

Active Directory diagnostics

Start with DNS, time, domain-controller health and replication evidence.

Establish the scope

Record the affected domain, site, client, domain controller (DC), UTC time and exact error. Compare one affected machine with a healthy machine. Commands here are diagnostic; domain membership, installed tools and delegated permissions affect availability.

Check DNS and DC discovery

```
ipconfig /all
```

Inspect client addresses and DNS servers. AD members should use DNS that can resolve their AD namespace.

```
nltest /dsgetdc:ad.example.com
```

Find a DC for an example domain; replace it with your domain.

```
Resolve-DnsName -Type SRV  
_ldap._tcp.dc._msdcs.ad.example.com
```

One PowerShell command. Join the lines and substitute your AD DNS domain.

Inspect time

```
w32tm /query /status
```

Review the local time source and synchronisation status.

Check the domain time hierarchy before changing clocks. Time problems can disrupt Kerberos authentication.

Inspect DC health

```
dcdiag /s:DC01 /q
```

Report errors from the selected DC; substitute its name.

```
dcdiag /s:DC01 /test:DNS /DnsBasic /v
```

Run basic DNS diagnostics without requesting dynamic-update tests.

Inspect replication

```
repadmin /replsummary
```

Summarise replication failures and the largest replication deltas.

```
repadmin /showrepl DC01
```

Inspect inbound replication partners and results for one DC.

Compare the last successful replication, failure count, naming context and exact error. DNS, connectivity, RPC, authentication and time can all affect replication.

Correlate supporting evidence

Review Directory Service, DNS Server, DFS Replication and System event logs as applicable. Check SYSVOL/NETLOGON access and site/subnet placement when symptoms point there. Diagnostic tools are commonly provided by AD DS tools or RSAT.

Keep remediation separate

Capture results before changing anything. A forced sync, DNS re-registration, secure-channel repair or metadata cleanup is a remediation action, not a routine first diagnostic step. Apply a targeted fix only after identifying the cause.

Backup & recovery

A practical checklist for planning, protecting and testing recovery.

Set recovery objectives

RPO describes the point in time to which data must be recovered; it expresses the tolerable data-loss window.

RTO is the target time to restore the required service after disruption.

Agree both with the service owner and test whether the design can meet them.

Know what must be recoverable

Inventory data, application configuration, identity services, encryption keys, certificates, licences and dependencies. Document owners and restore order. Protect the recovery documentation so it remains available when production systems are down.

Choose and document retention

A full backup copies the selected data set. An incremental usually contains changes since a previous backup; a differential usually contains changes since the last full. Product behaviour varies. Keep every dependency required by retained restore points.

Capacity is more than source size

Allow for change rate, retained chains, archives, extra copies, metadata and free space. Compression and deduplication depend on the workload. Measure actual stored growth rather than assuming a reduction ratio.

Protect the recovery path

Keep a protected copy separate from the production environment, using offline or appropriately isolated/immutable storage where suitable. Restrict backup administration, protect recovery credentials and verify that encryption keys can be recovered independently. Encryption alone does not stop deletion.

Budget the complete window

Include scanning, snapshots, data transfer, verification and retries. Jobs can compete for network, source, repository and processing capacity. A network-only transfer estimate is a starting point, not a completion guarantee.

Test a real restoration

1. Select a representative restore point.
2. Restore in a safe, isolated environment.
3. Verify data and application function.
4. Check permissions and dependent services.
5. Record elapsed time, recovered point and issues.
6. Update the runbook and repeat on a planned schedule and after material changes.

Daily evidence to review

Failed or missing jobs, backup age, repository capacity, protected-copy status and unresolved restore-test findings. A green backup job does not by itself prove recoverability.

Simple Systems tools

Backup retention calculator, Backup window planner and Storage growth planner.
simplesys.dev/other-tools/

Common network ports

Typical destination ports and transports used in everyday administration.

Core network services

- 22 TCP** - SSH; also SFTP over SSH.
- 53 UDP/TCP** - DNS; TCP is also used for normal DNS queries when needed.
- 67/68 UDP** - DHCPv4 server/client.
- 80 TCP** - HTTP.
- 123 UDP** - NTP time service.
- 161 UDP** - common SNMP queries.
- 162 UDP** - common SNMP traps.
- 443 TCP** - HTTPS over TCP.
- 443 UDP** - commonly HTTP/3 over QUIC.

