Kerberos Constrained Delegation
Feature Description

VERSION: 9.0
UPDATED: JULY 2016
Copyright Notices

Copyright © 2002-2016 KEMP Technologies, Inc.. All rights reserved.. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

Limitations: This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933.
# Table of Contents

1  Introduction ........................................................................................................... 6  
   1.1  Document Purpose ......................................................................................... 6  
   1.2  Intended Audience ....................................................................................... 6  
   1.3  Prerequisites ................................................................................................. 6  
2  Using KCD with Form-Based Authentication ...................................................... 7  
   2.1  Create the SSO Domains ............................................................................. 7  
      2.1.1  Configure the Server SSO Domain ......................................................... 7  
      2.1.2  Configure the Client SSO Domain ........................................................ 8  
   2.2  Configure the Virtual Service ....................................................................... 9  
3  Using KCD with Client Certificate Authentication ............................................. 13  
   3.1  Prerequisites ............................................................................................... 13  
   3.2  Install the Root Certificate on the LoadMaster ........................................... 13  
   3.3  Generate and Import a Client Certificate ..................................................... 13  
   3.4  Configure the Client Side SSO Domain in the LoadMaster ...................... 14  
      3.4.1  Check Certificate to User Mapping ...................................................... 15  
   3.5  Configure the Server Side SSO Domain in the LoadMaster ....................... 18  
   3.6  Configure the Virtual Service .................................................................... 18  
4  KCD WUI Options ............................................................................................... 20  
   4.1  Manage SSO Screen .................................................................................... 20  
   4.2  Modify Virtual Service Screen .................................................................... 21  
5  Appendix A: Configure the Active Directory Settings ..................................... 24  
   5.1  Add a Certificate to the Active Directory for TLS/LDAPS .......................... 24  
   5.2  Create DNS Entries .................................................................................... 25  
   5.3  Create a LoadMaster Trusted User ............................................................. 26  
   5.4  Associate an SPN with the User Entry ......................................................... 30  
   5.5  Configure Delegation for the User Entry ..................................................... 31  
6  Appendix B: Using KCD with Microsoft Exchange ........................................... 32  
References .............................................................................................................. 33  
Document History .................................................................................................... 34
1 Introduction

As part of 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 that 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.

1.1 Document Purpose

This document provides step-by-step instructions on how to configure endpoint authentication and Single Sign On (SSO) using Kerberos in the LoadMaster. This document only provides instructions relating to the LoadMaster. For further information on configuring KCD for your application/service, please refer to the KCD documentation.

1.2 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.

1.3 Prerequisites

Before following the steps below to configure the LoadMaster, there are some prerequisites that need to be in place:

- The Active Directory settings must be configured correctly. If they are not configured correctly, constrained delegation will not work. For more information on what needs to be configured, please refer to Section 5.
- Relevant DNS entries must be added. For more information, refer to Section 5.2.
- The LoadMaster needs to be connected to a Network Time Protocol (NTP) host to avoid problems with synchronization. The NTP service used should be the same used by clients and servers in the Active Directory infrastructure. This can be set in the LoadMaster Web User Interface (WUI) by going to System Configuration > System Administration > Date/Time and setting the NTP host(s). An external NTP host server address can be used if the LoadMaster can access it. However, if the LoadMaster is internal only – you will need to set up your own NTP server. Also, the time zone needs to be set manually in the Date/Time screen even when an NTP server is used.
2 Using KCD with Form-Based Authentication

KCD can be used with either form-based authentication or client certificate authentication. If you want to use client certificate authentication, KEMP recommends setting up form-based authentication first to ensure that the KCD functionality is working.

To use KCD with client certificate authentication, refer to Section 3.

2.1 Create the SSO Domains

In order for KCD to work with the LoadMaster, both a client and server SSO domain need to be created. In principal, both of these SSO domains in the LoadMaster can point towards the same server, if needed. The client domain should be the Active Directory domain.

