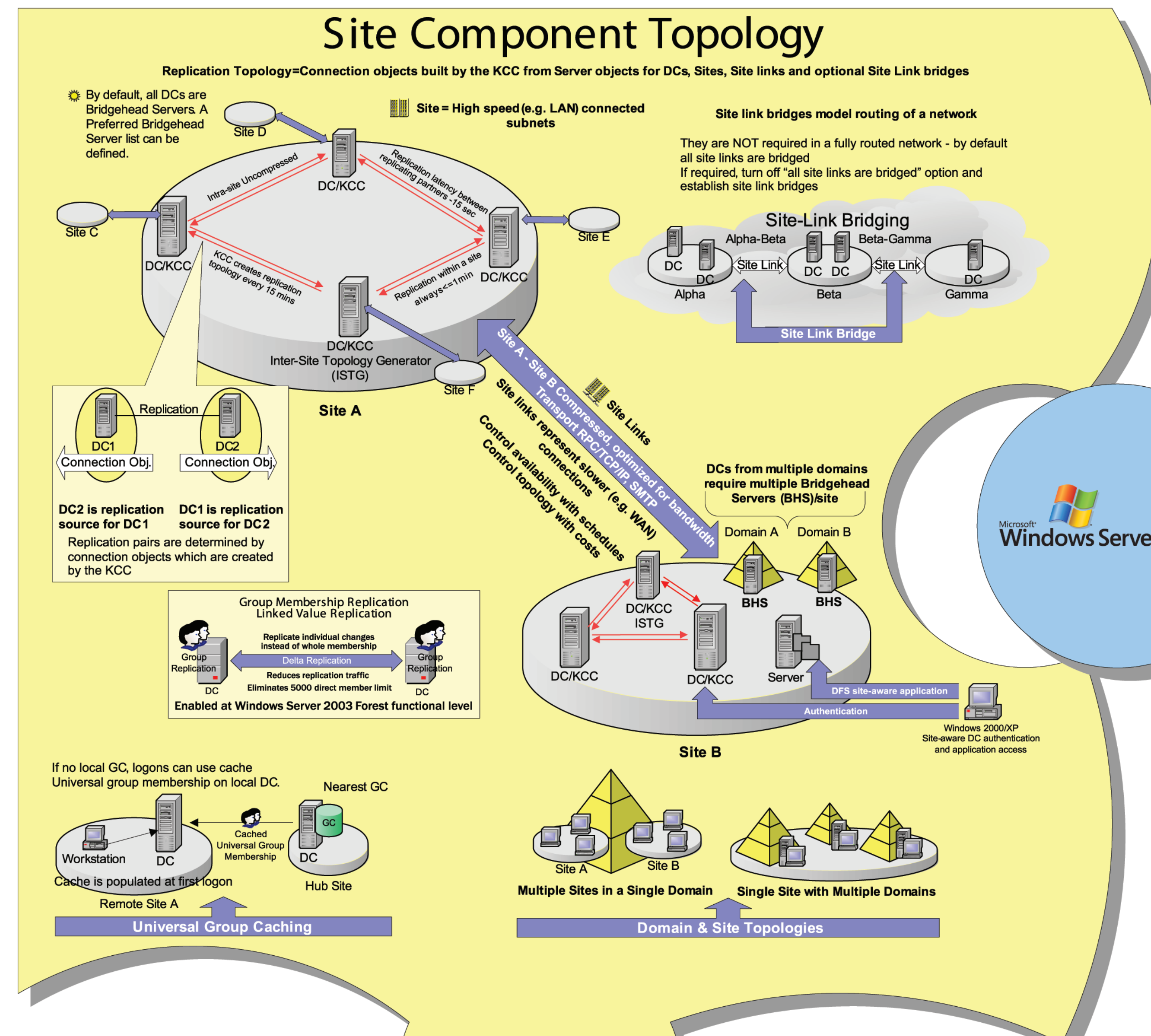
Microsoft Windows Server 2003
www.microsoft.com/activedirectory
www.technetmagazine.com

TechNet MAGAZINE
The Microsoft Journal For IT Professionals

Microsoft Windows Server 2003
Active Directory Component Jigsaw

Site Component Topology

Replication Topology=Connection objects built by the KCC from Server objects for DCs, Sites, Site links and optional Site Link bridges


Site D
Site C
Site E
Site F
DC/KCC
Intra-site Uncompressed
Replication latency between replicating partners -15 sec
KCC creates replication topology every 15 mins
Replication within a site always<=1min
DC/KCC Inter-Site Topology Generator (ISTG)
Site A
Site-Link Bridging
Alpha-Beta
Beta-Gamma
Site Link
DC
Alpha
Beta
Gamma
Site Link Bridge
Site Links
Site A - Site B Compressed, optimized for bandwidth
Transport RPC/TCP/IP, SMTP
Replication
DC1
DC2
Connection Obj.
Domain A
Domain B
BHS
DC/KCC ISTG
Server
DFS site-aware application
Authentication
Site B
Group Replication
Nearest GC
GC
Cached Universal Group Membership
Workstation
Hub Site
Remote Site A
Site A
Site B

By default, all DCs are Bridgehead Servers. A Preferred Bridgehead Server list can be defined.

Site = High speed (e.g. LAN) connected subnets

Site link bridges model routing of a network

They are NOT required in a fully routed network - by default all site links are bridged
If required, turn off "all site links are bridged" option and establish site link bridges

Site links represent slower (e.g. WAN) connections
Control availability with schedules
Control topology with costs

DC2 is replication source for DC1

DC1 is replication source for DC2

Replication pairs are determined by connection objects which are created by the KCC

DCs from multiple domains require multiple Bridgehead Servers (BHS)/site

Group Membership Replication
Linked Value Replication
Replicate individual changes instead of whole membership
Delta Replication
Reduces replication traffic
Eliminates 5000 direct member limit
Enabled at Windows Server 2003 Forest functional level

Windows 2000/XP Site-aware DC authentication and application access

If no local GC, logons can use cache Universal group membership on local DC.