Mail services

- 25 TCP** - SMTP transport / server relay.
 - 465 TCP** - submission with implicit TLS.
 - 587 TCP** - message submission, commonly with STARTTLS.
 - 143 / 993 TCP** - IMAP / IMAP over implicit TLS.
 - 110 / 995 TCP** - POP3 / POP3 over implicit TLS.
- Port 25 is not interchangeable with authenticated client submission.

Web and file access

- 445 TCP** - SMB.
 - 3389 TCP/UDP** - RDP.
 - 2049 TCP** - commonly NFSv4; other NFS versions and setups can need additional ports.
- A service can be configured to use a different port.

Active Directory-related services

- 88 TCP/UDP** - Kerberos.
 - 389 TCP/UDP** - LDAP / CLDAP.
 - 636 TCP** - LDAP over TLS.
 - 3268 / 3269 TCP** - Global Catalog / TLS.
 - 135 TCP** - RPC endpoint mapper.
 - 49152-65535 TCP** - default modern Windows dynamic RPC server range; configuration and workload matter.
- AD also relies on DNS, time and SMB. This is not a complete firewall rule set.

Management and databases

- 5985 / 5986 TCP** - WinRM HTTP / HTTPS.
- 1433 TCP** - common SQL Server listener.
- 3306 TCP** - MySQL / MariaDB.
- 5432 TCP** - PostgreSQL.
- 514 UDP / 6514 TCP** - syslog / syslog over TLS.

Test the correct transport

Test-NetConnection host.example -Port 443

Windows TCP check. Replace the target with your host.

```
ss -lntup
```

Linux local listeners; process details can require privileges.

A TCP test cannot prove that a UDP service works. For DNS, make a DNS query. For HTTPS, also test the TLS connection and application response.

Before changing a firewall

Confirm source, destination, traffic direction, transport, destination port and actual listener. Limit access to the intended systems. An open port does not prove a service is healthy or encrypted; a timeout alone does not identify which device dropped the traffic.

DNS quick reference

Record types, practical queries and a short troubleshooting sequence.

Read the records

A / AAAA - IPv4 / IPv6 address.

CNAME - alias to another hostname; normally cannot coexist with other data at the same name.

MX - mail exchange; lower preference values are tried first.

NS - authoritative name server.

TXT - text used by policies and verification.

SOA - zone administration and serial.

PTR - reverse address-to-name mapping.

Query with dig

```
dig example.com A
```

Show the response, status and answer TTLs.

```
dig example.com MX +short
```

Compact mail-exchange answer.

```
dig @1.1.1.1 example.com TXT
```

Ask a specific resolver.

```
dig -x 192.0.2.10
```

Reverse lookup for an example address.

Query with PowerShell

```
Resolve-DnsName example.com -Type MX
```

Inspect MX records on Windows.

```
Resolve-DnsName example.com -Type TXT  
-Server 1.1.1.1
```

One command; join the two lines before running.

Know which answer you are seeing

A recursive resolver answers from its cache or follows DNS delegation. An authoritative server answers for its zone. Different resolver answers can reflect caching, geography or load balancing.

TTL and changes

TTL is a cache lifetime in seconds. A cached answer usually displays its remaining lifetime. Lowering the TTL now does not shorten copies already cached under the previous TTL. Negative answers can also be cached.

Troubleshoot in order

1. Confirm the exact name, record type and DNS zone.
2. Compare your configured resolver with another resolver.
3. Check delegation and query the authoritative servers.
4. Distinguish NXDOMAIN (name absent), NOERROR with no matching data, and SERVFAIL (lookup failure).
5. Check split DNS, local hosts files and application caches.

Keep the context

Save the queried name, type, resolver, UTC time, response status and TTL. A matching pair of resolver answers is useful evidence, but does not prove global propagation.

Simple Systems tools

DNS lookup, DNS propagation checker, Reverse DNS checker and DNS record generator.

simplesys.dev/dns-tools/

E-mail authentication

MX, SPF, DKIM and DMARC: what each check can tell you.

