Nltest

Article • 08/31/2016

In this article

Applies To: Windows Server 2003, Windows Server 2008, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012, Windows Server 2003 with SP1, Windows 8

Performs network administrative tasks.

Nltest is a command-line tool that is built into Windows Server 2008 and Windows Server 2008 R2. It is available if you have the AD DS or the AD LDS server role installed. It is also available if you install the Active Directory Domain Services Tools that are part of the Remote Server Administration Tools (RSAT). For more information, see How to Administer Microsoft Windows Client and Server Computers Locally and Remotely (https://go.microsoft.com/fwlink/?LinkID=177813). To use **nltest**, you must run the **nltest** command from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

For examples of how to use this command, see Examples.

Nltest.exe

You can use **nltest** to:

- Get a list of domain controllers
- Force a remote shutdown
- Query the status of trust
- Test trust relationships and the state of domain controller replication in a Windows domain
- Force a user-account database to synchronize on Windows NT version 4.0 or earlier domain controllers

Nltest can test and reset the secure channel that the NetLogon service establishes between clients and the domain controller that logs them

on. Clients using Kerberos authentication cannot use this secure channel.

> **Note**
>
> You must run **nltest** from the command prompt.

Concepts

A discrete communication channel, known as the secure channel, exists between trusted domains in a Windows NT 4.0 environment and parent domains and their immediate children in an Active Directory environment. In a Windows NT 4.0 environment, **nltest** uses these channels to authenticate user accounts when a remote user connects to a network resource and the user account exists in a trusted domain. This is called pass-through authentication.

Nltest provides diagnostic features that you can use for troubleshooting Windows Server 2008 operating system configurations. However, because **nltest** is designed primarily for system administrators and support personnel, its output may be difficult to analyze. In this case, you can review the appropriate troubleshooting sections in the Windows Deployment and Resource Kits. Search for any of the keywords from the bulleted list in the **nltest** description above.

Syntax

```
nltest [/server:<servername>] [<operation>[<parameter>]
```

- /server: <ServerName> Runs **nltest** at a remote domain controller that you specify. If you do not specify this parameter,

nltest runs on the local computer, which is the domain controller.

Parameters

Expand table

Parameter	Description
/query	Reports on the state of the secure channel the last tim secure channel is the one that the NetLogon service e
/repl	Forces synchronization with the primary domain contr synchronizes only changes that are not yet replicated domain controller (BDC). You can use this parameter f BDCs only, not for Active Directory replication. You mu administrative credentials to use this parameter.
/sync	Forces an immediate synchronization with the PDC of Accounts Manager (SAM) database. You can use this p Windows NT 4.0 BDCs only, not for Active Directory re have administrative credentials to use this parameter.
/pdc_repl	Forces the PDC to send a synchronization notification use this parameter for Windows NT 4.0 PDCs only, no replication. You must have administrative credentials t
/sc_query: <DomainName>	Reports on the state of the secure channel the last tim (The secure channel is the one that the NetLogon serv parameter lists the name of the domain controller tha secure channel, also.
/sc_reset:[<DomainName>]	Removes, and then rebuilds, the secure channel that t established. You must have administrative credentials parameter.
/sc_verify:[<DomainName>]	Checks the status of the secure channel that the NetL established. If the secure channel does not work, this p the existing channel, and then builds a new one. You r administrative credentials to use this parameter. This p valid on domain controllers that run Windows 2000 w and later.

/sc_change_pwd:[<DomainName>]	Changes the password for the trust account of a dom If you run **nltest** on a domain controller, and an explic exists, then **nltest** resets the password for the interdo Otherwise, **nltest** changes the computer account pass that you specify. You can use this parameter only for c running Windows 2000 and later.
/dclist:[<DomainName>]	Lists all domain controllers in the domain. In a Windov environment, this parameter uses the Browser service domains. In an Active Directory environment, this com Active Directory for a list of domain controllers. If this **nltest** then uses the Browser service.
/dcname:[<DomainName>]	Lists the primary domain controller or the PDC emulat
/dsgetdc:[<DomainName>]	Queries the Domain Name System (DNS) server for a l controllers and their corresponding IP addresses. This contacts each domain controller to check for connectiv The following list shows the values that you can use to domain controllers or specify alternate names types in • **/PDC**: Returns only the PDC (Windows NT 4.0) c that you designate as the PDC emulator (Windc • **/DS**: Returns only those domain controllers that and later. • **/DSP**: Returns only Windows 2000 and later do the query finds no such server, then this value r Windows NT 4.0 domain controllers. • **/GC**: Returns only those domain controllers that global catalog servers. • **/KDC**: Returns only those domain controllers th Kerberos key distribution centers. • **/TIMESERV**: Returns only those domain control designate as time servers. • **/GTTIMESERV**: Returns only those domain cont designate as master time servers. • **/WS**: • **/NetBIOS**: Specifies computer names in the synt names. If you do not specify a return format, th can return either NetBIOS or DNS format. • **/DNS**: Specifies computer names in the syntax a domain names (FQDNs). If you do not specify a

