Progress®
Kemp® LoadMaster®

Feature Description Kerberos Constrained Delegation

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Document Purpose 4

Intended Audience 5

Chapter 2: Configuring KCD and the LoadMaster. 6

Lab Topology 7

Ensure All Relevant Stations Use the Same Domain Name System (DNS) Server 8

Check if the LoadMaster is Configured to Reverse Resolve IP Addresses 8

Ping Simple Host Names 9

Specify a Search Domain 10

Ensure Time/Date/Time Zone Settings Are Correct 11

Create the Trusted User 11

Create the Outbound Single Sign On (SSO) Domain 17

Set the L7 Wait after POST Value 18

Chapter 3: KCD Compatibility with Other LoadMaster Features 20

KCD Compatibility with NTLM 21

Chapter 4: Appendix – Kerberos (krb5) Error Messages 22

Chapter 5: References 41

1

Introduction

Introduction

As part of Progress Kemp's Edge Security Pack (ESP), the LoadMaster supports a number of authentication protocols, including Kerberos Constrained Delegation (KCD). When using KCD as the server authentication protocol, the LoadMaster provides seamless access to protected resources in a Kerberos realm, even when credentials provided are not directly valid for such an environment.

The KCD authentication protocol is used to confirm the identity of the users who are attempting to access resources on a network. KCD authentication uses tickets that are encrypted and decrypted by secret keys and do not contain user passwords. These tickets are requested and delivered in Kerberos messages. When the user's password is not provided, a trusted administrator user account is used to get tickets on behalf of services and users.

Related Links

- Document Purpose
- Intended Audience

Document Purpose

Document Purpose

This document provides instructions on how to configure Kerberos in the LoadMaster.

Intended Audience

Intended Audience

This document is intended to be read by anyone who is interested in finding out how to configure the LoadMaster to authenticate using KCD.

2

Configuring KCD and the LoadMaster

Configuring KCD and the LoadMaster

Refer to the sections below for instructions on how to configure KCD and the LoadMaster.

Note: Cross-domain delegation (where a resource resides in a different domain to the user) is not supported.

Related Links

- Lab Topology
- Ensure All Relevant Stations Use the Same Domain Name System (DNS) Server
- Check if the LoadMaster is Configured to Reverse Resolve IP Addresses
- Ping Simple Host Names
- Specify a Search Domain
- Ensure Time/Date/Time Zone Settings Are Correct
- Create the Trusted User
- Create the Outbound Single Sign On (SSO) Domain
- Set the L7 Wait after POST Value

Lab Topology

Lab Topology

Here are the details for the example topology used to create the instructions in this document:

Item	Value
Domain	KempLAB.intra
Domain Controller	ad01.kemplab.intra
IP	192.168.1.50

Item	IP Address	Fully Qualified Domain Name (FQDN)
Kemp-HA Shared IP	192.168.1.35	kempha.kemplab.intra
High Availability (HA) Unit 1	192.168.1.30	kempvlm01.kemplab.intra
HA Unit 2	192.168.1.50	kempvlm02.kemplab.intra

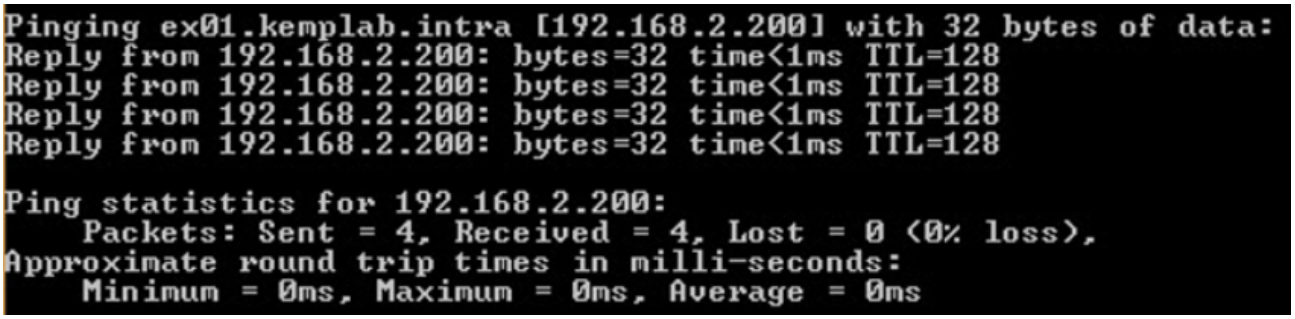
Item	IP Address	FQDN
Virtual Service	192.168.1.90	vx13.kemplab.intra

Real Server	IP Address	FQDN
Exchange 2013 CU13	192.168.2.200	ex01.kemplab.intra
Exchange 2013 CU13	192.168.2.201	ex02.kemplab.intra
Exchange 2016	192.168.2.202	ex03.kemplab.intra

Ensure All Relevant Stations Use the Same Domain Name System (DNS) Server

Ensure All Relevant Stations Use the Same Domain Name System (DNS) Server

Verify that the Virtual Service and the Real Servers have Pointer (PTR) records by running a ping command, for example **ping -a 192.168.2.200**.



Check if the LoadMaster is Configured to Reverse Resolve IP Addresses

Check if the LoadMaster is Configured to Reverse Resolve IP Addresses

From the SSOMGR in debug mode, you should see similar logs:

Aug 4 15:56:54 vwagwosevlb00 ssomgr: #18806# >>> kcd_get_user_ticket

Aug 4 15:56:54 vwagwosevlb00 ssomgr: #18806# >>>resolve_destination_address: Attempt to resolve destination [10.179.194.80][2]

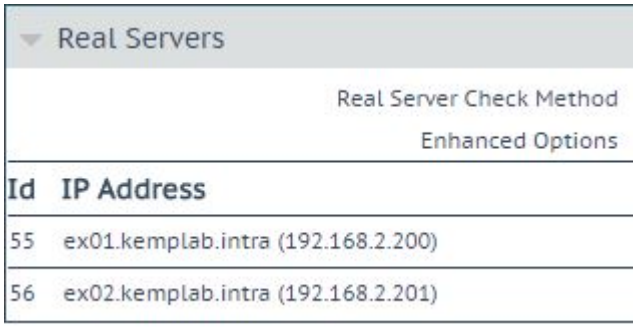
Aug 4 15:56:54 vwagwosevlb00 ssomgr: #18806# <<<resolve_destination_address: Resolved destination host name [wosevtspf3.wof.az.xyz]

This provides a quick indication that the LoadMaster is correctly configured to reverse resolve IP addresses.

