IOPLEX
Communications Software

http://www.ioplex.com/
support@ioplex.com
Plexcel 2.7.27
January 5, 2012

Plexcel Operator's Manual

Table of Contents

Overview

Plexcel is a PHP extension that provides a number of features ideal for integrating non-Windows systems into Windows centric networks. This document contains step-by-step instructions on how to install Plexcel. The second half of this document is dedicated to troubleshooting most issues an operator might encounter.

Requirements

To run the Plexcel PHP extension the following requirements must be satisfied.

- Linux or FreeBSD on i386 or x86_64 is required.
- PHP 4.3, 5.0, 5.1, 5.2 or 5.3 is required. The installer script also requires the CLI. The CLI is usually a separate package (such as "php-cli").
- Apache 2 or later is required.
- For Single Sign-On (SSO), clients must be members of a Microsoft Active directory domain and must be a version of Windows supported by Microsoft[1]. Web browsers must support Kerberos authentication (such as IE, Firefox on Linux, etc).
- The web server must have valid A records in DNS (more below).
- For Unicode support, Apache must run in a UTF-8 locale (more below).
- HTTP authentication mechanisms such as "Authorization: Basic" and "Authorization: Digest" will conflict with the "Authorization: Negotiate" mechanism used by Plexcel and therefore must not be used at the same time on the target resource.
- SELinux Apache access controls must be sufficiently disabled.
- Firewall rules (such as iptables) must permit UDP and TCP communication on DNS, LDAP, Kerberos and Kpasswd[2] ports (53, 389, 88 and 464 respectively).
- Installing Plexcel requires running some basic UNIX commands as root on the web server. Additionally, someone with sufficient Active Directory privileges will need to create the required HTTP service account (either using Plexcel Setup or by conventional methods).

If these requirements are satisfied, an experienced operator can install Plexcel in less than 5 minutes.

Note: For best results, try to use the stock packages provided by your OS (for example just do 'yum install php' on Red Hat systems) with default configurations. Packages like XAMPP are not recommended.

DNS

The #1 problem reported by users is DNS failure caused by not using a suitable DNS server. Please read this section carefully.

Plexcel will attempt to locate Active Directory servers by querying DNS for the below SRV records. Therefore it is very important that Plexcel be configured to use an appropriate DNS server. This section will show you how to determine if your DNS server is suitable, how to find one that is and how to set the DNS server that Plexcel should use. We will also describe how to use the phosts file to bypass some of these SRV queries.

Active Directory Sites and Services

Active Directory Sites and Services allow network architects to partition their domain controllers geographically by marking them with a "site". This greatly improves the performance of some operations. To

1 Windows 2000 SP4 is also known to work although it is not tested regularly. Non-Windows clients like Linux running Firefox will also work if properly configured.

2 The Kpasswd port may be excluded from this requirement if the operator can be certain that Plexcel will never need to set or change account passwords.

enable Plexcel to use a site, simply set it with the `plexcel.dns.site` property.

For example, if a company WAN has servers in Paris and Quebec, the following setting will ensure that Plexcel only communicate with domain controllers in Paris:

```
plexcel.dns.site = Paris
```

This property simply causes Plexcel to use the following SRV DNS lookups (assumes site is `Paris` and `example.com` domain):

```
_kerberos._tcp.Paris._sites.dc._msdcs.example.com
_ldap._tcp.Paris._sites.dc._msdcs.example.com
```

Otherwise, if the `plexcel.dns.site` property is not specified, or the above records were not found, Plexcel will use the following SRV DNS lookups (again assuming `example.com` domain):

```
_kerberos._tcp.dc._msdcs.example.com
_ldap._tcp.dc._msdcs.example.com
```

To determine what site name is appropriate for your web server look at the Active Directory Sites and Services tool or ask your WAN administrator. If you do not use the AD sites feature (because your network is not distributed geographically), you can simply leave the `plexcel.dns.site` property unset.

Testing DNS with the dig command

To determine if your DNS server will answer the necessary SRV queries, use the "dig" command as shown below on the web server (but substitute `example.com` with the AD domain that your web server is in[3] and substitute `1.2.3.4` with the IP address of the DNS server being tested).

Note: The space preceding the '@' sign is *not* a typo and must be present.

```
$ dig -t SRV _kerberos._tcp.dc._msdcs.example.com  @192.168.2.110
```

The output of the above dig command should look something like the following:

```
; <<>> DiG 9.2.4 <<>> -t SRV _kerberos._tcp.dc._msdcs.example.com  @192.168.2.110
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8538
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;_kerberos._tcp.dc._msdcs.example.com.        IN      SRV

;; ANSWER SECTION:
_kerberos._tcp.dc._msdcs.example.com. 3600 IN SRV     0 100 88 dc2.example.com.
_kerberos._tcp.dc._msdcs.example.com. 3600 IN SRV     0 100 88 dc3.example.com.
_kerberos._tcp.dc._msdcs.example.com. 3600 IN SRV     0 100 88 dc1.example.com.

;; ADDITIONAL SECTION:
dc2.example.com.              3600    IN      A       192.168.2.110
dc3.example.com.              3600    IN      A       192.168.3.10
dc1.example.com.              3600    IN      A       192.168.4.10

;; Query time: 1 msec
```

3 AD maintains mappings between domains and AD domains (just like the [domain_realms] section in a krb5.conf). Usually they are the same or it is obvious but if you're not certain, ask an AD administrator what AD domain they think your web server should be a member of.

```
;; SERVER: 192.168.2.110#53(192.168.2.110)
;; WHEN: Fri May 18 21:30:59 2007
;; MSG SIZE  rcvd: 183
```

If you see `ANSWER: 0` and an empty `ANSWER SECTION` then the specified DNS server is not suitable for use with Plexcel.

If you get a positive reply with one or more answer records, repeat the procedure for `_ldap._tcp.dc._msdcs.example.com`. If *both* of these queries are successful, then the specified DNS server should be suitable for use with Plexcel.

If you use Active Directory Sites and Services to partition your domain controllers geographically, you may also try dig with the appropriate site name like:

```
dig -t SRV _ldap._tcp.Paris._sites.dc._msdcs.example.com  @192.168.2.110
```

Finding a DNS Server

If the DNS server being tested does not answer each of the queries successfully, you will need to find an alternative DNS server that will.

> Note: All Active Directory networks require at least one DNS server that answers successfully for the above names. So if you have AD, you have a suitable DNS server – you just need to find it.

The best way to determine definitively which DNS server(s) to use, is to login to an AD server, run the following command at a command prompt, and look at the DNS Servers line in the output:

```
C:\>ipconfig /all
```

The plexcel.dns.servers INI Parameter

By default, Plexcel uses the list of nameserver entires from the web server's `/etc/resolv.conf`.

> Note: If the resolv.conf file is modified, it will automatically be reloaded after 5 seconds. The DNS client will also be disconnected so that it can re-evaluate any changes. It is not necessary to restart Apache.