Cache is populated at first logon

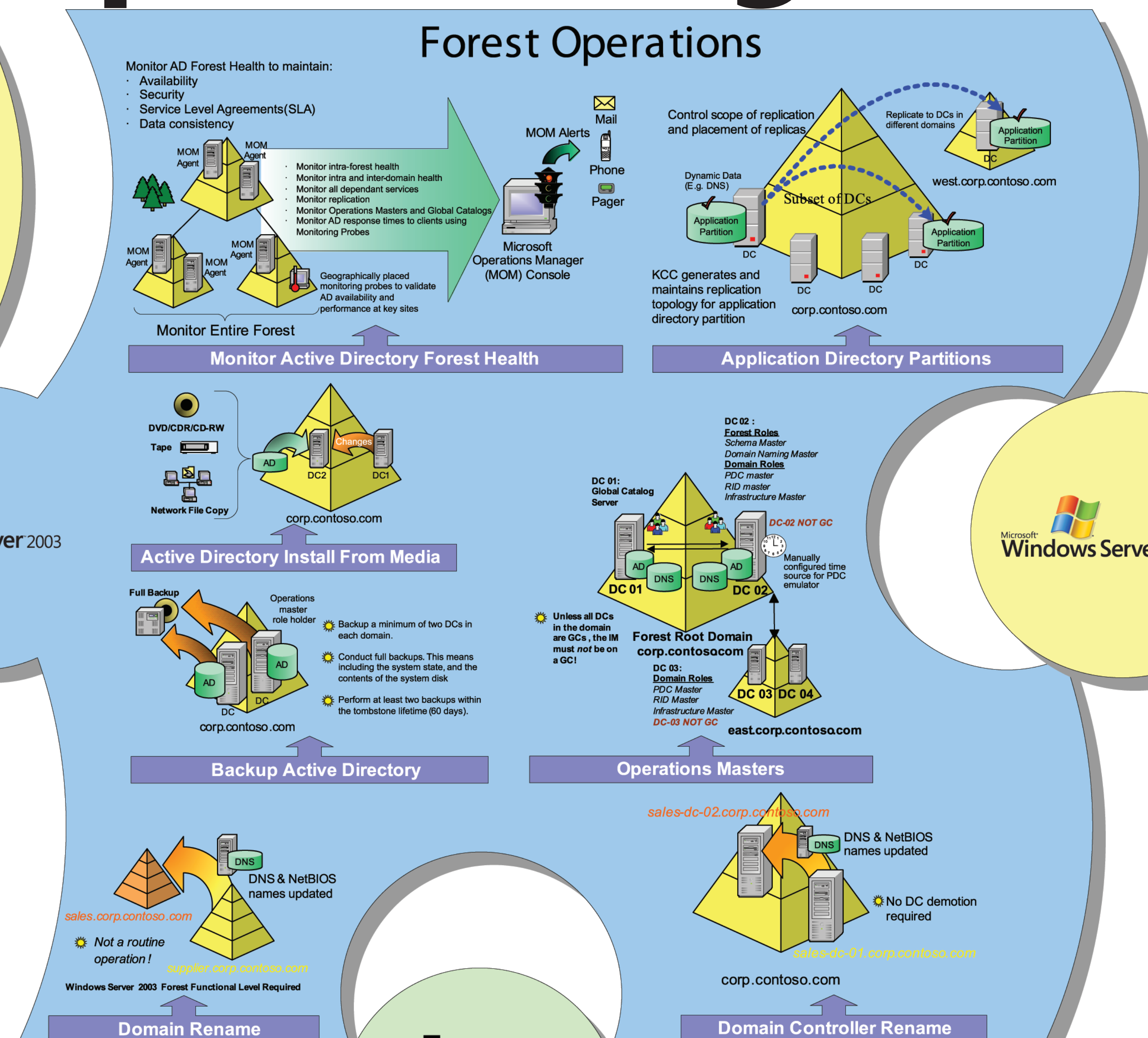
Universal Group Caching

Multiple Sites in a Single Domain

Single Site with Multiple Domains

Domain & Site Topologies

Forest Operations



Monitor AD Forest Health to maintain:
- Availability
- Security
- Service Level Agreements(SLA)
- Data consistency

- Monitor intra-forest health
- Monitor intra and inter-domain health
- Monitor all dependant services
- Monitor replication
- Monitor Operations Masters and Global Catalogs
- Monitor AD response times to clients using Monitoring Probes

Geographically placed monitoring probes to validate AD availability and performance at key sites

Monitor Active Directory Forest Health

Control scope of replication and placement of replicas

KCC generates and maintains replication topology for application directory partition

Application Directory Partitions

Active Directory Install From Media

Backup a minimum of two DCs in each domain.

Conduct full backups. This means including the system state, and the contents of the system disk

Perform at least two backups within the tombstone lifetime (60 days).

Backup Active Directory

DC 02 :
Forest Roles
Schema Master
Domain Naming Master
Domain Roles
PDC master
RID master
Infrastructure Master
DC-02 NOT GC

Manually configured time source for PDC emulator

Unless all DCs in the domain are GCs , the IM must *not* be on a GC!

DC 03:
Domain Roles
PDC Master
RID Master
Infrastructure Master
DC-03 NOT GC

Operations Masters

DNS & NetBIOS names updated

Not a routine operation !

