Enable Kerberos event logging - Windows Server

learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/enable-kerberos-event-logging

How to enable Kerberos event logging

- Article
- 01/15/2025

This article describes how to enable Kerberos event logging.

Original KB number: 262177

Summary

Windows 7 Service Pack 1, Windows Server 2012 R2, and later versions offer the capability of tracing detailed Kerberos events through the event log. You can use this information when troubleshooting Kerberos.

Important

The change in logging level will cause all Kerberos errors to be logged in an event. In the Kerberos protocol, some errors are expected based on the protocol specification. As a result, enabling Kerberos logging may generate events containing expected false-positive errors even when there are no Kerberos operational errors.

Examples of false-positive errors include:

1. KDC_ERR_PREAUTH_REQUIRED is returned on the initial Kerberos AS request. By default, the Windows Kerberos Client is not including pre-authentication information in this first request. The response contains information about the supported encryption types on the KDC, and in case of AES, the salts to be used to encrypt the password hashes with.

   Recommendation: Always ignore this error code.

2. KDC_ERR_S_BADOPTION is used by the Kerberos client to retrieve tickets with particular options set, for example, with certain delegation flags. When the requested type of delegation is not possible, this is the error that is returned. The Kerberos client would then try to get the requested tickets using other flags, which may succeed.

   Recommendation: Unless you are trouble-shooting a delegation problem, ignore this error.

3. KDC_ERR_S_PRINCIPAL_UNKNOWN may be logged for a wide variety of problems with the application client and server liaison. The cause can be:

    - Missing or duplicate SPNs registered in AD.
    - Incorrect server names or DNS suffixes used by the client, for example, the client is chasing DNS CNAME records and use the resulting A record in SPNs.
    - Using non-FQDN server names that need to be resolved across AD forest boundaries.

    Recommendation: Investigate the use of server names by the applications. It is most likely a client or server configuration problem.

4. KRB_AP_ERR_MODIFIED is logged when an SPN is set on an incorrect account, not matching the account the server is running with. The second common problem is that the password between the KDC issuing the ticket and the server hosting the service is out of sync.

    Recommendation: Similar to KDC_ERR_S_PRINCIPAL_UNKNOWN, check whether the SPN is correctly set.

Other scenarios or errors require the attention of the System or Domain Administrators.

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information, see How to back up and restore the registry in Windows.

Enable Kerberos event logging on a specific computer

1. Start Registry Editor.

2. Add the following registry value:

    > HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters
    > Registry Value: LogLevel
    > Value Type: REG_DWORD
    > Value Data: 0x1

    If the **Parameters** subkey does not exist, create it.

    Note

    Remove this registry value when it is no longer needed so that performance is not degraded on the computer. Also, you can remove this registry value to disable Kerberos event logging on a specific computer.

3. Quit Registry Editor. The setting will become effective immediately on Windows Server 2012 R2, Windows 7, and later versions.

4. You can find any Kerberos-related events in the system log.

More information

Kerberos event logging is intended only for troubleshooting purpose when you expect additional information for the Kerberos client-side at a defined action timeframe. Restated, kerberos logging should be disabled when not actively troubleshooting.

From a general point of view, you may receive additional errors that are correctly handled by the receiving client without user or admin intervention. Restated, some errors captured by Kerberos logging don't reflect a severe problem that must be solved or even can be solved.

For example, an event log 3 about a Kerberos error that has the error code **0x7 KDC_ERR_S_PRINCIPAL_UNKNOWN** for Server Name cifs/<**IP address**> will be logged when a share access is made against a server IP address and no server name. If this error is logged, the Windows client automatically tries to fail back to NTLM authentication for the user account. If this operation works, receive no error.

Additional resources

Training

Module

Implement Windows Server auditing and diagnostics - Training

Learn to audit and diagnose your Windows Server environment for regulatory compliance, user activity, and troubleshooting. Implement security best practices through regular audits of your network environment to gain early warning of potential malicious activity.