2.1.1 Configure the Server SSO Domain

To configure the server side SSO domain, follow the steps below in the LoadMaster Web User Interface (WUI):

1. In the main menu, select Virtual Services > Manage SSO.

![Add SSO domain](image1)

Figure 2-1: Add SSO domain

2. In the Server Side Single Sign On Configurations section, enter the name of the Single Sign On (SSO) domain in the Name text box and click Add.

![SSO Domain Settings](image2)

Figure 2-2: SSO Domain Settings

4. Enter the Kerberos Realm address and click Set Kerberos realm. Click OK.

The Kerberos realm is usually the domain. The Kerberos realm should be a name (not an IP address), such as kemptech.local. If an IP address is specified, authentication will not work. This field only accepts one name.
5. Enter the **Kerberos Key Distribution Center** name and click **Set Kerberos KDC**. Click **OK**.

   This field only accepts one Key Distribution Center. The Key Distribution Center address is usually the IP address of the Active Directory instance.

   Double quotes are not allowed in this field.

6. Enter the **Kerberos Trusted User Name** and click **Set KCD trusted user name**. Click **OK**.

   The **Kerberos Trusted User Name** needs to be the same as the LoadMaster host name. The trusted user represents the LoadMaster. Refer to **Section 5.2** of this document for some further key requirements relating to this trusted user account.

   Double and single quotes are not allowed in the **Kerberos Trusted User Name** field.

7. Enter the **Kerberos Trusted User Password** and click **Set KCD trusted user password**. Click **OK**.

### 2.1.2 Configure the Client SSO Domain

![Figure 2-3: Client SSO domain](image)

The client SSO domain can be created by going to **Virtual Services > Manage SSO > Add** (in the **Client Side Single Sign On Configurations** section) and filling out the details as needed. Any option can be set for the **Authentication Protocol**.
2.2 Configure the Virtual Service

Now that the SSO domain has been created, the Virtual Service needs to be configured.

KCD authentication needs access the IP address of the Real Server in order to work. Therefore, KCD authentication must be set on the Virtual Service which has the Real Servers added. If a Virtual Service has a SubVS, KCD must be enabled on the SubVS because the Real Servers are added on the SubVS, not on the parent Virtual Service.

There are a number of different settings that can be configured in a Virtual Service. For more information, refer to the various documents at www.kemptechnologies.com/documentation

In this document we refer only to the KCD-specific settings. To configure a Virtual Service to use KCD server authentication and Form Based client authentication, follow the steps below in the LoadMaster WUI:

1. In the main menu, select Virtual Services > View/Modify Virtual Services.

2. Click Modify on the relevant Virtual Service. Alternatively, you can add a new Virtual Service by clicking the Add New button.

3. Expand the SSL Properties section.
4. Select **Enabled**.
5. Click **OK**.
6. Expand the **ESP Options** section.
7. Select **Form Based** as the **Client Authentication mode**.
8. Select the relevant client side **SSO Domain**.
9. Assign alternative SSO Domains (if required):
   a) Highlight each of the domains you wish to assign and click the > button.

   An assigned domain is a domain which can be authenticated using a particular Virtual Service.

   All domains which appear as available may be assigned to a Virtual Service.

   b) Click the **Set Alternative SSO Domains** button to confirm the updated list of Assigned Domain(s).
   c) Choose Basic Authentication from the Server Authentication Mode drop-down list.

10. Select **KCD** as the **Server Authentication mode**.
11. Select the relevant server side KCD SSO domain in the **Server Side configuration** drop-down list.

   This is the server SSO domain that was configured in Section 2.1.1.
12. Expand the Real Servers section.
13. Click Add New.
14. Enter the details of the Real Server.
15. Click Add This Real Server.

Configure any other settings as needed. For more information on the ESP options, refer to the ESP, Feature Description.
3 Using KCD with Client Certificate Authentication

Using certificates for authentication can be considered more secure because a user cannot gain access to something simply by knowing the username and password. Using certificates prevents key loggers or other malware on a client machine from capturing keystrokes to identify user accounts and passwords.