domain controller can return either NetBIOS or

- **/IP**: Returns only domain controllers that have I value returns only domain controllers that use T protocol stacks.
- **/FORCE**: Forces the computer to run the comm server instead of looking in the cache for the inf
- **/Writable**: Requires that the returned domain c that is, host a writable copy of the directory serv 2000 and later DCs, or of SAM (for DCs in opera Windows 2000). A DC in an operating system p 2000 is writable only if it is a primary domain cc 2000 domain controllers are writable
- **/Avoidself**: When called from a domain controll returned domain controller name should not be computer. If the current computer is not a dom flag is ignored. This flag can be used to obtain tl domain controller in the domain.
- **/LDAPOnly**: Specifies that the server returned is server returned is not necessarily a domain cont services are implied to be present at the server. does not necessarily have a writable config cont schema container. The server returned may not to create or modify security principles. This flag DS_GC_SERVER_REQUIRED flag to return an LD hosts a global catalog server. The returned glob not necessarily a domain controller. No other se be present at the server. If this flag is specified, t DS_PDC_REQUIRED, DS_TIMESERV_REQUIRED, DS_GOOD_TIMESERV_PREFERRED, DS_DIRECTORY_SERVICES_PREFERED, DS_DIRECTORY_SERVICES_REQUIRED, and DS_K are ignored.
- **/Backg**: If the DS_FORCE_REDISCOVERY flag is r function uses cached domain controller data. If t more than 15 minutes old, the cache is refreshe domain controller. If this flag is specified, this ref if the cached data is expired. This flag should be DsGetDcName function is called periodically.
- **/DS_6**: Requires that the returned domain contr Windows Server 2008 or later.
- **/DS_8**: Requires that the returned domain contr Windows Server 2012 or later.

- **/Try_Next_Closest_Site**: When this flag is specifi
  attempts to find a domain controller in the sam
  no such domain controller is found, it will find a
  that can provide topology information and call D
  obtain a bind handle, then call DsQuerySitesByC
  determine the "next closest site," and finally cach
  site found. If no domain controller is found in th
  DsGetDcName falls back on the default method
  controller.

  If this flag is used in conjunction with a non-NU
  parameter *SiteName*, then ERROR_INVALID_FLA
  the kind of search employed with DS_TRY_NEXT
  site-specific, so this flag is ignored if it is used in
  DS_PDC_REQUIRED. Finally, DS_TRY_NEXTCLOS
  when used in conjunction with DS_RETURN_FLA
  that uses NetBIOS to resolve the name, but the
  domain controller found won't necessarily matcl
  which the client is joined.

  Note

  This flag is Group Policy enabled. If you ena
  Closest Site" policy setting, Next Closest Site
  be turned on for the machine across all avai
  configured network adapters. If you disable
  setting, Next Closest Site DC Location will n
  default for the machine across all available b
  configured network adapters. However, if a
  made using the DS_TRY_NEXTCLOSEST_SITE
  DsGetDcName honors the Next Closest Site
  do not configure this policy setting, Next Cl
  Location will be not be used by default for t
  across all available but un-configured netwo
  the DS_TRY_NEXTCLOSEST_SITE flag is used
  Next Closest Site behavior will be used.

- **/Ret_DNS**: Specifies that the names returned in
  DomainControllerName and DomainName mem