Ping Simple Host Names

Ping Simple Host Names

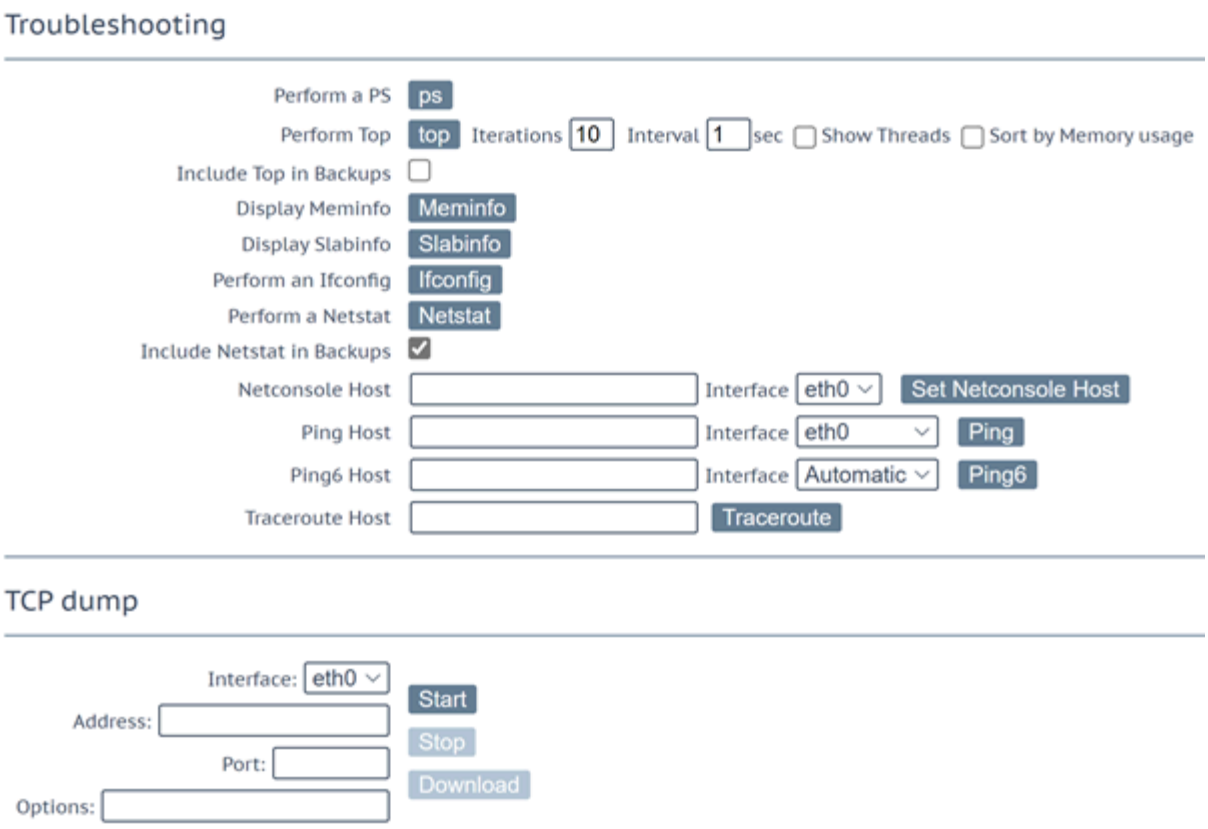
Ensure that it works with just the name, not the Fully Qualified Domain Name (FQDN).



When adding Real Servers to the **Delegation** tab of the trusted user (in a later step), Windows automatically adds both simple host names and FQDNs.

To test if the host name works, ping it by following the steps below:

1. In the main menu of the LoadMaster Web User Interface (WUI), expand **System Configuration > Troubleshooting**.



2. Type the host name in the **Ping Host** text box and click **Ping**.

If the result is **unknown host**, you must provide the domain realm to append to the hostname as a Search Domain. Refer to the Specify a Search Domain section for steps on how to do this.

Specify a Search Domain

Specify a Search Domain

If you got an **unknown host** error when pinging the host name in the Ping Simple Host Names section, you must provide the domain realm to append to the hostname as a Search Domain. To do this, follow the steps below:

1. In the main menu of the LoadMaster WUI, expand **System Configuration > Network Setup** and click **Host & DNS Configuration**.



2. Type the domain realm in the **Domain** field and click **Add**.



3. Run a ping again (follow the steps in the Ping Simple Host Names section). Now that the search domain is added, the ping should be successful.
4. Run a ping on each of the relevant Real Servers to ensure they correctly resolve.

Ensure Time/Date/Time Zone Settings Are Correct

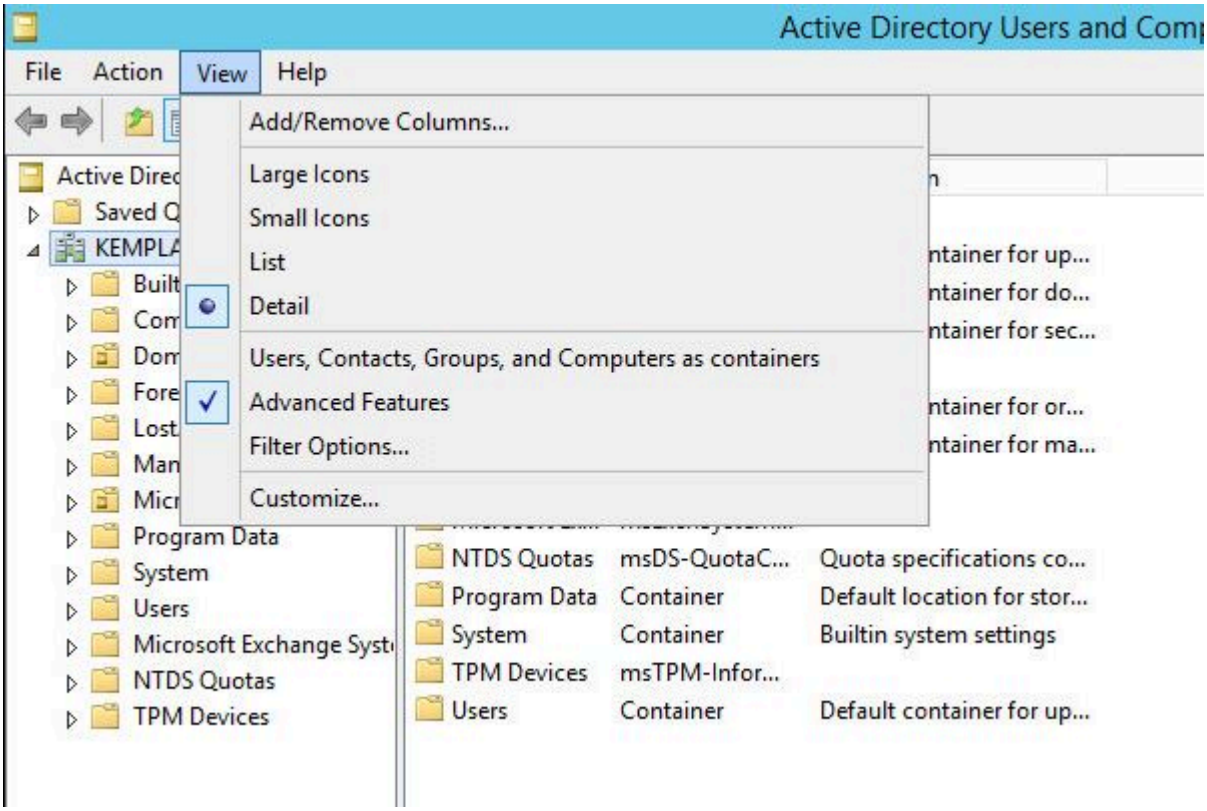
Ensure Time/Date/Time Zone Settings Are Correct

Ensure that all devices are on the same time, date and time zone settings. The LoadMaster settings are available in **System Configuration > System Administration > Date/Time**.