Windows Server 2003 Forest Functional Level Required

Domain Rename

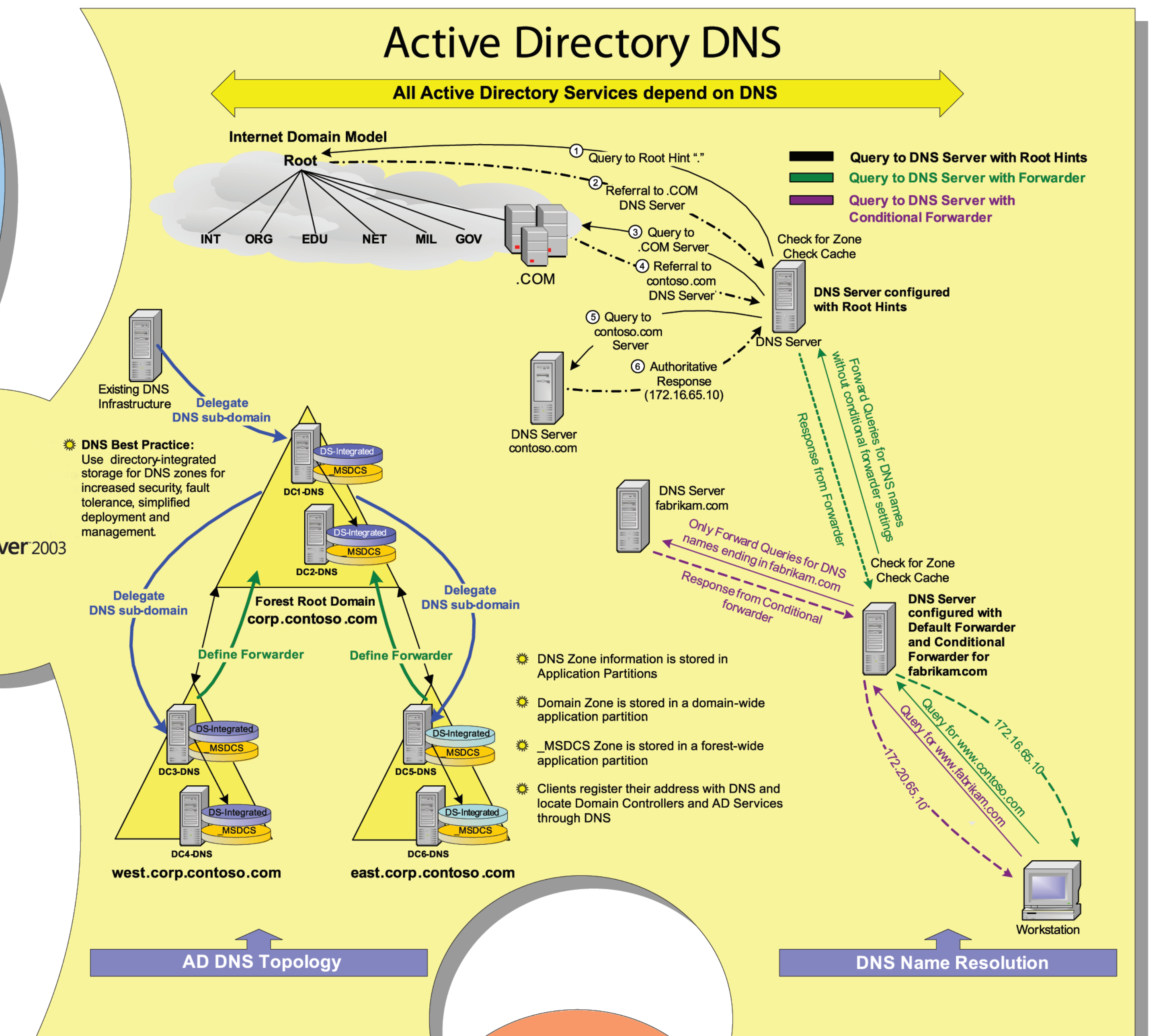
DNS & NetBIOS names updated

No DC demotion required

Domain Controller Rename

Active Directory DNS

All Active Directory Services depend on DNS


Internet Domain Model
Root
INT
ORG
EDU
NET
MIL
GOV
.COM
1 Query to Root Hint "."
2 Referral to .COM DNS Server
3 Query to .COM Server
4 Referral to contoso.com DNS Server
5 Query to contoso.com Server
6 Authoritative Response (172.16.65.10)
Check for Zone Check Cache
DNS Server configured with Root Hints
DNS Server
DNS Server contoso.com
Forward Queries for DNS names without conditional forwarder settings
Response from Forwarder
DNS Server fabrikam.com
Only Forward Queries for DNS names ending in fabrikam.com
Response from Conditional forwarder
DNS Server configured with Default Forwarder and Conditional Forwarder for fabrikam.com
Query for www.contoso.com
172.16.65.10
Query for www.fabrikam.com
172.20.65.10
Workstation
Existing DNS Infrastructure
Delegate DNS sub-domain
DS-Integrated
_MSDCS
DC1-DNS
DC2-DNS
DC3-DNS
DC4-DNS
DC5-DNS
DC6-DNS
Forest Root Domain corp.contoso .com
Define Forwarder
west.corp.contoso.com
east.corp.contoso .com

▬	Query to DNS Server with Root Hints
🟩	Query to DNS Server with Forwarder
🟪	Query to DNS Server with Conditional Forwarder

DNS Best Practice: Use directory-integrated storage for DNS zones for increased security, fault tolerance, simplified deployment and management.

DNS Zone information is stored in Application Partitions

Domain Zone is stored in a domain-wide application partition

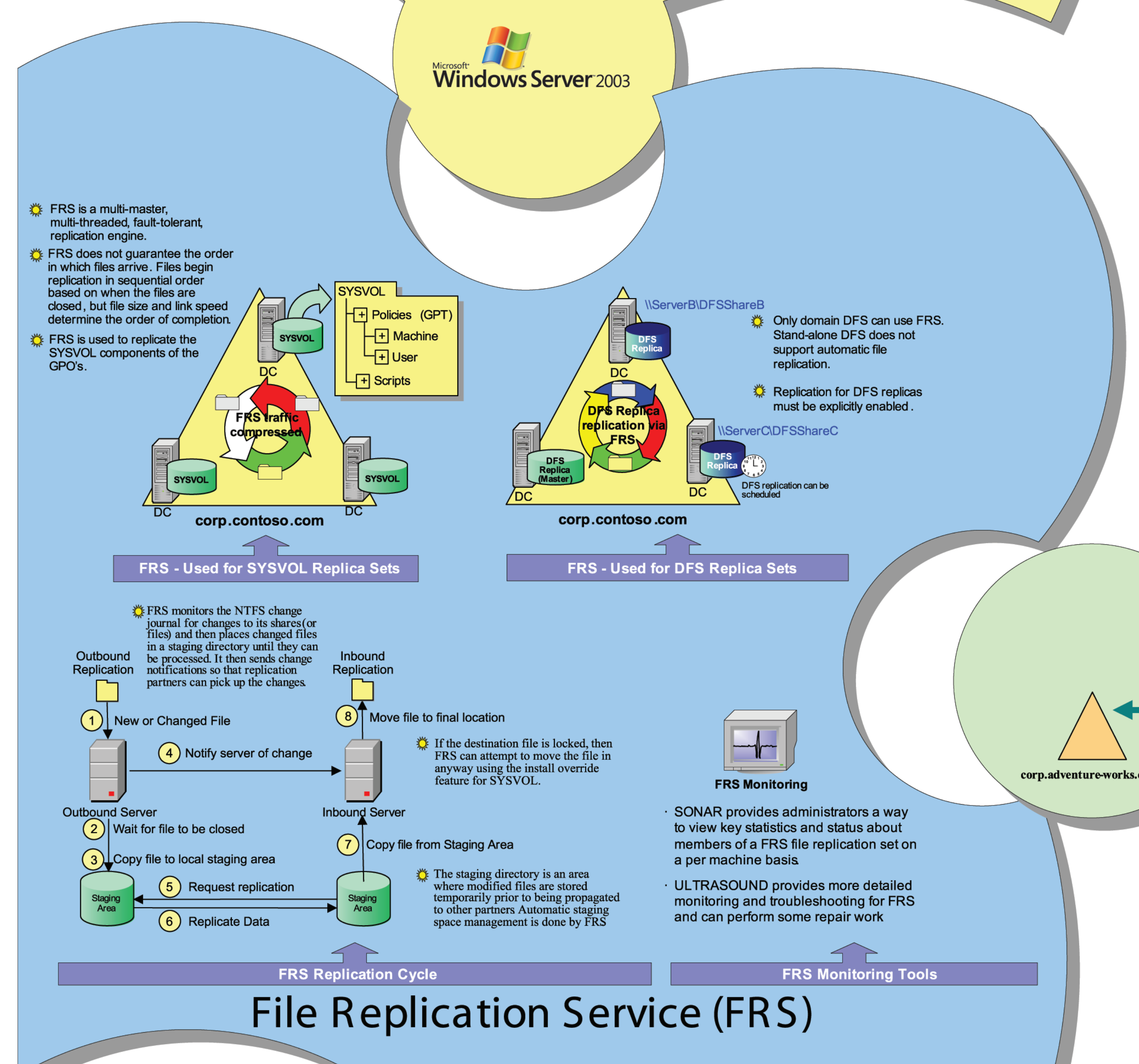
_MSDCS Zone is stored in a forest-wide application partition