The LoadMaster supports the use of certificates with KCD authentication. For instructions on how to implement this, refer to the sections below.

3.1 Prerequisites

The LDAP server must support LDAP over a secure transport, for example LDAPS or StartTLS.

3.2 Install the Root Certificate on the LoadMaster

First, the root certificate (which client certificates will chain to) needs to be installed on the LoadMaster. To do this, follow the steps below in the LoadMaster WUI:

1. In the main menu, select Certificates & Security > Intermediate Certs.

   ![Add a new Intermediate Certificate](image1)

   **Figure 3-1: Upload Certificate**

   2. Click Choose File.
   3. Browse to and select the relevant certificate file.
   4. Enter the Desired File Name.
   5. Click Add Certificate.
   6. Click OK.

3.3 Generate and Import a Client Certificate

Generate a client certificate, for example with OpenSSL or Active Directory, which is signed by the root certificate. The client certificate must include a SubjectAltName (SAN) section with the User Principal Name (UPN) of the clients. This is typically in e-mail format. This will be used to check if a particular user exists in the LDAP database. This client certificate must be imported in the clients’ browser.

   ![Please import the certificate in the Personal store of the browser certificate settings.](image2)
3.4 Configure the Client Side SSO Domain in the LoadMaster

A client side SSO domain needs to be created in the LoadMaster. This should contain the IP address of the LDAP database as well as an administrator username and password. These login details are used to log in to the database and check if the user from the certificate does exist.

To create and configure this SSO domain, follow the steps below:

1. In the main menu of the LoadMaster WUI, select Virtual Services > Manage SSO.

![Add new Client Side Configuration](image1.png)

Figure 3-2: Add the SSO domain

2. In the Client Side Single Sign On Configurations section, enter the Name of the SSO domain.
3. Click Add.

![SSO domain details](image2.png)

Figure 3-3: SSO domain details

4. Select Certificates as the Authentication Protocol.
5. Enter the IP address of the LDAP database in the LDAP Server(s) text box.
6. Click Set LDAP Server(s).
7. Click OK.
8. In the LDAP Administrator and LDAP Administrator Password text boxes, enter administrator login details and click the buttons to set these values. These are used to log in to the database to check if the user from the certificate exists.
9. Enable or disable the Check Certificate to User Mapping option.
For more information, refer to Section 3.4.1.

10. Enable or disable the Allow fallback to check Common Name option. Enabling this option allows a fallback to check the Common Name (CN) in the certificate when the SAN is not available.

11. Enter the login domain to be used in the Domain/Realm text box.

This is also used with the logon format to construct the normalized username, for example:

Principalname: <username>@<domain>

Username: <domain><username>

If the Domain/Realm field is not set, the Domain name set when initially adding an SSO domain will be used as the Domain/Realm name.

3.4.1 Check Certificate to User Mapping

This section provides further information about the Check Certificate to User Mapping option. The Check Certificate to User Mapping option is only available when the Authentication Protocol is set to Certificates. When this option is enabled - in addition to checking the validity of the client certificate, the client certificate will also be checked against the altSecurityIdentities (ASI) attribute of the user on the Active Directory.
Figure 3-4: Security Identify Mapping
The altSecurityAttribute can be set in the Active Directory Users and Computers (data.msc) console by using the Name Mappings task (see screenshots above). Both the Issuer and Subject are used for alternate security identity. Using the Name Mappings method will create an altSecurityIdentities entry on the form:

```
X509:<I>issuer data...<S>subject data...
```

There are other formats (created by other methods) but this is currently the only supported one.

When changing the mapping in the Active Directory, the changes do not take effect immediately. To see the changes immediately, the SSO cache would need to be flushed or the user ticket would need to time out.

Flushing the SSO cache will flush all Single Sign-On (SSO) records, reset all authentication server statuses, reset the KCD domain (if relevant) and re-read the configuration. This has the effect of logging off all clients using Single Sign-On to connect to the LoadMaster.
If the **Check Certificate to User Mapping** option is enabled and the check fails, the login attempt will fail. If this option is not enabled, only a valid client certificate (with the username in the SubjectAltName (SAN)) is required to log in, even if the altSecurityIdentities attribute for the user is not present or not matching.

