Pyramid 2018 Kerberos Guide

Guidelines and best practices for how deploy Pyramid 2018 with Kerberos

Contents

Overview 3
Warning 3
Prerequisites 3
Operating System 3
Pyramid 2018 3
Delegation Introduction 4
The Double Hop 4
Constrained vs. Full Delegation 4
Local Service Account vs. Domain Account 4
Standard Setup 5
Advanced Options 8
Friendly URL Setup 8
DNS Setup 8
URL SPNs 10
Constrained Delegation with the System Account 11
Constrained Delegation with Domain Accounts 12
Register New SPNs 12
Pyramid Database Repository Update 12
Changes for the Domain Account 13
Appendix 15
Documentation & Tools 15
Setting Service Principal Names (SPNs) 16
Template for adding SPNs 16
Microsoft SQL Server SPNs 17
Client Browser Settings 18
Internet Explorer 18
Firefox 18
Chrome 18
Edge 18
Troubleshooting 19
Windows Authentication Check List 19
Access Token Problems 20
Verifying the Existence of Kerberos Tickets 21
Kerberos Troubleshooting 22
Microsoft SQL Server Kerberos Issues 23

Overview

In general, Pyramid 2018 **DOES NOT REQUIRE** complex configurations for Kerberos and delegation. However, it is required if the deployment requirements include the use of BOTH:

- **Windows Authentication** as the authentication *method* for sign-on to the web application
- AND the use of end-user **Windows authenticated access** to Microsoft SQL Server[1].

It is currently only possible to implement this functionality if:

1. The *authentication provider* is Windows Active Directory
2. AND, all servers hosting Pyramid 2018 are Windows based

Exclusions

Fortunately, Kerberos and delegation is NOT necessary in these scenarios:

1. The authentication *method* is 'basic' or 'forms'
2. The target data source is MS Analysis Services (which uses the more modern 'user token' method instead).

Warning

The setup and maintenance of Kerberos and Delegation can be complex to implement and maintain. It requires expertise and knowledge by system administrators.

Prerequisites

Operating System

Prior to these configuration steps, your environment should have the following prerequisites. If any of these items are not configured, delegation might not function correctly.

- Check your Active Directory Forest and Domain functional levels. They should be set to Native or 2008 or later.
    - Windows 2008 machines should have the Microsoft hotfix **KB969083** applied to correct the Kerberos issues with SQL Server 2005/8/12/14/16. This does not need to be applied to Windows 2008 R2 / 2012 / 2016.
- Kerberos delegation can function between trusted forests and domains. The resource forest or domain must trust the user forest or domain.

All Active Directory settings can only be set by a domain/forest administrator with permissions.

Pyramid 2018

The following core settings are necessary for this type of deployment:

- The web authentication *provider* is Active Directory
- The web authentication *method* is Windows Authentication
- The client browser supports Windows Authentication. See Client Browser Settings for more information.
- The MS SQL Server data source in Pyramid 2018 has been set-up to use the end-users' Windows credentials for authentication and connectivity.

[1] Currently, Windows Authentication for data sources is limited to Microsoft SQL Server. Support for Oracle, DB2, Teradata and others will be added in due course.

Delegation Introduction

Administrators must configure Kerberos delegation in the Active Directory for users to authenticate and subsequently query the designated data source successfully using their Windows security tokens. Active Directory settings provide an option, through Kerberos delegation, to pass the user's security tokens from the client browser to the Web server, and then on to other servers and finally to the data source.

The Double Hop

Kerberos authentication can produce more challenges when there is a multi-leg or "double-hop" between multiple servers. The *double-hop* problem is an intentional security restriction to discourage Active Directory objects from acting on behalf of other security accounts.

As a web-based platform, Pyramid 2018 creates double-hops when there is one hop from the browser to the Web server and another hop to the Runtime server and then a final hop to the data source server.

The process of configuring delegation is how the "hops" are configured and resolved.

Constrained vs. Full Delegation

When setting a server to allow full trust (unconstrained) delegation, a Kerberos token from any service will be transferred to any other service on the target server from the source machine. Constrained delegation allows you to define which specific service(s) on the target machine will accept the Kerberos token.

Due to the way Kerberos is implemented in Java, Pyramid 2018 uses a combination of delegation types. At the very least, the delegation can be full trust on all hops except for the last one (the connection to the data source), which MUST be constrained. Alternatively, the entire delegation chain can be set as constrained.

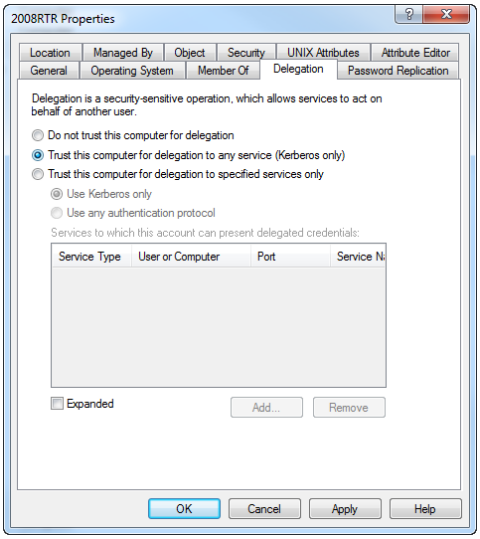
Local Service Account vs. Domain Account

When setting up Pyramid 2018 delegation, administrators can elect to use the default local service accounts or domain account. By **default**, the application is installed with local services accounts. Which, in many respects, is simpler and cleaner to implement than domain accounts.