Clients register their address with DNS and locate Domain Controllers and AD Services through DNS

AD DNS Topology

DNS Name Resolution

File Replication Service (FRS)



FRS is a multi-master, multi-threaded, fault-tolerant, replication engine.

FRS does not guarantee the order in which files arrive. Files begin replication in sequential order based on when the files are closed, but file size and link speed determine the order of completion.

FRS is used to replicate the SYSVOL components of the GPO's.

FRS - Used for SYSVOL Replica Sets

Only domain DFS can use FRS. Stand-alone DFS does not support automatic file replication.

Replication for DFS replicas must be explicitly enabled.

DFS replication can be scheduled

FRS - Used for DFS Replica Sets

FRS monitors the NTFS change journal for changes to its shares(or files) and then places changed files in a staging directory until they can be processed. It then sends change notifications so that replication partners can pick up the changes.

If the destination file is locked, then FRS can attempt to move the file in anyway using the install override feature for SYSVOL.

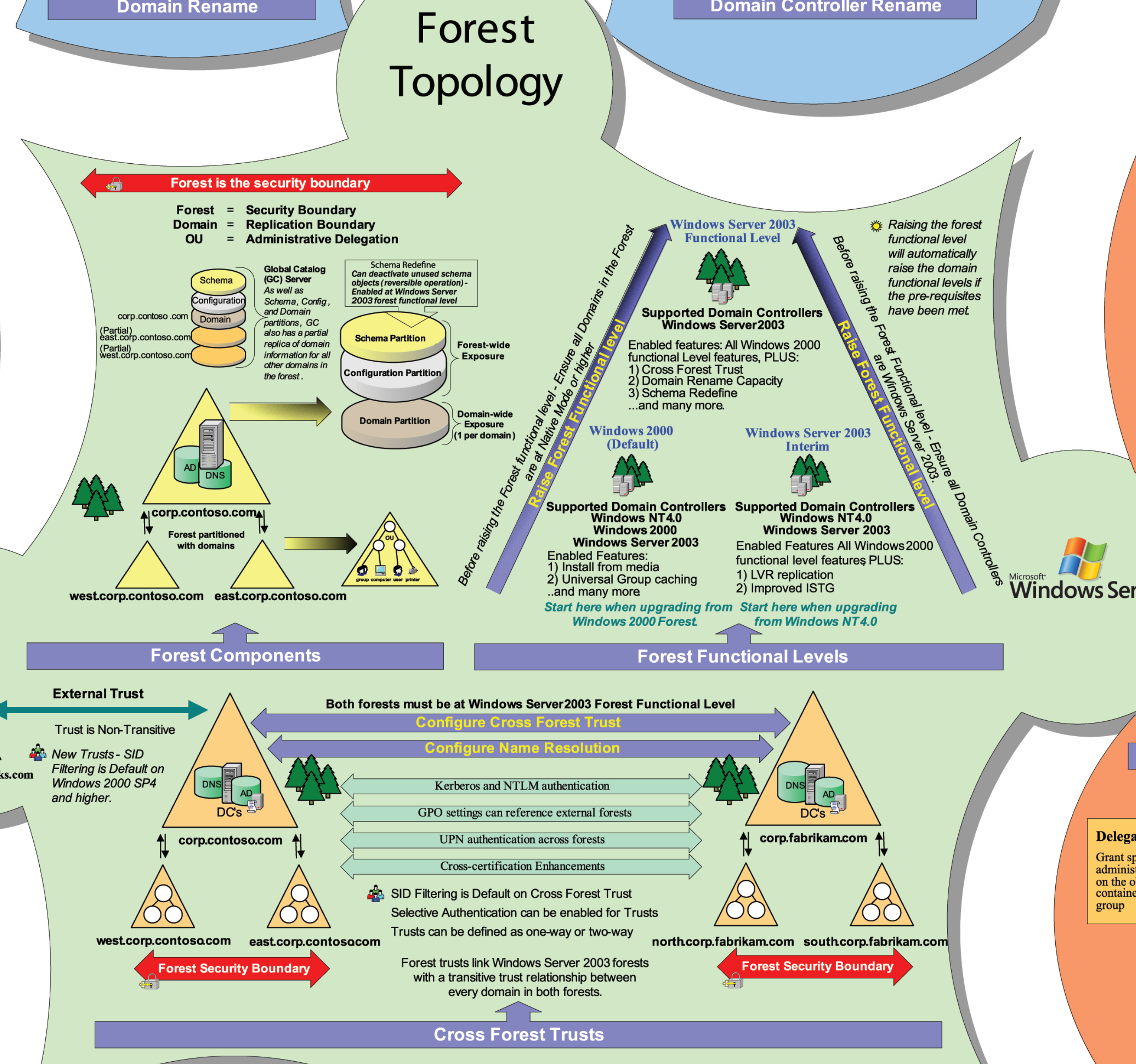
The staging directory is an area where modified files are stored temporarily prior to being propagated to other partners Automatic staging space management is done by FRS

FRS Replication Cycle

- SONAR provides administrators a way to view key statistics and status about members of a FRS file replication set on a per machine basis.
- ULTRASOUND provides more detailed monitoring and troubleshooting for FRS and can perform some repair work

