a full automation flow in two parts:

**🧩 PART 1 – Windows PowerShell Script (Generate & Transfer Keytab)**

This script:

* Creates SPN and keytab
* Sets service account password to never expire
* Transfers keytab to a remote Linux machine via scp (requires scp in PATH)

powershell

CopyEdit

param(

[string]$ServiceAccount = "DOMAIN\svc\_sql\_linux",

[string]$ServicePrincipal = "MSSQLSvc/sqlserver.domain.com",

[string]$Realm = "DOMAIN.COM",

[string]$KeytabPath = "C:\Temp\service.keytab",

[string]$LinuxHost = "linux-host.domain.com",

[string]$LinuxUser = "ec2-user",

[string]$RemotePath = "/etc/security/keytabs/service.keytab",

[string]$Password = "SuperSecretPass123"

)

# 1. Set password never expires

net user $ServiceAccount.Split('\')[1] /domain /expires:never

# 2. Set SPN

setspn -S "$ServicePrincipal:1433" $ServiceAccount

# 3. Create keytab

ktpass -princ "$ServicePrincipal@$Realm" `

-mapuser $ServiceAccount `

-pass $Password `

-out $KeytabPath `

-ptype KRB5\_NT\_PRINCIPAL `

-crypto AES256-SHA1

# 4. Transfer to Linux

scp $KeytabPath "$LinuxUser@$LinuxHost:$RemotePath"

✅ Requires admin rights and domain tools.  
🛡️ Password is exposed — use Read-Host -AsSecureString and ConvertFrom-SecureString for secure handling if needed.

**🧩 PART 2 – Linux Script (Configure krb5, kinit with keytab)**

This bash script:

* Sets up /etc/krb5.conf
* Runs kinit using the keytab
* Accepts parameters

bash

CopyEdit

#!/bin/bash

REALM="$1" # e.g., DOMAIN.COM

KDC="$2" # e.g., dc01.domain.com

SERVICE\_PRINCIPAL="$3" # e.g., MSSQLSvc/sqlserver.domain.com@DOMAIN.COM

KEYTAB\_PATH="$4" # e.g., /etc/security/keytabs/service.keytab

if [ -z "$REALM" ] || [ -z "$KDC" ] || [ -z "$SERVICE\_PRINCIPAL" ] || [ -z "$KEYTAB\_PATH" ]; then

echo "Usage: $0 <REALM> <KDC> <SERVICE\_PRINCIPAL> <KEYTAB\_PATH>"

exit 1

fi

# 1. Configure krb5.conf

cat <<EOF | sudo tee /etc/krb5.conf

[libdefaults]

default\_realm = $REALM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

[realms]

$REALM = {

kdc = $KDC

}

[domain\_realm]

.$REALM = $REALM

$REALM = $REALM

EOF

# 2. Run kinit using keytab

kinit -k -t "$KEYTAB\_PATH" "$SERVICE\_PRINCIPAL"

# 3. Check ticket

klist

**✅ Example usage:**

**On Windows (PowerShell):**

powershell

CopyEdit

.\gen\_keytab.ps1 `

-ServiceAccount "DOMAIN\svc\_sql\_linux" `

-ServicePrincipal "MSSQLSvc/sqlserver.domain.com" `

-Realm "DOMAIN.COM" `

-LinuxHost "192.168.1.100" `

-LinuxUser "ubuntu" `

-Password "SuperSecret123!"

**On Linux:**

bash

CopyEdit

chmod +x setup\_kerberos.sh

./setup\_kerberos.sh DOMAIN.COM dc01.domain.com MSSQLSvc/sqlserver.domain.com@DOMAIN.COM /etc/security/keytabs/service