However, to provide graceful failover, you should explicitly supply multiple DNS servers by using the `plexcel.dns.servers` PHP INI property. Consider the following example:

```
plexcel.dns.servers = 192.168.2.110,192.168.2.111
```

If a list of nameservers is provided, Plexcel will attempt to query each in order. If the currently selected nameserver is not responding or refuses the connection, Plexcel will automatically rotate the list and repeat pending operation. Any nameserver failure should be largely transparent to users although they may experience a brief delay while Plexcel determines that the DNS server is not responding.

> Note: Any NS records placed into the phosts file (described below) take precedence over both the plexcel.dns.servers INI property and the resolv.conf file. Both the plexcel.dns.servers property and resolv.conf will be ignored.

The Web Server Hostname

There are two issues related to the hostname of the web server.

1. The hostname within the URL used to access the target script must be a fully qualified DNS name (FQDN). An IP address in the URL will not work. Clients will not be able to acquire Kerberos tickets without an FQDN and some Plexcel functions need the domain component of the hostname to locate services and compute

SPNs.

To satisfy the above requirement, the web server will need at least one A record in the appropriate forward zone in your DNS server (but add a PTR record while your at it, more below).

2. When Plexcel asks the system for the hostname of the local system, it must be supplied with fully qualified domain name (FQDN). To determine if the web server satisfies this requirement, run the following command:

```
$ hostname --fqdn
www1.example.com
```

If the above command outputs only the first label of the name (such as `www1`) or `localhost`, you will need to change the hostname of the web server. There are a variety of ways to get the `hostname --fqdn` command to return an actual FQDN and the procedure for changing a machine's hostname depends on the system.

For Red Hat systems, the hostname is specified in `/etc/sysconfig/network`. On Debian based systems like Ubuntu, the hostname is specified in `/etc/hostname`. It may also suffice to add a PTR record to DNS but this does not always work. Another, albeit less desirable method, is to simply place the FQDN in `/etc/hosts` such that it looks something like the following example:

```
$ cat /etc/hosts
127.0.0.1  www1.example.com  localhost.localdomain  localhost
```

Using a non-Microsoft DNS Server

If you are using BIND or another DNS server, you will need to create slave zones. A slave zone (or “secondary master”) gets information for a zone from another DNS server. For example, this is useful when machines are already configured to use non-Microsoft DNS servers but also need to query zones owned by Microsoft DNS servers as well.

But unless you have other software that requires the slave zones, we recommend that you simply set the `plexcel.dns.servers` property to point Plexcel at a Microsoft DNS server.

The phosts file

The Plexcel phosts file is a text file containing DNS records that bypasses normal DNS lookups and effectively instructs Plexcel to use a specific domain controller or rotate through a set of domain controllers. The default path of the phosts file is `/var/lib/plexcel/phosts`.

The posts file format follows the common DNS "zone file" format and currently supports `SRV`, `A` and `NS` record types. Plexcel only queries DNS for a narrow subset of `SRV` records (for Kerberos and LDAP services) and only for `A` records for the target names returned in those `SRV` records.

> Note: The phosts file will be automatically reloaded within 5 seconds if it is modified. It is not necessary to restart Apache after modifying the phosts file.

The following examples illustrate how to use the phosts file. Substitute domain names, hostnames, site names and IP addresses as necessary to match your environment.

The following example will set Plexcel to use one specific domain controller:

```
; Comments are prefixed with a semi-colon
_kerberos._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc01.example.com
_ldap._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc01.example.com
```

However, if the `plexcel.dns.site` property is set, the `SRV` records will need to include the `_sites` component like the following example for a domain controller in the site "Paris":

```
; Same as above but with plexcel.dns.site component
_kerberos._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc01.example.com
_ldap._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc01.example.com
```

Records of type A are useful if a particular hostname has multiple addresses and you want Plexcel to use one specific IP address.

```
dc01.example.com IN A 10.1.2.11
```

Multiple entries for the same name may be supplied. In this case, the phosts logic will rotate through the entries to provide load-balancing.

The following phosts file example illustrates how to bypass DNS completely[4] and fix Plexcel to rotate through a set of three domain controllers at specific IP addresses with optional sites for both "Paris" and "Quebec":

```
;
; An elaborate phosts file example that uses all of the above
; features to completely[4] override DNS lookups in Plexcel
;

; SRV records for Kerberos
_kerberos._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc01.example.com
_kerberos._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc02.example.com
_kerberos._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc03.example.com

; SRV records for LDAP
_ldap._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc01.example.com
_ldap._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc02.example.com
_ldap._tcp.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc03.example.com

; SRV records for Kerberos in the site Paris
_kerberos._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc01.example.com
_kerberos._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc02.example.com
_kerberos._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc03.example.com

; SRV records for LDAP in the site Paris
_ldap._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc01.example.com
_ldap._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc02.example.com
_ldap._tcp.Paris._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc03.example.com

; SRV records for Kerberos in the site Quebec
_kerberos._tcp.Quebec._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc04.example.com
_kerberos._tcp.Quebec._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 88 dc05.example.com

; SRV records for LDAP in the site Quebec
_ldap._tcp.Quebec._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc04.example.com
_ldap._tcp.Quebec._sites.dc._msdcs.EXAMPLE.COM SRV 0 100 389 dc05.example.com

; A records for all above mentioned targets
dc01.example.com IN A 10.1.2.11
dc02.example.com IN A 10.1.2.12
dc03.example.com IN A 10.1.2.13
dc04.example.com IN A 10.1.99.11
dc05.example.com IN A 10.1.99.12
```

4 Plexcel can still query DNS for names that cannot be resolved such as _ldap._tcp.dc._msdcs.SUB.EXAMPLE.COM and therefore communication with the DNS server cannot be completely eliminated.

Note: Plexcel will also use any NS records in the phosts file as DNS servers. The nsdname must be in IP form. Both the plexcel.dns.servers property and resolv.conf file will be ignored if there are any NS records in the phosts file.

Internationalization (I18N)

By default, Apache is usually configured to run in the "C" locale which supports only ASCII text. Therefore, to ensure that internationalized text is properly handled, Plexcel requires that Apache run in a UTF-8 locale.

Note: A future version of Plexcel will eliminate this requirement and handle all necessary conversions internally.

On Red Hat Linux systems the locale Apache runs under can be set in `/etc/sysconfig/httpd`. The setting should look something like the following.

```
HTTPD_LANG=en_US.UTF-8
```

On Debian Linux based systems the locale can be set in the Apache init-script (e.g. `/etc/init.d/apache2`).

```
LANG=en_US.UTF-8
```

On FreeBSD you can set the local Apache uses by setting the LANG variable before you start Apache (we do not know how to make this change permanent – if you know please send us an email):

```
# setenv LANG "en_US.UTF-8"
# apachectl start
```

Use the `plexcel/examples/locale.php` example to verify that the value is set properly.

Note: You must have the necessary locale files installed. These files are usually in `/usr/lib/locales/`. For example, the German locate files on Ubuntu can be installed with the command `apt-get install language-pack-de-base`.