FRS Monitoring Tools

Forest Topology


Schema
Configuration
Domain
corp.contoso .com
(Partial) east.corp.contoso.com
(Partial) west.corp.contoso.com
Schema Partition
Configuration Partition
Domain Partition
Forest-wide Exposure
Domain-wide Exposure (1 per domain)
AD
DNS
corp.contoso.com
Forest partitioned with domains
west.corp.contoso.com
east.corp.contoso.com
OU
group computer user printer
Windows Server 2003 Functional Level
Windows 2000 (Default)
Windows Server 2003 Interim
Raise Forest Functional level
Before raising the Forest functional level - Ensure all Domains in the Forest are at Native Mode or higher
Before raising the Forest Functional level - Ensure all Domain Controllers are Windows Server 2003.
External Trust
corp.adventure-works.com
DC's
corp.fabrikam.com
north.corp.fabrikam.com
south.corp.fabrikam.com
Forest Security Boundary

Forest is the security boundary

Forest	=	Security Boundary
Domain	=	Replication Boundary
OU	=	Administrative Delegation

Global Catalog (GC) Server
As well as Schema, Config, and Domain partitions, GC also has a partial replica of domain information for all other domains in the forest.

Schema Redefine
Can deactivate unused schema objects (reversible operation) - Enabled at Windows Server 2003 forest functional level

Forest Components

Supported Domain Controllers
Windows Server2003
Enabled features: All Windows 2000 functional Level features, PLUS:
1) Cross Forest Trust
2) Domain Rename Capacity
3) Schema Redefine
...and many more.

Raising the forest functional level will automatically raise the domain functional levels if the pre-requisites have been met

Supported Domain Controllers
Windows NT4.0
Windows 2000
Windows Server 2003
Enabled Features:
1) Install from media
2) Universal Group caching
..and many more
Start here when upgrading from Windows 2000 Forest.

Supported Domain Controllers
Windows NT4.0
Windows Server 2003
Enabled Features All Windows2000 functional level features, PLUS:
1) LVR replication
2) Improved ISTG
Start here when upgrading from Windows NT4.0

Forest Functional Levels

Trust is Non-Transitive

New Trusts - SID Filtering is Default on Windows 2000 SP4 and higher.

Both forests must be at Windows Server2003 Forest Functional Level

Configure Cross Forest Trust

Configure Name Resolution

Kerberos and NTLM authentication

GPO settings can reference external forests

UPN authentication across forests

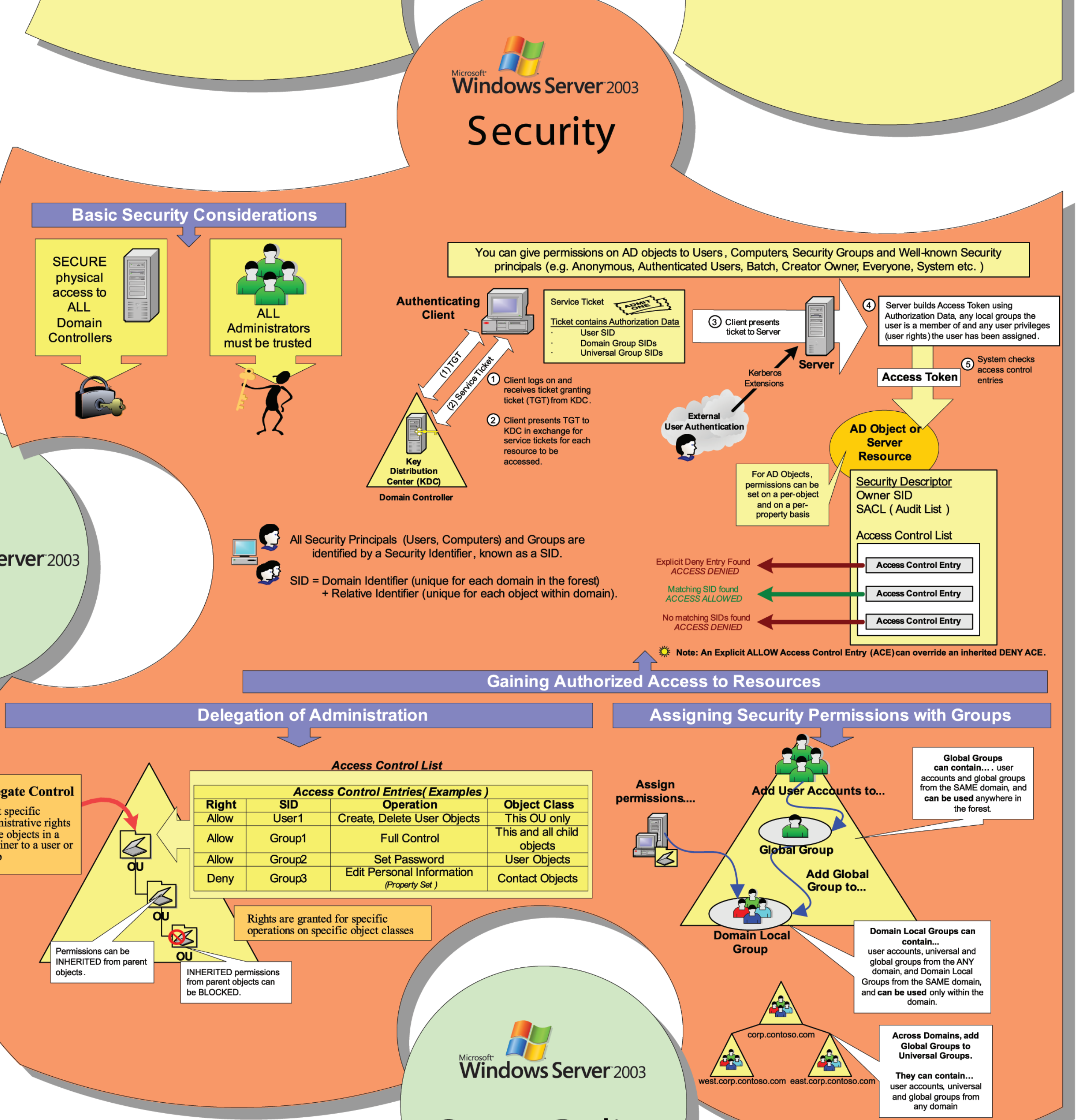
Cross-certification Enhancements

SID Filtering is Default on Cross Forest Trust
Selective Authentication can be enabled for Trusts
Trusts can be defined as one-way or two-way

Forest trusts link Windows Server 2003 forests with a transitive trust relationship between every domain in both forests.