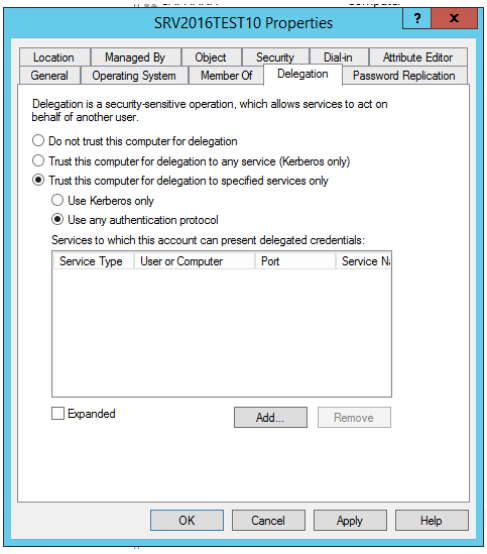
Standard Setup

The following basic setup guide assumes that the web server tier, the runtime/task server tier and data source are all installed on different machines. It also assumes that we are not using a Friendly URL website address.

1. Before starting, ensure that Pyramid is set to using Active Directory as the authentication provider in the Pyramid admin console. Also, make sure Windows Authentication is the web authentication method.
2. Next, configure the web server's delegation. Open the Active Directory "Users and Computers" panel in Windows Administrative Tools on an AD domain controller server (see below).
3. Find the machine entry in the AD for the web server and edit its properties. From the tabs, choose Delegation and set it to "Trust the Computer for Delegation to any Service". Click OK.

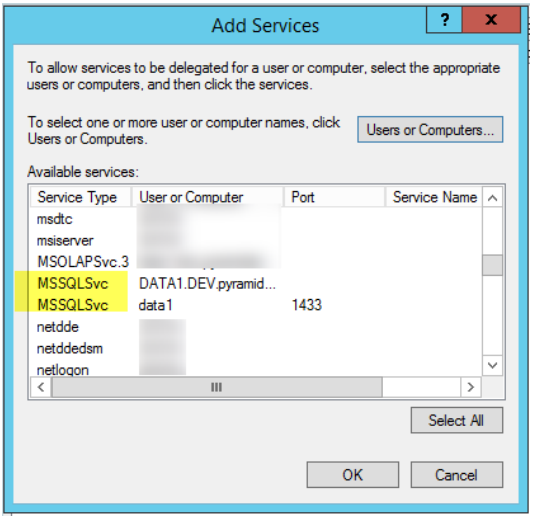


4. Next, configure the runtime server's delegation. Find the machine entry in the AD for the web server and edit its properties. From the tabs, choose Delegation and set it to "Trust the Computer for Delegation to specified services only" [2]. Then select "Use any authentication protocol"[3].

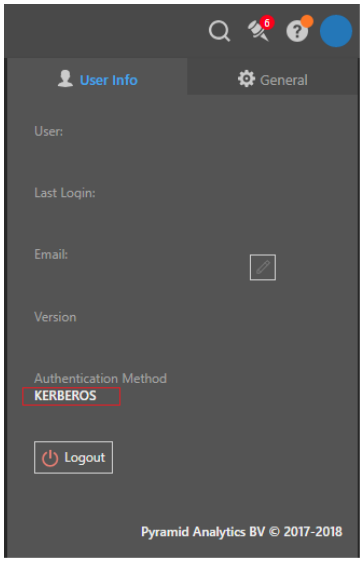


[2] As the runtime server is the last step to the data source, it CANNOT use the full delegation option.
[3] Java can only pass Kerberos tokens using this option.

5. Next, click the ADD button. In the pop-up, click the "Users or Computers" button, and find the machine hosting your database server. Click Ok and you will see a listing of available services.