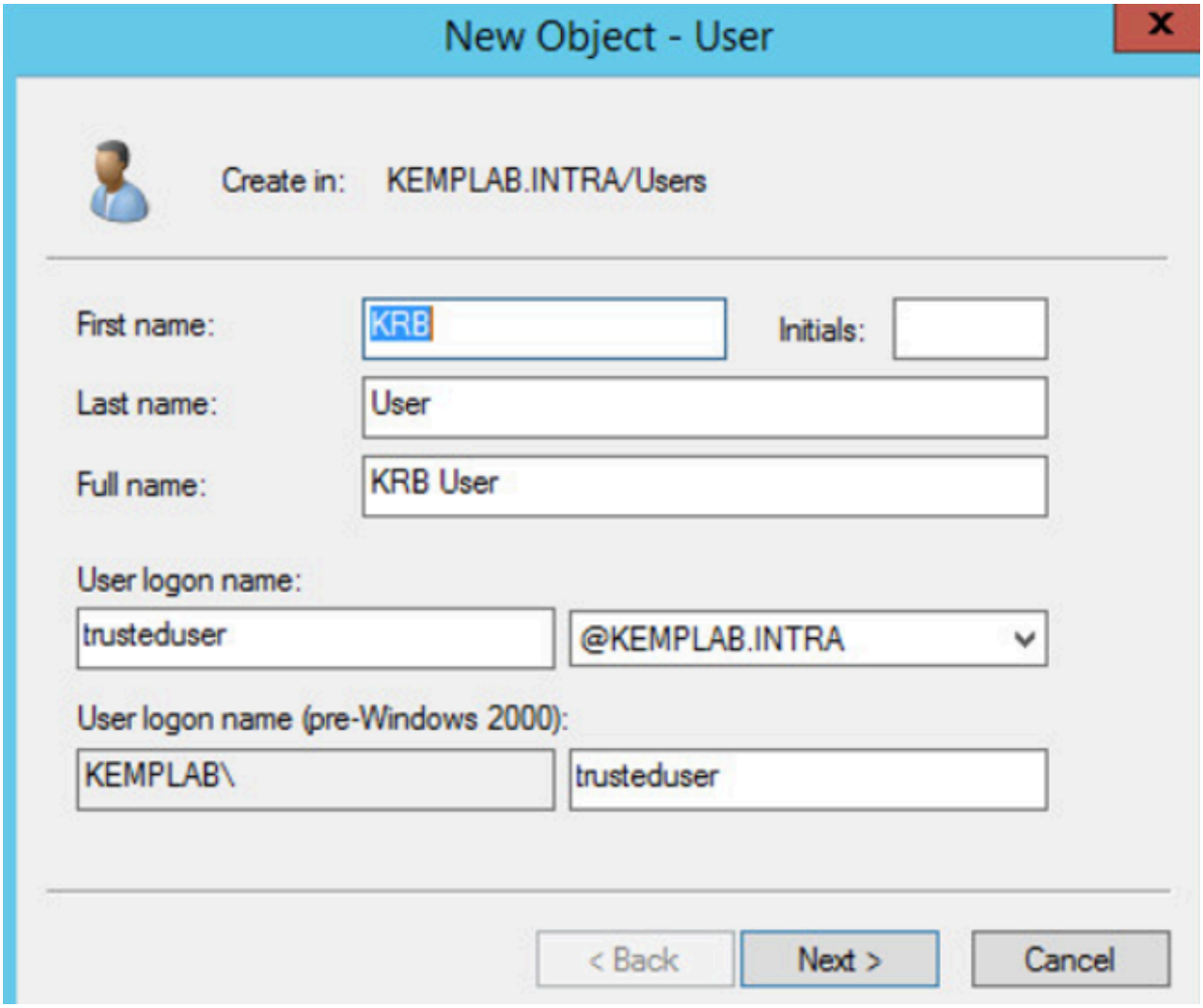
Create the Trusted User

Follow the steps below to create the trusted user in the Active Directory settings.

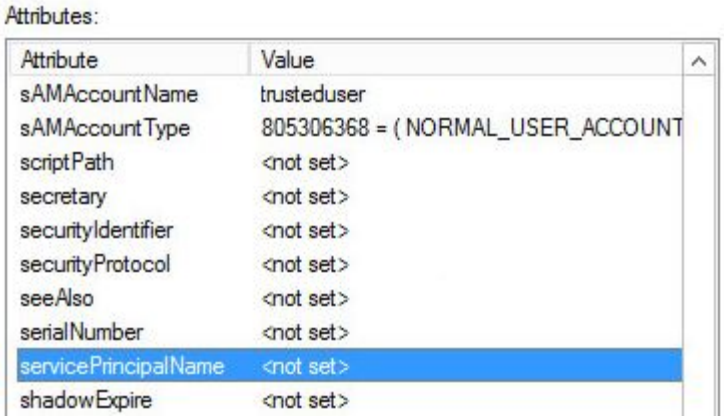
1. Log in to your Domain Controller.
2. Launch Active Directory Users and Computers and select **Advanced Features** from the **View** menu.



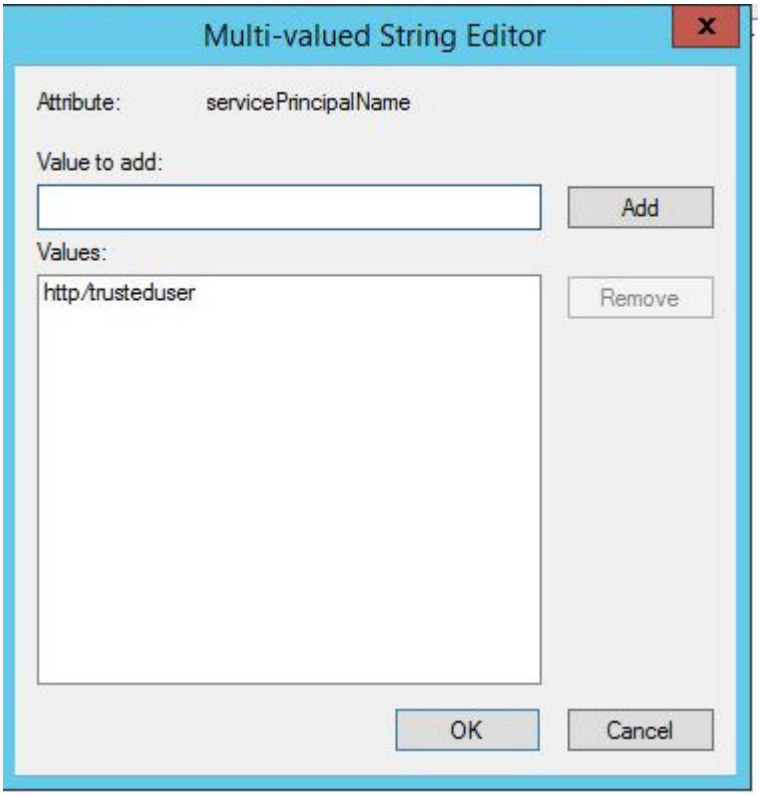
3. Click **View** and click **Advanced Features**.
4. Create a new user as shown below.



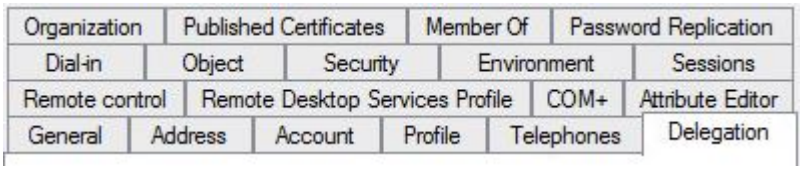
5. Set the password to never expire.
6. Select the **Attribute Editor** tab.
7. Navigate to **servicePrincipalName**.



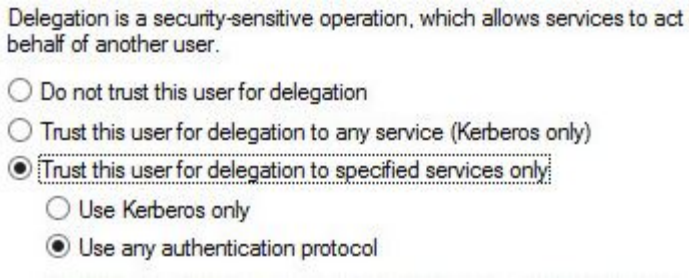
8. Select **servicePrincipalName** and click **Edit**.