### 3.5 Configure the Server Side SSO Domain in the LoadMaster

In addition to creating a client side SSO domain, you also need to create a server side SSO domain containing the KCD details. To do this, follow the steps in **Section 2.1.1**.

### 3.6 Configure the Virtual Service

The relevant Virtual Service must be configured appropriately. To do this, follow these steps:

1. In the main menu, select **Virtual Services > View/Modify Services**.

   ![Figure 3-6: Modify](image)

   2. Click **Modify** on the relevant Virtual Service.
   3. Expand the **SSL Properties** section.

   ![Figure 3-7: SSL Properties](image)

   4. Select **Enabled**.
   5. Expand the **ESP Options** section.
6. Select **Client Certificate** as the **Client Authentication mode**.
7. Select the client side SSO domain from the **SSO Domain** drop-down list.
8. Enter any **Allowed Virtual Hosts** and click the **Set Allowed Virtual Hosts** button.
9. Fill out any other settings as needed.

Users should now be able to connect by typing https://host: - the browser will send the certificate and the LoadMaster will perform the appropriate checks (checking if the certificate has been signed by the root certificate uploaded in **Section 3.2** and checking if the SAN user exists in Active Directory).
4 KCD WUI Options

This section describes the different KCD-related options in the LoadMaster WUI. For descriptions on the remaining fields in the WUI, refer to the Web User Interface, Configuration Guide.

4.1 Manage SSO Screen

The fields below are all in the Manage SSO screen which can be accessed via the Virtual Services option in the main menu.

![Domain KCD.ESPTEST.LOCAL](image)

**Authentication Protocol**

This dropdown list allows you to select the transport protocol used to communicate with the authentication server. The fields on this screen change depending on the authentication protocol selected. To see the KCD fields, select Kerberos Constrained Delegation.

**Kerberos Realm**

The address of the Kerberos Realm. This is usually the domain.

Colons and slashes are not accepted in this field.

**Kerberos Key Distribution Center (KDC)**

Enter the name of the Kerberos Key Distribution Center (KDC). The KDC is a domain controller that issues session tickets and temporary session keys to users and computers within an Active Directory domain. The Kerberos Key Distribution Center address is usually the IP address of the Active Directory instance.

**Kerberos Trusted User Name**

Before configuring the LoadMaster, a user account must be created and trusted in the Windows domain (Active Directory). This user should also be set to use delegation.

Refer to Section 5.2 of this document for some key requirements relating to this trusted user account.
The trusted user name should be the same as the LoadMaster host name. This trusted administrator user account represents the LoadMaster. It is used to get tickets on behalf of users and services when a password is not provided. The user name of this trusted user should be entered in this text box.

**Kerberos Trusted User Password**

The password of the Kerberos trusted user.

### 4.2 Modify Virtual Service Screen

In the ESP Options section of the Virtual Service modify screen there are some options specifically relating to KCD.

**Client Authentication mode**

Specifies how clients attempting to connect to the LoadMaster are authenticated. The types of methods available are listed below:

- **Delegate to Server**: the authentication is delegated to the server
- **Basic Authentication**: standard Basic Authentication is used
• **Form Based**: clients must enter their user details within a form to be authenticated on the LoadMaster

• **Client Certificate**: clients must present the certificate which is verified against the issuing authority

• **NTLM**: NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name and a one-way hash of the user’s password

The remaining fields in the ESP Options section will change based on the Client Authentication Mode selected.

**SSO Domain**

Select the relevant client side SSO domain.

**Alternative SSO Domains**

Many organizations use extranets to share information with customers and partners. It is likely that extranet portals will have users from two or more Active Directory domains. Rather than authenticating users from individual domains one at a time, assigning Alternative SSO Domains gives the ability to simultaneously authenticate users from two or more domains using one Virtual Service.