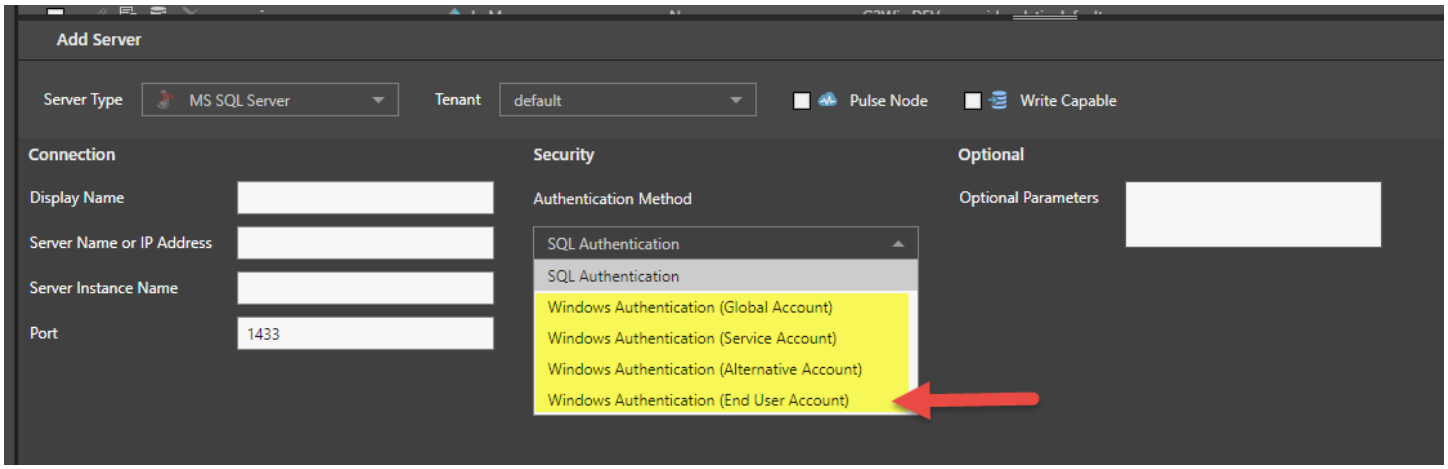


6. From the listing, choose the two SPN items of type "MSSQLSvc[4]" and then choose OK. Once that pop-up is closed, click Apply. If the SPNs for MS SQL server are missing, you may need to add them manually.
7. To have the delegation settings flushed through the domain, rebooting the affected servers is highly recommended.
8. Once all servers and services are back up launch a client browser, going to the Pyramid application. The user should be able to enter the application without a login prompt[5]. Open the user panel in Pyramid and ensure that the browser authentication method is Windows Authentication with Kerberos. If it is NTLM[6], the data authentication process will not work.



[4] The Name of the SPN will differ depending on which database technology and SPN has been created. MSSQLSvc is the standard name given for SQL Server.
[5] If there are prompts, Windows Authentication is not operational or enabled in either Pyramid or the browser, or both.
[6] NTLM "fall back" authentication occurs when Kerberos fails.

9. Add a new DataSource Server in the Admin. Select “Windows Authentication End-User”



10. Last, create a data model on your database using one of the various data modeling tools in Pyramid and then you can begin a Discovery session to start querying your database.

Advanced Options

Friendly URL Setup

A computer that is joined to an Active Directory Domain typically gets an A-record (URL) created automatically based on its fully qualified domain name. However, most of the time, websites are used with friendly URL names.

Clients may use the friendly host header name (*http://myanalytics.com*) instead of the computer name as the Pyramid URL to make it easier to access the application. To use a host header for the Pyramid site, administrators typically create a DNS host entry.

- If the site is deployed on the Internet/Extranet, the DNS entries are made in the public DNS records.
- Otherwise, if it's an intranet deployment, the records are made on the local DNS server. If it is multi-domain Active Directory, the DNS entries should be added into the global DNS for the forest.

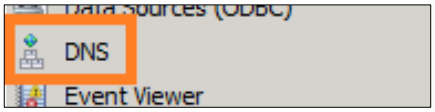
Windows IIS

If using an internal DNS hosted site and optionally using Windows IIS, make sure that both the short name for the site (*http://mysite*) and the fully qualified domain name for the site (*http://mysite.mycompany.com*) are added to the bindings for that site in IIS.

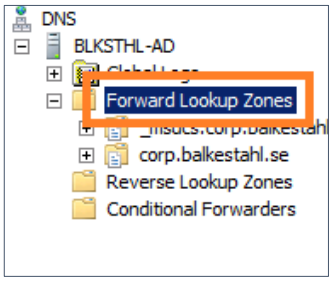
DNS Setup

To create an A-Record in DNS for a friendly URL use the following steps.

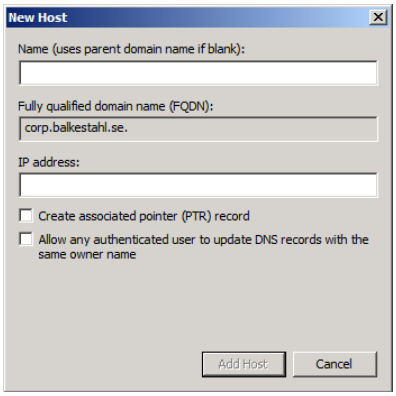
- Open DNS Management in Administrative Tools on a DNS server.



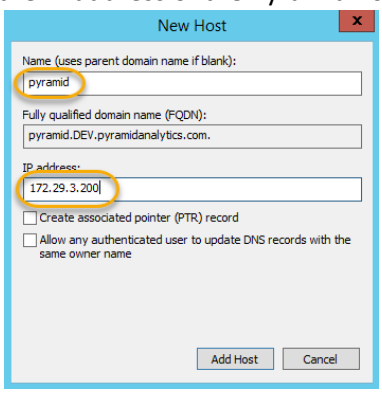
- Expand forward lookup zones container.



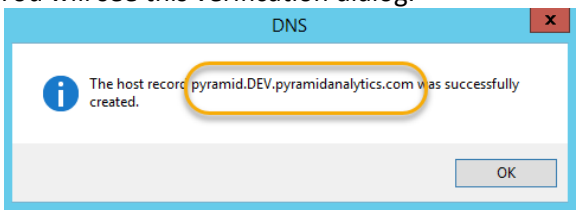
- Right click on the zone (domain name) and click on new host (A or AAAA).



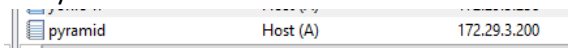
- Type in the name of the record, this is the URL of Pyramid (minus the domain part in a FQDN) and type in the IP address of the Pyramid 2018 Web Server.



- Click on **Add Host**.
- Click on **Done**.
- You will see this verification dialog.



- Verify that the record has been created.



Global Names Zone Setup

In case of a Multi-Domain environment, add C-Name (alias) pointing to the A-Record, from previous section, in the Global Names Zone. In this way the Pyramid 2018 URL friendly name will be supported from other Domains in your network with Kerberos enabled.

