nltest - Windows CMD - SS64

Archived: 2026-04-06 03:14:15 UTC

NLTEST.exe

Network Location Test - List domain controllers(DCs), Force a remote shutdown, Query the status of trust, test trust relationships and the state of domain controller replication.

```
Syntax
      NLTEST [/server:servername] [operation[parameter]

Key
   /server:ServerName
            Run nltest at a remote domain controller: ServerName.
            default = the local computer (a domain controller).

   /dbflag:HexadecimalFlags
            Set a new debug flag.
            The entry in the Windows Server registry for debug flags is
            HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DBFlag.

            A value of 0x2080FFFF (decimal 545325055) for HexadecimalFlags will enable verbose Netlo
            A value of 0x0 (decimal 0) or deleting the registry key, will disable Netlogon logging.

   /cDigest:Message /domain:DomainName
            Display the current digest that the client uses for the secure channel.
            (The digest is the calculation that nltest derives from the password.)
            This parameter displays the digest that is based on the previous password, also. Nltest
            the secure channel for logons between client computers and a domain controller, or for
            directory service replication between domain controllers. You can use this parameter in
            conjunction with the /sdigest parameter to check the synchronization of trust account pa

   /sDigest:Message /rid:RID_In_Hexadecimal
            Display the current digest that the server uses for the secure channel.
            (The digest is the calculation that nltest derives from the password.)
            This parameter displays the digest for the previous password, also. If the digest from t
            server matches the digest from the client, then nltest synchronizes the passwords that i
            uses for the secure channel. If the digests do not match, then nltest might not have rep
```

```
         the password change yet.

/dclist:[DomainName]
         List all DCs in the domain.
         This command first queries Active Directory for a list of DCs.
         If this query is unsuccessful, nltest then uses the Browser service (if netbios is enabl

/dcname:[DomainName]
         List the primary domain controller or the PDC emulator for DomainName.

/domain_trusts [/Primary | /Forest | /Direct_Out | /Direct_In | /All_Trusts | /v]
         Return a list of trusted domains.
         Optional Flags to filter the list of domains:
            /Primary    Return only the domain to which the computer account belongs.
            /Forest     Return only those domains that are in the same forest as the primary doma
            /Direct_Out Return only the domains that are explicitly trusted with the primary doma
            /Direct_In  Return only the domains that explicitly trust the primary domain.
            /All_Trusts Return all trusted domains.
            /v          Display verbose output, including any domain SIDs and GUIDs that are avai

/dnsgetdc:DomainName
         Query the DNS server for a list of domain controllers and their corresponding IP address
         values that you can use to filter the list of DCs:
            /PDC  Return only those DCs that are PDCs (NT 4.0) or designated as PDC emulators.
            /GC   Return only those DCs that you designate as global catalogs.
            /KDC  Return only those DCs that you designate as Kerberos key distribution centers.
            /WRITABLE  Return only those DCs that can accept changes to the directory database.
                        This value returns all Active Directory DCs, but not Windows NT 4.0 BDCs.
            /LDAPONLY  Return servers that are running a Lightweight Directory Access Protocol (LI
                        The servers can include LDAP servers that are not DCs.
            /FORCE     Run the command against the DNS server instead of looking in cache.
            /SITE Sitename  Sort to list first the records that pertain to Sitename.
            /SITESPEC  Filter the returned records to display only Sitename, used only with /SITE

/DSAddressToSite:MachineName
         Call DsAddressToSiteNamesEx

/DSgetdc:[DomainName]
         Query the Domain Name System (DNS) server for a list of DCs and their
         IP addresses. This parameter also contacts each domain controller to check for connectiv

         The following case sensitive flags can be used to filter the list of DCs
         or specify alternate names types in the syntax.

         /PDC : Return only the PDC or domain controllers designated as the PDC emulator.
         /DS  : Return only those DCs that are Windows 2000 and later.
```

```
/DSP : Return only Windows 2000 and later DCs. If the query finds no such server,
       then return Windows NT 4.0 DCs.

/GC  : Return only those DCs that are designated as global catalog servers.
/KDC : Return only those DCs that are designated as Kerberos key distribution centers.

/TIMESERV   : Return only those DCs that are designated as time servers.
/GTTIMESERV : Return only DCs designated as master time servers.

/WS
/NetBIOS : Specify computer names in the syntax as NetBIOS names.

/DNS : Specify computer names in the syntax as fully qualified domain names (FQDNs).
       If you do not specify a return format, the DC can return either NetBIOS or DNS fo

/IP :  Return only DCs that have IP addresses. i.e. return only TCP/IP DCs.

/FORCE : Force the computer to run the command against the DNS server instead of looking
        the cache for the information.

/Writable : Require that the returned DC be writable; All Windows 2000 DCs are writable

/Avoidself : When called from a DC, specifies that the returned DC name should
             not be the current computer. If the current computer is not a DC, this flag
             This flag can be used to obtain the name of another DC in the domain.

/LDAPOnly : Specifies that the server returned is an LDAP server. The server returned is
            necessarily a DC. This flag can be used with the DS_GC_SERVER_REQUIRED flag
            to return an LDAP server that also hosts a global catalog server.
            If this flag is specified, the DS_PDC_REQUIRED, DS_TIMESERV_REQUIRED,
            DS_GOOD_TIMESERV_PREFERRED, DS_DIRECTORY_SERVICES_PREFERED,
            DS_DIRECTORY_SERVICES_REQUIRED, and DS_KDC_REQUIRED flags are ignored.