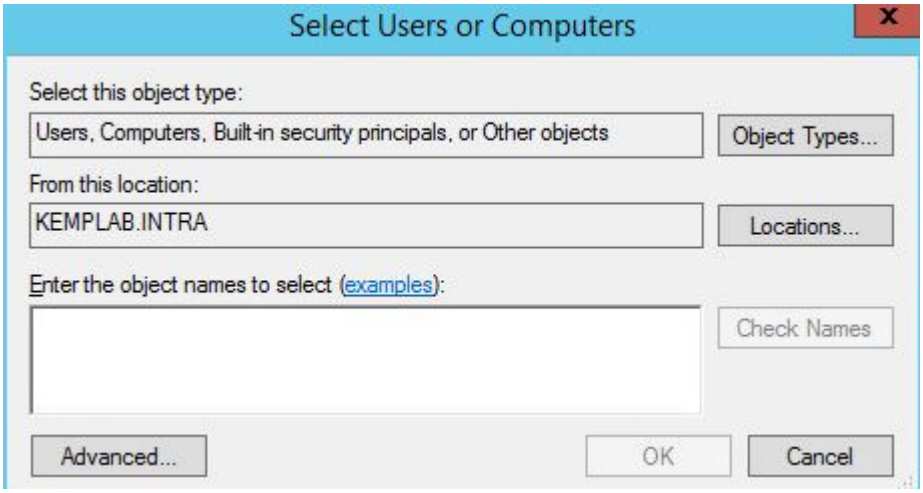
9. Type **http/trusteduser** in the **Value to add** field and click **Add**.
10. Click **Apply** and **OK**. The window must close before you open it again (to see the new **Delegation** tab).
11. Open the user properties window again and the **Delegation** tab becomes available.



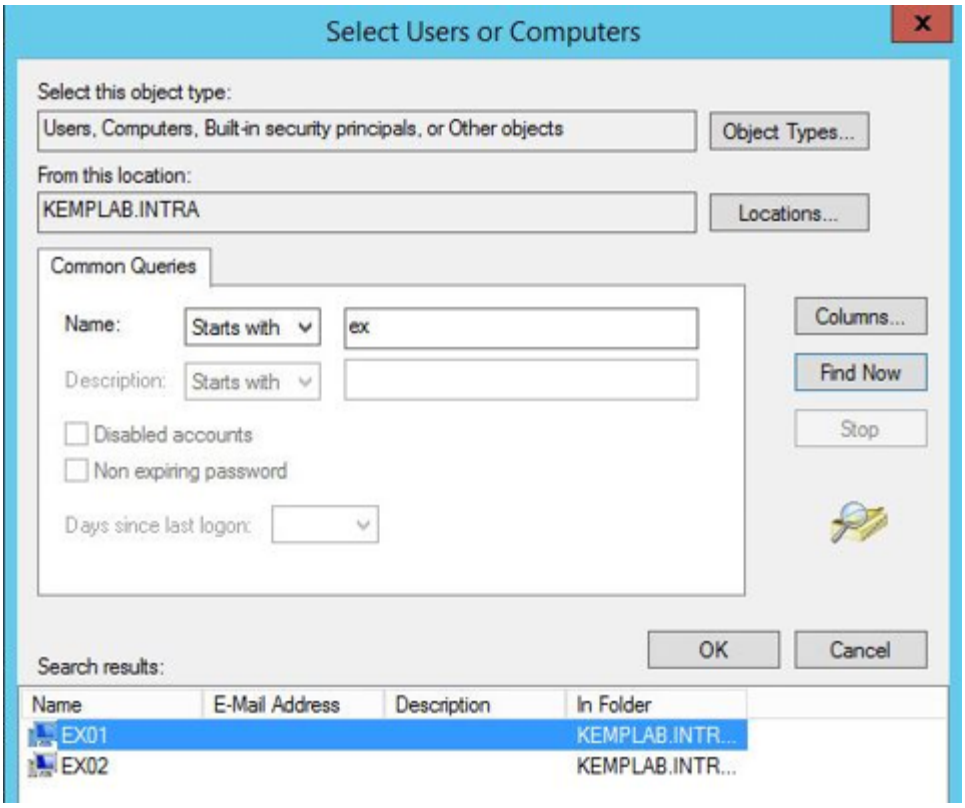
12. Select the **Delegation** tab.



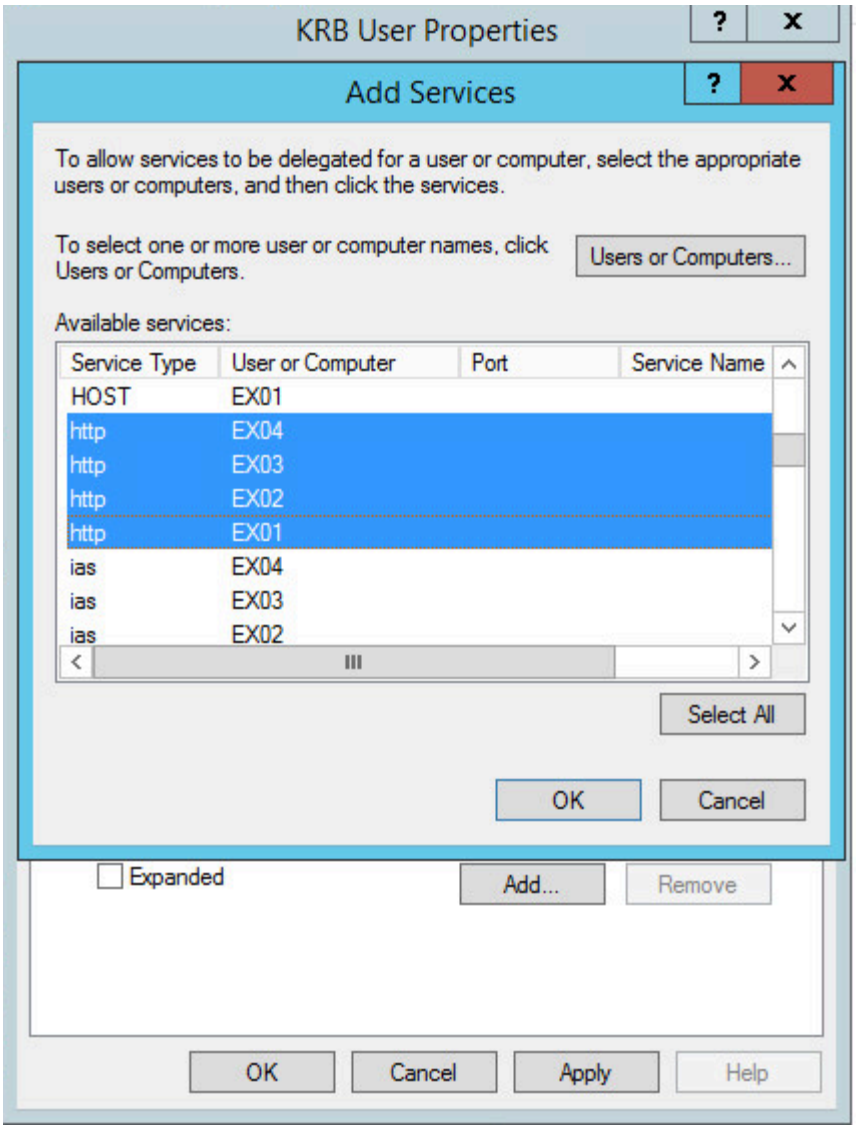
13. Select **Trust this user for delegation to specified services only**.
14. Select **Use any authentication protocol**.



15. Add the Real Servers and add **http** as the service. For SharePoint Apps: You might have to add the namespace published by SharePoint to enable KCD, instead of the actual server FQDNs.
16. Click **Advanced**.



17. Find the servers by name.
18. Select the **Expanded** check box.



19. You can see all servers with both the host name and the FQDN.

Note: If you have a SharePoint environment that uses distributed name spaces, you must register these name spaces instead of the actual servers hosting the content.