	DomainControllerInfo should be DNS names. If available, an error is returned. This switch canno the /Ret_NETBIOS switch. This flag implies the D • **/Ret_NETBIOS**: Specifies that the names returne DomainControllerName and DomainName mem *DomainControllerInfo* should be flat names. If a available, an error is returned. This switch canno the /Ret_DNS switch.
/dnsgetdc: <DomainName>	Queries the DNS server for a list of domain controllers corresponding IP addresses. The following list shows the values that you can use to domain controllers. • **/PDC**: Returns only those domain controllers th (Windows NT 4.0) or designated as PDC emulat • **/GC**: Returns only those domain controllers that global catalogs. • **/KDC**: Returns only those domain controllers th Kerberos key distribution centers. • **/WRITABLE**: Returns only those domain control changes to the directory database. This value re Active Directory domain controllers, but not Wi • **/LDAPONLY**: Returns servers that are running a Directory Access Protocol (LDAP) application. Th LDAP servers that are not domain controllers. • **/FORCE**: Forces the computer to run the comm server instead of looking in cache for the inform • **/SITE** *Sitename*: Sorts the returned records to li that pertain to the site that you specify. • **/SITESPEC**: Filters the returned records to displa that pertain to the site that you specify. This op used with the **/SITE** parameter.
/dsgetfti: <DomainName>[/UpdateTDO]	Returns information about interforest trusts. You use t for a Windows Server 2008 domain controller that is i forest. If no interforest trusts exist, this parameter retu The **/UpdateTDO** value updates the locally stored info interforest trust.

/dsgetsite	Returns the name of the site in which the domain con
/dsgetsitecov	Returns the name of the site that the domain controll controller can cover a site that has no local domain co
/parentdomain	Returns the name of the parent domain of the server.
/dsregdns	Refreshes the registration of all DNS records that are s controller that you specify.
/dsderegdns: <DnsHostName>	Deregisters DNS host records for the host that you sp *DnsHostName* parameter. The following list shows the values that you can use to records **nltest** deregisters. • **/DOM**: Specifies a DNS domain name for the ho search for records on the DNS server. If you do **nltest** uses the DNS domain name as the suffix parameter. • **/DSAGUID**: Deletes Directory System Agent (DS based on a GUID. • **DOMGUID**: Deletes DNS records that are based identifier (GUID).
/whowill: <Domain>/<User>	Finds the domain controller that has the user account can use this parameter to determine whether **nltest** ha account information to other domain controllers.
/finduser: <User>	Finds the directly-trusted domain that the user accour belongs to. You can use this parameter to troubleshoo older client operating systems.
/transport_notify	Flushes the negative cache to force the discovery of a You can use this parameter for Windows NT 4.0 doma This operation is done automatically when clients log and Windows Server 2003 domain controllers.
/dbflag: <HexadecimalFlags>	Sets a new debug flag. For most purposes, use 0x200 *HexadecimalFlags*. The entry in the Windows Server 2 debug flags is **HKLM\System\CurrentControlSet\Services\Netlogor**

/user: <UserName>	Displays many of the attributes that you maintain in t database for the user that you specify. You cannot use user accounts that are stored in an Active Directory da
/time: <HexadecimalLSL> <HexadecimalMSL>	Converts Windows NT Greenwich Mean Time (GMT) ti *HexadecimalLSL* is a hexadecimal value for least signifi *HexadecimalMSL* is a hexadecimal value for most signi
/logon_query	Queries the cumulative number of NTLM logon attem over a network.
/domain_trusts	Returns a list of trusted domains. /Primary /Forest /Di /All_Trusts /v. The following list shows the values that you can use to domains. • **/Primary**: Returns only the domain to which the belongs. • **/Forest**: Returns only those domains that are in the primary domain. • **/Direct_Out**: Returns only the domains that are the primary domain. • **/Direct_In**: Returns only the domains that explic domain. • **/All_Trusts**: Returns all trusted domains. • **/v**: Displays verbose output, including any doma that are available.
/dsquerydns	Queries for the status of the last update for all DNS re specific to a domain controller that you specify.
/bdc_query: <DomainName>	Queries for a list of BDCs in *DomainName*, and then c synchronization and replication status. You can use thi Windows NT 4.0 domain controllers.
/sim_sync: <DomainName> <ServerName>	Simulates full synchronization replication. This is a usef environments.
/list_deltas: <FileName>	Displays the contents of the *FileName* change log file, to the user account database. Netlogon.chg is the defa file, which resides only on Windows NT 4.0 BDCs.

/cdigest: <Message> /domain: <DomainName>	Displays the current digest that the client uses for the digest is the calculation that **nltest** derives from the pa parameter displays the digest that is based on the pre **Nltest** uses the secure channel for logons between clie domain controller, or for directory service replication b controllers. You can use this parameter in conjunction parameter to check the synchronization of trust accou
/sdigest: <Message> /rid: <RID_In_Hexadecimal>	Displays the current digest that the server uses for the digest is the calculation that **nltest** derives from the pa parameter displays the digest for the previous passwo from the server matches the digest from the client, the synchronizes the passwords that it uses for the secure digests do not match, then **nltest** might not have repl change yet.
/shutdown: <Reason>[<Seconds>]	Remotely shuts down the server that you specify in *Se* string to specify the reason for the shutdown in the *Re* use an integer to specify the amount of time before th in the *Seconds* value. For a complete description, see t documentation for **InitiateSystemShutdown**.
/shutdown_abort	Terminates a system shutdown.
{/help | /?}	Displays help at the command prompt.

