

# Kerberos authentication troubleshooting guidance

 [learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-authentication-troubleshooting-guidance](https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-authentication-troubleshooting-guidance)

- Article
- 01/15/2025

## In this article

This guide provides you with the fundamental concepts used when troubleshooting Kerberos authentication issues.

## Troubleshooting checklist

- A Kerberos-related error is a symptom of another service failing. The Kerberos protocol relies on many services that must be available and functioning properly for any authentication to take place.
- To determine whether a problem is occurring with Kerberos authentication, check the System event log for errors from any services by filtering it using the "source" (such as Kerberos, kdc, LsaSrv, or Netlogon) on the client, target server, or domain controller that provide authentication. If any such errors exist, there might be errors associated with the Kerberos protocol as well.
- Failure audits on the target server's Security event log might show that the Kerberos protocol was being used when a logon failure occurred.
- Before you inspect the Kerberos protocol, make sure that the following services or conditions are functioning properly:
  - The network infrastructure is functioning properly, and all computers and services can communicate.
  - The domain controller is accessible. You can run the command `nltest /dsgetdc:<Domain Name> /force /kdc` (for example, `nltest /dsgetdc:contoso.com /force /kdc`) on the client or target server.
  - Domain Name System (DNS) is configured properly and resolves host names and services appropriately.
  - The clocks are synchronized across the domain.
  - All critical updates and security updates for Windows Server are installed.
  - All software, including non-Microsoft software, is updated.
  - The computer is restarted if you're running a server operating system.
  - The required services and server are available. The Kerberos authentication protocol requires a functioning domain controller, DNS infrastructure, and network to work properly. Verify that you can access these resources before you begin troubleshooting the Kerberos protocol.

If you've examined all these conditions and are still having authentication problems or Kerberos errors, you need to look further for a solution. The problems can be caused by how the Kerberos protocol is configured or by how other technologies that work with the Kerberos protocol are configured.

## Common issues and solutions

### Kerberos delegation issues

In a typical scenario, the impersonating account would be a service account assigned to a web application or the computer account of a web server. The impersonated account would be a user account requiring access to resources via a web application.

There are three types of delegation using Kerberos:

- Full delegation (unconstrained delegation)

Full delegation should be avoided as much as possible. The user (front-end user and back-end user) can be located in different domains and also in different forests.

- Constrained delegation (Kerberos only and protocol transition)

The user can be from any domain or forest, but the front-end and the back-end services should be running in the same domain.

- Resource-based constrained delegation (RBCD)

The user can be from any domain, and front-end and back-end resources can be from any domain or forest.

## Most common Kerberos delegation troubleshooting

---

- Service principal name missing or duplicated
- Name resolution failures or incorrect responses (wrong IP addresses given for a server name)
- Large Kerberos tickets size (MaxTokenSize) and environment not set up properly
- Ports being blocked by firewalls or routers
- Service account not given appropriate privileges (User Rights Assignment)
- Front-end or back-end services not in the same domain and constrained delegation setup (not RBCD)

For more information, see:

- [Constrained delegation for CIFS fails with ACCESS\\_DENIED error](#)
- [Configure constrained delegation for a custom service account](#)
- [Configure constrained delegation on the NetworkService account](#)

## Single sign-on (SSO) broken and prompting for authentication once

---

Consider the following scenarios:

- A client and server application like Microsoft Edge and Internet Information Services (IIS) server. The IIS server is configured with Windows Authentication (Negotiate).
- A client and server application like an SMB client and SMB server. By default, the SMB server is configured with Negotiate Security Support Provider Interface (SSPI).

A User opens Microsoft Edge and browses an internal website <http://webserver.contoso.com>. The website is configured with Negotiate, and this website prompts for authentication. After the user manually enters the username and password, the user gets authentication, and the website works as expected.

Note

This scenario is an example of a client and server. The troubleshooting technique is the same for any client and server configured with Integrated Windows authentication.

Integrated Windows authentication is broken on the user level or the machine level.

## Troubleshooting methods

---

- Review the client configuration for an integrated authentication setting, which can be enabled at an application or machine level. For example, all HTTP-based applications would look for the site to be in a Trusted zone when trying to perform integrated authentication.

