|  |  |
| --- | --- |
| Category | Best Practice |
| *Forest - General* | Forest count:   * A single forest is ideal when possible |
| *Forest - General* | Forest trusts:   * When your forest contains domain trees with many child domains and you observe noticeable user authentication delays between the child domains, you can optimize the user authentication process between the child domains by creating shortcut trusts to mid-level domains in the domain tree hierarchy. |
| *Forest - General* | Forest functional level for Windows 2003 forests:   * If all of your DCs are Windows 2003 or higher OS versions then ensure that you raise the forest functional level to 2003 (or higher). This enables the following benefits: * Ability to use forest trusts * Ability to rename domains * The ability to deploy a read-only domain controller (RODC) * Improved Knowledge Consistency Checker (KCC) algorithms and scalability |
| *Forest - General* | Forest functional level for Windows 2008 forests:   * If all of your DCs are Windows 2008 or higher OS versions then ensure that you raise the forest functional level to 2008 (or higher). This enables the following benefits: * Active Directory Recycle Bin, which provides the ability to restore deleted objects in their entirety while AD DS is running. |
| *Forest - FSMO* | Schema Master placement:   * Place the schema master on the PDC of the forest root domain. |
| *Forest - FSMO* | Domain Naming Master placement:   * Place the domain naming master on the forest root PDC. |
| *Domain - General* | Domain count:   * To reap the maximum benefits from Active Directory, try to minimize the number of domains in the finished forest. For most organizations an ideal design is a forest root domain and one global domain for a total of 2 domains. |
| *Domain - General* | Domain root:   * The best practices approach to domain design dictates that the forest root domain be dedicated exclusively to administering the forest infrastructure and be mostly empty. |
| *Domain - General* | Domain functional level:   * If all of your DCs are Windows 2003 or higher OS versions then ensure that you raise the domain functional level to 2003 (or higher). This enables the following benefits:   + Renaming domain controllers   + LastLogonTimeStamp attribute   + Replicating group change deltas   + Renaming domains   + Cross forest trusts   + Improved KCC scalability |
| *Domain - General* | Old DC Metadata:   * In the event that a DC has to be forcibly removed (dcpromo /forceremoval) such as when it has not replicated beyond the TSL, you will need to clean up the DC Metadata on the central DCs. Metadata includes elements such as the Computer Object, NTDS Settings, FRSMember object and DNS Records. Use ntdsutil to perfom this. |
| *Domain - FSMO* | PDC FSMO placement:   * Place the PDC on your best hardware in a reliable hub site that contains replica domain controllers in the same Active Directory site and domain. |
| *Domain - FSMO* | PDC FSMO colocation:   * PDC and RID FSMO roles should be held by the same DC. |
| *Domain - FSMO* | RID FSMO placement:   * Place the RID master on the domain PDC in the same domain. |
| *Domain - FSMO* | RID FSMO in windows 2008 environment:   * On 2008 R2 DCs ensure that hotfix 2618669 is applied |
| *Domain - FSMO* | RID FSMO colocation:   * PDC and RID FSMO roles should be held by the same DC |
| *Domain - FSMO* | RID pool size:   * Ensure that the RID pool is large to avoid possible RID depletion. |
| *Domain - FSMO* | Infrastructure Master in a single domain forest:   * In a forest that contains a single Active Directory domain, there are no phantoms. Therefore, the infrastructure master has no work to do. The infrastructure master may be placed on any domain controller in the domain, regardless of whether that domain controller hosts the global catalog or not. |
| *Domain - FSMO* | Infrastructure Master in a multiple domain forest:   * If every domain controller in a domain that is part of a multidomain forest also hosts the global catalog, there are no phantoms or work for the infrastructure master to do. The infrastructure master may be put on any domain controller in that domain. In practical terms, most administrators host the global catalog on every domain controller in the forest. |
| *Domain - FSMO* | Infrastructure Master in a multiple domain forest where not all DCs are hosting a global catalog:   * If every domain controller in a given domain that is located in a multidomain forest does not host the global catalog, the infrastructure master must be placed on a domain controller that does not host the global catalog. |
