riverbed

TECHNICAL BRIEF

SteelHead Domain Join Integration with Active Directory

Microsoft started enforcing **msds-KrbTgtLink** validation with the release of **January 2022** Security Updates for NTLM authentication. As a result, SteelHead Domain Integrated Windows 2008 (aka RODC) machine accounts fail to establish a NetLogon secure channel (see S35726). This document provides the official explanation and solution for this behavior.

Riverbed SteelHead is an innovative WAN optimization appliance designed to enhance network performance and efficiency. This document aims to explain how the Riverbed SteelHead appliance works in conjunction with Microsoft Active Directory to optimize network traffic with the latest security enhancements to improve user experience. End-users will not be required to modify their login procedures or adopt new authentication mechanisms. SteelHead works seamlessly behind the scenes, optimizing secure traffic while maintaining the familiar Active Directory login process.

Once joined to the domain, the SteelHead appliance has sufficient privileges to communicate with domain controllers safely and securely to fully optimize intercepted traffic where there is NTLM or Kerberos authentication in use between the client and server. The communication between server-side SteelHead and domain controller(s) only occurs to determine the session key in use between the client and server for a signed and encrypted traffic that is to be optimized for SMB or encrypted MAPI (eMAPI) protocols. The mechanism used in this case is generally described by Microsoft as “NTLM Pass-Through Authentication”. The use of it is not unique to SteelHeads but this is also used in some cases by web proxy devices and load-balancers. A more detailed description of the mechanism can be found here http://msdn.microsoft.com/en-us/library/cc224019.aspx

The advantage of AD integrated mode is that no client-side configuration is required, and no impersonation account is required for NTLM pass-through authentication. The server-side SteelHead joins the domain and receives a minimal set of additional privileges that permit the appliance to obtain sessions keys to decrypt, optimize, and re-encrypt or re-sign protected traffic. While the appliance's machine account will appear in various management tools as if it were a domain controller. However, the appliance cannot perform any domain controller functions and does not replicate any accounts in the domain. Refer to KB article S35942 containing a detailed explanation of Riverbed's testing and validation.

📌 *IMPORTANT: It is recommended using the same level of physical and network protection and auditing for SteelHeads, as you use for your Domain Controllers. When the SteelHead needs to interact with the domain controller as a Tier 0 device right alongside domain controllers, the deployment of WinSec Controller is advisable to comply with Microsoft Enterprise Access Model.*

The Issue

After a recent security focused release by Microsoft, the Riverbed SteelHead RiOS code was updated to prevent failures when riverbed devices attempt to join, rejoin, or communicate with the Windows domain in Active Directory Integrated Mode 2008 (RODC). Microsoft modified the attribute **msds-KrbTgtLink** with the release of January 2022 Security Updates for NTLM authentication causing a failure while establishing a secure channel with Netlogon.

Solution

As result of latest Microsoft security enhancements, Riverbed deprecated Active Directory Integrated Mode 2008 (aka RODC), and created 3 new configuration options:

1. **Kerberos Authentication:** This mode is used for End-to-End Kerberos (eeKRB) environments where NTLM authentication is not required. The SteelHead will join as a regular machine object with the userAccountControl attribute WORKSTATION_TRUST_ACCOUNT (0x11000) to proxy Kerberos TGS request (KRB_TGS_REQ) on behalf of a client up to a Domain Controller (DC) to perform mutual authentication and integrity. Since the SteelHead integrated with Active Directory does not advertise itself or provide domain functions, the actual changes are few. The machine account is placed in the *Computers* organizational unit and NO, DNS and SRV records are created. In terms of optimization, the NTLM authentication will enter bypass mode at the application layer, while only sessions authenticated with Kerberos will undergo optimized at layer 7 for the SMB protocol.

2. **NTLM Authentication:** This mode performs NTLM pass-through authentication in transparent mode and support Kerberos authentication. The SteelHead will join as a regular machine object with the userAccountControl attribute SERVER_TRUST_ACCOUNT (0x12000). The SteelHead appliance is going to proxy Kerberos TGS request (KRB_TGS_REQ) on behalf of a client up to a Domain Controller (DC) to perform mutual authentication. Since the SteelHead integrated with Active Directory does not advertise itself or provide domain functions, the actual changes are few. The machine account is placed in the *Computers* organizational unit and NO DNS SRV records are created. From optimization perspective, both NTLM and Kerberos will be optimized at layer 7 for the SMB protocol.

3. **Domain Independent SteelHead Kerberos Optimization (DISKO):** This configuration mode exclusively supports Kerberos Authentication, eliminating the need to join SteelHead to the AD domain for optimizing SMB3 secure dialects or UNC hardened connections required in Windows, and MAPI Encryption protocols starting from RiOS 9.14.2. The main benefits of this new feature are:

   - Make configurations simple
   - Reduce some security concerns
   - Improve resiliency
   - Added support for optimizing unrelated domains

   Refer to KB article S37314 for details.

SteelHead WAN Optimization appliances are the cornerstone of SMB traffic optimization. However, maintaining proper operational, administrative, and security workflows is also vital. These new configuration options provide the flexibility to accommodate Windows, systems, and security teams, at the same time providing the level of optimization our customers have enjoyed from Riverbed WAN Optimization for years. To learn more about our application acceleration solutions, visit riverbed.com/products/acceleration