Open *inetctl.cpl* (**Internet Options**), which all HTTP-based applications use for Internet Explorer configurations, and review if the website is configured as **Local intranet**.

- Applications also have a configuration to perform Integrated Windows authentication.

Microsoft Edge or Internet Explorer has a setting **Enable Integrated Windows Authentication** to be enabled.

- Review the application configuration, and the client computer can obtain a Kerberos ticket for a given service principal name (SPN). In this example, the SPN is [http/webserver.contoso.com](http://webserver.contoso.com).
  - Success message when you can find the SPN:

#### Console

```
C:>klist get http/webserver.contoso.com
Current LogonId is 0:0x9bd1f
A ticket to http/webserver.contoso.com has been retrieved successfully.
```

- Error message when you can't find the SPN:

#### Console

```
C:>klist get http/webserver.contoso.com
klist failed with 0xc000018b/-1073741429: The SAM database on the Windows Server does not have a
computer account for this workstation trust relationship.
```

Identify and add the respective SPNs to the appropriate user, service, or machine accounts.

- If you've identified that the SPNs can be retrieved, you can verify if they're registered on the correct account by using the following command:

#### Console

```
setspn -F -Q */webserver.contoso.com
```

## Authentication DC discovery issues

---

Application servers configured with Integrated Windows authentication need domain controllers (DCs) to authenticate the user/computer and service.

The inability to contact a domain controller during the authentication process leads to error 1355:

- | The specified domain either does not exist or could not be contacted

## Unable to access a resource configured with Integrated Windows authentication with an error 1355

---

### Note

Error messages may differ from an application standpoint, but the meaning of the error is that the client or server is unable to discover a domain controller.

Here are examples of such error messages:

- | The following error occurred attempting to join the domain "Contoso":  
| The specified domain either does not exist or could not be contacted.
- | The Domain Controller for the domain contoso.com could not be found
- | Could not contact domain Controller 1355

## Top causes of the issue

---

- DNS misconfiguration on the client

You can run the [ipconfig /all](#) command and review the DNS servers list.

- DNS misconfiguration on the domain controllers in a trusted domain or forest
- Network ports blocked between the client and domain controllers

DC Discovery ports: UDP 389 (UDP LDAP) and UDP 53 (DNS)

## Troubleshooting steps

---

1. Run the `nslookup` command to identify any DNS misconfigurations.
2. Open required ports between the client and the domain controller. For more information, see [How to configure a firewall for Active Directory domains and trusts](#).

## Log analysis test scenario

---

### Environment and configuration

---

- Client machine

`Client1.contoso.com` (a Windows 11 machine) joins the domain `Contoso.com`.

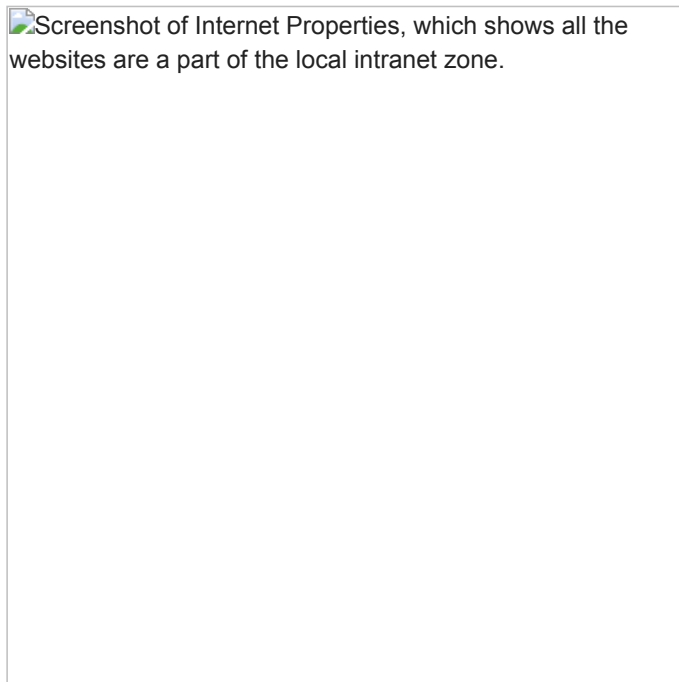
- User `John`

The user belongs to `Contoso.com` and signs in on the client machine.

- Internet options on the client machine

All the websites are a part of the local intranet zone.