This option appears only when more than one domain has been configured and when the Authentication Protocol for the SSO domains are set to LDAP.

Please refer to Section 4.1 for further information on configuring SSO Domains.

![SSL Properties](image)

**Figure 4-3: Enabled and Reencrypt tick boxes selected**

Before configuring the ESP Options to use Alternative SSO Domains ensure that, in the SSL Properties section, the Enabled and Reencrypt tick boxes are selected.
The domain name which appears in the SSO Domain drop-down list is the default domain. This is also the domain which will be used if only one is configured.

Previously configured alternative domains appear in the Available Domain(s) list.

**Server Authentication mode**

> This field is only updatable when the Client Authentication Mode is set to Form Based.

Specifies how the LoadMaster is authenticated by the Real Servers. There are three types of methods available:

- **None**: no client authentication is required
- **Basic Authentication**: standard Basic Authentication is used
- **KCD**: KCD authentication is used

> This must be set to KCD for KCD to work.

**Server Side configuration**

> This option is only visible when the Server Authentication mode is set to KCD.

Select the relevant server side SSO domain.
5 Appendix A: Configure the Active Directory Settings

There are certain Active Directory settings that need to be configured correctly in order for KCD to work with the LoadMaster. Follow the steps below to configure these settings. If this account is not set up correctly, KCD authentication will not work.

The steps below are functionally equivalent for Windows Server 2008 and Windows Server 2012 R2. For more information, please refer to the Microsoft documentation.

5.1 Add a Certificate to the Active Directory for TLS/LDAPS

A certificate needs to be added to the Active Directory for Transport Layer Security (TLS)/Lightweight Directory Access Protocol over SSL (LDAPS).
5.2 Create DNS Entries

A DNS entry representing the Fully Qualified Domain Name (FQDN) must be created in the DNS Manager. An A record (for IPv4), or AAAA record (for IPv6), must be created for the LoadMaster host name (Kerberos trusted user).

Ideally, a PTR record for the FQDN should also be added for reverse lookup. A reverse DNS lookup zone needs to be set up which is able to resolve the IP address of the Real Server.
There can be multiple entries for Real Servers in the DNS server. As a result of this, when the LoadMaster does a reverse lookup in order to get the FQDN, the result may not match the Service Principal Name (SPN). This may result in a mismatch between the SPN the LoadMaster generates and the one configured under the trusted user in the Active Directory. To mitigate this issue, it is possible to override the DNS server entries by adding hosts for local resolution in the LoadMaster (System Configuration > Host & DNS Configuration).

5.3 Create a LoadMaster Trusted User

A LoadMaster trusted user must be created in the Windows domain (Active Directory). The Active Directory account for the trusted user is a user account, but it represents the LoadMaster. The name of the trusted user must be the same as the LoadMaster host name.

Some guidelines regarding configuring the trusted user are listed below:

- The User Principal Name (UPN) (User logon name) must take the form of a Service Principal Name (SPN) for the LoadMaster.
  Format: host/<LoadMasterFQDN>@<UPNSuffix>
  Example for LoadMaster trusted user: host/lm60.espatest.local@ESPTEST.local

  The default UPN suffix must be used.

- The pre-Windows 2000 user logon name (which corresponds to the sAMAccountName) has to be the name part of the FQDN that is part of the UPN above, for example KEMPDEV\.
When the User logon name field is filled out, the second box in the User logon name (pre-Windows 2000) section gets automatically populated. In some cases the text will be truncated, for example host/lm60.esptest.lo. Delete the host/ part and ensure to include the full FQDN, for example lm60.esptest.local.

A DNS entry representing the FQDN must be created, ideally with a PTR record for reverse lookup.

In the LoadMaster, the Kerberos Trusted User Name will be set to the FQDN name above, which should be the host name of the LoadMaster.

For backward compatibility reasons, the User logon name (pre-Windows 2000) has a size limit of less than 20 characters.