MX: inbound routing

MX identifies the servers that receive mail for a domain. Lower preference values are tried first. MX does not authorise outbound senders or prove that a mailbox exists. A Null MX explicitly says the domain accepts no e-mail.

SPF: sending infrastructure

SPF checks the connecting IP against the envelope sender domain, or HELO identity where applicable. Publish one SPF policy at a name. A policy can span several TXT character strings.

SPF essentials

ip4 / **ip6** authorise address ranges.

include incorporates another policy.

redirect= delegates policy evaluation.

-all fail; **~all** softfail; **?all** neutral; **+all** authorises everyone.

SPF limits DNS-query-causing terms to 10 across evaluation, including nested policies. This is not simply a count of TXT queries.

DKIM: message signatures

Read **d=** (signing domain) and **s=** (selector) from DKIM-Signature. The public key is at **selector._domainkey.domain**. Finding a key does not prove a particular message has a valid signature.

DMARC: authentication plus alignment

DMARC passes when at least one of SPF or DKIM passes and aligns with the visible From domain. SPF alignment uses the authenticated envelope sender domain; DKIM alignment uses **d=**. Relaxed and strict alignment apply different domain matching rules.

Read the policy

Query **_dmarc.example.com TXT**.

p=none requests monitoring.

p=quarantine requests suspicious treatment.

p=reject requests rejection.

rua= specifies aggregate reporting destinations.

A receiver can apply local policy. Do not enforce a stricter policy until legitimate senders have been checked.

Quick queries

`dig example.com MX +short`

Inbound mail servers.

`dig example.com TXT +short`

Find the SPF policy.

`dig selector1._domainkey.example.com TXT`

Replace selector1 with the actual selector.

`dig _dmarc.example.com TXT +short`

Read the published DMARC policy.

Diagnose a real message

Use authentication results from a trusted receiving system. Compare the visible From domain, envelope sender and DKIM signing domains. Forwarding may break SPF; message changes may break DKIM. DNS-only checks do not replace a real delivery test.

Group Policy troubleshooting

Find the applicable policy, the processing instance and the reason a setting differs.

Start in the affected context

Record the computer, affected user, domain/OU, expected setting and UTC time. Separate User Configuration from Computer Configuration. Compare a healthy machine or user. Confirm that the setting is managed by a domain GPO rather than MDM, a script or a local preference.

Capture the resultant policy

```
gpresult /scope user /r
```

Run in the affected user session to see a user-policy summary.

```
gpresult /scope computer /r
```

Inspect computer-policy results; an elevated prompt may be required.

```
gpresult /h .\gp-report.html
```

Write an HTML report in the current writable folder. Review applied and denied GPOs and the winning setting.

Check scope and precedence

Confirm the correct site, domain and OU links; link status; enabled user/computer sections; security filtering and permissions; WMI filter; and inheritance. Normal processing runs Local > Site > Domain > parent OU > child OU. Link order, Enforced and Block Inheritance can change which setting wins.

Check loopback when relevant

Loopback uses the computer location to influence user policy. Merge and Replace behave differently. Check this on shared workstations, kiosks and session hosts before assuming that user OU links alone determine the result.

Read the processing evidence

Start with Group Policy errors and warnings in Windows Logs > System. Then inspect Applications and Services Logs > Microsoft > Windows > GroupPolicy > Operational. Correlate the same processing instance using its ActivityID, user/computer context and timestamps.

Find the failing dependency

Read the full event text, error code and affected client-side extension. Check DNS/DC discovery, access to SYSVOL/NETLOGON, replication and connectivity when the evidence points there. Distinguish a denied GPO from a GPO that applied but did not configure the expected setting.

Refresh only after collecting evidence

```
gpupdate /target:user
```

Apply changed user policies in the current context.

```
gpupdate /target:computer
```

Apply changed computer policies.

This changes policy state. /force reapplies all settings; it is not a substitute for diagnosing scope or access. Some settings need sign-out or restart. Plan that separately; do not add /logoff or /boot casually. A refresh creates a new processing ActivityID.

Keep a useful handover

Save the report, affected setting, GPO name/GUID, ActivityID, full errors and a before/after comparison. Reports can contain internal names and user information. Share only the material needed for the investigation.