 Screenshot of Internet Properties, which shows all the websites are a part of the local intranet zone.




- Server

`IIServer.contoso.com` (Windows Server 2019) joins the domain `Contoso.com`.

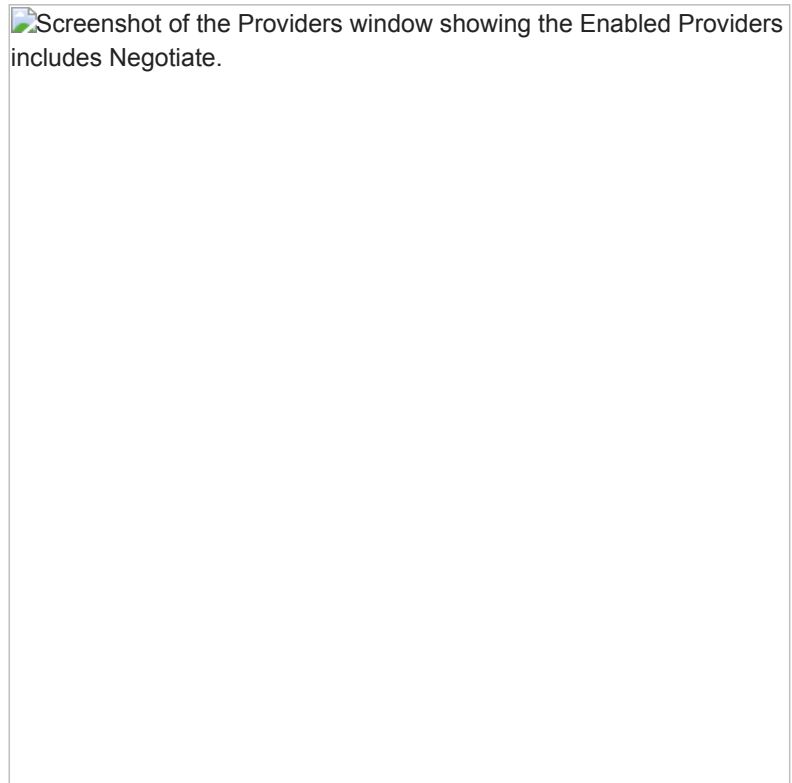
- Authentication configuration

**Windows Authentication is Enabled.**

 Screenshot of the Internet Information Services Manager window showing Windows Authentication is Enabled.

- Authentication Providers: Negotiate

Enabled providers are set as follows:



## Authentication flow

---

 Screenshot of an authentication flow.

1. User **John** signs in to **Client1.contoso.com**, opens a Microsoft Edge browser and connects to **IISServer.contoso.com**.
2. The client machine will perform the below steps (Step 1 in the above diagram):
  1. The DNS resolver caches **IISServer.contoso.com** to verify if this information is already cached.
  2. The DNS resolver checks the HOSTS file for any mapping of **IISServer.contoso.com** located in **C:\Windows\System32\drivers\etc\Hosts**.
  3. Send a DNS query to the preferred DNS server (configured on the IP configuration settings), which is also a domain controller in the environment.
3. The DNS service running on the domain controller will look into its configured zones, resolve the Host A record, and respond back with an IP address of **IISServer.contoso.com** (Step 2 in the above diagram).
4. The client machine will perform a TCP three-way handshake on TCP port 80 to **IISServer.contoso.com**.
5. The client machine will send an anonymous HTTP request to **IISServer.contoso.com**.
6. The IIS server listening on port 80 will receive the request from **Client1.contoso.com**, look into the IIS servers authentication configuration and send back an HTTP 401 challenge response to the client machine with Negotiate as the authentication configuration (Step 3 in the above diagram).
7. The Microsoft Edge process running on **Client1.contoso.com** will know that the IIS server is configured with Negotiate and will verify if the website is a part of the local intranet zone. If the website is in the local intranet zone, then the Microsoft Edge process will call into **LSASS.exe** to get a Kerberos ticket with an SPN **HTTP\IISServer.contoso.com** (Step 5 in the above diagram).

