


ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

Recommended Version

✕

 Filter by title

> Nslookup

Ntbackup

Ntcmdprompt

> Ntfsutil

Ntfrsutl

Openfiles

Pagefileconfig.vbs

Path

Pathping

Pause

Pbadmin

Pentnt

Perfmon

Ping

Pnpunattend

Pnputil

Popd

Powercfg

PowerShell

PowerShell_Ise

Print

Prncnfg.vbs

Prndrvr.vbs

Prnjobs.vbs

Prnmngr.vbs

Prnport.vbs

Prnqctl.vbs

Prompt

Pubprn.vbs

Pushd

Pushprinterconnections

Pwlauncher

Qappsrv

Qprocess

> Query

Quser

Qwinsta

Rasdial

Rcp

Rd

Rdpsign

Nltest

Article • 08/31/2016

In this article

- [Nltest.exe](#)
- [Concepts](#)
- [Syntax](#)
- [Parameters](#)
- Show 2 more

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

 Copy

```
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 time you used it. (The secure channel is the one that the NetLogon service established.) |
| /repl | Forces synchronization with the primary domain controller (PDC). Nltest synchronizes only changes that are not yet replicated to the backup domain controller (BDC). You can use this parameter for Windows NT 4.0 BDCs only, not for Active Directory replication. You must have administrative credentials to use this parameter. |
| /sync | Forces an immediate synchronization with the PDC of the entire Security Accounts Manager (SAM) database. You can use this parameter for Windows NT 4.0 BDCs only, not for Active Directory replication. You must have administrative credentials to use this parameter. |
| /pdc_repl | Forces the PDC to send a synchronization notification to all BDCs. You can use this parameter for Windows NT 4.0 PDCs only, not for Active Directory replication. You must have administrative credentials to use this parameter. |
| /sc_query: <DomainName> | Reports 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>] | Removes, and then rebuilds, the secure channel that the NetLogon service established. You must have administrative credentials to use this parameter. |
| /sc_verify:[<DomainName>] | Checks 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. This parameter is only valid on domain controllers that run Windows 2000 with Service Pack 2 and later. |

| | |
|-------------------------------|---|
| /sc_change_pwd:[<DomainName>] | Changes 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. You can use this parameter only for computers that are running Windows 2000 and later. |
| /dclist:[<DomainName>] | Lists all domain controllers in the domain. In a Windows NT 4.0 domain environment, this parameter uses the Browser service to retrieve the list of domains. In an Active Directory environment, this command first queries Active Directory for a list of domain controllers. If this query is unsuccessful, nltest then uses the Browser service. |
| /dcname:[<DomainName>] | Lists the primary domain controller or the PDC emulator for <i>DomainName</i> . |
| /dsgetdc:[<DomainName>] | <p>Queries the Domain Name System (DNS) server for a list of domain controllers and their corresponding IP addresses. This parameter also contacts each domain controller to check for connectivity.</p> <p>The following list shows the values that you can use to filter the list of domain controllers or specify alternate names types in the syntax.</p> <ul style="list-style-type: none">• /PDC: Returns only the PDC (Windows NT 4.0) or domain controller that you designate as the PDC emulator (Windows 2000 and later).• /DS: Returns only those domain controllers that are Windows 2000 and later.• /DSP: Returns only Windows 2000 and later domain controllers. If the query finds no such server, then this value returns Windows NT 4.0 domain controllers.• /GC: Returns only those domain controllers that you designate as global catalog servers.• /KDC: Returns only those domain controllers that you designate as Kerberos key distribution centers.• /TIMESERV: Returns only those domain controllers that you designate as time servers.• /GTTIMESERV: Returns only those domain controllers that you designate as master time servers.• /WS:• /NetBIOS: Specifies computer names in the syntax as NetBIOS names. If you do not specify a return format, the domain controller can return either NetBIOS or DNS format.• /DNS: Specifies computer names in the syntax as fully qualified domain names (FQDNs). If you do not specify a return format, the domain controller can return either NetBIOS or DNS format.• /IP: Returns only domain controllers that have IP addresses. This value returns only domain controllers that use TCP/IP as their protocol stacks.• /FORCE: Forces the computer to run the command against the DNS server instead of looking in the cache for the information.