/Backg : If the DS_FORCE_REDISCOVERY flag is not specified, this function uses cached DC
         If the cached data is more than 15 minutes old, the cache is refreshed by pingi
         the DC. If this flag is specified, this refresh is avoided even if the cached da
         is expired. This flag should be used if the DsGetDcName function is called peri

/DS_6 : Require that the returned DC be running Windows Server 2008 or later.
/DS_8 : Require that the returned domain controller be running Windows Server 2012 or la

/Try_Next_Closest_Site :  When this flag is specified, DsGetDcName attempts to find a DC
                          the same site as the caller.

/Ret_DNS : Specifies that the names returned in the DomainControllerName and DomainName r
           of DomainControllerInfo should be DNS names.
/Ret_NETBIOS : Specifies that the names returned in the DomainControllerName and DomainNa
```

```
                        of DomainControllerInfo should be flat names.

/DSgetsite
         Return the name of the site in which the DC resides.

/DSgetsitecov
         Return the name of the site that the DC covers. A DC can cover a site
         that has no local DC of its own.

/DSgetfti:DomainName[ /UpdateTDO]
         Return information about interforest trusts. You use this parameter only for a Windows S
         domain controller that is in the root of the forest. If no interforest trusts exist, thi
         returns an error. The /UpdateTDO value updates the locally stored information on the int

/DSquerydns
         Query for the status of the last update for all DNS records that are specific to a DC.

/DSregdns
         Refreshe the registration of all DNS records that are specific to a DC that you specify.

/DSderegdns:DnsHostName
         Deregister DNS host records for the host that you specify in the DnsHostName parameter.
         values you can use to specify which records nltest deregisters:
            /DOM  Specify a DNS domain name for the host to use when you search for records on th
                  If you do not specify this value, nltest uses the DNS domain name as the suffix
                  DnsHostName parameter.

            /DSAGUID  Delete Directory System Agent (DSA) records that are based on a GUID.
            /DOMGUID  Delete DNS records that are based on a globally unique identifier (GUID).

/finduser:User
         Find the directly-trusted domain that the user account User belongs to.
         Use this parameter to troubleshoot logon issues of older client Operating Systems.

/list_deltas:FileName
         Display the contents of the FileName change log file, which lists changes to the user ac
         database. Netlogon.chg is the default name for this log file, which resides only on Wind

/logon_query
         Query the cumulative number of NTLM logon attempts at a console or over a network.

/LSAGETFTI:DomainName
         Call DsGetForestTrustInformation
   /UPDATE_TDQ

/LSAQUERYFTI:DomainName
         Call LsaQueryForestTrustInformation
```

```
/ParentDomain
         Return the name of the parent domain of the server.

/query   Report on the state of the secure channel the last time you used it.
         (The secure channel is the one that the NetLogon service established.)

/repl    Force synchronization with the primary domain controller (PDC).
         NT 4.0 BDCs only, not for Active Directory replication.

/sc_query:DomainName
          Report on the state of the secure channel the last time that you used it.
         (The secure channel is the one that the NetLogon service established.)
         This parameter lists the name of the domain controller that you queried on the
         secure channel, also.

/sc_reset:[DomainName]
         Remove, and then rebuild, the secure channel that the NetLogon service established.
         You must have administrative credentials to use this parameter.

/sc_verify:[DomainName]
         Check the status of the secure channel that the NetLogon service established.
         If the secure channel does not work, this parameter removes the existing channel, and
         then builds a new one. You must have administrative credentials to use this parameter.

/sc_change_pwd:[DomainName]
         Change the password for the trust account of a domain that you specify.
         If you run nltest on a domain controller, and an explicit trust relationship exists,
         then nltest resets the password for the interdomain trust account.
         Otherwise, nltest changes the computer account password for the domain that you specify.

/bdc_query:DomainName
         Query for a list of BDCs in DomainName, and then display their state of synchronization
         and replication status. You can use this parameter only for Windows NT 4.0 domain contro

/sim_sync:DomainName ServerName
         Simulate full synchronization replication. This is a useful parameter for test environme

/sync    Force an immediate synchronization with the PDC of the entire SAM database.
         NT 4.0 BDCs only, not for Active Directory replication.

/pdc_repl Force the PDC to send a synchronization notification to all BDCs.
         NT 4.0 PDCs only, not for Active Directory replication.

/shutdown:Reason [Seconds]
         Remotely shut down the server that you specify in ServerName.
         Use a string to specify the reason for the shutdown in the Reason value.
```

```
            Use an integer value of Seconds before the shutdown will occur.
            (see InitiateSystemShutdown in the Platform SDK documentation.)

   /shutdown_abort
            Terminate a system shutdown.

   /time:HexadecimallSL HexadecimalMSL
            Convert Windows NT Greenwich Mean Time (GMT) time to ASCII. HexadecimallSL is a hex valu
            least significant longword. HexadecimalMSL is a hexa value for most significant longword

   /transport_notify    Force the discovery of a domain controller. Windows NT 4.0 domain controller
                        Automatic for later DCs.
   /user:UserName
            Display many of the attributes that you maintain in the SAM account database for the use
            you specify. You cannot use this parameter for user accounts that are stored in an AD da

   /whowill:Domain/ User
            Find the DC that has the user account that you specify. Use this parameter to determine
            whether nltest has replicated the account information to other DCs.

  {/help | /?}   Display help at the command prompt.
```