Cross Forest Trusts

Security



Basic Security Considerations

SECURE physical access to ALL Domain Controllers

ALL Administrators must be trusted

You can give permissions on AD objects to Users, Computers, Security Groups and Well-known Security principals (e.g. Anonymous, Authenticated Users, Batch, Creator Owner, Everyone, System etc.)

Ticket contains Authorization Data
- User SID
- Domain Group SIDs
- Universal Group SIDs

1 Client logs on and receives ticket granting ticket (TGT) from KDC.

2 Client presents TGT to KDC in exchange for service tickets for each resource to be accessed.

3 Client presents ticket to Server

4 Server builds Access Token using Authorization Data, any local groups the user is a member of and any user privileges (user rights) the user has been assigned.

5 System checks access control entries

For AD Objects, permissions can be set on a per-object and on a per-property basis

Security Descriptor
Owner SID
SACL (Audit List)
Access Control List

Explicit Deny Entry Found ACCESS DENIED

Matching SID found ACCESS ALLOWED

No matching SIDs found ACCESS DENIED

All Security Principals (Users, Computers) and Groups are identified by a Security Identifier, known as a SID.

SID = Domain Identifier (unique for each domain in the forest) + Relative Identifier (unique for each object within domain).

Note: An Explicit ALLOW Access Control Entry (ACE) can override an inherited DENY ACE.

Gaining Authorized Access to Resources

Delegation of Administration

Delegate Control
Grant specific administrative rights on the objects in a container to a user or group

Access Control List

Access Control Entries(Examples)

Right	SID	Operation	Object Class
Allow	User1	Create, Delete User Objects	This OU only
Allow	Group1	Full Control	This and all child objects
Allow	Group2	Set Password	User Objects
Deny	Group3	Edit Personal Information *(Property Set)*	Contact Objects

Rights are granted for specific operations on specific object classes

Permissions can be INHERITED from parent objects.

INHERITED permissions from parent objects can be BLOCKED.

Assigning Security Permissions with Groups

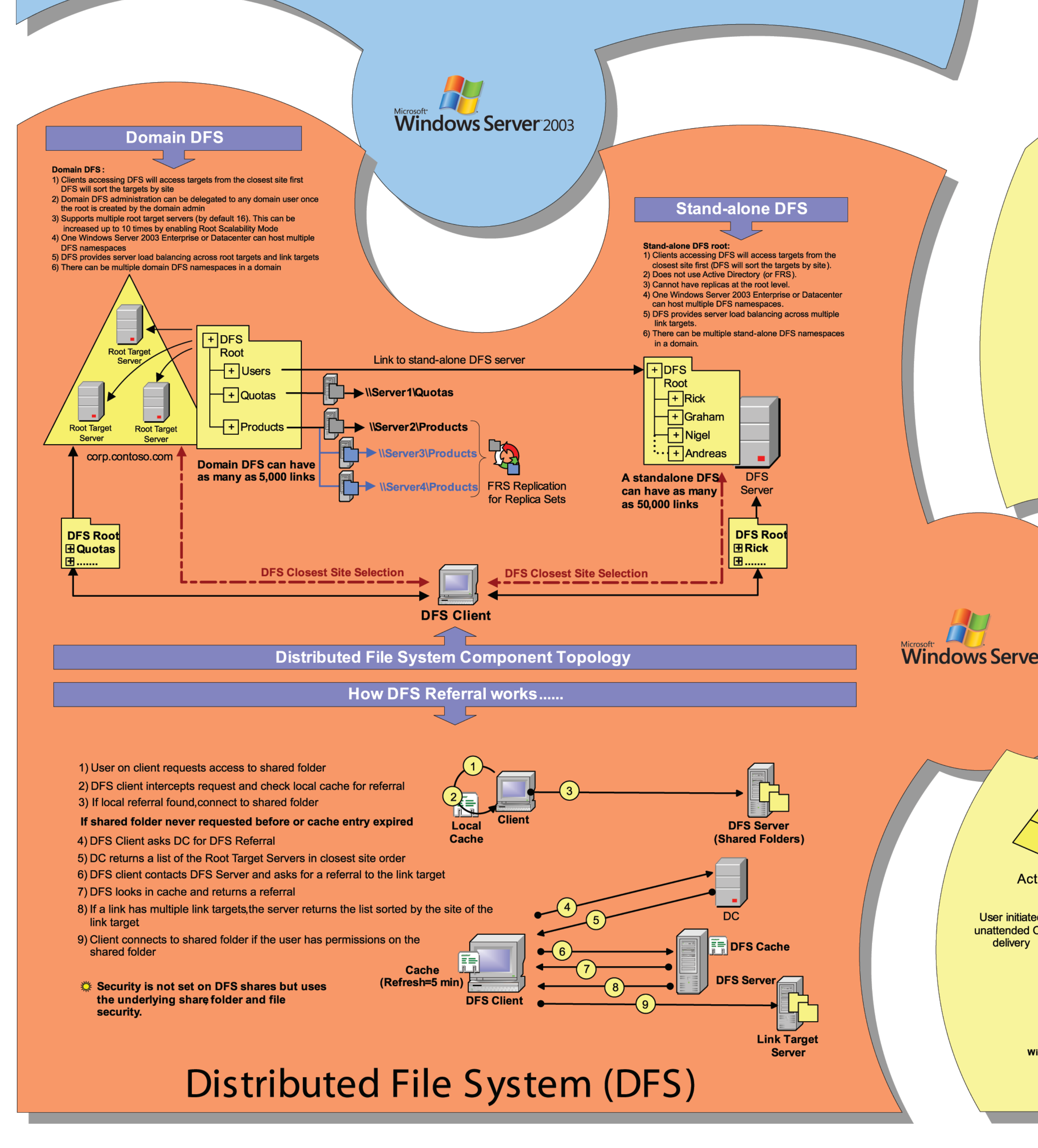
Global Groups can contain.... user accounts and global groups from the SAME domain, and can be used anywhere in the forest.

Domain Local Groups can contain... user accounts, universal and global groups from the ANY domain, and Domain Local Groups from the SAME domain, and can be used only within the domain.

Across Domains, add Global Groups to Universal Groups.