| *DC - General* | DC organizational unit:   * DCs should not be moved from the Domain Controllers OU or the Default Domain Controllers GPO won’t apply to them. |
| *DC – Network Configuration* | DNS NIC configuration in a single DC domain:   * If the server is the first and only domain controller that you install in the domain, and the server runs DNS, configure the DNS client settings to point to that first server's IP address. For example, you must configure the DNS client settings to point to itself. Do not list any other DNS servers until you have another domain controller hosting DNS in that domain. |
| *DC – Network Configuration* | DNS NIC configuration in a multiple DC domain where all DCs are also DNS servers:   * In a domain with multiple domain controllers, DNS servers should include their own IP addresses on their interface lists of DNS servers. We recommend that the DC local IP address be the primary DNS server, another DC be the secondary DNS server (first local and then remote site), and that the localhost address act as a tertiary DNS resolver on the network cards for all DCs. |
| *DC – Network Configuration* | DNS Configuration in a multiple DC domain where not all DCs are DNS servers:   * If you do not use Active Directory-integrated DNS, and you have domain controllers that do not have DNS installed, Microsoft recommends that you configure the DNS client settings according to these specifications:   + Configure the DNS client settings on the domain controller to point to a DNS server that is authoritative for the zone that corresponds to the domain where the computer is a member. A local primary and secondary DNS server is preferred because of Wide Area Network (WAN) traffic considerations.   + If there is no local DNS server available, point to a DNS server that is reachable by a reliable WAN link. (Up-time and bandwidth determine reliability.)   + Do not configure the DNS client settings on the domain controllers to point to your ISP's DNS servers. Instead, the internal DNS server should forward to the ISP's DNS servers to resolve external names. |
| *DC – Network Configuration* | Multi-homed DC NIC configuration:   * It is recommended not to run a domain controller on a multi-homed server. If server management adapters are present or multi-homing is required then the extra adapters should not be configured to register within DNS. If these interfaces are enabled and allowed to register in DNS, computers could try to contact the domain controller using this IP address and fail. This could potentially exhibit itself as sporadic failures where clients seemingly authenticate against remote domain controllers even though the local domain controller is online and reachable. |
| *DC – Network Configuration* | WINS NIC configuration on DCs where the WINS service is hosted:   * Unlike other systems, WINS servers should only point to themselves for WINS in their client configuration. This is necessary to prevent possible split registrations where a WINS server might try to register records both on itself and on another WINS server. |
| *DC – DNS Server Configuration* | External name resolution:   * It is recommended to configure DNS forwarders first for internet traffic. This will result in faster and more reliable name resolution. If that is not an option then utilize root hints. |
| *DC – DNS Server Configuration* | DNS Zone Types:   * Use directory-integrated storage for your DNS zones for increased security, fault tolerance, simplified deployment and management. |
| *DC – DNS Server Configuration* | DNS Scavenging:   * DNS scavenging is recommended to clean up stale and orphaned DNS records that were dynamically created. This process keeps the database from growing unnecessarily. It also reduces name resolution issues where multiple records could unintentionally point to the same IP address. This is often seen in workstations that use DHCP, because the same IP address can be assigned to different workstations over time. |
| *DC – DNS Server Configuration* | DNS \_msdcs.forestdomain zone authoritation:   * It is recommended that every DNS server be authoritative for the \_msdcs.forestdomain zone. A freshly created Windows 2003 forest places \_msdcs in it’s own zone and this zone is replicated forest wide. If the domain began as a Windows 2000 forest the \_msdcs zone is a subzone of the forest root zone. The \_msdcs zone could be placed in it’s own zone or the forest root zone could be replicated forest wide. Having \_msdcs on every Domain Controller running DNS allows the Domain Controllers to look for other Domain Controllers without having to forward the query.   The dnslint.exe tool can be used to validate that each DNS server it queries is authoritative for the\_msdcs.forestdomain zone. |