• /Writable: Requires that the returned domain controller be writable; that is, host a writable copy of the directory service, for Windows 2000 and later DCs, or of SAM (for DCs in operating systems prior to Windows 2000). A DC in an operating system prior to Windows 2000 is writable only if it is a primary domain controller. All Windows 2000 domain controllers are writable• /Avoidself: When called from a domain controller, specifies that the returned domain controller name should not be the current computer. If the current computer is not a domain controller, this flag is ignored. This flag can be used to obtain the name of another domain controller in the domain.• /LDAPOnly: Specifies that the server returned is an LDAP server. The server returned is not necessarily a domain controller. No other services are implied to be present at the server. The server returned does not necessarily have a writable config container nor a writable schema container. The server returned may not necessarily be used to create or modify security principles. This flag may be used with the DS_GC_SERVER_REQUIRED flag to return an LDAP server that also hosts a global catalog server. The returned global catalog server is not necessarily a domain controller. No other services are implied to be present at the server. If this flag is specified, the DS_PDC_REQUIRED, DS_TIMESERV_REQUIRED, DS_GOOD_TIMESERV_PREFERRED, |

| | |
|--|--|
| | <ul style="list-style-type: none">• /PDC: Returns only those domain controllers that are PDCs (Windows NT 4.0) or designated as PDC emulators.• /GC: Returns only those domain controllers that you designate as global catalogs.• /KDC: Returns only those domain controllers that you designate as Kerberos key distribution centers.• /WRITABLE: Returns only those domain controllers that can accept changes to the directory database. This value returns all Active Directory domain controllers, but not Windows NT 4.0 BDCs.• /LDAPONLY: Returns servers that are running a Lightweight Directory Access Protocol (LDAP) application. The servers can include LDAP servers that are not domain controllers.• /FORCE: Forces the computer to run the command against the DNS server instead of looking in cache for the information.• /SITE <i>Sitename</i>: Sorts the returned records to list first the records that pertain to the site that you specify.• /SITESPEC: Filters the returned records to display only those records that pertain to the site that you specify. This operation can only be used with the /SITE parameter. |
| <code>/dsgetfti: <DomainName> [/UpdateTDO]</code> | <p>Returns information about interforest trusts. You use this parameter only for a Windows Server 2008 domain controller that is in the root of the forest. If no interforest trusts exist, this parameter returns an error.</p> <p>The /UpdateTDO value updates the locally stored information on the interforest trust.</p> |
| <code>/dsgetsite</code> | Returns the name of the site in which the domain controller resides. |
| <code>/dsgetsitecov</code> | Returns the name of the site that the domain controller covers. A domain controller can cover a site that has no local domain controller of its own. |
| <code>/parentdomain</code> | Returns the name of the parent domain of the server. |
| <code>/dsregdns</code> | Refreshes the registration of all DNS records that are specific to a domain controller that you specify. |
| <code>/dsderegdns: <DnsHostName></code> | <p>Deregisters DNS host records for the host that you specify in the <i>DnsHostName</i> parameter.</p> <p>The following list shows the values that you can use to specify which records nltest deregisters.</p> <ul style="list-style-type: none">• /DOM: Specifies a DNS domain name for the host to use when you search for records on the DNS server. If you do not specify this value, nltest uses the DNS domain name as the suffix of the <i>DnsHostName</i> parameter.• /DSAGUID: Deletes Directory System Agent (DSA) records that are based on a GUID.• DOMGUID: Deletes DNS records that are based on a globally unique identifier (GUID). |
| <code>/whowill: <Domain>/ <User></code> | Finds the domain controller that has the user account that you specify. You can use this parameter to determine whether nltest has replicated the account information to other domain controllers. |
| <code>/finduser: <User></code> | Finds the directly-trusted domain that the user account that you specify belongs to. You can use this parameter to troubleshoot logon issues of older client operating systems. |
| <code>/transport_notify</code> | Flushes the negative cache to force the discovery of a domain controller. You can use this parameter for Windows NT 4.0 domain controllers only. This operation is done automatically when clients log on to Windows 2000 and Windows Server 2003 domain controllers. |