IPv4 subnetting

Address counts, masks, private ranges and a worked example.

Core calculations

An IPv4 address has 32 bits. A /n prefix fixes n network bits and leaves 32-n host bits.

Total addresses = $2^{(32-n)}$

For a conventional /30 or larger subnet, usable hosts are normally total minus two: network and broadcast addresses.

Common prefixes

Prefix	Mask	Total	Hosts
/16	255.255.0.0	65,536	65,534
/20	255.255.240.0	4,096	4,094
/22	255.255.252.0	1,024	1,022
/24	255.255.255.0	256	254
/25	255.255.255.128	128	126
/26	255.255.255.192	64	62
/27	255.255.255.224	32	30
/28	255.255.255.240	16	14
/29	255.255.255.248	8	6
/30	255.255.255.252	4	2

Special cases

/31: two endpoints on an IPv4 point-to-point link when both ends support RFC 3021; no network/broadcast subtraction.

/32: one exact address or host route.

/0: the complete IPv4 space.

Worked example: 192.168.10.77/26

The final mask octet is 192, so the block size is 256-192 = 64. Boundaries are 0, 64, 128 and 192.

Network: 192.168.10.64

Broadcast: 192.168.10.127

Host range: 192.168.10.65-126

Usable hosts: 62

Private IPv4 ranges

10.0.0.0/8

172.16.0.0/12 (172.16-172.31)

192.168.0.0/16

Private addressing does not provide encryption or replace firewall policy. Private addresses are not globally unique.

Plan beyond the address count

Allow space for gateways, infrastructure, reservations and growth. A subnet calculator does not know your DHCP exclusions or vendor-reserved addresses. Cloud networks can reserve additional addresses. Check the target platform before sizing.

Avoid common mistakes

A /24 is a prefix length, not a host count. Larger prefix numbers mean smaller networks. The gateway is a chosen usable address, not automatically the first host. Networks can overlap even when their written base addresses differ.

Simple Systems tools

Subnet calculator and IP range comparison.

simplesys.dev/subnet-calculator/

Linux diagnostics

Inspect networking, storage, services and logs without changing configuration.

Interfaces and routes

`ip -brief address`

Show interface addresses and state.

`ip route show`

Show the IPv4 routing table.

`ip -6 route show`

Show the IPv6 routing table.

Sockets and DNS

`ss -lntup`

List listening TCP/UDP sockets numerically. Process details may require extra privileges.

`dig example.com A`

Query an address record if dig is installed.

`dig @1.1.1.1 example.com MX`

Ask a specific resolver for MX records.

Storage and capacity

`df -h`

Show mounted filesystem usage in human-readable units.

`df -i`

Check inode use when free space alone does not explain a write failure.

Services on systemd hosts

`systemctl --failed`

Show units in a failed state.

`systemctl status ssh.service --no-pager`

Inspect a service; substitute its actual unit name. Some distributions use `sshd.service`.

Journal queries

`journalctl -b -p err --no-pager`

Show error and higher-priority entries from this boot.

`journalctl -u ssh.service --since "1 hour ago"`

Inspect one unit over a recent period.

`journalctl -n 100 --no-pager`

Show the most recent 100 journal entries.

How to approach an incident

Record UTC time and symptoms first. Check interface state, routes, DNS and the listening service separately. Keep the original error message and correlate it with nearby log entries. A successful ping does not prove an application works.

Environment notes

Commands depend on installed packages, permissions and the init system. These examples do not modify configuration, but DNS queries leave the machine and logs may reveal sensitive data. Read the local man page for version-specific details.

Microsoft 365 mail troubleshooting

A practical sequence for investigating Exchange Online delivery problems.

1. Capture one specific example

Record sender, recipient, UTC time, message subject and Message-ID if available. Establish whether the issue affects inbound, outbound or internal mail; one user or many; one domain or many. Keep the original nondelivery report (NDR) and headers.

2. Check service and recipient state

Review Microsoft 365 service health. Confirm the recipient address, mailbox and applicable licence/service configuration. Compare webmail with the desktop client to distinguish service-side delivery from a local display or sync issue.