| *DC – DNS Server Configuration* | DNS on servers with multiple NICs:   * If multiple NICs exist on the DNS server, make sure that the DNS services are only listening on the LAN interface. |
| *DC – DNS Server Configuration* | DNS services in multiple DC environments:   * Configure all DNS Servers to have either local copies of all DNS Zones or to appropriately forward to other DNS servers.   Replicating DNS zones across domain lines will allow all domains in the forest to share DNS information easier and ultimately make DNS administration easier. Simply secure each DNS zone as needed if decentralized administration and security is a concern. Replicate to "all Domains in the Forest" even if you have only one domain, this will save you time in the future should a second domain be added.   * Use Active Directory (AD) Integrated DNS Forwarders instead of normal standalone DNS Forwarders when possible   1. Example:  dnscmd /ZoneAdd domain.com /DsForwarder 10.10.10.10 [/DP /forest]  Using AD integrated forwarders will replicate the information to all the DNS servers in the domain or the forest (/DP /Forest). This will simplify DNS administration. Replicating to the forest (/DP /Forest) is preferred.   * Use AD Integrated Stub Zones instead of standalone DNS Domain Forwards.   Stub Zones can automatically be replicated to all DNS servers when AD integrated Zones are used and they work similar to DNS forwards. Using DNS Stubs will decrease administration as DNS servers are replaced overtime. Using standalone server based DNS Domain Forwards can require configuration of every DNS server, increasing DNS administration   * Configure Zone Transfers by using the Name Servers tab, and configuring the Zone Transfers tab to transfer to and notify the Name Servers of changes. Do not use Zone Transfers to IP Addresses.   Using the Name Servers tab to configure the Zone Transfer creates a better documented DNS server. An Active Directory integrated DNS Server will replicate the Name Server information to each DNS server. As DNS servers are added or replaced this information is kept, using only the Zone Transfers tab and transferring by IP Address can result in lost information when a server is replaced. |
| *DC – DNS Server Configuration* | DNS services in environments which integrate with other companies:   * Use AD Integrated DNS forwarders to resolve DNS Zones across independent companies/forests, or replicate DNS Zones onto all DNS servers if the companies are owned by the same parent company and in the same forest. |
| *DC – DNS Server Configuration* | DNS record caching:   * Configure all DNS Servers to be a Caching DNS Server in addition to hosting DNS Zones.   This is the default configuration for Windows 2003 DNS servers. Leaving this enabled simplifies DNS administration and speeds DNS queries. |
| *DC – DNS Server Configuration* | DNS Dynamic Updates:   * Configure DNS Zones that are used by Active Directory domains to accept Dynamic Updates   Allowing Dynamic DNS (DDNS) updates on DNS zone used by the Active Directory domain is the default/recommended configuration. This configuration is fundamental to having good communication between all devices in the AD domain. |
| *DC – DNS Server Configuration* | DNS manually created records in dynamic zones:   * Do NOT manually create Host (A) records in the same domain with records where dynamic Host records are created via DDNS. Instead create a SubZone (or new Zone) and create the Host records there, then create an Alias (CNAME) record in the appropriate zone for user friendly DNS searches.   The SubZone (or new Zone) can be used to document the device type as server, router, appliance, etc., this provides a better documented DNS environment. This also allows manual DNS host records to be easily monitored and maintained. As equipment is replace over time easier DNS maintenance is achieved.  a. Bad Practice Example: domain.com is used for DDNS registration, do not manually create a Host (A) record in this Zone.  b. Best Practice Example: domain.com is used for DDNS registration, serv.domain.com is used for manual Host records, then place an Alias record in domain.com to allow easy client configuration. |
| *DC – Time Configuration* | DC NT5DS configuration for servers not hosting the PDC FSMO role:   * Configure NTP on all domain controllers to point to the domain controller hosting the PDC FSMO role. |