Condensed Dialog of Red Hat Install

The following is a condensed command line dialog of installing Plexcel on a Red Hat Linux system. We highly recommend that you skip this section and carefully read the full installation instructions.

```
# apachectl stop
# tar -xvzf plexcel-2.7.27.tar.gz
# cd plexcel-2.7.27
# ./install
<enter>
y<enter>
# vi /etc/php.d/plexcel.ini
```

Uncomment the `;extension=plexcel.so` line to enable the Plexcel extension.

```
# apachectl start
# cp -a plexcel /var/www/html/
```

Using a suitable browser, visit the Plexcel Setup script. The URL should look something like the following:

http://www1.example.com/plexcel/setup.php

Logon as a Domain Admin, consider any warnings in blue text and select *Create a new account* > *Create Account* > *Set Password*.

As instructed by Plexcel Setup, restart Apache:

```
# apachectl restart
```

Finally, try the examples. The URL should look something like the following:

http://www1.example.com/plexcel/examples/

Note: It is very common to get errors at this step due to browser settings and / or invalid Kerberos tickets (from resetting the account password). Consult the Possible Issues section for solutions.

Installation

Installing Plexcel involves running an install script, visiting a setup page through which an HTTP service account is created, restarting the web server and trying the examples. These steps are enumerated in detail below.

If an unexpected result or an error occurs, consult the Possible Issues section.

Step 1: As root, run the installer on the web server

Run the following commands shown below.

IMPORTANT: Always stop the web server daemon while running the installer[5].

Note: If you wish to install Plexcel in a location other than `/var/lib` you must specify the alternate path by setting the `$PREFIX` variable at the top of the file `_install` in the top directory. This guide assumes the path is `/var/lib`.

```
[root@www1 ~]# apachectl stop
Stopping httpd:                                            [  OK  ]
[root@www1 ~]# tar -xvzf plexcel-2.7.27.tar.gz
<skip output>
[root@www1 ~]# cd plexcel-2.7.27
[root@www1 plexcel-2.7.27]# ./install
Plexcel 2.7.27
Copyright (c) 2012 IOPLEX Software
http://www.ioplex.com/
PHP version 5.2.1
--
WARNING: You are about to install Plexcel 2.7.27 on this host. Are you certain you
want to do that? [y]: <enter>
<read the license agreement and enter 'y' if you agree to the terms>
Do you agree to the terms of this EULA? [n]: y<enter>
<snip verbose output>
```

Note: If you get an `ldap_sasl_bind_s: Strong(er) authentication required` error here you will need to set `plexcel.ldap.signing = On`. See Issue 13 in the Possible Issues section for details.

Note: If you get a `cannot restore segment prot after reloc: Permission denied` error running the install script, you need to disable SELinux. See Issue 6 in the Possible Issues section.

Note: If the installer complains about not being able to find php, you most likely need to install the php-cli package. Or, if you are using a custom installation of PHP, you will need to modify the install script to point to the php CLI of your custom install. The install script needs the CLI to determine the proper PHP modules directory, binary version, etc.

Step 2: Activate the Plexcel extension and start Apache.

Uncomment the `;extension=plexcel.so` line in the Plexcel INI file (default locations are `/etc/php.d/plexcel.ini` on Red Hat Linux and `/usr/local/etc/php/plexcel.ini` on FreeBSD).

```
[root@quark plexcel-2.7.27]# vi /etc/php.d/plexcel.ini
<enable the extension by uncommenting the ";extension=plexcel.so" line>
```

If you do not have a php "scan" directory for INI files (e.g. `/etc/php.d` on Red Hat Linux) you will need to add the contents of the `plexcel.ini` to your `php.ini` (the convention is to add it at the end).

5 Updating libraries while a server is running can cause it to crash and leak semaphores.

Now start Apache. The Plexcel extension should be loaded when Apache initializes PHP. If the extension fails to load, error messages may be logged in the Apache error log (`/var/log/httpd/error_log` on Red Hat systems) or in the Plexcel log file (/var/lib/plexcel/plexcel.log by default). If the Plexcel extension is loaded successfully, check the Plexcel log file for any error messages. The last log entry should contain the text "Plexcel Context Initialized":

```
[root@www1 plexcel-2.7.27]# apachectl start
Starting httpd:                                            [  OK  ]
[root@www1 plexcel-2.7.27]# tail -5 /var/lib/plexcel/plexcel.log
<snip verbose output>
Mar  3 12:43:30 src/plexcel.c:388:plexcel_ctx_new: Plexcel Context Initialized:
version=2.7.27,uid=0,pid=29296,ctx=0x8e315d8,pnet=...
```

Note: If the log reports Plexcel Context Deinitialized on startup or if it does not initialize at all and the extension is in fact enabled, see Issue 6 about SELinux in the Possible Issues section.

Step 3: Copy the Plexcel Setup script and examples into a PHP enabled location

The Plexcel setup script and examples are in the `plexcel-2.7.27/plexcel` subdirectory. Copy that entire directory into a PHP enabled location. For example, if `/var/www/html/` is a PHP enabled location, the following command could be used:

```
[root@www1 plexcel-2.7.27]# cp -a plexcel /var/www/html/
[root@www1 plexcel-2.7.27]# ls /var/www/html/plexcel/
common.php  config.php  examples/  plexcel.php  PlexcelTest.php  setup.php  style.css
```

Note: If Apache is configured to follow links you can also create a soft link with `cd /var/www/html` and then `ln -s /path/to/plexcel-2.7.27/plexcel`.

Step 4: Use Plexcel Setup to create the service account in AD and restart Apache

Plexcel requires an HTTP service account in Active Directory to act as the acceptor when performing Single Sign-On (SSO) authentication with web clients. The Plexcel Setup script (`plexcel/setup.php`) uses Plexcel functions to communicate with AD and create the required account.

If you want to setup the account in AD manually instead of through Plexcel Setup, you may skip this step and follow the section titled *Creating the HTTP Service Account in Windows without Plexcel Setup*.

If the plexcel directory was copied into the document root of the web server (e.g. `/var/www/html` on Red Hat Linux systems) the following example URL might be used to invoke Plexcel Setup:

`http://www1.example.com/plexcel/setup.php`

Note: The hostname in the URL used to run Plexcel Setup should be a hostname that users will be using when the site is complete. Plexcel Setup will use this hostname has the basis for some default values.

Accessing this script should present a domain controller selection screen. Enter the domain or specific domain controller on which the service account should be created. If a domain controller is found successfully, you will be asked to login.

Because the HTTP service account is required to query the directory and for SSO to work, you must initially logon manually using a qualified UPN like `administrator@example.com`. The credentials used must have the privileges necessary to create and modify accounts in AD.

After successfully logging on, select:

Create a new account > Create Account > Set Password

Read the blue text carefully to follow your progress (for example - if a valid account was already setup you will

see an “appears to be correct” message). Error messages appear in dark red text.