8. The domain controller (KDC service) will receive the request from `Client1.contoso.com`, search its database for the SPN `HTTP\IISServer.contoso.com` and find `IISServer.contoso.com` is configured with this SPN.
9. The domain controller will respond back with a TGS response with the ticket for the IIS server (Step 6 in the above diagram).
10. The Microsoft Edge process on the client machine will send a Kerberos Application Protocol (AP) request to the IIS web server with the Kerberos TGS ticket issued by the domain controller.
11. The IIS process will call into `LSASS.exe` on the web server to decrypt the ticket and create a token with SessionID and Users group membership for authorization.
12. IIS process will get a handle from `LSASS.exe` to the token to make authorization decisions and allow the User to connect with an AP response.

## Network Monitor analysis of the workflow

---

### Note

You need to be a user of the local Administrators group to perform the below activities.

1. Install Microsoft Network Monitor on the client machine (`Client1.contoso.com`).
2. Run the following command in an elevated command prompt window (`cmd.exe`):  
  
Console  
  
`ipconfig /flushdns`
3. Start the Network Monitor.
4. Open Microsoft Edge browser and type `http://iisserver.contoso.com`.



## 5. Network trace analysis:

1. DNS query to the domain controller for a Host A record: **IIServer.contoso.com**.

### Output

```
3005    00:59:30.0738430    Client1.contoso.com    DCA.contoso.com    DNS    DNS:QueryId =
0x666A, QUERY (Standard query), Query for iiserver.contoso.com of type Host Addr on class
Internet
```

2. DNS response from the DNS service on the domain controller.

### Output

```
3006    00:59:30.0743438    DCA.contoso.com    Client1.contoso.com    DNS    DNS:QueryId =
0x666A, QUERY (Standard query), Response - Success, 192.168.2.104
```

3. The Microsoft Edge process on **Client1.contoso.com** connects to the IIS web server **IIServer.contoso.com** (anonymous connection).

### Output

```
3027    00:59:30.1609409    Client1.contoso.com    iiserver.contoso.com    HTTP    HTTP:Request,
GET /
Host: iiserver.contoso.com
```

4. IIS server responds back with HTTP response 401: Negotiate and NTLM (configuration performed on the IIS server).

### Output

```
3028    00:59:30.1633647    iiserver.contoso.com    Client1.contoso.com    HTTP
HTTP:Response, HTTP/1.1, Status: Unauthorized, URL: /favicon.ico Using Multiple Authentication
Methods, see frame details
```

```
WWWAuthenticate: Negotiate
WWWAuthenticate: NTLM
```

5. Kerberos request from **Client1.contoso.com** goes to the domain controller **DCA.contoso.com** with an SPN: **HTTP/iiserver.contoso.com**.

### Output

```
3034    00:59:30.1834048    Client1.contoso.com    DCA.contoso.com    KerberosV5
KerberosV5:TGS Request Realm: CONTOSO.COM Sname: HTTP/iiserver.contoso.com
```

6. Domain controller **DCA.contoso.com** responds back with the Kerberos request, which has a TGS response with a Kerberos ticket.

### Output

```
3036    00:59:30.1848687    DCA.contoso.com    Client1.contoso.com    KerberosV5
KerberosV5:TGS Response Cname: John
Ticket: Realm: CONTOSO.COM, Sname: HTTP/iiserver.contoso.com
Sname: HTTP/iiserver.contoso.com
```

7. The Microsoft Edge process on **Client1.contoso.com** now goes to the IIS server with a Kerberos AP request.

#### Output

```
3040    00:59:30.1853262    Client1.contoso.com    iisserver.contoso.com    HTTP    HTTP:Request,
GET /favicon.ico , Using GSS-API Authorization
Authorization: Negotiate
Authorization: Negotiate
YIIHGwYGKwYBBQUCoIIHDzCCBwugMDAuBgkqhkiC9xIBAgIGCSqGSIB3EgECAGYKKwYBBAGCNwICHgYKKwYBBAGCNwICCqKCB
tUEggbRYIIgZQYJKoZIhvcSAQICAQBugga8MIIGuKADAgEFOQMCAQ6iBwMFACAAACjggTVYYIE6zCCB0egAwIBBaENGwtDT0
5UT1NPLkNPTaIoMCagAwIBAqEfMB0bBEhUVFABF
SpnegoToken: 0x1
NegTokenInit:
ApReq: KRB_AP_REQ (14)
Ticket: Realm: CONTOSO.COM, Sname: HTTP/iisserver.contoso.com
```

