PRODUCTS   COMPANY   PARTNERS   CUSTOMERS   SUPP

CredSSP required by server – Solutions

Published: May 16, 2017
Published in: SysKit Monitor
Author: Silvio Rahle

Failed to connect, CredSSP required by server is an error line returned when trying to connect remotely to a Windows machine using RDP version 6 or newer with the Rdesktop client. It represents a frequent problem for Windows and Linux administrators alike.

```
~ rdesktop -f 1xx.1xx.1xx.1xx
Failed to connect, CredSSP required by server.
```

Rdesktop client is UNIX based client software for Microsoft's Remote Desktop Protocol. It is commonly used on ReactOS and Linux installations to connect to Windows machines running Remote Desktop Services, which often leads to the *CredSSP required by server* error.

Why does it happen?

All Windows clients have a credential cache used for authentication against services in a network called NTLM or Windows NT LAN Manager. RDP supports SSO (single sign-on) authentication enabling a user to log in with a single ID and password to gain access to a connected system. However, **Linux clients do not support this type of authentication** and they require that credentials are provided, either via a Rdesktop command line or via a login window when initiating the remote session.

Linux has Kerberos, which is an authentication mechanism for requesting access to

❮   **PRODUCT COMPANY PARTNER CUSTOMER SUPP**

Granting Ticket), which is used to access other services, such as RDP. When running Rdesktop, CredSSP will check if you have Kerberos TGT to access the remote service and use that for SSO authentication against the remote RDS server. If there is no Kerberos TGT, the Rdesktop will **fall back to a lower, insecure level of network connection** without the requirement for network-level authentication.

Solutions for *CredSSP required by server* error

Three solutions are commonly mentioned, though none of them is really THE solution, but still they can help if you stumble upon the *CredSSP required by server* problem:

Downgrade security on the Windows server to accept SSL/TLSv2

This is generally not a solution, but a workaround. **Turning security down is never a good solution**, but only a temporary fix.

1. Go to **Control Panel** -> **System**
2. Click on "**Allow remote access to your computer**"
3. Click on the "**Remote**" tab
4. Uncheck the box next to "**Allow connections only from computers running Remote Desktop with Network Level Authentication**"

This will allow insecure connections without NLA (network-level authentication) and you will no longer be prompted with failed connections to a Windows machine due to the CredSSP requirement.

Initialize Kerberos TGT

This is a solution if you receive the *CredSSP required by server* error when connecting to a remote computer without proper Kerberos identities set up.

What you need to do is initialize a Kerberos TGT to be able to connect using CredSSP. Here you can find a full guide on how to configure a Kerberos client for Windows Active Directory. You must also **configure Kerberos on the client side** against MS KDC (Active Directory Service), so that the remote server can obtain a login to pass NLA.

Use the Freerdp client

Freerdp is a free implementation of the Remote Desktop Protocol (RDP) for Linux, released under the Apache license. It works over SSH (Secure Shell), which functions well

PRODUCT   COMPANY   PARTNER   CUSTOMER   SUP

Rdesktop lacks the much needed support for newer protocols.

What is CredSSP really and why should you use it?

CredSSP (Credential Security Support Provider protocol) is a security support provider that **enables an application to delegate the user's credentials from the client computer to the target remote server**. It provides an encrypted transport layer security protocol channel. The client is authenticated over the encrypted channel using the Simple and Protected Negotiate (SPNEGO) protocol with either Microsoft Kerberos or Microsoft NTLM.

CredSSP has many use cases, but perhaps the most common is for remote server management with PowerShell. For example, it is used if a system administrator needs to delegate a user's credentials to get SharePoint server data from a content database or simply needs to execute a specific PowerShell command on the domain controller.

The SysKit tool enables you to do just that, providing you with **built-in support for CredSSP** and an **online repository full of PowerShell scripts intended for system administration**. SysKit also enables you to **track all sessions via RDP and ICA** and to track published applications, and it shows you the real-time performance of your servers.

Article by   Share on: in   f   🐦
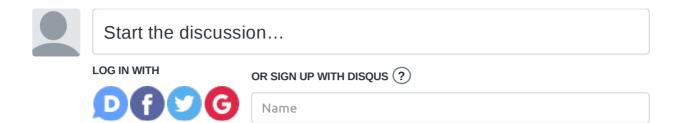
Silvio Rahle
Business Development Manager

PRODUCT   COMPANY   PARTNER   CUSTOMER   SUP

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ⑦

Name

Be the first to comment.

✉ Subscribe   Ⓓ Add Disqus to your siteAdd DisqusAdd   🔒 Privacy

Categories

SysKit Monitor

SysKit SQL Manager

Tags

Application Usage Monitoring

Autodiscover SQL Servers

Citrix Xenapp Monitoring

Comparing SQL Server Configurations

Custom Reports

Inventory Management

Monitor Terminal Server

Monitor User Activity

PRODUCT   COMPANY   PARTNER   CUSTOMER   SUP

Remote Desktop Services

Server Monitoring Templates

Server Performance

SQL Server Administration

SQL Server Best Practices

SQL Server Databases

SQL Server Documentation

SQL Server Inventory

Subscribe to our RSS feed

PRODUCTS

Monitor

SQL Manager

SPDocKit

Pulse

Shell

COMPANY

About Us

Contact Us

Careers

Our Stories

PARTNERS

Partner Program

Our Partners

Become a Partner

CUSTOMERS

SUPPORT

BLOG

Sitemap • Privacy Policy • EULA • Terms of Use • Return to top