3. Trace the message

In the Exchange admin center, open Mail flow > Message trace. Search by sender, recipient and a suitably narrow time range. Inspect the event details, not just the summary status. Trace visibility, available detail and retention depend on the current service and your role.

Interpret the result

Delivered does not guarantee that the user sees the message in Inbox. Review rules, forwarding, Junk Email and quarantine where applicable.

Deferred / pending: inspect the reported reason and later events.

Failed / rejected: read the full error and the system that generated it.

4. Read the complete NDR

Capture the enhanced status code, diagnostic text and generating server. Check the documented meaning of that exact error. Common causes include an invalid recipient, policy restrictions, routing problems, authentication or temporary delivery issues. Avoid diagnosing from the numeric code alone.

5. Validate DNS and authentication

Compare MX and Autodiscover with the intended deployment. Check that SPF covers every legitimate sender and that the actual DKIM selectors resolve correctly. Inspect DMARC alignment in a real message. Use tenant-provided values; third-party gateways, hybrid routing and sovereign clouds can differ.

6. Follow the actual route

Review connectors, accepted-domain settings, transport rules and gateway logs when relevant. For suspected filtering, check quarantine and security-policy results with an authorised administrator. Keep the evidence before making a change.

Escalation evidence

Provide the UTC window, affected addresses, Message-ID, trace details, full NDR and relevant headers. Redact unrelated personal data. Record recent changes and compare a successful message with a failed one. Test a targeted correction rather than changing multiple policies together.

References (click to open): [Microsoft: message trace](#) | [Microsoft: NDRs and SMTP errors](#) | [Microsoft: external DNS records](#)

PowerShell diagnostics

Read-only checks for Windows systems, networking and event logs.

Network configuration

```
Get-NetIPConfiguration
```

Show addresses, gateways and DNS settings.

```
Get-NetIPAddress -AddressFamily IPv4
```

List IPv4 addresses on interfaces.

DNS and connectivity

```
Resolve-DnsName example.com -Type A
```

Resolve an IPv4 record.

```
Resolve-DnsName example.com -Type MX
```

Inspect inbound mail routing.

```
Test-NetConnection example.com -Port 443
```

Test TCP connectivity; does not validate HTTPS content or the certificate.

Listening TCP ports

```
Get-NetTCPConnection -State Listen
```

Show local listeners and their owning process IDs.

```
Get-Process -Id 1234
```

Look up a process ID from the previous result. Replace 1234.

Learn a command

```
Get-Help Test-NetConnection -Examples
```

Read installed usage examples. Some help content or modules may need installation.

Services and processes

```
Get-Service | Where-Object Status -eq Stopped
```

List stopped services; stopped does not necessarily mean faulty.

```
Get-Process | Sort-Object CPU -Descending |  
Select-Object -First 10 Name,Id,CPU
```

One pipeline; CPU is cumulative processor time, not current percentage.

Recent system events

```
Get-WinEvent -LogName System -MaxEvents 30
```

Read the most recent system events. Permissions vary by log.

```
Get-WinEvent -FilterHashtable @{  
  LogName="System"; Level=2  
} -MaxEvents 20
```

Read recent error-level events. The brace block is one command.

Check file integrity

```
Get-FileHash .\download.iso -Algorithm SHA256
```

Compare against a trusted, independently obtained checksum. A matching untrusted checksum proves little.

Use the right environment

Network cmdlets here use Windows modules and may not exist in PowerShell on Linux/macOS. Commands inspect local state or contact the named target. Review output for internal names and other private information before sharing.

RAID and storage

Usable capacity, failure tolerance and the assumptions behind the numbers.

Capacity assumptions

N = active disks, excluding hot spares.

S = capacity of the smallest active disk.

Formulas below assume equal effective disk sizes and conventional layouts, before filesystem, controller and reserved-space overhead.

Common RAID levels

RAID 0: $N \times S$. No disk-failure tolerance.

RAID 1: S for a two-disk mirror. One disk can fail.

RAID 5: $(N-1) \times S$. At least three disks; any one disk can fail.

RAID 6: $(N-2) \times S$. At least four disks; any two disks can fail.