Additional reference see: http://technet.microsoft.com/en-us/library/cc731744.aspx

Note: If a web-farm is being deployed, see the following steps in the appendix.

URL SPNs

Adding a DNS Host will require new SPNs to be added to correspond to the friendly URL name – if the DNS is being setup internally on the local DNS server and Active Directory. (This usually coincides with the deployment of a Windows Authentication based system).

For detailed instructions on setting SPNs see the appendix.

1. In an administrative command prompt run the following:

   ```
   Setspn.exe -s HTTP/Pyramid-URL <host account>
   ```

2. If the URL is an internal URL on an internal DNS Server (Active Directory), then add the follow SPN as well:

   ```
   Setspn.exe -s HTTP/Pyramid-URL.fully-qualified-name <host account>
   ```

3. As before, ensure there are no duplicate SPN entries:

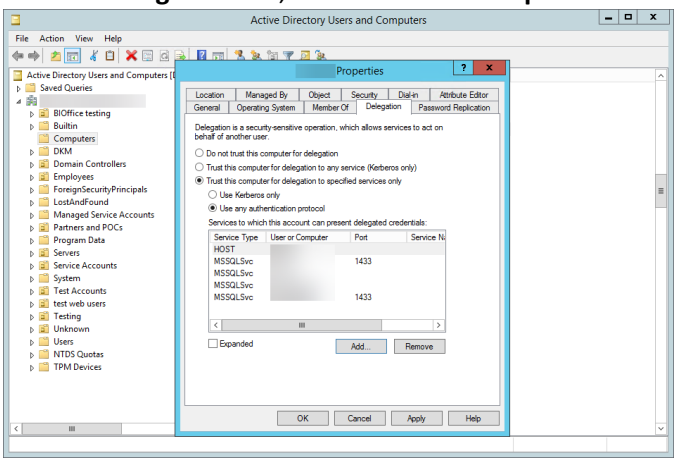
   `Setspn.exe -x` or `-q <SPN>`

Constrained Delegation with the System Account

The following steps are required if you choose to deploy constrained delegation throughout the delegation "hop chain".

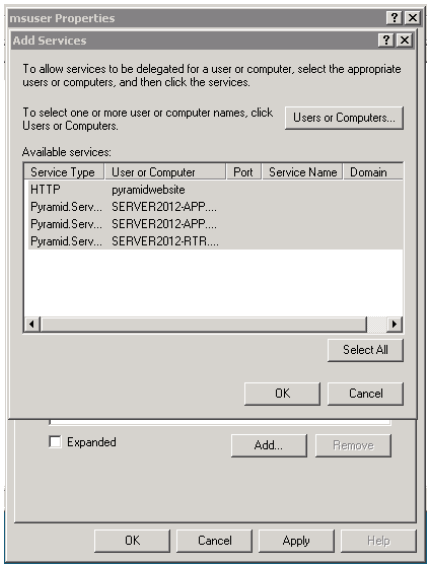
Repeat the following process for each computer running the Pyramid Services: Web server, Runtime engine and Tasks engine. (The runtime and task engines should already be running with constrained delegation as per the basic setup flow).

1. From **Active Directory Users and Computers**, right-click on the <`Computer`>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**.



Active Directory Kerberos delegation configuration

4. Click **Use any authentication protocol.**
5. Click **Add**, and then click **Users and Computers**.
6. Type the name of a computer running a Pyramid Service.
7. Click **Select All** and click **OK.**



Constrained Delegation with Domain Accounts

By default, Pyramid services are installed with the LocalSystem, so a service principal name (SPN) exists by default in the form of:

```
HOST/<NetBIOS-name>
HOST/<FQDN-name>
```

The following changes are required to the SPNs of Pyramid when using constrained delegation and services running under a *Domain Account*. See the appendix for general instructions on setting SPNs.

Register New SPNs

1. Remove the HTTP/Pyramid-Site-URL SPNs from the Web server machine:

```
Setspn.exe -d HTTP/Pyramid-Site-URL Domain\NetBIOS-name$
```

If the URL is an internal URL listed on the internal DNS Server (Active Directory), then remove the following SPN as well:

```
Setspn.exe -d HTTP/Pyramid-Site-URL.fully-qualified-name Domain\NetBIOS-name$
```

2. Specify the new SPNs in the Active Directory, Use "`SetSpn.exe -s`" to add the following:

```
Pyramid.Server.Runtime/NetBIOS-name <Domain\Runtime Username>
Pyramid.Server.Runtime/ fully-qualified-name <Domain\Runtime Username>

Pyramid.Server.Task/NetBIOS-name <Domain\Task Username>
Pyramid.Server.Task/ fully-qualified-name <Domain\Task Username>

HTTP/Pyramid-Site-URL <Domain\app pool Username>
```

If the URL is an internal URL listed on the internal DNS Server (Active Directory), then add the following SPN as well:

```
HTTP/Pyramid-Site-URL.fully-qualified-name <Domain\app pool Username>
```

3. Verify SPNs by running: "`SetSpn -l Domain\Username`" for each user.
4. Verify no duplications by running "`SetSpn -x`" " or "`SetSpn -q <SPN>`"
    - Duplicate SPN definitions break the Kerberos authentication process.

Pyramid Database Repository Update

Manual changes need to be made in the Pyramid Repository Database table **[server_instances]**.