| *DC – Time Configuration* | DC NT5DS configuration for the domain PDC FSMO role:   * Configure the Windows Time service (on the PDC FSMO role holder) to synchronize with an external time server. |
| *DC – Time Configuration* | External NTP server definition:   * When specifying specific NTP servers it is possible to define one or more servers. It is important to follow the correct syntax when defining multiple NTP servers. Failure to do so may invalid the list and cause time synchronization failures. The main point to focus on is the delimiters between each value. The correct delimiter is a space. Commas, semi-colons and anything other than a space is invalid. |
| *Sites and Services* | Sites:   * Do not disable the Knowledge Consistency Checker (KCC). * Do not specify bridgehead servers. * Keep the replication schedule open as long as is practical. * Remove empty domains and consolidate any IP subnets associated therein to sites which have domain controllers. * Do not enable Universal Group Membership Caching in sites where a global catalog resides. Universal Group Membership Caching is set at the site level and affects all DCs in the site.  If one of the DCs is a GC, the remaining DCs will continue to cache Universal Group Membership resulting un unpredictable authentication failures (dependent on which DC is chosen for authentication by the DS Locator Service). * All sites should contain at least one global catalog server. In order to logon, a user account needs to be evaluated against Universal Group Membership which is stored on GCs. A site without GCs can cause logon failure as a result. A new option is to enable Universal Group Membership Caching in order not to require a GC in each site. |
| *Sites and Services* | Connection objects:   * Do not manually create connection objects. Do not manually modify default connection objects. If you leave the KCC to do it's job, it will automatically create the necessary connection objects. However, any manually created connection object (INCLUDING an automatically created object that has been modified) will remain static. "Admin made it, so admin must know something I don't know" is the general logic behind this. Only create manual connection objects if you know something the KCC doesn't know. Don't confuse a connection object with a site link. * Connection objects should maintain default schedules. By default, connection objects will inherit their schedule based on the site link.  However, they can be changed directly.  Once you make a change to a connection object, it will no longer be managed by the KCC and will be treated as a manual connection object. * If you are cleaning up the connection objects, don't delete more than 10 connections at a time or a Version Vector Join (vv join) might be required to re-join the DC. * Do not disable connection objects. |
| *Sites and Services* | Site links:   * Do not manually create site-links, let the ISTG create links based on KCC results. * All sites need to be contained in at least one Site Link in order to replicate to other sites.  Automatic Site Covering and DFS costing might be affected if sites are not within site links. * There must be 2 or more sites associated with a site link.  The deletion of a site may require the manual clean-up of the respective site link. * If two site links contain the same two remote sites, a suboptimal replication topology may result. * Do not disable site link transitivity. |
| *Sites and Services* | Site subnets:   * All infrastructure ip subnet ranges where servers or workstations login from should be defined within ad sites and services. Sites consist of one or more subnets and allow clients to logon to a local Domain Controller quickly through the DC Locator Process. If the subnet definition is missing from AD, the client will logon to any generic DC which may be on the other side of the world. You can easily find subnets not defined in AD by reviewing the Netlogon.log file in %systemroot%\debug folder. You can look for all DCs with event 5778 using eventcomb and then selectively gather the various netlogon.log files. |
| *Sites and Services* | Inter-Site Change Notification:   * Replication of AD is always pulled and not pushed. Within a site, when a change occurs, a DC will notify other DCs of the change so that they can pull the change. Between sites, this is not used and rather a schedule is used with the lowest time being 15 minutes.   This can be changed to work with Change Notification making inter-site replication much faster (but using more bandwidth as a consequence). It is recommended to only enable change notification on a link if it is a high speed link or a dedicated Exchange site.  To enable Change Notification, use adsiedit.msc and update the attribute called "Options" on the site link to a value of 1. You can find this object in the Configuration NC. |