RAID 10: $(N/2) \times S$ for mirrored pairs. At least four disks, even N . One failure per pair can be tolerated; losing both disks of a pair loses the array.

Nested parity arrays

With **G** equal-size groups:

RAID 50: $(N-G) \times S$; at least three disks per group; one failure per group.

RAID 60: $(N-2G) \times S$; at least four disks per group; two failures per group.

Failures must stay within each group tolerance.

Controller support varies.

Worked example

Six active 8 TB disks in RAID 6:

$(6-2) \times 8 \text{ TB} = \mathbf{32 \text{ TB}}$, approximately **29.10 TiB**, before overhead. A separate hot spare adds no usable capacity.

TB and TiB are different

1 TB = 1,000,000,000,000 bytes.

1 TiB = 1,099,511,627,776 bytes.

Divide decimal TB by about 1.0995 to estimate TiB. A lower displayed binary number is not automatically missing capacity.

Spares and rebuilds

A hot spare waits to replace a failed disk; it is not extra parity or a backup. Rebuilds can take substantial time and reduce performance. Remaining disks are still exposed to additional failures and read errors. Monitor rebuild progress and backups together.

Provisioning terminology

Raw: total device capacity.

Usable: capacity after redundancy and relevant overhead.

Allocated / provisioned: capacity assigned to workloads.

Used: data currently consumed.

Thin provisioning: logical allocations can exceed physical capacity; monitor actual free space and growth.

Plan the workload, not just capacity

Consider latency, IOPS, throughput, write patterns, controller/cache protection, failure domains and expansion options. Compression and deduplication depend on the data. Storage pools, erasure coding and vendor-specific layouts can follow different rules.

RAID is not a backup

Redundancy can preserve service through certain disk failures. It does not provide independent recovery from deletion, ransomware, corruption or loss of the entire array. Keep and test separate backups.

Windows event logs

Choose the right channel, filter the time window and preserve the evidence.

Choose the relevant log

System - operating system, drivers and services.

Application - application/provider events.

Security - configured security audit events; access and audit policy affect what is available.

Setup - installation/setup activity.

Forwarded Events - events received by a configured collector.

Applications and Services Logs contains provider-specific Operational channels, including GroupPolicy and TaskScheduler.

Interpret the fields together

Record computer, channel, provider, Event ID, Record ID, level, timestamp and full message. Inspect the XML details and ActivityID when available. An Event ID alone is not a diagnosis and is not globally unique across providers. Event Viewer displays local time; confirm the time zone when correlating systems.

Standard levels

1 Critical · **2** Error · **3** Warning

4 Information · **5** Verbose

0 LogAlways.

Audit Success/Failure are audit keywords, not a replacement for these numeric levels. Informational events can still be essential evidence.

Inspect recent events

```
Get-WinEvent -LogName System -MaxEvents 30
```

Read recent system events.

```
Get-WinEvent -ListLog *
```

Discover log names and their configuration. Permissions affect visibility.

Filter at the source

```
Get-WinEvent -FilterHashtable @{
    LogName="System"; Level=1,2,3
    StartTime=(Get-Date).AddHours(-2)
} -MaxEvents 100
```

One PowerShell command: critical, error and warning events from the last two hours. Add EndTime for a bounded window.

Add ProviderName and Id when investigating a known provider/event combination. Filtering in the query avoids loading an entire log before Where-Object filters it. No matches can mean the window, provider or channel is wrong.

Export the original events

```
wevtutil epl System .\System.evtx
```

Export the System log to a new EVTX file in the current writable folder. Choose a unique filename; no overwrite is requested.

```
Get-WinEvent -Path .\System.evtx
-MaxEvents 30
```

One PowerShell command; join the lines. Inspect a saved EVTX without importing it into the live log.

Preserve context

In Event Viewer, use Filter Current Log or a Custom View, then export the required events. Keep EVTX for original event data; CSV or copied message text is useful for summaries but is not a full substitute. Protect originals and note the collection time and filter.

Investigate before changing logging

Correlate events before and after the symptom across related providers. Log retention, disabled channels or audit settings can explain missing history. Enabling extra logging changes collection and will not recreate old events. Do not clear logs during evidence collection. Redact sensitive information from shared summaries.