20. For SharePoint, the settings may need to be configured as outlined in the above screenshot.

Note: The trusted user account must be a member of the **Windows Authorization Access Group**. This is required to properly determine a user's group membership and therefore effective permissions over a resource. If a trusted user account is not a member of the **Windows Authorization Access Group**, the KCD authentication protocol will not confirm the identity of the trusted users who are attempting to access resources on a network.

Create the Outbound Single Sign On (SSO) Domain

Create the Outbound Single Sign On (SSO) Domain

To create the outbound SSO domain, follow the steps below in the LoadMaster WUI:

1. Expand **Virtual Services > Manage SSO**.

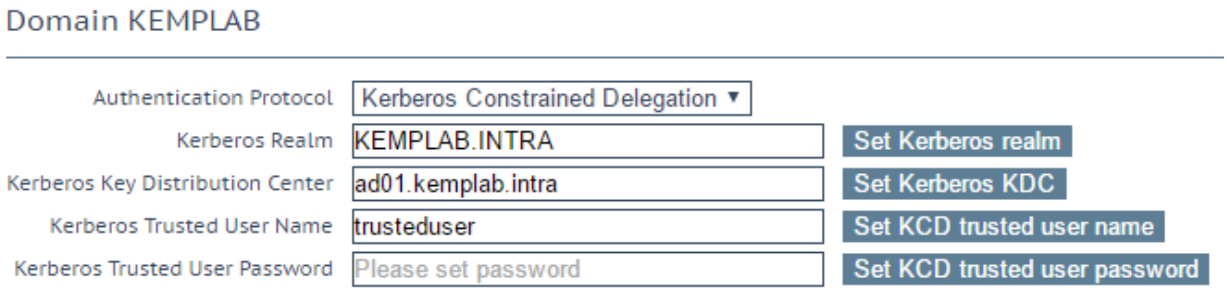


2. Enable or disable the **Use AES56 SHA1 KCD cipher** check box.

Note: When this check box is selected, the AES256 SHA1 KCD cipher is used (by default the RC4, DES, and DES3 ciphers are used).

---

3. Type a name in the **Add new Server Side Configuration** text box and click **Add**.



4. Type the **Kerberos Realm** and click **Set Kerberos realm**.
5. Type the **Kerberos Key Distribution Center** and click **Set Kerberos KDC**.

   As of LoadMaster firmware version 7.2.51, two Key Distribution Center (KDC) servers can be set per domain. The first one entered becomes active until it fails. KDC availability is checked and if the KDC fails to respond successfully three times or if it times out for five seconds, the active KDC is switched. The active Kerberos KDC is shown underneath when two addresses are entered in the Kerberos Key Distribution Center field.

Note: If you are entering more than one KDC, the username and password must be the same for both KDCs.

Note: Double and single quotes are not allowed in the Kerberos Key Distribution Center field.

---

6. Type the **Kerberos Trusted User Name** and click **Set KCD trusted user name**.

7. Type the **Kerberos Trusted User Password** and click **Set KCD trusted user password**.

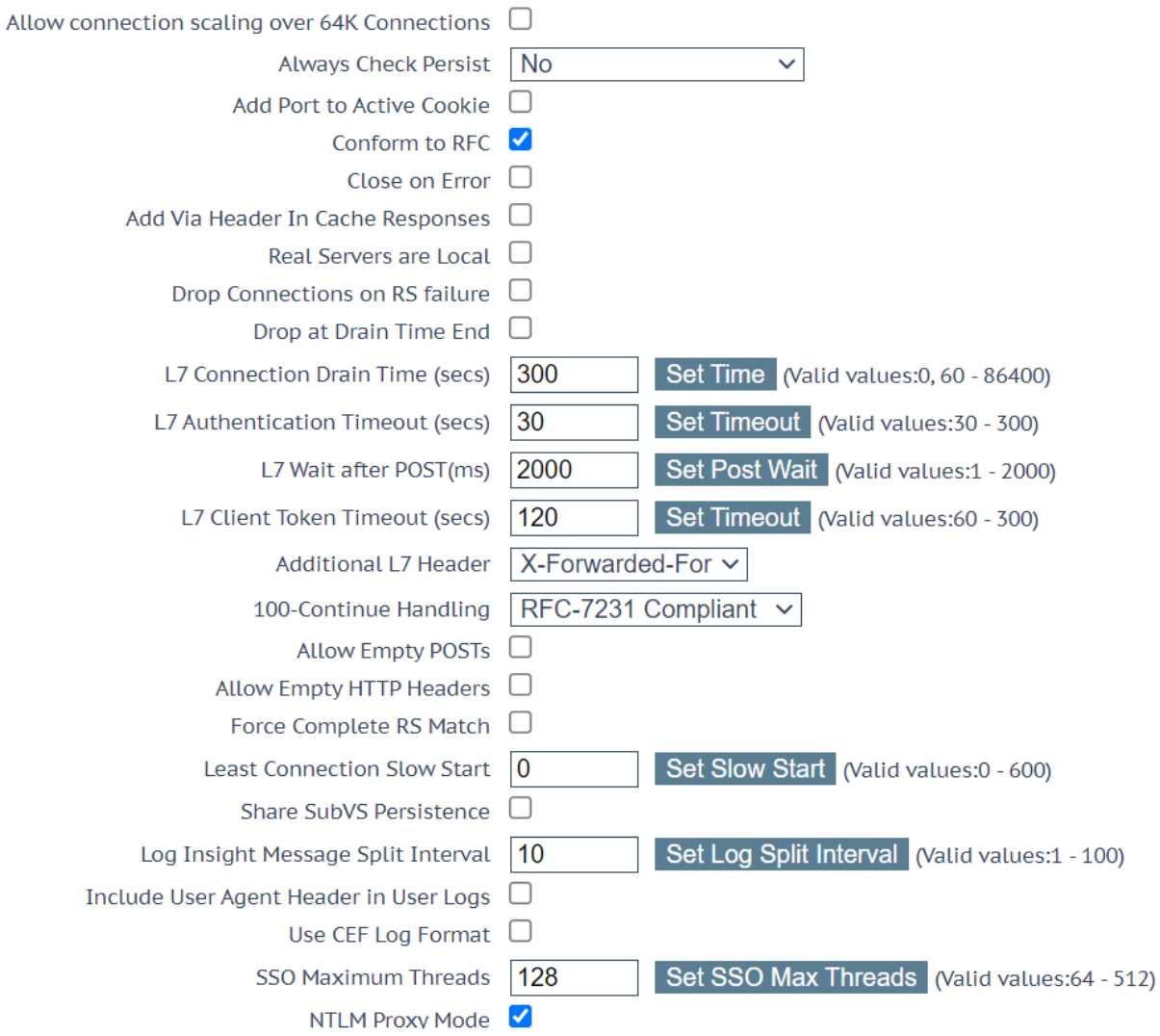
Set the L7 Wait after POST Value

Set the L7 Wait after POST Value

In LoadMaster firmware version 7.2.51, a new option was introduced that is applicable when performing Kerberos Constrained Delegation (KCD) back-end authentication. The field is called **L7 Wait after POST**. This option is configurable in the LoadMaster User Interface (UI). The **L7 Wait after POST** option allows you to change the length of time to wait for a 401 response from a POST before sending the remainder of the POST body. Valid values for the wait period range from 1 to 2000 milliseconds (ms). The default value is 2000. If KCD is not being used, this option has no effect.

To configure the **L7 Wait after POST** value, follow the steps below:

1. In the main menu, go to System **Configuration > Miscellaneous Options > L7 Configuration**.



2. Enter the new value in the **L7 Wait after POST** text box and click **Set Post Wait**.

3

KCD Compatibility with Other LoadMaster Features

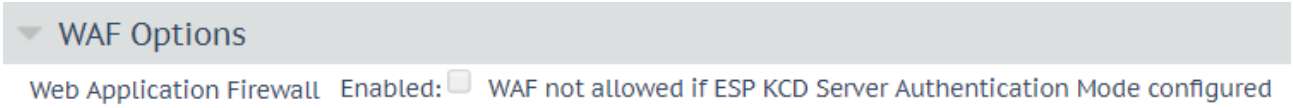
KCD Compatibility with Other LoadMaster Features

There are some compatibility issues with KCD and other LoadMaster features. For further information, refer to the sections below.