- The password should be set to never expire
- The user must have permissions to perform protocol transition
• If using KCD in a SharePoint 2013 environment – the Real Servers (SharePoint servers) must be added to the `servicePrincipalName` attribute
The user must be a member of the relevant domain.

In the example, the items are mapped as follows:

<table>
<thead>
<tr>
<th>Item</th>
<th>Mapping</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>lm60</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>esptest.local</td>
<td></td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td>esptest.local</td>
<td></td>
</tr>
<tr>
<td>Default UPN-suffix</td>
<td>esptest.local</td>
<td></td>
</tr>
<tr>
<td>LoadMaster FQDN</td>
<td>lm60.esptest.local</td>
<td>DNS entry</td>
</tr>
<tr>
<td>LoadMaster hostname</td>
<td>Lm60</td>
<td></td>
</tr>
<tr>
<td>LoadMaster SPN</td>
<td>host/lm60.esptest.local</td>
<td></td>
</tr>
</tbody>
</table>
## 5.4 Associate an SPN with the User Entry

Execute the `ktpass.exe` file in the command prompt to associate a Service Principal Name (SPN) with the user entry.

**Example Syntax**

```
ktpass.exe /princ host/<LoadMasterSPN>@<Domain> /ptype KRB5_NT_PRINCIPAL /mapuser <Domain>\<TrustedUserLogonName> /mapop set /setupn /crypto all
```

**Example Command**

```
ktpass.exe /princ host/lm60.esptest.local@ESPTEST.local /ptype KRB5_NT_PRINCIPAL /mapuser ESPTEST\lm60.esptest.local /mapop set /setupn /crypto all
```

The `ktpass.exe` file is a Microsoft command-line utility and will be present on any Windows Server installation.

For further information about the `ktpass` command, please refer to the *Ktpass* Microsoft TechNet article:


Alternatively, enter `ktpass.exe /h` for help on the `ktpass` command.

When this has been completed, the user properties window will have the **Delegation** tab.
5.5 Configure Delegation for the User Entry

Some guidelines relating to the delegation settings for the trusted user are provided below:

- The trusted user account must have delegation enabled (the ability to request a ticket on behalf of a user logging in) and be set to **Use any authentication protocol**

- Delegation is not enabled by default when a user is created.

- In constrained delegation mode, the service(s) that need to be available must be selected.
When using KCD in a Microsoft Exchange environment, ensure to enable the **Integrated Windows authentication** check box in the **Exchange admin center**.

There are a number of other considerations to be aware of when using KCD in an Exchange environment. For more information, please refer to the following TechNet article: [https://technet.microsoft.com/en-us/library/ff808312%28v=exchg.150%29.aspx](https://technet.microsoft.com/en-us/library/ff808312%28v=exchg.150%29.aspx)
## References

Unless otherwise specified, the following documents can be found at [http://kemptechnologies.com/documentation](http://kemptechnologies.com/documentation).

**ESP, Feature Description**

**Web User Interface, Configuration Guide**

**TechNet article: Configuring Kerberos authentication for load-balanced Client Access servers**


**TechNet article: Ktpass**

# Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Version</th>
<th>Resp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 2015</td>
<td>Minor updates</td>
<td>Enhancements made</td>
<td>4.0</td>
<td>LB</td>
</tr>
<tr>
<td>Dec 2015</td>
<td>Release updates</td>
<td>Updates for 7.1-32 release</td>
<td>5.0</td>
<td>LB</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Minor updates</td>
<td>Updated Copyright Notices</td>
<td>6.0</td>
<td>LB</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Release updates</td>
<td>Updates for 7.1-34 release</td>
<td>7.0</td>
<td>LB</td>
</tr>
<tr>
<td>May 2016</td>
<td>Release updates</td>
<td>Updates for 7.1.34 release</td>
<td>8.0</td>
<td>LB</td>
</tr>
<tr>
<td>July 2016</td>
<td>Release updates</td>
<td>Updates for 7.1.35 release</td>
<td>9.0</td>
<td>LB</td>
</tr>
</tbody>
</table>