| *Replication* | Morphed folders:   * A morphed folder refers to a folder that has been renamed by FRS to resolve a conflict. FRS identifies the conflict during replication, and the receiving member protects the original copy of the folder and renames (morphs) the later inbound copy of the folder. The morphed folder names have a suffix of "\_NTFRS\_xxxxxxxx," where "xxxxxxxx" represents eight random hexadecimal digits.   If morphed folders are found within SYSVOL they should be fixed or they may not be linked to other AD components properly. Fixing a morphed folder involves removing or renaming the folder and its morphed pair and waiting for replication to complete. Then the correct folder is identified and renamed to its correct name or copied to its correct location. |
| *Replication* | Lingering objects:   * Lingering objects are objects that exist on 1 or more DCs but not on others. Lingering objects can occur if a domain controller does not replicate for an interval of time that is longer than the tombstone lifetime (TSL). The domain controller then reconnects to the replication topology. Objects that are deleted from the Active Directory directory service when the domain controller is offline can remain on the domain controller as lingering objects. This can be caused from recovering a DC from a virtual snapshot or from reviving a domain controller which has been off the network or not replicating with the domain for longer than the tombstone lifetime. |
| *Replication* | GPT and GPC lingages:   * Group Policy Objects have two parts consisting of the Group Policy Template (GPT) residing in the SYSVOL and the Group Policy Container (GPC) in Active Directory. When problems occur with SYSVOL replication or in the AD itself, the two halves can become unsynchronized. When this happens, Group Policy can cease to function or start behaving strangely.   To validate synchronization of GPTs and GPCs, use the Resource Kit tool gptool.exe. In a healthy domain all policies should return a "Policy OK" result. When a policy fails to do so, some troubleshooting of SYSVOL replication and GPO version numbers is in order. |
| *Replication* | Topology clean-up setting:   * This should be enabled. This option controls the automatic clean-up of unnecessary connection objects and replication links. To enable it, run:   repadmin /siteoptions HubServer1 -IS\_TOPL\_CLEANUP\_DISABLED |
| *Replication* | Detect stale topology setting:   * This site option is used by the KCC Branch Office Mode which tells the KCC to ignore failed replication and not to try to find a path around.   repadmin /siteoptions BranchServer1 -IS\_TOPL\_DETECT\_STALE\_DISABLED  This should not be enabled on Central or Hub Sites or replication failures can result. To undo this:  repadmin /siteoptions HubServer1 +IS\_TOPL\_DETECT\_STALE\_DISABLED |
| *Replication* | KCC Intra-site topology setting:   * If the KCC Intra-Site Topology is disabled, all replication connections need to be manually maintained which will have a high administrative burden. This is not recommended. Rather allow the KCC to dynamically build the topology every 15 minutes.   repadmin /siteoptions HubServer1 +IS\_AUTO\_TOPOLOGY\_DISABLED  For inter-site, you may choose to disable the KCC and create manual connection objects as follows:  repadmin /siteoptions HubServer1 IS\_INTER\_SITE\_AUTO\_TOPOLOGY\_DISABLED |
| *Replication* | Inbound replication setting:   * Disabling inbound replication should only be used for testing and should be removed once complete. Leaving inbound replication disabled will eventually orphan the DC once the TSL has expired. To re-enable inbound replication, run the following (Note the + and - switches on the Repadmin options to confirm or negate the option):   repadmin /options site:Branch -DISABLE\_INBOUND\_REPL |
| *Replication* | Outbound Replication setting:   * Outbound replication is disabled automatically when a DC has not replicated within it's tombstone linetime (180 days). If it has been disabled manually you need to reenable it as follows:   repadmin /options site:Branch -DISABLE\_OUTBOUND\_REPL |
| *Replication* | Ignore schedules setting:   * If you've configured replication on a schedule on a site link, this schedule will be ignored if the "Ignore IP Schedules" option is set on the IP Container.   This is NOT the GUI for "Options = 1" which enables inter-site change notification. |