KCD Compatibility with the Web Application Firewall

As of the 7.2.40 LoadMaster firmware version, you cannot enable both WAF and KCD at the same Virtual Service level. For example:

- If WAF is enabled in the parent Virtual Service, you cannot enable KCD as the **Server Authentication Mode** in the parent Virtual Service



- If KCD is enabled in the parent Virtual Service, you cannot enable WAF

However, you can enable ESP/KCD in the SubVS and then enable WAF in the parent Virtual Service.

If you had WAF and KCD enabled at the same level before upgrading to 7.2.40 and you upgrade the firmware to 7.2.40 or above, the configuration will not be changed. File attachments in SharePoint will not

work. To resolve this, enable WAF on the parent Virtual Service and ESP/KCD on the SubVS.

The following combination is not supported: WAF with ESP Client Certificate authentication and KCD.

KCD Compatibility with Response Body Modification Rules

Response body rules are not compatible with KCD. If KCD is enabled on a Virtual Service, it is not possible to assign a body rule to it.

Related Links

- KCD Compatibility with NTLM

KCD Compatibility with NTLM

KCD Compatibility with NTLM

When using KCD with NTLM, the recommended best practice is to enable **NTLM Proxy Mode** in the **System Configuration > Miscellaneous Options > L7 Configuration** settings. **NTLM Proxy Mode** increases the security of Client Authentication by proxying NTLM Authentication with the Real Server. Authentication is verified by validating that a successful NTLM handshake has taken place with the Real Server before performing the proceeding steps (such as performing the required Server Side Kerberos Authentication where the Server Side configuration is set to KCD). This requires that the Real Server support NTLM Authentication. The legacy “NTLM” user authentication mode verified user credentials through a configured LDAP endpoint. With **NTLM Proxy Mode**, the Client Side SSO configuration only requires an LDAP endpoint in the case where Permitted Groups or Steering Groups are in use.

4

Appendix – Kerberos (krb5) Error Messages

Appendix – Kerberos (krb5) Error Messages

Refer to the table below for a list of Kerberos error messages, their symbolic names and descriptions.

Error Number	Symbolic Name	Descriptive Text
-1765328383	KRB5KDC_ERR_NAME_EXP	Client's entry in database has expired
-1765328382	KRB5KDC_ERR_SERVICE_EXP	Server's entry in database has expired
-1765328381	KRB5KDC_ERR_BAD_PVNO	Requested protocol version not supported
-1765328380	KRB5KDC_ERR_C_OLD_MAST_KVNO	Client's key is encrypted in an old master key

Error Number	Symbolic Name	Descriptive Text
-1765328379	KRB5KDC_ERR_S_OLD_MAST_KVNO	Server's key is encrypted in an old master key
-1765328378	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN	Client not found in Kerberos database
-1765328377	KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN	Server not found in Kerberos database
-1765328376	KRB5KDC_ERR_PRINCIPAL_NOT_UNIQUE	Principal has multiple entries in Kerberos database
-1765328375	KRB5KDC_ERR_NULL_KEY	Client or server has a null key
-1765328374	KRB5KDC_ERR_CANNOT_POSTDATE	Ticket is ineligible for postdating
-1765328373	KRB5KDC_ERR_NEVER_VALID	Requested effective lifetime is negative or too short
-1765328372	KRB5KDC_ERR_POLICY	KDC policy rejects request
-1765328371	KRB5KDC_ERR_BADOPTION	KDC cannot fulfil requested option
-1765328370	KRB5KDC_ERR_ETYPE_NOSUPP	KDC has no support for encryption type
-1765328369	KRB5KDC_ERR_SUMTYPE_NOSUPP	KDC has no support for checksum type
-1765328368	KRB5KDC_ERR_PADATA_TYPE_N	KDC has no support for padata type

Error Number	Symbolic Name	Descriptive Text
	OSUPP	
-1765328367	KRB5KDC_ERR_TRTYPE_NOSUPP	KDC has no support for transited type
-1765328366	KRB5KDC_ERR_CLIENT_REVOKED	Clients credentials have been revoked
-1765328365	KRB5KDC_ERR_SERVICE_REVOKED	Credentials for server have been revoked
-1765328364	KRB5KDC_ERR_TGT_REVOKED	TGT has been revoked
-1765328363	KRB5KDC_ERR_CLIENT_NOTYET	Client not yet valid - try again later
-1765328362	KRB5KDC_ERR_SERVICE_NOTYET	Server not yet valid - try again later
-1765328361	KRB5KDC_ERR_KEY_EXP	Password has expired
-1765328360	KRB5KDC_ERR_PREAUTH_FAILED	Pre-authentication failed
-1765328359	KRB5KDC_ERR_PREAUTH_REQUIRED	Additional pre-authentication required
-1765328358	KRB5KDC_ERR_SERVER_NOMATCH	Requested server and ticket do not match
-1765328357	KRB5PLACEHOLD_27	KRB5 error code 27
-1765328356	KRB5PLACEHOLD_28	KRB5 error code 28

Error Number	Symbolic Name	Descriptive Text
-1765328355	KRB5PLACEHOLD_29	KRB5 error code 29
-1765328354	KRB5PLACEHOLD_30	KRB5 error code 30
-1765328353	KRB5KRB_AP_ERR_BAD_INTEGRITY	Decrypt integrity check failed
-1765328352	KRB5KRB_AP_ERR_TKT_EXPIRED	Ticket expired
-1765328351	KRB5KRB_AP_ERR_TKT_NYV	Ticket not yet valid
-1765328350	KRB5KRB_AP_ERR_REPEAT	Request is a replay
-1765328349	KRB5KRB_AP_ERR_NOT_US	The ticket is not for us
-1765328348	KRB5KRB_AP_ERR_BADMATCH	Ticket/authenticator do not match
-1765328347	KRB5KRB_AP_ERR_SKEW	Clock skew too great
-1765328346	KRB5KRB_AP_ERR_BADADDR	Incorrect net address
-1765328345	KRB5KRB_AP_ERR_BADVERSION	Protocol version mismatch
-1765328344	KRB5KRB_AP_ERR_MSG_TYPE	Invalid message type
-1765328343	KRB5KRB_AP_ERR_MODIFIED	Message stream modified
-1765328342	KRB5KRB_AP_ERR_BADORDER	Message out of order

Error Number	Symbolic Name	Descriptive Text
-1765328341	KRB5KRB_AP_ERR_ILL_CR_TKT	Illegal cross-realm ticket
-1765328340	KRB5KRB_AP_ERR_BADKEYVER	Key version is not available
-1765328339	KRB5KRB_AP_ERR_NOKEY	Service key not available
-1765328338	KRB5KRB_AP_ERR_MUT_FAIL	Mutual authentication failed
-1765328337	KRB5KRB_AP_ERR_BADDIRECTIO N	Incorrect message direction
-1765328336	KRB5KRB_AP_ERR_METHOD	Alternative authentication method required
-1765328335	KRB5KRB_AP_ERR_BADSEQ	Incorrect sequence number in message
-1765328334	KRB5KRB_AP_ERR_INAPP_CKSU M	Inappropriate type of checksum in message
-1765328333	KRB5PLACEHOLD_51	KRB5 error code 51
-1765328332	KRB5PLACEHOLD_52	KRB5 error code 52
-1765328331	KRB5PLACEHOLD_53	KRB5 error code 53
-1765328330	KRB5PLACEHOLD_54	KRB5 error code 54
-1765328329	KRB5PLACEHOLD_55	KRB5 error code 55