They can contain... user accounts, universal and global groups from any domain

Distributed File System (DFS)



Domain DFS

Domain DFS :
1) Clients accessing DFS will access targets from the closest site first DFS will sort the targets by site
2) Domain DFS administration can be delegated to any domain user once the root is created by the domain admin
3) Supports multiple root target servers (by default 16). This can be increased up to 10 times by enabling Root Scalability Mode
4) One Windows Server 2003 Enterprise or Datacenter can host multiple DFS namespaces
5) DFS provides server load balancing across root targets and link targets
6) There can be multiple domain DFS namespaces in a domain

Stand-alone DFS

Stand-alone DFS root:
1) Clients accessing DFS will access targets from the closest site first (DFS will sort the targets by site).
2) Does not use Active Directory (or FRS).
3) Cannot have replicas at the root level.
4) One Windows Server 2003 Enterprise or Datacenter can host multiple DFS namespaces.
5) DFS provides server load balancing across multiple link targets.
6) There can be multiple stand-alone DFS namespaces in a domain.

Domain DFS can have as many as 5,000 links

A standalone DFS can have as many as 50,000 links

Distributed File System Component Topology

How DFS Referral works......

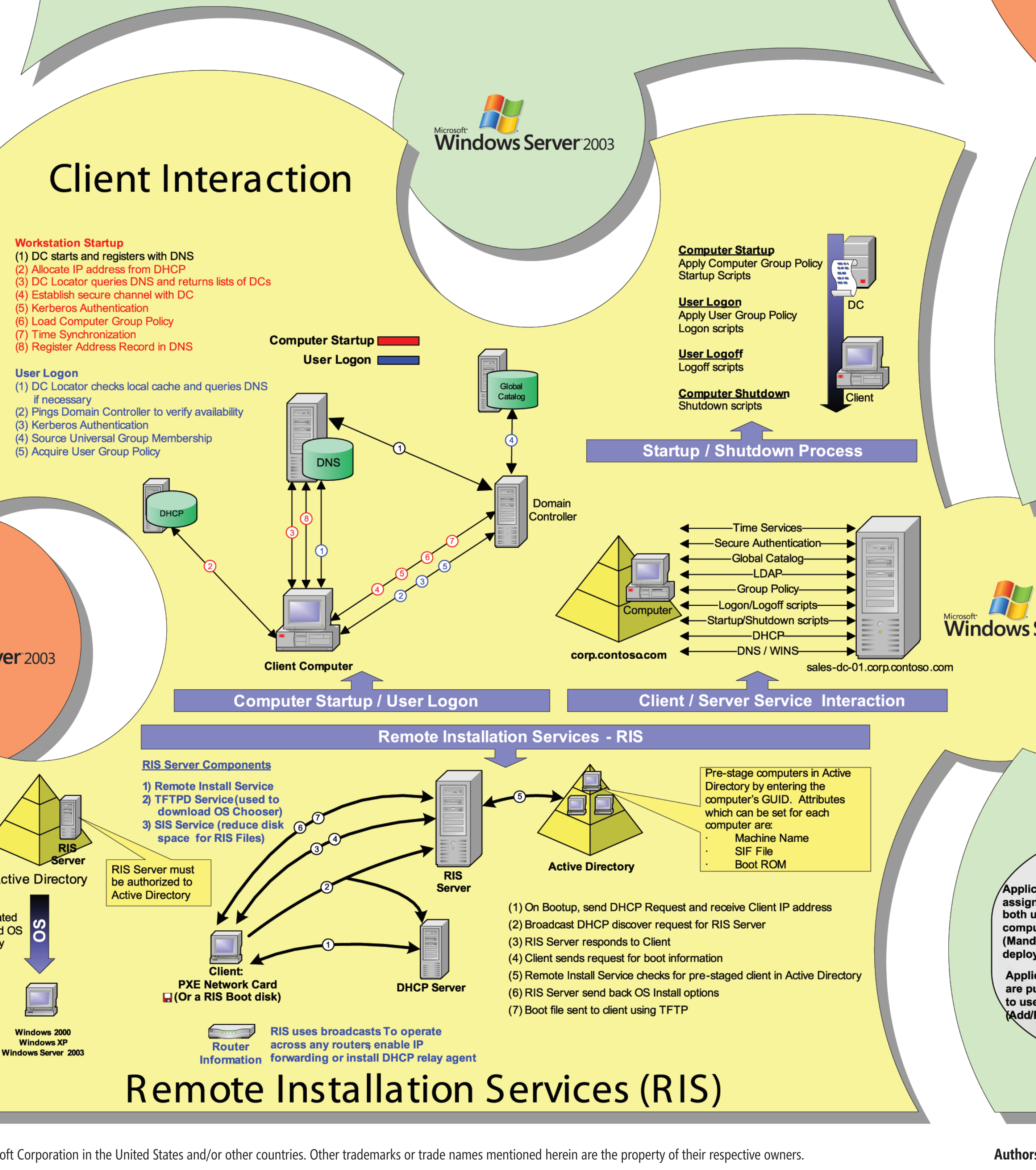
1) User on client requests access to shared folder
2) DFS client intercepts request and check local cache for referral
3) If local referral found,connect to shared folder

If shared folder never requested before or cache entry expired

4) DFS Client asks DC for DFS Referral
5) DC returns a list of the Root Target Servers in closest site order
6) DFS client contacts DFS Server and asks for a referral to the link target
7) DFS looks in cache and returns a referral
8) If a link has multiple link targets,the server returns the list sorted by the site of the link target
9) Client connects to shared folder if the user has permissions on the shared folder

Security is not set on DFS shares but uses the underlying share folder and file security.

Client Interaction



Workstation Startup
(1) DC starts and registers with DNS
(2) Allocate IP address from DHCP
(3) DC Locator queries DNS and returns lists of DCs
(4) Establish secure channel with DC
(5) Kerberos Authentication
(6) Load Computer Group Policy
(7) Time Synchronization
(8) Register Address Record in DNS

User Logon
(1) DC Locator checks local cache and queries DNS if necessary
(2) Pings Domain Controller to verify availability
(3) Kerberos Authentication
(4) Source Universal Group Membership
(5) Acquire User Group Policy

Computer Startup	🟥
User Logon	🟦

Computer Startup / User Logon

Computer Startup
Apply Computer Group Policy
Startup Scripts

User Logon
Apply User Group Policy
Logon scripts

User Logoff
Logoff scripts

Computer Shutdown
Shutdown scripts

Startup / Shutdown Process

Client / Server Service Interaction

Remote Installation Services - RIS

RIS Server Components
1) Remote Install Service
2) TFTPD Service(used to download OS Chooser)
3) SIS Service (reduce disk space for RIS Files)