Update values in the **[spn]** column according to the following:

Service	Service Type	SPN
Runtime Engine	0	Pyramid.Server.Runtime/FQDN
Tasks Engine	4	Pyramid.Server.Task/FQDN

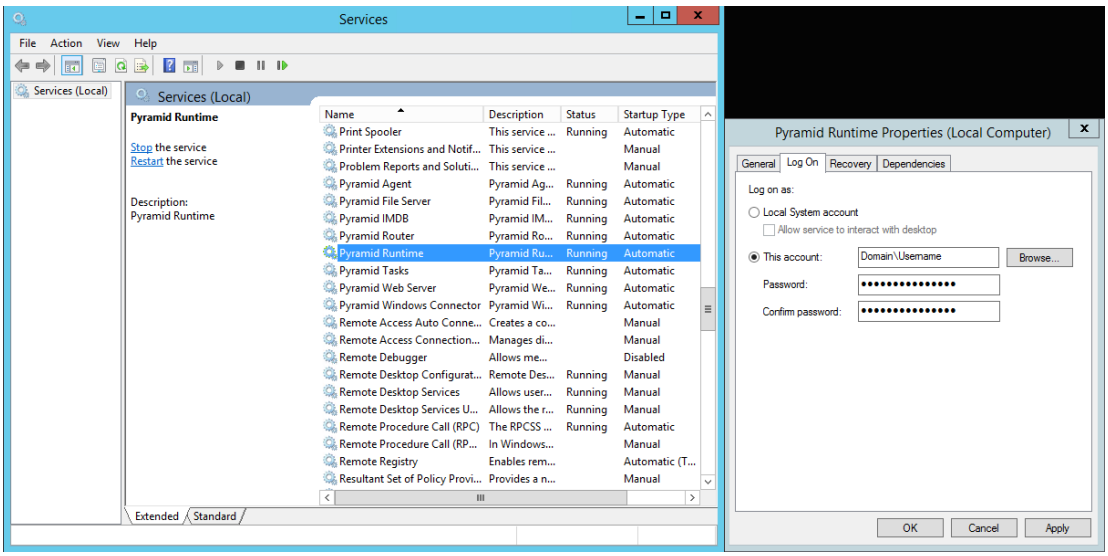
Each FQDN will be the Fully Qualified Domain Name of the machine running the specific Service.

NOTE : Other services with [ServiceTypeID] 1, 2, 3 or 5, cannot have an SPN value and should be left as *NULL*.

Changes for the Domain Account

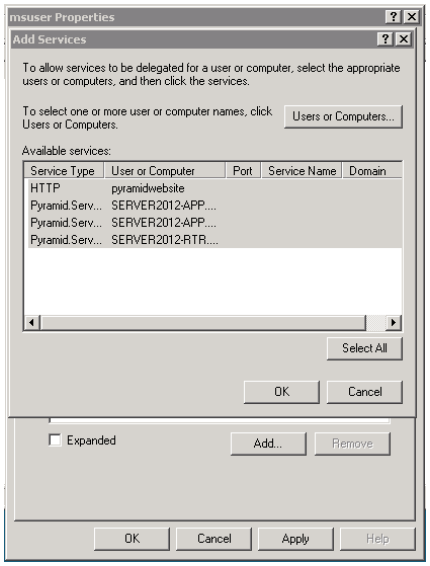
Configuring the Domain Account(s)

1. In Active Directory under **Users and Computers**, go to the **Account Options** list on the **Account tab** of the domain account and verify that the **Account is sensitive and cannot be delegated** option is not selected.
2. For each machine in the deployment add the domain account to the local administrators group, and open **Local Security Policy** in the Administrative Tools program group. Expand Local Policies, and click User Rights Assignment. Add the custom service account to the following policies:
    a. Log on as a service.
    b. Impersonate a client after authentication.
    c. Enable computer and user accounts to be trusted for delegation.
    d. Act as part of the operating system.
3. Next, change all Pyramid services from Administrative Tools to run under the specific domain account(s) and restart the services.
    a. Note: these changes should not be made to the services running the database repository.



Changing to custom account

4. In the Active Directory, make the following changes for domain account running Pyramid 2018: Runtime engine, Tasks engine and (optionally) Web server.
    1. From **Active Directory Users and Computers**, right-click on the <Username>, and choose **Properties**.
    2. Go to the **Delegation** tab.
    3. On the **Delegation** tab, click **Trust this user for delegation to specified services only**.
    4. Click **Use any authentication protocol**.
    5. Click **Add**, and then click **Users and Computers**.
    6. Type the name of a user running a Pyramid 2018 Service.
    7. Click **OK** after selecting the all the relevant SPNs.



Full Delegation Alternative

Since Pyramid Web servers can optionally use full delegation, the following steps should be applied for each domain account running Pyramid 2018 Web servers if you elect not to use constrained delegation for them.

1. From **Active Directory Users and Computers**, right-click on the <`Username`>, and choose **Properties**.
2. Go to the **Delegation** tab.
3. Select the second option **Trust this user for delegation to any service (Kerberos only)**.

Appendix

Documentation & Tools

- For more information see http://blogs.technet.com/b/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx
- Review the section “Infrastructure Requirements” in Microsoft’s Troubleshooting Kerberos Delegation
- There are two common tools for editing SPN entries in Active Directory: AdsiEdit.msc and setSPN.exe.

Setting Service Principal Names (SPNs)

SPNs are “addresses” - they specify the location and type of a specific service running under a specific account in the system. They are **critical** to the delegation process, because they allow the entire platform to direct requests to the right address while also indicating which addresses the source server has the right to delegate to.