Error Number	Symbolic Name	Descriptive Text
-1765328328	KRB5PLACEHOLD_56	KRB5 error code 56
-1765328327	KRB5PLACEHOLD_57	KRB5 error code 57
-1765328326	KRB5PLACEHOLD_58	KRB5 error code 58
-1765328325	KRB5PLACEHOLD_59	KRB5 error code 59
-1765328324	KRB5KRB_ERR_GENERIC	Generic error (see e-text)
-1765328323	KRB5KRB_ERR_FIELD_TOOLONG	Field is too long for this implementation
-1765328322	KRB5PLACEHOLD_62	KRB5 error code 62
-1765328321	KRB5PLACEHOLD_63	KRB5 error code 63
-1765328320	KRB5PLACEHOLD_64	KRB5 error code 64
-1765328319	KRB5PLACEHOLD_65	KRB5 error code 65
-1765328318	KRB5PLACEHOLD_66	KRB5 error code 66
-1765328317	KRB5PLACEHOLD_67	KRB5 error code 67
-1765328316	KRB5PLACEHOLD_68	KRB5 error code 68
-1765328315	KRB5PLACEHOLD_69	KRB5 error code 69

Error Number	Symbolic Name	Descriptive Text
-1765328314	KRB5PLACEHOLD_70	KRB5 error code 70
-1765328313	KRB5PLACEHOLD_71	KRB5 error code 71
-1765328312	KRB5PLACEHOLD_72	KRB5 error code 72
-1765328311	KRB5PLACEHOLD_73	KRB5 error code 73
-1765328310	KRB5PLACEHOLD_74	KRB5 error code 74
-1765328309	KRB5PLACEHOLD_75	KRB5 error code 75
-1765328308	KRB5PLACEHOLD_76	KRB5 error code 76
-1765328307	KRB5PLACEHOLD_77	KRB5 error code 77
-1765328306	KRB5PLACEHOLD_78	KRB5 error code 78
-1765328305	KRB5PLACEHOLD_79	KRB5 error code 79
-1765328304	KRB5PLACEHOLD_80	KRB5 error code 80
-1765328303	KRB5PLACEHOLD_81	KRB5 error code 81
-1765328302	KRB5PLACEHOLD_82	KRB5 error code 82
-1765328301	KRB5PLACEHOLD_83	KRB5 error code 83

Error Number	Symbolic Name	Descriptive Text
-1765328300	KRB5PLACEHOLD_84	KRB5 error code 84
-1765328299	KRB5PLACEHOLD_85	KRB5 error code 85
-1765328298	KRB5PLACEHOLD_86	KRB5 error code 86
-1765328297	KRB5PLACEHOLD_87	KRB5 error code 87
-1765328296	KRB5PLACEHOLD_88	KRB5 error code 88
-1765328295	KRB5PLACEHOLD_89	KRB5 error code 89
-1765328294	KRB5PLACEHOLD_90	KRB5 error code 90
-1765328293	KRB5PLACEHOLD_91	KRB5 error code 91
-1765328292	KRB5PLACEHOLD_92	KRB5 error code 92
-1765328291	KRB5PLACEHOLD_93	KRB5 error code 93
-1765328290	KRB5PLACEHOLD_94	KRB5 error code 94
-1765328289	KRB5PLACEHOLD_95	KRB5 error code 95
-1765328288	KRB5PLACEHOLD_96	KRB5 error code 96
-1765328287	KRB5PLACEHOLD_97	KRB5 error code 97

Error Number	Symbolic Name	Descriptive Text
-1765328286	KRB5PLACEHOLD_98	KRB5 error code 98
-1765328285	KRB5PLACEHOLD_99	KRB5 error code 99
-1765328284	KRB5PLACEHOLD_100	KRB5 error code 100
-1765328283	KRB5PLACEHOLD_101	KRB5 error code 101
-1765328282	KRB5PLACEHOLD_102	KRB5 error code 102
-1765328281	KRB5PLACEHOLD_103	KRB5 error code 103
-1765328280	KRB5PLACEHOLD_104	KRB5 error code 104
-1765328279	KRB5PLACEHOLD_105	KRB5 error code 105
-1765328278	KRB5PLACEHOLD_106	KRB5 error code 106
-1765328277	KRB5PLACEHOLD_107	KRB5 error code 107
-1765328276	KRB5PLACEHOLD_108	KRB5 error code 108
-1765328275	KRB5PLACEHOLD_109	KRB5 error code 109
-1765328274	KRB5PLACEHOLD_110	KRB5 error code 110
-1765328273	KRB5PLACEHOLD_111	KRB5 error code 111

Error Number	Symbolic Name	Descriptive Text
-1765328272	KRB5PLACEHOLD_112	KRB5 error code 112
-1765328271	KRB5PLACEHOLD_113	KRB5 error code 113
-1765328270	KRB5PLACEHOLD_114	KRB5 error code 114
-1765328269	KRB5PLACEHOLD_115	KRB5 error code 115
-1765328268	KRB5PLACEHOLD_116	KRB5 error code 116
-1765328267	KRB5PLACEHOLD_117	KRB5 error code 117
-1765328266	KRB5PLACEHOLD_118	KRB5 error code 118
-1765328265	KRB5PLACEHOLD_119	KRB5 error code 119
-1765328264	KRB5PLACEHOLD_120	KRB5 error code 120
-1765328263	KRB5PLACEHOLD_121	KRB5 error code 121
-1765328262	KRB5PLACEHOLD_122	KRB5 error code 122
-1765328261	KRB5PLACEHOLD_123	KRB5 error code 123
-1765328260	KRB5PLACEHOLD_124	KRB5 error code 124
-1765328259	KRB5PLACEHOLD_125	KRB5 error code 125

Error Number	Symbolic Name	Descriptive Text
-1765328258	KRB5PLACEHOLD_126	KRB5 error code 126
-1765328257	KRB5PLACEHOLD_127	KRB5 error code 127
-1765328256	KRB5_ERR_RCSID	$Id: krb5_err.et,v 1.1 1998/05/06 20:23:54 mione Exp $
-1765328255	KRB5_LIBOS_BADLOCKFLAG	Invalid flag for file lock mode
-1765328254	KRB5_LIBOS_CANTREADPWD	Cannot read password
-1765328253	KRB5_LIBOS_BADPWDMATCH	Password mismatch
-1765328252	KRB5_LIBOS_PWDINTR	Password read interrupted
-1765328251	KRB5_PARSE_ILLCHAR	Illegal character in component name
-1765328250	KRB5_PARSE_MALFORMED	Malformed representation of principal
-1765328249	KRB5_CONFIG_CANTOPEN	Cannot open/find Kerberos configuration file
-1765328248	KRB5_CONFIG_BADFORMAT	Improper format of Kerberos configuration file
-1765328247	KRB5_CONFIG_NOTENUFSPACE	Insufficient space to return complete information
-1765328246	KRB5_BADMSGTYPE	Invalid message type specified for encoding

Error Number	Symbolic Name	Descriptive Text
-1765328245	KRB5_CC_BADNAME	Credential cache name malformed
-1765328244	KRB5_CC_UNKNOWN_TYPE	Unknown credential cache type
-1765328243	KRB5_CC_NOTFOUND	Matching credential not found
-1765328242	KRB5_CC_END	End of credential cache reached
-1765328241	KRB5_NO_TKT_SUPPLIED	Request did not supply a ticket
-1765328240	KRB5KRB_AP_WRONG_PRINC	Wrong principal in request
-1765328239	KRB5KRB_AP_ERR_TKT_INVALID	Ticket has invalid flag set
-1765328238	KRB5_PRINC_NOMATCH	Requested principal and ticket do not match
-1765328237	KRB5_KDCREP_MODIFIED	KDC reply did not match expectations
-1765328236	KRB5_KDCREP_SKEW	Clock skew too great in KDC reply
-1765328235	KRB5_IN_TKT_REALM_MISMATCH	Client/server realm mismatch in initial ticket request
-1765328234	KRB5_PROG_ETYPE_NOSUPP	Program lacks support for encryption type
-1765328233	KRB5_PROG_KEYTYPE_NOSUPP	Program lacks support for key type