8. IIS server responds back with a response that the authentication is complete.

#### Output

```
3044    00:59:30.1875763    iisserver.contoso.com    Client1.contoso.com    HTTP
HTTP:Response, HTTP/1.1, Status: Not found, URL: / , Using GSS-API Authentication
WWWAuthenticate: Negotiate
oYG2MIGzoAMKAQChCwYJKoZIgvcSAQICooGeBIGbYIGYBgkqhkiG9xIBAgICAG+BiDCBhaADAgEFOQMCAQ+ieTB3oAMCARKic
ARuIF62dHj2/qKDRV5XjGKmyFl2/z6b90HTCTKigAatXS1vZTVc1dMvtNniSN8GpXJspqNvEfbETSinF0ee7KLaprxNgTYwTr
MVMnd95SoqBkm/FuY7WbTAuPvyRmUuBY3EKZEy
NegotiateAuthorization:
GssAPI: 0x1
NegTokenResp:
ApRep: KRB_AP_REP (15)
```

6. Run the **klist tickets** command to review the Kerberos ticket in the command output on **Client1.contoso.com**.

#### Output

```
Client: John @ CONTOSO.COM
Server: HTTP/iisserver.contoso.com @ CONTOSO.COM
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 11/28/2022 0:59:30 (local)
End Time:    11/28/2022 10:58:56 (local)
Renew Time:  12/5/2022 0:58:56 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DCA.contoso.com
```

7. Review Event ID 4624 on the IIS server showing the **Success** audit:

- By default, the **Success** or **Failure** audits is enabled on all server operating system of Windows. You can verify whether the auditing is enabled by the following command.
- If you find auditing is not enabled, then enable the auditing. Review the logon category in the below list. As you can observe, the logon subcategory is enabled with **Success and Failure**.

#### Console

```
C:\>auditpol /get /Subcategory:"logon"
System audit policy
Category/Subcategory          Setting
Logon/Logoff
    Logon                      Success and Failure
```

If you don't observe logon with **Success and Failure**, then run the command to enable it:

#### Console

```
C:\>auditpol /set /subcategory:"Logon" /Success:enable /Failure:enable
The command was successfully executed.
```

## Review the success security Event ID 4624 on IISServer.contoso.com

---

Observe the following fields:

- Logon type: 3 (network logon)
- Security ID in New Logon field: Contoso\John
- Source Network Address: IP address of the client machine
- Logon Process and Authentication Package: Kerberos

### Output

Log Name: Security  
Source: Microsoft-Windows-Security-Auditing  
Date: 11/28/2022 12:59:30 AM  
Event ID: 4624  
Task Category: Logon  
Level: Information  
Keywords: Audit Success  
User: N/A  
Computer: IISServer.contoso.com  
Description:  
An account was successfully logged on.

Subject:  
Security ID: NULL SID  
Account Name: -  
Account Domain: -  
Logon ID: 0x0

Logon Information:  
Logon Type: 3  
Restricted Admin Mode: -  
Virtual Account: No  
Elevated Token: No

Impersonation Level: Impersonation

New Logon:  
Security ID: CONTOSO\John  
Account Name: John  
Account Domain: CONTOSO.COM  
Logon ID: 0x1B64449  
Linked Logon ID: 0x0  
Network Account Name: -  
Network Account Domain: -  
Logon GUID: {<GUID>}

Process Information:  
Process ID: 0x0  
Process Name: -

Network Information:  
Workstation Name: -  
Source Network Address: 192.168.2.101  
Source Port: 52655

Detailed Authentication Information:  
Logon Process: Kerberos  
Authentication Package: Kerberos

## Troubleshoot authentication workflow

---

Use one of the following methods to troubleshoot the issue.

- Verify if you can resolve the name of the IIS web server (IISServer.contoso.com) from Client1.contoso.com.