SPNs are required in both full or constrained delegation models.

Template for adding SPNs

In an administrative command prompt running the following will add the SERVICE SPN:

```
Setspn.exe -s SERVICE/<host name> <host account>
Setspn.exe -s SERVICE/<fully qualified domain host name> <host account>
```

- If installing under the local services (the default), the host account is the machine name followed by a “$” sign.
- If installing under a domain account, the host account is the domain account name.
- If installing an HTTP service the host name is the host header or URL of the website.

Duplicate SPNs break Kerberos Authentication. As such, once completed, run the following to ensure there are no duplicate SPN entries: `Setspn.exe -x` or `-q <SPN>`

Setting SPNs Manually

In the event the SPNs are not created correctly or when there are advanced configuration changes, new SPNs may need to be set manually by a domain administrator.

1. Specify the SPNs in the Active Directory, Use “`SetSpn.exe -s`” to add the following:

Runtime Engine machine
```
HOST/NetBIOS-name <machine name>$
HOST/NetBIOS-name.fully-qualified-name <machine name>$
```
Task Engine machine
```
HOST/NetBIOS-name <machine name>$
HOST/NetBIOS-name.fully-qualified-name <machine name>$
```
Web Server machine
```
HTTP/Pyramid-Site-URL <machine name>$
HTTP/Pyramid-Site-URL.fully-qualified-name <machine name>$
```

2. Verify SPNs by running: “`SetSpn -l`” for each machine.
3. Verify no duplications by running “`SetSpn -x`” or “`SetSpn -q <SPN>`”.
    - Duplicate SPN definitions break the Kerberos authentication process.

Account Configuration

User Accounts

User accounts on the Active Directory, by default, should not need additional configuration. You may want verify the *Account is sensitive and cannot be delegated* box is NOT checked in the Active Directory account properties. **If checked, the account will be inoperable for delegation**.

Testing

The users should log out and back in to their machine after changing any properties and before running Kerberos Delegation tests. This will clear cached Kerberos tickets. You may also use the **Kerbtray** utility to clear Kerberos tickets without logging out and back in.

Microsoft SQL Server SPNs

1. MS SQL Server usually comes installed with its SPNs in the domain. In some circumstances, these SPNs could be broken or missing. The following steps explain how to add them manually.

MS SQL with the default instance name:

```
Setspn.exe -S MSSQLSvc/myhost.pyramid.com domain\accountname
Setspn.exe -S MSSQLSvc/myhost domain\accountname
```

For a names instance, use:

```
Setspn.exe -S MSSQLSvc/myhost.pyramid.com domain\accountname
Setspn.exe -S MSSQLSvc/myhost domain\accountname
```

For MS SQL SPN registration see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/register-a-service-principal-name-for-kerberos-connections.

A Restart on all the machines in the deployment and restart the client machine is required for changes to take effect.

Client Browser Settings

Not all browsers and operating systems support Windows Authentication. Most that do require special settings. The following are guides to the three most popular HTML5 compliant web browsers.

Internet Explorer

From the client machine (browser) make sure the following settings are configured:

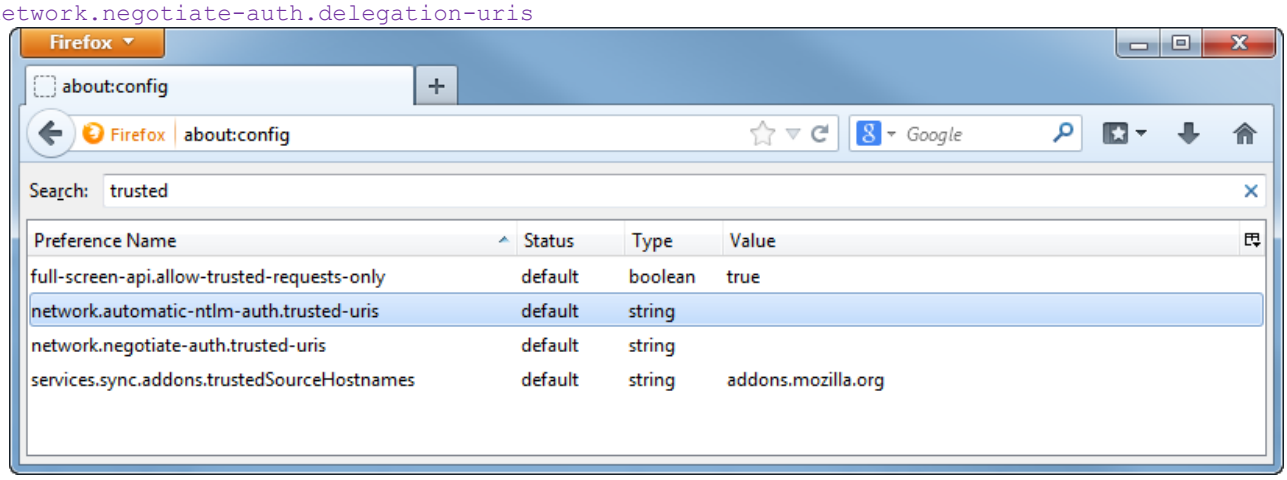
- Ensure the Pyramid 2018 Web address has been added to the list of TRUSTED SITES in the browser (or INTRANET sites for internal site addresses).
- Update automatic logon through Internet Explorer > Internet Options > *Security >Trusted sites > Custom level > Automatic Logon* with current username and password.
- Make sure Internet Explorer is set to use *Integrated Authentication* in advanced Internet Options.
- Have the end user log off and log on or use kerbtray.exe to clear cached security tickets.