Error Number	Symbolic Name	Descriptive Text
-1765328232	KRB5_WRONG_ETYPE	Requested encryption type not used in message
-1765328231	KRB5_PROG_SUMTYPE_NOSUPP	Program lacks support for checksum type
-1765328230	KRB5_REALM_UNKNOWN	Cannot find KDC for requested realm
-1765328229	KRB5_SERVICE_UNKNOWN	Kerberos service unknown
-1765328228	KRB5_KDC_UNREACH	Cannot contact any KDC for requested realm
-1765328227	KRB5_NO_LOCALNAME	No local name found for principal name
-1765328226	KRB5_MUTUAL_FAILED	Mutual authentication failed
-1765328225	KRB5_RC_TYPE_EXISTS	Replay cache type is already registered
-1765328224	KRB5_RC_MALLOC	No more memory to allocate (in replay cache code)
-1765328223	KRB5_RC_TYPE_NOTFOUND	Replay cache type is unknown
-1765328222	KRB5_RC_UNKNOWN	Generic unknown RC error
-1765328221	KRB5_RC_REPLAY	Message is a replay

Error Number	Symbolic Name	Descriptive Text
-1765328220	KRB5_RC_IO	Replay I/O operation failed XXX
-1765328219	KRB5_RC_NOIO	Replay cache type does not support non-volatile storage
-1765328218	KRB5_RC_PARSE	Replay cache name parse/format error
-1765328217	KRB5_RC_IO_EOF	End-of-file on replay cache I/O
-1765328216	KRB5_RC_IO_MALLOC	No more memory to allocate (in replay cache I/O code)
-1765328215	KRB5_RC_IO_PERM	Permission denied in replay cache code
-1765328214	KRB5_RC_IO_IO	I/O error in replay cache i/o code
-1765328213	KRB5_RC_IO_UNKNOWN	Generic unknown RC/IO error
-1765328212	KRB5_RC_IO_SPACE	Insufficient system space to store replay information
-1765328211	KRB5_TRANS_CANTOPEN	Cannot open/find realm translation file
-1765328210	KRB5_TRANS_BADFORMAT	Improper format of realm translation file
-1765328209	KRB5_LNAME_CANTOPEN	Cannot open/find lname translation database

Error Number	Symbolic Name	Descriptive Text
-1765328208	KRB5_LNAME_NOTRANS	No translation available for requested principal
-1765328207	KRB5_LNAME_BADFORMAT	Improper format of translation database entry
-1765328206	KRB5_CRYPTO_INTERNAL	Cryptosystem internal error
-1765328205	KRB5_KT_BADNAME	Key table name malformed
-1765328204	KRB5_KT_UNKNOWN_TYPE	Unknown Key table type
-1765328203	KRB5_KT_NOTFOUND	Key table entry not found
-1765328202	KRB5_KT_END	End of key table reached
-1765328201	KRB5_KT_NOWRITE	Cannot write to specified key table
-1765328200	KRB5_KT_IOERR	Error writing to key table
-1765328199	KRB5_NO_TKT_IN_RLM	Cannot find ticket for requested realm
-1765328198	KRB5DES_BAD_KEYPAR	DES key has bad parity
-1765328197	KRB5DES_WEAK_KEY	DES key is a weak key
-1765328196	KRB5_BAD_ENCTYPE	Bad encryption type

Error Number	Symbolic Name	Descriptive Text
-1765328195	KRB5_BAD_KEYSIZE	Key size is incompatible with encryption type
-1765328194	KRB5_BAD_MSIZE	Message size is incompatible with encryption type
-1765328193	KRB5_CC_TYPE_EXISTS	Credentials cache type is already registered.
-1765328192	KRB5_KT_TYPE_EXISTS	Key table type is already registered.
-1765328191	KRB5_CC_IO	Credentials cache I/O operation failed XXX
-1765328190	KRB5_FCC_PERM	Credentials cache file permissions incorrect
-1765328189	KRB5_FCC_NOFILE	No credentials cache file found
-1765328188	KRB5_FCC_INTERNAL	Internal file credentials cache error
-1765328187	KRB5_CC_WRITE	Error writing to credentials cache file
-1765328186	KRB5_CC_NOMEM	No more memory to allocate (in credentials cache code)
-1765328185	KRB5_CC_FORMAT	Bad format in credentials cache
-1765328184	KRB5_INVALID_FLAGS	Invalid KDC option combination (library internal error)

Error Number	Symbolic Name	Descriptive Text
-1765328183	KRB5_NO_2ND_TKT	Request missing second ticket
-1765328182	KRB5_NOCREDS_SUPPLIED	No credentials supplied to library routine
-1765328181	KRB5_SENDAUTH_BADAUTHVERS	Bad sendauth version was sent
-1765328180	KRB5_SENDAUTH_BADAPPLVERS	Bad application version was sent (using sendauth)
-1765328179	KRB5_SENDAUTH_BADRESPONSE	Bad response (during sendauth exchange)
-1765328178	KRB5_SENDAUTH_REJECTED	Server rejected authentication (during sendauth exchange)
-1765328177	KRB5_PREAUTH_BAD_TYPE	Unsupported preauthentication type
-1765328176	KRB5_PREAUTH_NO_KEY	Required pre-authentication key not supplied
-1765328175	KRB5_PREAUTH_FAILED	Generic pre-authentication failure
-1765328174	KRB5_RCACHE_BADVNO	Unsupported replay cache format version number
-1765328173	KRB5_CCACHE_BADVNO	Unsupported credentials cache format version number
-1765328172	KRB5_KEYTAB_BADVNO	Unsupported key table format version number

Error Number	Symbolic Name	Descriptive Text
-1765328171	KRB5_PROG_ATYPE_NOSUPP	Program lacks support for address type
-1765328170	KRB5_RC_REQUIRED	Message replay detection requires rcache parameter
-1765328169	KRB5_ERR_BAD_HOSTNAME	Hostname cannot be canonicalized
-1765328168	KRB5_ERR_HOST_REALM_UNKNOWN	Cannot determine realm for host
-1765328167	KRB5_SNAME_UNSUPP_NAMETYPE	Conversion to service principal undefined for name type
-1765328166	KRB5KRB_AP_ERR_V4_REPLY	Initial Ticket response appears to be Version 4 error
-1765328165	KRB5_REALM_CANT_RESOLVE	Cannot resolve KDC for requested realm
-1765328164	KRB5_TKT_NOT_FORWARDABLE	Requesting ticket cannot get forwardable tickets
-1765328163	KRB5_FWD_BAD_PRINCIPAL	Bad principal name while trying to forward credentials
-1765328162	KRB5_GET_IN_TKT_LOOP	Looping detected inside krb5_get_in_tkt
-1765328161	KRB5_CONFIG_NODEFREALM	Configuration file does not specify default realm

Error Number	Symbolic Name	Descriptive Text
-1765328160	KRB5_SAM_UNSUPPORTED	Bad SAM flags in obtain_sam_padata
-1765328159	KRB5_KT_NAME_TOOLONG	Keytab name too long
-1765328158	KRB5_KT_KVNONOTFOUND	Key version number for principal in key table is incorrect

5

References

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

ESP, Feature Description