| <code>/dbflag: <HexadecimalFlags></code> | Sets a new debug flag. For most purposes, use 0x2000FFFF as the value for <i>HexadecimalFlags</i> . The entry in the Windows Server 2003 registry for debug flags is HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DBFlag . |
| <code>/user: <UserName></code> | Displays many of the attributes that you maintain in the SAM account database for the user that you specify. You cannot use this parameter for user |

| | |
|--|--|
| | accounts that are stored in an Active Directory database. |
| /time: <HexadecimalLSL> <HexadecimalMSL> | Converts Windows NT Greenwich Mean Time (GMT) time to ASCII. <i>HexadecimalLSL</i> is a hexadecimal value for least significant longword. <i>HexadecimalMSL</i> is a hexadecimal value for most significant longword. |
| /logon_query | Queries the cumulative number of NTLM logon attempts at a console or over a network. |
| /domain_trusts | Returns a list of trusted domains. /Primary /Forest /Direct_Out /Direct_In /All_Trusts /v. The following list shows the values that you can use to filter the list of domains. <ul style="list-style-type: none">• /Primary: Returns only the domain to which the computer account belongs.• /Forest: Returns only those domains that are in the same forest as the primary domain.• /Direct_Out: Returns only the domains that are explicitly trusted with the primary domain.• /Direct_In: Returns only the domains that explicitly trust the primary domain.• /All_Trusts: Returns all trusted domains.• /v: Displays verbose output, including any domain SIDs and GUIDs that are available. |
| /dsquerydns | Queries for the status of the last update for all DNS records that are specific to a domain controller that you specify. |
| /bdc_query: <DomainName> | Queries for a list of BDCs in <i>DomainName</i> , and then displays their state of synchronization and replication status. You can use this parameter only for Windows NT 4.0 domain controllers. |
| /sim_sync: <DomainName> <ServerName> | Simulates full synchronization replication. This is a useful parameter for test environments. |
| /list_deltas: <FileName> | Displays the contents of the <i>FileName</i> change log file, which lists changes to the user account database. Netlogon.chg is the default name for this log file, which resides only on Windows NT 4.0 BDCs. |
| /cdigest: <Message> /domain: <DomainName> | Displays 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 uses 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 passwords. |
| /sdigest: <Message> /rid: <RID_In_Hexadecimal> | Displays 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 the server matches the digest from the client, then nltest synchronizes the passwords that it uses for the secure channel. If the digests do not match, then nltest might not have replicated the password change yet. |
| /shutdown: <Reason> [<Seconds>] | Remotely shuts down the server that you specify in <i>ServerName</i> . You use a string to specify the reason for the shutdown in the <i>Reason</i> value., and you use an integer to specify the amount of time before the shutdown occurs in the <i>Seconds</i> value. For a complete description, see the Platform SDK 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:

Copy

```
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: LasVegas
fourthcoffee-dc-04.forthcoffee.com      [DS] Site: LA
fourthcoffee-dc-09.forthcoffee.com      [DS] Site: NYC
fourthcoffee-dc-12.forthcoffee.com      [DS] Site: Paris
fourthcoffee-dc-24.forthcoffee.com      [DS] Site: Chattaroy
fourthcoffee-dc-32.forthcoffee.com      [DS] Site: Haifa
fourthcoffee-dc-99.forthcoffee.com      [DS] Site: Redmond
fourthcoffee-dc-63.forthcoffee.com [PDC] [DS] Site: London
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:

Copy

```
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 00000044 00300002 00000002 0014c002 01050045 00000101 01000000 00000000 0014c002 000f07ff 00000101 05000000 00000007 00580012 00000003 00240000 00020044 00000501 05000000 00000015 22cc0000 b7b4 7112b3f1 2b3be507 000003eb 00180000 000f07ff 00000201 05000000 00000020 00000000 00140000 0002035b 00000101 01000000 00000000 00000201 05000000 00000020 00000220 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:

Copy

```
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:

📄 Copy

```
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:

📄 Copy

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

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

Additional references

[Command-Line Syntax Key](#)