| *Replication* | Topology Minimum Hops setting:   * By default, the KCC will create the intra-site repl topology so that no replication partner is more than 3 hops away. This 3 hop limit can be disabled as follows:   repadmin /siteoptions server1 +IS\_TOPL\_MIN\_HOPS\_DISABLED  To undo this, negate the option (-) as follows:  repadmin /siteoptions server1 -IS\_TOPL\_MIN\_HOPS\_DISABLED |
| *Replication* | Non-default dSHeuristics setting:   * The dSHeuristics attribute modifies the behaviour of certain aspects of the Domain Controllers. An examples of behavioral changes include enabling anonymous LDAP operations. The dsHeuristics attribute is located at CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<forest root domain>   The data is a Unicode string where each value may represent a different possible setting.  The default value is <not set>  For more information on dSHeuristics:  <http://msdn.microsoft.com/en-us/library/cc223560(PROT.10).aspx> |
| *Replication* | Recycle bin deleted object lifetime setting:   * Without knowing the Recycle Bin Deleted Object Lifetime, it's not possible to know if a deleted object will be recoverable. By default, the value is set to Null and it uses the value of the TombStone Lifetime instead. The TSL is also set to Null by default and if it remains null, it uses the hard coded value of 60 (or 180 if the forest was deployed on 2003 SP1 or above). If the value is changed, ensure it is longer than your backup schedule to avoid having to do authoritative restores on deleted objects.   The location of the TombStone Lifetime and the Deleted Object Lifetime are both at CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<forest root domain> with the following Attribute Names:  TombStone Lifetime (TSL): tombstoneLifetime  Deleted Object Lifetime: msDS-DeletedObjectLifetime |
| *Replication* | Inbound Replication Connections:   * Do not manually create inbound replication connections on an RODC. A manually created inbound replication connection from an RODC will result in failed replication as an RODC will never replicate outbound. |
| *Read Only DCs* | Site links to RODC sites:   * In a mixed environment of both 2003 and 2008 DCs, ensure the lowest cost site link for an RODC site is to a site with more than 1 writeable 2008 domain controller. The Filtered Attribute Set (FAS) is the definition of what an RODC may replicate (some attributes being filtered). It only recognises the FAS when replicating to a 2008 RWDC. If there is only 1 RWDC at the next hop which fails, the RODC may replicate with a 2003 DC including all attributes. It's important to validate the site links, site link bridges and costs to ensure that there are at least 2 RWDCs each RODC can replicate from. |
| *Read Only DCs* | RODCs per site:   * Ideally each RODC site contains only a single RODC. RODCs cache users passwords. In the event of a disconnection to a RWDC, the users can logon using the cached RODC password.   In the event that there are multiple RODCs in the Site for the same domain, it is unpredictable which RODC will respond to an Authentication Request. Therefore, user logon experience will be equally unpredictable. |
| *Read Only DCs* | RODCs and RWDCs in the same site:   * Typically, RODCs are placed in remote branch sites by themselves. In the event that there are both RWDCs and RODCs, there will be a noticeable and unpredictable user experience in the event of the RWDC being unavailable. This is especially true during WAN outages where passwords are not cached. |
| *Read Only DCs* | Number of non-RODCs per domain.   * It is recommended to always have more than a single read/write domain controller per domain. Although a single RWDC and many RODCs can exist in a domain, this is not recommended. RODCs can't replicate outbound and in the event of failure of the RWDC an undesirable AD Restore would be required. |
|  | AutoSiteCoverage:   * AutoSiteCoverage enables a DC to cover a site where no DCs exist by registering the relevant SRV records for the site in question. Windows 2003 DCs don't recognise RODCs and if AutoSiteCoverage is enabled on these DCs, they will register their SRV records in this site. This will result in users authenticating to the 2003 DC even though an RODC exists in the site.   To resolve this, either disable AutoSiteCoverage on the 2003 DC or install the RODC Compatibility Pack on the 2003 DCs.  HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters  REG\_DWORD called AutoSiteCoverage, value = 1 or 0 |