Examples

Example 1: Verify domain controllers in a domain

The following example uses the **/dclist** parameter to create a list of domain controllers of the domain fourthcoffee.com

nltest /dclist:fourthcoffee

This command displays output similar to the following:

```
Get list of DCs in domain 'ntdev' from '\\fourthcoffee-dc-01
    fourthcoffee-dc-01.forthcoffee.com       [DS] Site: Rome
    fourthcoffee-dc-03.forthcoffee.com       [DS] Site: Las\
```

```
    fourthcoffee-dc-04.forthcoffee.com       [DS] Site: LA
    fourthcoffee-dc-09.forthcoffee.com       [DS] Site: NYC
    fourthcoffee-dc-12.forthcoffee.com       [DS] Site: Pari
    fourthcoffee-dc-24.forthcoffee.com       [DS] Site: Chat
    fourthcoffee-dc-32.forthcoffee.com       [DS] Site: Hait
    fourthcoffee-dc-99.forthcoffee.com       [DS] Site: Redm
    fourthcoffee-dc-63.forthcoffee.com [PDC] [DS] Site: Lond
The command completed successfully
```

Example 2: Advanced information about users

The following example shows detailed information about a specific user.

nltest /user:"TestAdmin"

This command displays output similar to the following:

```
User: User1
Rid: 0x3eb
Version: 0x10002
LastLogon: 2ee61c9a 01c0e947 = 5/30/2001 13:29:10
PasswordLastSet: 9dad5428 01c0e577 = 5/25/2001 17:05:47
AccountExpires: ffffffff 7fffffff = 9/13/30828 19:48:05
PrimaryGroupId: 0x201
UserAccountControl: 0x210
CountryCode: 0x0
CodePage: 0x0
BadPasswordCount: 0x0
LogonCount: 0x33
AdminCount: 0x1
SecurityDescriptor: 80140001 0000009c 000000ac 00000014 0000
02 0014c002 01050045 00000101 01000000 00000000 0014c002 000
000 00000007 00580012 00000003 00240000 00020044 00000501 05
b7b4 7112b3f1 2b3be507 000003eb 00180000 000f07ff 00000201 0
00220 00140000 0002035b 00000101 01000000 00000000 00000201
000220 00000201 05000000 00000020 00000220
AccountName: User1
Groups: 00000201 00000007
LmOwfPassword: fb890c9c 5c7e7e09 ee58593b d959c681
NtOwfPassword: d82759cc 81a342ac df600c37 4e58a478
NtPasswordHistory: 00011001
```

```
LmPasswordHistory: 00010011
The command completed successfully
```

Example 3: Verify trust relationship with a specific server

The following example verifies that the a-dc1 server has a valid trust relationship with the domain.

nltest.exe /server:fourthcoffee-dc-01 /sc_query:fourthcoffee

This command displays output similar to the following:

```
Flags: 30 HAS_IP  HAS_TIMESERV
Trusted DC Name \\fourthcoffee-dc-01.forthcoffee.com
Trusted DC Connection Status Status = 0 0x0 NERR_Success
The command completed successfully
```

> **Note**
>
> The DNS_DC and DNS_DOMAIN flags indicate the format of the information returned in the request (as opposed to a flag like GC or TIMESERV, which tell you something about the domain controller returning the information). Specifically, the presence of them indicates the returned domain controller name and domain name, respectively, were in DNS format. The absence of them indicates the returned domain controller name and domain name were in NetBIOS format.

Example 4: Determine the PDC emulator for a domain

The following example identifies the domain controller that Windows NT 4.0–based computers see as the PDC emulator for a domain.

nltest /dcname:fourthcoffee

This command displays output similar to the following:

```
PDC for Domain fourthcoffee is \\fourthcoffee-dc-01
The command completed successfully
```

You can see that a-dcp is the PDC emulator for your domain.

Example 5: Show trust relationships for a domain

The following example lists the established trust relationships for your domain.

nltest /domain_trusts

This command displays output similar to the following:

```
List of domain trusts:
    0: forthcoffee forthcoffee.com (NT 5) (Forest Tree Root)
The command completed successfully
```

This example shows that one domain trusts itself but not other domains.

Additional references

Command-Line Syntax Key