorly planned deployments
  - Delays, political problems with naming and tree design
- Deploying multiple forests is complex
  - 1 schema per forest, no inter-forest synchronization
  - Creates need for meta-directory services
- Enterprises must plan carefully or they will fail to realize many of Windows 2000 Server's benefits
- A poorly planned AD deployment will be no better than an NT Server domain deployment

Active Directory in Context

Success is a function of planning

- Forest(s), domain(s), and tree design
  - Multiple forests are complex, but likely
  - Don’t underestimate difficulty of naming/tree design
  - It’s political, not technical, so get started early
- DNS and domain controller deployment
  - Physical topology requires careful balance of tradeoffs
  - Many want to deploy servers in data centers, but it’s difficult for distributed orgs with low-bandwidth links
  - Login via global catalog complicates deployment across remote offices
  - Integration with existing DNS/DHCP can also be a complex undertaking

Active Directory in Context

Success is a function of planning

- Migration planning
  - Modeling and piloting in advance
  - Choosing in-place upgrades vs. parallel deployments
  - Use of third-party tools highly recommended; will minimize issues like managing SID history, coexistence with other directories, others
- Active Directory is a work in progress
  - You'll need other third-party tools to augment functionality and manageability after migration
    - Migration
    - Post migration management/administration
    - Enterprise DNS Management

E-Business Infrastructure

Conclusion

- Its important to set realistic expectations, separate theory from practice
- Organizations must consider AD migration within the framework of an overall enterprise architecture
  - When (or if) AD makes sense in your environment
  - What roles Active Directory can and should play
- Active Directory promises value to large enterprises, but migration will be a large effort
- Organizations must conduct extensive planning and preparation efforts before making the leap