RIS Server must be authorized to Active Directory

User initiated unattended OS delivery

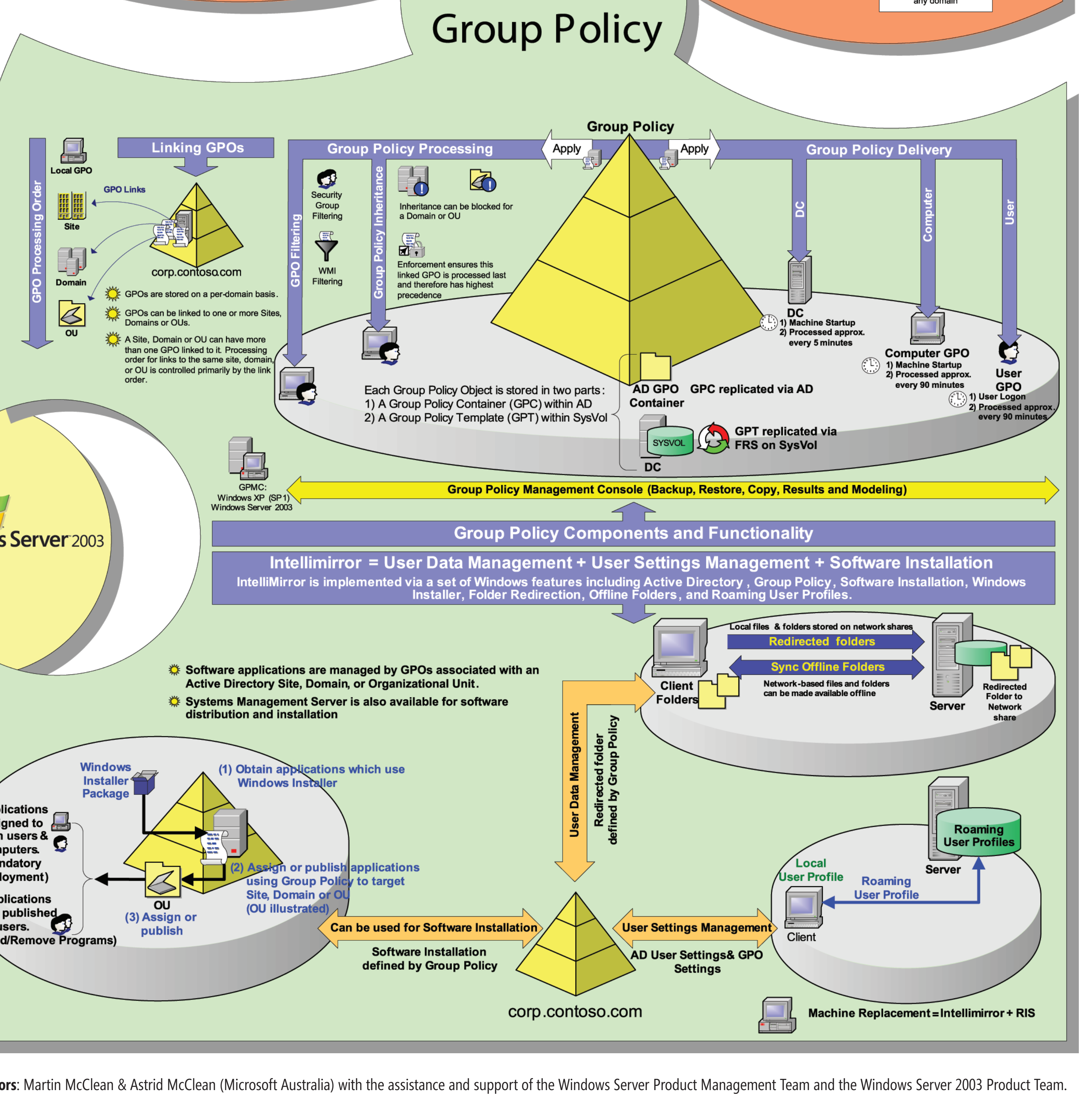
Pre-stage computers in Active Directory by entering the computer's GUID. Attributes which can be set for each computer are:
- Machine Name
- SIF File
- Boot ROM

(1) On Bootup, send DHCP Request and receive Client IP address
(2) Broadcast DHCP discover request for RIS Server
(3) RIS Server responds to Client
(4) Client sends request for boot information
(5) Remote Install Service checks for pre-staged client in Active Directory
(6) RIS Server send back OS Install options
(7) Boot file sent to client using TFTP

RIS uses broadcasts To operate across any routers enable IP forwarding or install DHCP relay agent

Remote Installation Services (RIS)

Group Policy



Linking GPOs

GPOs are stored on a per-domain basis.

GPOs can be linked to one or more Sites, Domains or OUs.

A Site, Domain or OU can have more than one GPO linked to it. Processing order for links to the same site, domain, or OU is controlled primarily by the link order.

Group Policy Processing

Inheritance can be blocked for a Domain or OU

Enforcement ensures this linked GPO is processed last and therefore has highest precedence

Group Policy Delivery

DC
1) Machine Startup
2) Processed approx. every 5 minutes

Computer GPO
1) Machine Startup
2) Processed approx. every 90 minutes

User GPO
1) User Logon
2) Processed approx. every 90 minutes

Each Group Policy Object is stored in two parts:
1) A Group Policy Container (GPC) within AD
2) A Group Policy Template (GPT) within SysVol

GPC replicated via AD

GPT replicated via FRS on SysVol

Group Policy Management Console (Backup, Restore, Copy, Results and Modeling)

Group Policy Components and Functionality

Intellimirror = User Data Management + User Settings Management + Software Installation

IntelliMirror is implemented via a set of Windows features including Active Directory , Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles.

Network-based files and folders can be made available offline

Software applications are managed by GPOs associated with an Active Directory Site, Domain, or Organizational Unit.

Systems Management Server is also available for software distribution and installation

(1) Obtain applications which use Windows Installer

(2) Assign or publish applications using Group Policy to target Site, Domain or OU (OU illustrated)

(3) Assign or publish

Applications assigned to both users & computers. (Mandatory deployment)

Applications are published to users. (Add/Remove Programs)

Can be used for Software Installation

Software Installation defined by Group Policy

User Settings Management

AD User Settings& GPO Settings

corp.contoso.com

Machine Replacement=Intellimirror + RIS

Authors: Martin McClean & Astrid McClean (Microsoft Australia) with the assistance and support of the Windows Server Product Management Team and the Windows Server 2003 Product Team.