These configurations can also be enacted through GPO's on the Active Directory.

Firefox

Launch Firefox and go to *about:config* (shown below). Add the URL of the Web site to the following preferences:

```
network.automatic-ntlm-auth.trusted-uris
network.negotiate-auth.trusted-uris
network.negotiate-auth.delegation-uris
```



Firefox Integrated Windows Authentication

Chrome

Google Chrome in Windows will use the Internet Explorer settings, so configure within Internet Explorer's Tools, Internet Options dialog, or by going to Control Panel and selecting Internet Options within sub-category Network and Internet.

Edge

Microsoft Edge in Windows will use the Internet Explorer settings, so configure within Internet Explorer's Tools, Internet Options dialog, or by going to Control Panel and selecting Internet Options within sub-category Network and Internet.

Troubleshooting

Windows Authentication Check List

The details behind each of the following steps can be found in the body of this document. The list below is merely a checklist summary to follow.

1. Ensure the Authentication METHOD was set to Windows Authentication.
2. Ensure that the ports on the server's firewall are not blocking ports required for Windows Authentication.
3. To ensure the Kerberos authentication does not fail:
    a. For servers with internal DNS hosting on the Active Directory – ensure that both the website name and the fully qualified domain name of the website are registered as SPNs.
    b. Ensure there are no duplicate SPNs.
    c. Ensure there are no duplicate DNS entries for the Host site and IP.
    d. The delegation has been setup such that both sets of SPN's are registered for the account that will be delegating tokens.
    e. To check if Kerberos tickets are being issued use the "**Kerberos Authentication Tester"** tool (described above) to check if there is a fall back to NTLM. Windows Authentication will not work under NTLM. You can also check the user's panel in the client application to see if the detected authentication model is Kerberos or NTLM.
    f. Check if there is a Kerberos token "bloat" problem (see below).
4. Ensure that SPN column in the Database Repository matches the SPN's used. The default ones suit a Local Service Account model. If a domain account is used these need to be updated.
5. If using constrained delegation, remove and then re-add any SPN's that were modified.
6. If using a domain account, the account needs to be a local administrator on the host servers and have certain GPO rights (see above for more detail).
7. If using an internal DNS named site, make sure that both the short name for the site and the fully qualified domain name for the site are added to the bindings for that site in IIS.
    a. If it is multi-domain Active Directory, the DNS entries should be added into the global DNS for the forest.
8. On the client machine, ensure that the website address is **trusted** in the browser settings and that the authentication is set to automatically pass on the user's credentials. Ensure "integrated windows authentication" is enabled.
9. Once all settings have been made, it is a good idea to reboot all hosting servers and any client PCs before attempting to connect.

Access Token Problems

Active Directory 'Token Bloat' is a known issue where users are added as members to too many security groups. As such their account exceeds the default 12k token size limit in Windows that is set on their internal AD Security Token.

This is a common problem for many large organization that have many security groups and in most situations this problem is fixed by configuring a larger "MaxTokenSize" registry key on all the computers.

Configure all Pyramid servers - including the datasource servers - and client machines to accept larger headers.

To increase the header size you need to configure the following registry keys:

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters**
  MaxFieldLength

  Default Value: 16384

  Set value to: 65534 (64kb) bytes

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters**
  MaxRequestBytes

  Default value: 16384

  Set value to: 16777216 (16MB) bytes

Configure all servers hosting Pyramid 2018 - including the data source servers - and client machines to accept a larger token size.

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters**
  MaxTokenSize

  Default Value: 12000

  Set value to: 65535 (64kb) bytes

All values specified are decimal values.

Additional References

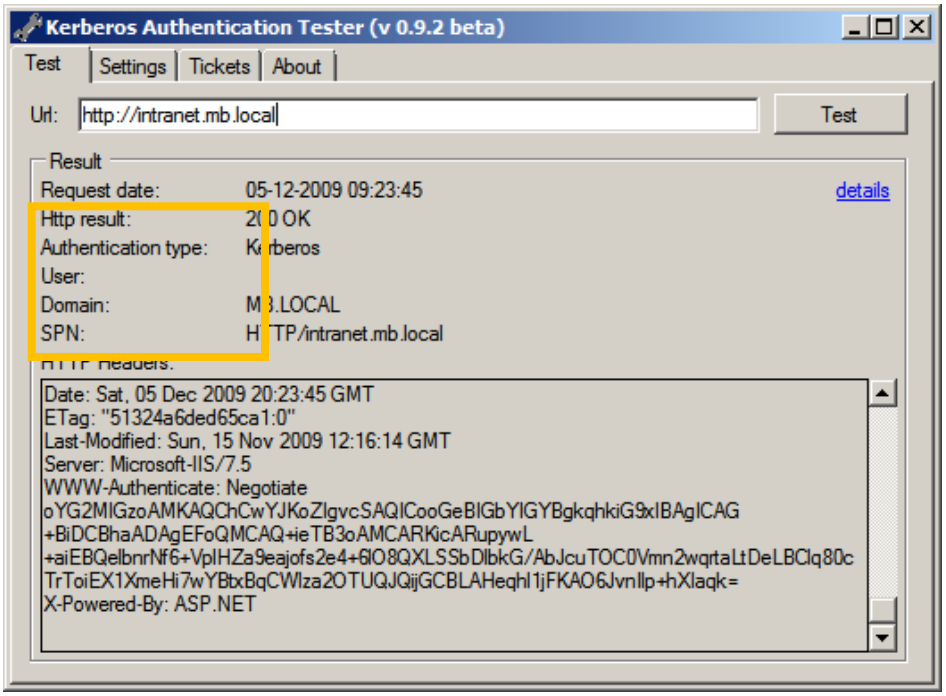
To configure these registry keys with Group Policy see: http://www.grouppolicy.biz/2013/06/how-to-configure-iis-to-support-large-ad-token-with-group-policy/