If nltest does not appear to be available, enable the *Active Directory Domain Services* or the *AD LDS server* role.

Examples

Verify domain controllers in a domain:

> Nltest /dclist:ss64dom

Show detailed information about a specific user:

> Nltest /user:"user64"

Enable debug logging for the Netlogon service:

> Nltest /DBFlag:2080FFFF

Disable debug logging for the Netlogon service:

> Nltest /DBFlag:0x0

Verify trust relationship with a specific server:

> nltest /server:ss64-DC01 /sc_query:ss64dom
>
> lags: 30 HAS_IP HAS_TIMESERV
> Trusted DC Name \\ss64-DC01.ss64.com

> Trusted DC Connection Status Status = 0 0x0 NERR_Success
> The command completed successfully

"..If it disagrees with experiment it is wrong. In that simple statement is the key to science. It does not make any difference how beautiful your guess is. It does not make any difference how smart you are, who made the guess, or what his name is – if it disagrees with experiment it is wrong" ~ Richard Feynman

Related commands

RepAdmin - Diagnose Active Directory replication problems between domain controllers.
DcDiag - Analyze the state of domain controllers and report any problems.
DsMgt - Manage password operations over unsecured connections, AD Lightweight Directory Services application partitions, flexible single master operations (FSMO), and clean up AD metadata.
SetSpn - Read, modify, or delete the Service Principal Names (SPN) for an Active Directory service account.