- Verify if the DNS server is responding back to the correct IIS server IP address by using the following cmdlet:

#### PowerShell

```
PS C:\> Resolve-DnsName -Name IIServer.contoso.com
```

Name	Type	TTL	Section	IPAddress
----	----	---	-----	-----
IIServer.contoso.com	A	1200	Answer	192.168.2.104

- Verify if the network ports are opened between the client machine and the IIS web server ([IIServer.contoso.com](http://IIServer.contoso.com)) by using the following cmdlet:

#### PowerShell

```
PS C:\> Test-NetConnection -Port 80 IIServer.contoso.com
```

```

ComputerName      : IIServer.contoso.com
RemoteAddress     : 192.168.2.104
RemotePort        : 80
InterfaceAlias    : Ethernet 2
SourceAddress     : 192.168.2.101
TcpTestSucceeded  : True

```

- Verify if you are getting a Kerberos ticket from the domain controller.
  1. Open a normal Command Prompt (not an administrator Command Prompt) in the context of the user trying to access the website.
  2. Run the `klist purge` command.
  3. Run the `klist get http/iisserver.contoso.com` command as follows:

#### Console

```
PS C:\> klist get http/iisserver.contoso.com
```

```

Current LogonId is 0:0xa8a98b
A ticket to http/iisserver.contoso.com has been retrieved successfully.

```

```
Cached Tickets: (2)
```

```

#0>      Client: John @ CONTOSO.COM
        Server: krbtgt/CONTOSO.COM @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 11/28/2022 1:28:11 (local)
        End Time:   11/28/2022 11:28:11 (local)
        Renew Time: 12/5/2022 1:28:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DCA.contoso.com

#1>      Client: John @ CONTOSO.COM
        Server: http/iisserver.contoso.com @ CONTOSO.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 11/28/2022 1:28:11 (local)
        End Time:   11/28/2022 11:28:11 (local)
        Renew Time: 12/5/2022 1:28:11 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DCA.contoso.com

```

You will find that you get a Kerberos ticket for the SPN [http/IIServer.contoso.com](http://IIServer.contoso.com) in the **Cached Ticket (2)** column.

- Verify if the IIS web service is running on the IIS server using the default credentials.

Open a normal PowerShell Prompt (not an administrator PowerShell Prompt) in the context of the user trying to access the website.

PowerShell

```
PS C:\> invoke-webrequest -Uri http://IISserver.contoso.com -UseDefaultCredentials
PS C:\> invoke-webrequest -Uri http://IISserver.contoso.com -UseDefaultCredentials
```

```

StatusCode      : 200
StatusDescription : OK
Content          : <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
                  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
                  <html xmlns="http://www.w3.org/1999/xhtml">
                  <head>
                  <meta http-equiv="Content-Type" cont...
RawContent       : HTTP/1.1 200 OK
                  Persistent-Auth: true
                  Accept-Ranges: bytes
                  Content-Length: 703
                  Content-Type: text/html
                  Date: Mon, 28 Nov 2022 09:31:40 GMT
                  ETag: "3275ea8a1d91:0"
                  Last-Modified: Fri, 25 Nov 2022...
```

- Review the Security event log on the IIS server:
  - Success event log 4624
  - Error event log 4625

- Process of isolation: You can use the troubleshooting steps below to verify if other services on the IIS server can process Kerberos authentication.

#### Prerequisites:

- The IIS server should be running a server version of Windows.
- The IIS server should have a port opened for services like SMB (port 445).
- Create a new share or provide the user **John** with permissions to Read on one of the Folders (for example, *Software\$*) that is already shared on the machine.

1. Sign in to **Client1.contoso.com**.
2. Open Windows Explorer.
3. Type **\\ISServer.contoso.com \Software\$**.
4. Open Security events on **ISServer.contoso.com** and verify if you observe Event ID 4624.
5. Open a normal Command Prompt on **Client1.contoso.com** as the user **John**. Run the **klist tickets** command and review for the ticket **CIFS/ISServer.contoso.com**.

#### Output

```
#1> Client: John @ CONTOSO.COM
      Server: cifs/iisserver.contoso.com @ CONTOSO.COM
      KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
      Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
      Start Time: 11/28/2022 1:40:22 (local)
      End Time: 11/28/2022 11:28:11 (local)
      Renew Time: 12/5/2022 1:28:11 (local)
      Session Key Type: AES-256-CTS-HMAC-SHA1-96
      Cache Flags: 0
      Kdc Called: DCA.contoso.com
```

6. Collect network traces on **Client1.contoso.com**. Review the network traces to observe which step fails so that you can further narrow down the steps and troubleshoot the issue.