Kerberos Authentication Problem with Active Directory:
http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx

Verifying the Existence of Kerberos Tickets

Often it is hard to detect the status of Kerberos tokens and tickets in the flow. There are a few ways to view the tickets and their status. This includes:

- **Klist**
- **Kerbtray**
- **Kerberos Authentication Tester (**[http://mbar.nl/michel/archive/2009/12/05/kerberos-authentication-tester.aspx)](http://mbar.nl/michel/archive/2009/12/05/kerberos-authentication-tester.aspx)



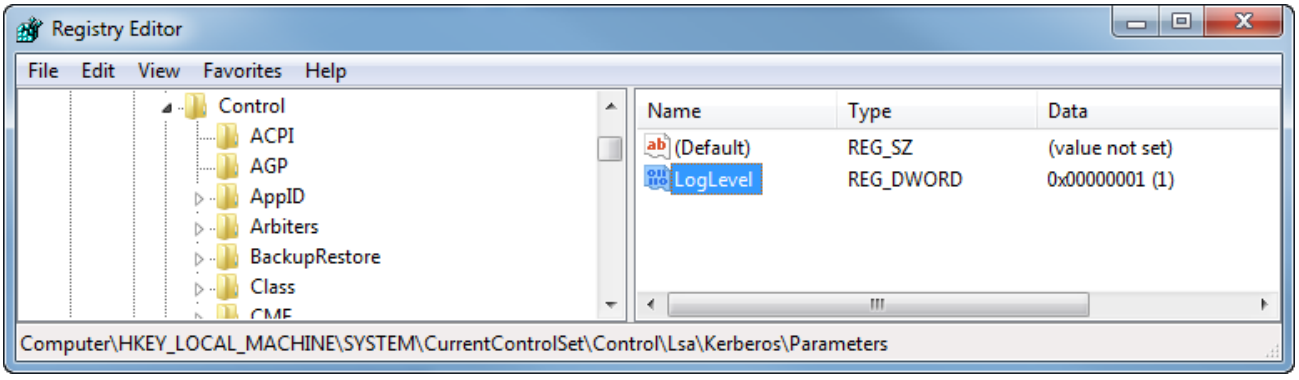
Kerberos results when it works

Kerberos Troubleshooting

It is important to first check that the Kerberos delegation failure is indeed the cause of the error you are receiving in the client. Many of the other possible causes of this error can be eliminated from consideration using the following steps:

- Restart all machines involved in the Kerberos Delegation setup. This will force services to be restarted, which is required after SPN changes, and Kerberos ticket caches to be cleared.
- Try to access the client by using a browser on the Web server itself. This will eliminate one of the credential hops and you should be able to log in. If you cannot see data, Kerberos delegation may not be the issue.
- Check the *Event Viewer Security* logs on the Web and data servers. The logs will report successes and failures and can identify if Kerberos or NTLM is being used. The audit logs in the Pyramid database will highlight what type of authentication the user was using when trying to log into the application.
- Check that database / data source security is set correctly and that the test user is a member of a role that has access to the database. It is recommended that you temporarily grant your test user membership to the server administrator role to help eliminate database security as a cause of any connection problems.
- Check that the Web server can communicate with the runtime server and that firewall ports are open. It is recommended that you temporarily disable firewalls to help eliminate them as possible causes of any connection problems. If there are firewalls between the client, Web server and runtime server, be sure that they have the correct ports open.
- Ensure the token "bloat" is not an issue (see above).
- If you are using *Constrained Delegation* on all hops, temporarily disable the constraint and retest.
    - Are you using a split domain where machines can resolve two different FQDNs? For example, when you ping the same server from two different machines and it returns different FQDNs – such as MyDataServer.Company.com as well as MyDataServer.AD.Company.com. If so, this may defeat the SPNs needed for Kerberos delegation. Please see your network administrator to verify that the DNS names being requested by the browser to the Web server match the SPNs on the server. Also, check that the DNS names requested by the Web server to the data server match the SPNs registered on the data server.
    - Troubleshoot with Network Monitor or Wireshark: [Two easy ways to pick Kerberos from NTLM in an HTTP capture.]

You may also turn on *verbose logging* to capture security traffic on your Web server and data server. http://support.microsoft.com/kb/262177



Log Level Setting in the Registry

Microsoft SQL Server Kerberos Issues

- Review the setup steps above to be sure your SPN entries are correct and that the data server, Web server and client machines have been properly configured for delegation.
- Check your SPNs and test for duplicates using a tool called `DHCheck`.
- Microsoft Kerberos Configuration Manager for SQL Server is a diagnostic tool that helps troubleshoot Kerberos related connectivity issues with SQL Server, SQL Server Reporting Services, and SQL Server Analysis Services.

  Can be found here: https://www.microsoft.com/en-us/download/details.aspx?id=39046