If the password on the HTTP service account is reset for any reason, the web server must be restarted to recognize it[6].

```
[root@www1 plexcel-2.7.27]# apachectl restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

If Apache starts cleanly, the Plexcel extension should be fully functional at this point.

Step 5: Check browser settings and try the examples

Before Internet Explorer will perform Single Sign-On (SSO), you must first add the target domain to IE's security settings. Go to *Internet Explorer* > *Tools* > *Internet Options* > *Security* > *Local intranet* and add the hostname or domain suffix for the target web server. For example, if the URL of the page is *http://www1.example.com/plexcel/examples/* you will need to add either *www1.example.com* or **.example.com* to the local intranet zone.

Note: In practice these settings should be deployed as a GPO. See the Adding Trusted Sites using Group Policy Objects (GPO) section for details.

Note: See Appendix B for Firefox instructions.

Now visit the examples directory at the below url (substituting your hostname and `plexcel` directory location accordingly):

```
http://www1.example.com/plexcel/examples/
```

This should present a "Plexcel Examples" page[7]. Try the whoami example. If it displays account information about the client you are currently logged in as, SSO is working and the installation is complete.

If clients have not previously been configured to perform Kerberos authentication through the browser, it is not uncommon to get errors at this step due to browser settings described in the Possible Issues section.

Note: If you get a `GSS_S_BAD_MECH` error here, see Issue 3 in the Possible Issues section.

Step 6: Reduce log level and configure log rotation

After you see Plexcel working in a production environment you should set the `plexcel.log.level` INI property to 2 or possibly 1. This will significantly reduce the information being logged thereby saving disk space and increasing application performance.

Additionally, you should add the plexcel log file to your log rotation configuration. The following is an example `/etc/logrotate.d/plexcel` file for Red Hat Linux:

```
/var/lib/plexcel/plexcel.log {
    missingok
    notifempty
    sharedscripts
    postrotate
        /etc/init.d/httpd restart >/dev/null 2>&1 || true
    endscript
}
```

6 Setting the password in the Plexcel Setup page also generates a credential file called a "keytab" in the plexcel tmp directory (/var/lib/plexcel/tmp/plexcel.keyab). When the web server is restarted it detects the new keytab file and moves it up into the Plexcel home directory where the extension proceeds to initialize as usual. See the Keyab Files section for details.

7 Unless you do not have directory indexes for index.php enabled in which case you will need to click on index.php

Note: The above postrotate command will start Apache even if it was not previously running.

Note: You can move the Plexcel log file using the plexcel.log.path INI property (e.g. plexcel.log.path = /var/log/plexcel.log).

Creating the HTTP Service Account in Windows without Plexcel Setup

Instead of requiring an administrator to login through Plexcel Setup, you can alternatively create the account entirely on the Windows side. The procedure below replaces Step 4. When you have completed it, return to Step 5 above.

1. To create the Plexcel HTTP service account using your conventional methods do the following:
2. Create a regular User account as you would normally minus any exceptions noted herein.
3. On the Account tab, un-check the 'User must change password at next logon' option.
4. Check the 'Password never expires' option. This is not required but if you do not check this option you will need to periodically reset the password in both Windows and Plexcel or Plexcel will stop functioning when the password expires.
5. On the Delegation tab, select the 'Trust this user for delegation to any service (Kerberos only)'. This is also not required but some operations may be significantly slower[8].
6. Set the account password (and remember it).
7. Finish creating the account (such as clicking *Finish* in ADUC).
8. Login to Plexcel Setup (you do not need to be a privileged user) and make a note of the SPN that Plexcel wants the account to have. You should see it in bold blue at the top of the page like the below example for SPN 'HTTP/wiki5.example.com':

   No accounts with the target SPN of **HTTP/wiki5.example.com** were found. Please select one of the options below.

9. Go back to Windows and add that SPN to the account. The setspn.exe utility may be used to do this as shown below (you can also use ADSI Edit or Plexcel Setup) but there are two important notes.

   a) You must use capital 'HTTP' in the SPN (such as HTTP/wiki5.example.com and *not* http/wiki...).

   b) You must use the SAM account name to identify the account. The CN does not appear to work.

   The following command demonstrates how to add an SPN to the service account using setspn.exe:

```
C:\tmp>setspn -A HTTP/wiki5.example.com wiki5_sso
Registering ServicePrincipalNames for CN=Wiki5 SSO,CN=Users,DC=example,DC=com
        HTTP/wiki5.example.com
Updated object
```

   Note: This command can take a few minutes to complete.

   Note: If you are doing virtual hosting, you may want to add more SPNs now. You must reset the password in Plexcel Setup as described in the next step after adding any SPNs to the HTTP service account. See the section on Virtual Hosting for details.

10. Go back into Plexcel Setup and search on the account you just created using the search box. You can enter a CN (e.g. 'Wiki5 SSO') or SAM account name (e.g. 'wiki5_sso').
11. Click on the account to view it and verify that the blue text indicates that the required SPN is correct. The blue text should read something like 'This service account has the required SPN HTTP/wiki5.example.com.'

8 If the HTTP service account is not 'Trusted for delegation', Plexcel will have to acquire a TGT to initiate authentication with other services. This can add ~200ms to request processing and may occur with every request depending on how Plexcel is being used.

12. Un-check the 'Set password in Active Directory' checkbox, enter the correct password for the account and click Set Password. If successful, you should see blue text to that effect that says 'the web server must now be restarted'.
13. Restart Apache and proceed with Step 5: Check browser settings and try the examples.

Possible Issues

Issue 1: The “GSS_S_FAILURE: Failed to find in keytab” error:

```
GSS_S_FAILURE: Failed to find HTTP/www1.example.com@EXAMPLE.COM(kvno 3) in keytab
MEMORY (arcfour-hmac-md5)
```

This error means that the particular principal, key version number and encryption type combination in the Kerberos ticket supplied by the client (from the domain controller) during authentication did not match an entry in the local credential file (the `/var/lib/plexcel/plexcel.keyab` file).

This error can occur if the hostname used to access the website does not have a corresponding SPN set on the service account. For example, if the URL used to access the website was *http://www1.example.com/*, the service account must have an SPN of *HTTP/www1.example.com*. Trying to use another name or an IP address will fail with this error.

> Note: SPNs are case-sensitive. If users enter a URL like http://www1.Example.com, that will not match an SPN of HTTP/www1.example.com. Users must use the correct case or the SPN must be changed or multiple SPNs must be added as necessary to satisfy the difference in case.
>
> Note: If the hostname of your website is a CNAME in DNS, you may need to add additional SPNs for both the CNAME and real FQDN hostname as some browsers may try to traverse these names when acquiring a Kerberos service ticket.

This error will also occur if the password on the HTTP service account has been changed but the client is using a cached ticket with an old key version number (kvno).

To resolve this issue, purge the clients cached tickets with kerbtray.exe (see *Purging Kerberos Tickets with Kerbtray.exe*). Logging off of the client and back on may also be sufficient to purge cached tickets. If the problem persists, try resetting the password on the HTTP service account using Plexcel Setup and purging client's tickets again. If the problem still persists, use klist to list the contents of the Plexcel keytab file:

```
# klist -k -e /var/lib/plexcel/plexcel.keytab
Keytab name: FILE:/var/lib/plexcel/plexcel.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 http_sso_www1@EXAMPLE.COM (ArcFour with HMAC/md5)
   2 HTTP/www1.example.com@EXAMPLE.COM (ArcFour with HMAC/md5)
```

The above example shows that the SPN and encryption type match correctly but that the key version number is wrong. In this case the client supplied a KVNO of 3 which means the keytab file is old (it has KNVOs of 2) and therefore the password needs to be reset.

Although unlikely, this error can also occur if the target SPN exists in a different domain and that SPN is masking the correct account. If the domain of the principal name in the error message (EXAMPLE.COM above) is incorrect, check that domain for an old or errant account with the target SPN and delete it (or delete the SPN). Then purge tickets and try again. In general SPNs should be unique throughout the entire organization.

Issue 2: The "unable to reach any KDC in realm" error.

The following error means that Plexcel could not communicate with an Active Directory server:

```
src/gss.c:705:psec_gss_init_sec_context: GSS_S_FAILURE: unable to reach any KDC in
realm EXAMPLE.COM: jespa1@EXAMPLE.COM: ldap/dc1.example.com@EXAMPLE.COM
  src/ldapx.c:412:ldapx_bind_gssapi:
  src/ldapx.c:1084:ldapx_bind:
```

Note: This error message text is not accurate. It should read simply "unable to reach KDC". Plexcel always selects a KDC to communicate with before trying a Kerberos operation (dc1.example.com in the above example).

The most common cause of this error is an inaccessible AD server in which case Plexcel (depending on how it was called) should gracefully failover to another server. See the various plugins and modules for examples of how to implement sophisticated server "stickyness" and failover.

Another possible cause of this error is insufficient DNS configuration. On the web server, use the “dig” command to simulate the DNS query being used by the Plexcel Kerberos libraries. Try the following command but substitute `EXAMPLE.COM` with your domain.

```
$ dig -t SRV _ldap._tcp.dc._msdcs.EXAMPLE.COM
```

A correct response has an `ANSWER SECTION` that lists a valid Active Directory server (`ad1.example.com` in the example below):

```
;; ANSWER SECTION:
_ldap._tcp.dc._msdcs.EXAMPLE.COM. 600 IN    SRV     0 100 389 ad1.example.com.
```

If DNS is returning correct responses, verify that the web server can communicate with the AD server using telnet as follows:

```
$ telnet ad1.example.com 389
Trying 10.1.2.110...
Connected to ad1.example.com.
Escape character is '^]'.
```

If telnet does not report "Connected to", then the server is not listening or the network is blocked.

See the *Requirements* section for details regarding DNS and firewall configuration.

Issue 3: The “GSS_S_BAD_MECH” error

The following error can occur trying to authenticate using Single Sign-On (SSO):

```
src/gss.c:369:psec_gss_accept_sec_context: GSS_S_BAD_MECH
  src/plexcel.c:748:plexcel_accept_token:
```

There could be a number of reasons for this error. These include the following:

1. The hostname used to visit the site must have a corresponding SPN set on the HTTP service account. Any hostname without an SPN such as a short hostname or IP address will not work and may generate this error[9]. See the *Installation* section for details regarding adding SPNs to the service account.
2. The target server must be listed in the browser's "trusted sites". See Step 5 in the Installation section

9 An IP address will work if the IP is added to the browser's trusted sites list but in this case the browser is simply treating the IP address as though it were a name. Trusted sites are identified by hostname and therefore we recommend that you use a real hostname.

for details.

3. The client could not obtain a Kerberos ticket from the domain controller. This can occur if the domain controller was momentarily unavailable, the client is not joined to the domain or the client's network configuration is blocking communication with the domain controller. For example, a laptop running over a VPN or running multiple network interfaces may not be able to properly communicate with a suitable DC.
4. Integrated Windows Authentication is not enabled. Go into *Internet Explorer > Tools > Internet Options > Advanced* > scroll all the way to the bottom and check "*Enable Integrated Windows Authentication (requires restart)*"[10].
5. There is a problem with the Kerberos service principal and the client is falling back to trying NTLM. Go back into to Plexcel Setup (`plexcel/setup.php`) and check for warnings in blue text about SPNs. For example, this error will occur if the target SPN is not set on the HTTP service account or if there are multiple service accounts with the same SPN. Plexcel Setup will warn the operator about both of these conditions.
6. The HTTP service account is disabled.
7. Plexcel requires a browser that can perform Kerberos authentication. See Issue 5 for a list of requirements for clients to properly negotiate Kerberos.
8. If credentials are submitted through the Network Password Dialog, the browser will remember them and continue to submit them using NTLM authentication even after fixing whatever problem caused the Network Password Dialog to appear originally. To purge save passwords check *Control Panel > User Accounts > Advanced > Manage Passwords* and make sure that there are no credentials saved for the target site.
9. Prior to Plexcel 2.5.0 there was a bug in Plexcel Setup (setup.php) that could cause this error.
10. This error may be an artefact of Issue 1. See Issue 1 solutions.

If none of these tests help resolve the issue, the next step is to narrow down which subsystem is responsible for the failure (is it the client or the server?). Some simple things to do is to login as a different user, try a different workstation, etc. If the problem persists then you should focus on the HTTP service account or DNS. Otherwise, the problem could be with the client such as browser settings.

See also the section on *Diagnosing Problems with wfetch.exe* which is very useful for diagnosing problems with Kerberos protected sites because it will tell you definitively if the problem is on the client or elsewhere.

Issue 4: The browser displays a "Kerberos Authentication Required" page.

The "Kerberos Authentication Required" page is displayed when the web browser fails to negotiate Kerberos authentication. The below list of reasons for this error are displayed on the error page itself.

- Your web browser does not support Kerberos authentication using the WWW-Authenticate: Negotiate method.
- Your web browser is not configured to negotiate WWW-Authenticate: Negotiate authentication.
  - For IE, check *Tools > Internet Options > Advanced* > scroll all the way to the bottom and select *Enable Integrated Windows Authentication (requires restart)*.
  - For IE, the target site may need to be added to the IntrAnet zone in your security preferences.
  - For Firefox you must add the target site or domain to both the *network.negotiate-auth.trusted-uris* and *network.negotiateauth.delegation-uris* properties.
  - If your browser is configured to use a proxy, the target site must be excluded from communication with the proxy server. For IE check *Tools > Internet Options > Connections > LAN Settings > Advanced* and add the URL prefix of the target site to the *Exceptions* box.

10 See also http://support.microsoft.com/kb/299838/ Unable to negotiate Kerberos authentication after upgrading to Internet Explorer 6.

- Your Kerberos ticket has expired.

Issue 5: Clients are not negotiating Kerberos.

Microsoft clients that support Integrated Windows Authentication (IWA) always attempt to negotiate Kerberos and then fall-back to NTLM. Plexcel only supports Kerberos authentication. It does not support NTLM at this time. Therefore if clients do not negotiate Kerberos authentication for any reason, Plexcel will not work.

For Microsoft clients to successfully authenticate using Kerberos, the following requirements must be satisfied. In a large Intranet environment all of the configuration options listed here should already be set correctly by default.

1. The client workstation must be running a version of Windows that is currently supported by Microsoft[11]. Previous versions of Windows or "Home Edition" versions may not support Integrated Windows Authentication.
2. The domain controller must be a version of Windows Server that is supported by Microsoft[12].
3. The client workstation must be joined to the target Windows domain or a domain with a trust relationship with the target domain. Check *Start* > *Control Panel* > *System* > *Computer Name* tab > *Change* ... and make sure the client is a member of the correct domain and not just a workgroup.
4. The user logged into the workstation using IE must be logged into the domain. Check *Ctrl+Alt+Del* and look at the "You are logged on as" dialog. The Windows domain shown must be the target domain and not the local machine name.
5. Integrated Windows Authentication (IWA) must be enabled. Check *Internet Explorer* > *Tools* > *Internet Options* > *Advanced* > scroll all the way to the bottom and make sure "*Enable Integrated Windows Authentication (requires restart)*" is checked.
6. Automatic logon must be enabled. Check *Internet Explorer* > *Tools* > *Internet Options* > *Security* > *Custom Level* > scroll all the way to the bottom and make sure "*Automatic logon only in Intranet zone*" is selected.
7. The target website must be listed in the Local IntrAnet zone. Check *Internet Explorer* > *Tools* > *Internet Options* > *Security* > *Local intranet* and make sure that the target domain or host is listed there (such as **.example.com*).
8. If your browser is configured to use a proxy server, the target site must be added to the exceptions list. Integrated Windows Authentication may not work through a proxy.
9. The network time protocol (NTP) must be functioning properly or some other method must be used to ensure that the time on the client, web server, and domain controller are all exactly in sync (at least within several minutes).

If the above requirements are not satisfied, the application may fall-back to the HTML form based on dialog. Otherwise a `GSS_S_BAD_MECH` error may occur or IE will display the "Kerberos Authentication Required" page.

Issue 6: SELinux causes “cannot restore segment prot after reloc” error

SELinux is a Linux kernel security feature that limits what certain processes can do. Plexcel reads a number of files, loads libraries, writes to the plexcel.log file, communicates over the network and does a number of things that the default SELinux configuration will not permit. This can cause PHP to emit errors like:

```
PHP Warning: PHP Startup: Unable to load dynamic library
'/usr/lib/php/modules/plexcel.so' - /usr/lib/php/modules/plexcel.so:
```

11 Windows 2000 is known to work although it is not tested regularly. Non-Windows clients such as Linux running Firefox also work if configured properly.
12 Windows 2000 Server is known to work although it is not tested regularly.

```
cannot restore segment prot after reloc: Permission denied in Unknown on line 0

or

peer_listen: EACCES: bind: /var/lib/plexcel/plexcel.supersock
...
plexcel_ctx_new: The Plexcel context could not be initialized.
```

SELinux can also cause Plexcel to deinitialize immediately after Apache starts (or not initialize at all) and will produce a variety of permissions errors and warnings in the Plexcel and system log files (/var/lib/plexcel/plexcel.log and /var/log/messages).

The easiest way to resolve this issue is to simply disable SELinux by editing `/etc/selinux/config` and setting:

```
SELINUX=permissive
```

If you wish to disable only the specific behavior necessary for Apache and Plexcel to coexist with SELinux, then you will need to examine the SELinux warnings as you encounter them and make changes accordingly.

Issue 7: The "KRB5: Clock skew too great" error

The following error can appear in the browser or the plexcel.log file:

```
src/creds.c:362:psec_logon_with_password: KRB5: Clock skew too great
  src/plexcel.c:712:plexcel_logon:
```

This error means that the time difference between the web server, AD server or client is too large for Kerberos authentication to occur. The Kerberos protocol requires that this difference be within a short time (usually 5 minutes).

To remedy this problem, start by trying to set the time on the web server by running the following commands as root:

```
# ntpdate clock.redhat.com
# hwclock –systohc
```

Note: Ideally you should enable and configure the NTP client and use a local NTP server.

If you still get the same error and the time on the web server is correct, make sure the time on domain controllers and clients is also correct.

Note: When setting the time in Windows (e.g. using the `time` command in a command prompt), make sure that AM vs PM, the day, ... etc is correct.

Issue 8: The "Failed to find DC" error

When running Plexcel Setup, if you repeatedly get "Failed to find DC" and you are certain you are entering a proper DNS suffix that corresponds to an AD domain, this is a strong indication that your DNS configuration is not correct. Please refer to the section on DNS.

Issue 9: The "GSS_S_FAILURE: Decrypt integrity check failed" error

This error means that the encryption key used to decode the client's ticket was incorrect. The cause of this

issue is essentially the same as Issue 1. Proceed with the solution for Issue 1.

Issue 10: The "Size of a request header field exceeds server limit"

This error will occur if the user's group membership causes the SPNEGO token to exceed the size of Apache's maximum request header size which by default is 8192 bytes.

There are generally three ways to address this issue.

1. Administrators in large organizations should try to reduce, refactor or eliminate obsolete groups so as to prevent large security tokens which can slow down authentications and congest the network. There are several tools available from Microsoft that may be used to assist in this process the most common of which is the `tokensz` utility.
2. Apache 2.0.53 and later permits increasing the maximum request header size. Add the following to your http.conf and restart Apache:
   `LimitRequestFieldSize 16382`
3. The size of the SPNEGO token can be significantly reduced by setting the `NO_AUTH_DATA_REQUIRED` (0x02000000) flag of the `userAccountControl` attribute on the HTTP service account. You can also use the 'acctmgr.php' example that comes with Plexcel to check the 'Do not include PAC information in Kerberos tickets' option on the HTTP service account. Note that this will have a negative impact on performance (see Issue 16).

Issue 11: The "domain cannot be queried by NetBIOS name" error

The above error occurs when Plexcel cannot retrieve domain information using the NetBIOS domain name. However, Plexcel can easily retrieve domain information by DNS domain name (such as with *example.com* instead of *EXAMPLE*) and will cache that information so that subsequent request for the NetBIOS domain name are successful. Therefore, to remedy this problem, set the `plexcel.precache.domains` INI parameter to a comma separated list of DNS domains that should be retrieved and cached when the server initializes like:

```
plexcel.precache.domains = example.com,sales.example.com,research.example.com
```

Issue 12: The plexcel_is_member_of function does not see all groups

If `plexcel_is_member_of` is not seeing all groups, check to see if your domain is running in "mixed mode". Windows "mixed mode" domains do not support Domain Local groups (except on domain controllers). If you wish to use Domain Local groups with Plexcel you have to options:

A) Increase the domain functional level to "Windows 2000 native" or higher.

B) Use the `plexcel.use_ldap_groups = 0`n INI property (added in 2.6.2). Turning on the `plexcel.use_ldap_groups` property will cause Plexcel to retrieve group information from the directory. Note that the `plexcel.use_ldap_groups` behavior is significantly slower as it requires communicating with the directory.

Issue 13: The "ldap_sasl_bind_s: Strong(er) authentication required" error

If your domain controllers have the setting *Domain Controller Security Policy > Local Policies > Security Options > Domain controller: LDAP server signing requirements* set to *Require signing*, you will get the following error:

```
src/ldapx.c:331:_bind_rfc2222: ldap_sasl_bind_s: Strong(er) authentication required:
```

```
00002028: LdapErr: DSID-0C09018A, comment: The server requires binds to turn on
integrity checking if SSL\TLS are not already active on the connection, data 0, vece
  src/ldapx.c:876:ldapx_bind:
  src/ldapx.c:159:ldapx_new:
```

To fix this issue, you must set `plexcel.ldap.signing = On` in your PHP INI file.

You may also set `plexcel.ldap.encryption = On` to indicate that all LDAP communication must be encrypted. These options can also be specified on a per-context basis using `plexcel_new` options. See the `plexcel_new` API documentation for details.

Issue 14: The "ENOSYS: Currently a domain cannot be queried by NetBIOS" error

This error occurs the first time Plexcel is asked to lookup domain information using only the NetBIOS name. For example, if you restart the web server and immediately try to perform an explicit login such as the MediaWiki's login form with a name like ACME\abaker, the NetBIOS domain ACME is yet unknown and because Plexcel does not support NetBIOS name lookups, it has no way to proceed.

The solution for this error is the same as Issue 11.

Issue 15: The "PLEXCEL_LDAP_UNWILLING_TO_PERFORM" error

This error is coming from the AD server and can occur under a wide variety of conditions. In general, this error indicates that the caller does not have permission to perform the operation or that the operation is not valid.

For example, this error will occur if you attempt to add a group to the memberOf attribute of an account. This is an invalid operation because the memberOf attribute is computed based on the member attributes of groups. Adding a member attribute to a group instead will automatically update the corresponding memberOf attribute on each account.

If you believe the problem is related to permissions, set `plexcel.log.level = 3` in your PHP INI, restart Apache if necessary, perform the errant operation and examine the log file for entries like the following:

```
initiator: abaker@ACME.NET target: ldap/dc1.acme.net@ACME.NET
```

In the above case, the caller initiating authentication is `abaker@ACME.NET`. Consider whether or not this account should have permission to perform the target operation (for example, to add, modify or delete accounts and groups in AD, the caller must be an Account Operator, Domain Admin or Administrator).

If the identity in the log is the HTTP service account (e.g. `http_sso_wiki5@ACME.NET`) check your delegation settings. If Plexcel cannot acquire a credential for the caller's identity it will fall-back to using the HTTP service account credential which, by default, does not have permission to perform many common operations.

To check your delegation settings, the service account must have the "Account is trusted for delegation" account option checked and the account of the user must *not* have "Account is sensitive and cannot be delegated" checked. Browser settings can also affect the caller's delegated credential. See Appendix A regarding Firefox's `network.negotiate-auth.delegation-uris` setting.

Issue 16: The "PAC not found in Kerberos ticket" log message

Kerberos tickets issued by AD contain a special authorization-data field called a PAC that includes account info and group SIDs which are used by Plexcel to perform group based access control checks. Under unusual circumstances the PAC may not be present which, with a sufficiently high log level, will result in the following log message:

```
src/pac.c:536:psec_gss_build_psec: PAC not found in Kerberos ticket, querying
directory (this is slower)
```

If no PAC is present, Plexcel will fall-back to querying AD for account and group information[13] if that information is required within a script. This can have a negative performance impact. Group access checks will be approximately 8 to 10 times slower (~0.025 seconds without PAC vs ~0.003 seconds with PAC). For this reason, it is recommended that the operator identify and change the setting responsible for the missing PAC. For example, if the `NO_AUTH_DATA_REQUIRED` (0x02000000) flag of the `userAccountControl` attribute on the HTTP service account is on, no PAC will be included in Kerberos tickets issued for that service.

Note: The *Do not include PAC information in Kerberos tickets* option in the "acctmgr" example that comes with the Plexcel package can be used to change the NO_AUTH_DATA_REQUIRED value on an account.

Issue 17: The "str_decode: EILSEQ" error

This error indicates that the web server is not running in a UTF-8 locale. See the Internationalization (I18N) section for details.

Issue 18: SELinux causes "EACCES: bind: /var/lib/plexcel" error

If this error appears in the Plexcel log file while trying to start Apache, the most likely cause is that SELinux is not sufficiently disabled. See issue 6.

Upgrading

To upgrade an existing installation, stop Apache, run the install script in the new package, re-copy the plexcel subdirectory into it's appropriate location and start Apache. Old libraries will be deleted and replaced with new ones as necessary. The license.key, phosts, and krb5.conf files will not be replaced.

Uninstalling

To uninstall Plexcel run the installer with the -u option and press 'y<enter>' twice.

```
[root@www1 plexcel-2.7.27]# ./install -u
... about to UNinstall Plexcel on this host! Are you certain you want to do that?
[n]: y<enter>
Do you want to delete everything including the keytab file? [n]: y<enter>
<snip verbose output>
```

Advanced Topics

The following sections are informational only. They may be helpful when diagnosing problems and making customizations.

Examining the Plexcel Log File

When diagnosing problems, the first place to look is the Plexcel log file (usually `/var/lib/plexcel/plexcel.log`). Even though the scripts and installer provide some diagnostic information, it may be different or incomplete when compared to the Plexcel log file.

13 The fall-back behavior was introduced in Plexcel 2.7.17. Prior to that update, a missing PAC result in an error: psec_gss_get_NetrSamInfo2: GSS_S_FAILURE: No such file or directory

Before trying the operation you are attempting to diagnose, run the following command in a large terminal window:

```
[root@www1 plexcel-2.7.27]# tail -f /var/lib/plexcel/plexcel.log
```

Press <enter> once to create a blank line thereby marking the last position in the log. Now perform the errant operation and examine the entries that appear after the blank line.

Purging Kerberos Tickets with Kerbtray.exe

Clients cache Kerberos tickets. If a client has previously tried to authenticated with Plexcel, any number of things can invalidate it's ticket (such as resetting the service account password) resulting in subsequent errors (probably the "*failed to find ... in keytab*" error). In this case, you must clear the ticket cache so that the client will acquire a new ticket. If Plexcel is not working, clearing the ticket cache is frequently necessary at some point.

There are two ways to clear a client's Kerberos ticket cache. One is to reboot the client computer (logging off and back on may also be sufficient). A more efficient way is to use the kerbtray.exe utility.

To purge Kerberos tickets on XP clients with the kerbtray.exe utility, download and install the Resource Kit Tools package from Microsoft's website. Locate and run the newly installed kerbtray.exe utility. This will display a small green icon in the client's systray. Right-click on the icon and select *Purge tickets*. Now try to visit the protected page again.

Note: Kerbtray may not update it's display when tickets change. It may be necessary to close and restart it.

Diagnosing Problems with wfetch.exe

The wfetch.exe utility from the IIS Resource Kit can be very useful when trying to diagnose problems with Kerberos protected sites. Wfetch operates completely independently of any browser settings and the current logged on user which eliminates a lot of guesswork.

To get the wfetch.exe utility, download and install the IIS Resource Kit Tools package from the following page:

http://support.microsoft.com/kb/284285

The installer gives you the option to install only the wfetch.exe utility if desired. Like kerbtray.exe, it is also a self contained executable that may be copied to another machine (of the same architecture) or launched from a network drive.

To use wfetch.exe to test a Plexcel protected site, launch it and enter the FQDN of the web server (like wiki5.example.com), the path to the whoami.php script (like /plexcel/examples/whoami.php), select 'Negotiate' for the authentication method, enter the domain, username and password and click *Go*.

If you get a `GSS_S_BAD_MECH` error, that indicates the problem is with getting the Kerberos ticket from the domain controller and rules out browser settings. If it works, whereas IE returns `GSS_S_BAD_MECH`, this suggests the problem is with browser settings.

Virtual Hosting

If you are serving multiple hostnames with the same web server instance, Plexcel should work using the default installation. However, under special circumstances, or with some browsers, it may be necessary to add the SPNs for all of the hostnames that will be used in URLs to the HTTP service account using Plexcel Setup.

For example, if you are serving content for *http://www1.example.com/* and *http://as1.example.com/* from the same Apache instance, you may need to have both the *HTTP/www1.example.com* and

HTTP/as1.example.com SPNs set on the HTTP service account. Go to Plexcel Setup (it does not matter which hostname is used to access Plexcel Setup) and select the HTTP service account. Add the additional SPNs, reset the password and restart Apache. Note that users who have cached Kerberos tickets will need to purge them by logging off and back on (or with kerbtray.exe).

Keytab Files

Plexcel stores the HTTP service account credential (the encryption key representing the service password) in what is known in Kerberos speak as a “keytab” file. It is not important to know about keytab files and as such this fact is hidden from the operator by Plexcel Setup. However, for the benefit of operators performing advanced analysis, the following is a detailed description of how Plexcel creates and uses keytab files.

When an operator clicks on the "Set Password" button in Plexcel Setup, in addition to (re)setting the password in AD, it also generates a keytab file in the Plexcel tmp directory (`/var/lib/plexcel/tmp/plexcel.keytab`). When the web server is restarted, the Plexcel extension initialization routine sees this file, moves it into the parent directory, changes it's permissions so that only root can access it, and loads it into an in-memory only table. The `plexcel.keytab` file is loaded once at startup. These precautions are necessary to prevent other users from accessing the keytab file as it is effectively the password for the HTTP service account.

When the keytab file is created, the key is actually duplicated for the UPN and all SPNs. This is why the password must be reset after changing the list of SPNs. You can use the “ktutil” command to list the keys in the `plexcel.keytab` file as illustrated by the following example. This example shows that the keytab file has entries for the UPN of the account and it's two SPNs.

```
[root@www1 plexcel-2.7.27]# ktutil -k /var/lib/plexcel/plexcel.keytab list
/var/lib/plexcel/plexcel.keytab:

Vno  Type              Principal
  5  arcfour-hmac-md5  http_sso_www1@EXAMPLE.COM
  5  arcfour-hmac-md5  HTTP/www1.example.com@EXAMPLE.COM
  5  arcfour-hmac-md5  HTTP/as1.example.com@EXAMPLE.COM
```

Adding Trusted Sites using Group Policy Objects (GPO)

A Group Policy Object (GPO) can be used to add your website to the trusted intranet zones of all IE clients in a domain. Otherwise, it will be necessary to modify each client's security settings manually. To add trusted sites using a GPO, Launch Active Directory Users and Computers (ADUC), right click on the domain the clients are in, select *Properties* > *Group Policy* > *New*, type in a name for the GPO (like "IE Security Settings") and then select *Edit* > *User Configuration* > *Windows Settings* > *Internet Explorer Maintenance* > *Security* > *Security Zones and Content Ratings*. Select *Import the current security zones and privacy settings* > *Modify Settings* > *Trusted Sites* > *Sites* and add your Plexcel protected websites just as you would on a client. Then wait for the policy to propagate throughout the domain.

Appendix A: Firefox Configuration

Just like IE, Firefox must also be explicitly allowed to perform HTTP Negotiate authentication. Unlike IE's security "zones", Firefox does not have a UI for these settings. Instead, you must do the following:

Into the Firefox address bar type *about:config* and hit <enter>. This will display a simple property editor. Search on the word "negotiate" to isolate the network-negotiate-auth.* properties. Modify the following properties but substitute example.com with the FQDN domain of the target web server (as seen in the URL entered into the address bar):

network.negotiate-auth.trusted-uris = example.com
network.negotiate-auth.delegation-uris = example.com

Note: In theory these settings could be deployed within a .js file as a GPO.

Beware that if you do not set **network.negotiate-auth.delegation-uris**, no delegated credential will be transmitted to the web server which will prevent the user's identity from being used to initiate authentication with other Kerberos protected servers. However, if the operator wants to restrict delegation, it is better to turn off the "Account is trusted for delegation" account option on the HTTP service account.

Note: To check if delegation is working, set the `plexcel.log.level = 4` in your PHP INI, restart Apache and look for log entires that read "no delegated credential supplied for ..." or "delegated credentials supplied for ...".

For more information about Firefox HTTP Negotiate authentication support, see the following page:

http://www.mozilla.org/projects/netlib/integrated-auth.html

Appendix B: FreeBSD Supplemental Information

All information in this manual applies to FreeBSD with the exception items listed in this section.

FreeBSD binaries are compiled on FreeBSD 6.2 systems which are deliberately old. At some point we will discontinue support for 6.2 and move to 7 but in the interim you may need to install compatibility libraries.

One FreeBSD user reported that /var/lib had 750 permissions. If you experience this issue, you will receive permissions errors trying to run Plexcel in which case you will need to either change the Plexcel base directory using the plexcel.home INI property or change /var/lib to 755.

Delays with Unresponsive Domain Controllers

Plexcel includes logic to interrogate domain controllers to detect and use only responsive servers. However, this logic is not engaged when using a non-authenticated Plexcel contexts (when `plexcel_accept_token` or `plexcel_logon` is *not* used). If a non-authenticated Plexcel context is used, and a domain controller is selected that it cannot communicate with for any reason, this can result in a delay of ~60 seconds. Plexcel should transparently recover from this condition. Linux also exhibits this behavior but the delay is much shorter.

System Specific Paths

The Plexcel base directory is always `/var/lib/plexcel` by default and does not change across systems. However, all other references to system specific paths should of course be substituted with their FreeBSD equivalent locations. The Plexcel INI file is likely `/usr/local/etc/php/plexcel.ini`. The Plexcel extension should be `/usr/local/lib/php/<zendapinumber>/plexcel.so`. The Plexcel library will be installed in `/usr/local/lib`.

System Specific Commands

Any references to copying subtrees of files with `cp -a <src> <dst>` should be replaced with `cp -pR <src> <dst>`.

Appendix C: Obtaining A Network Packet Capture

In the event that the IOPLEX support team has requested a packet capture for diagnostic purposes, follow these instructions.

Obtaining a Packet Capture on the Web Server

Install the `tcpdump` program (usually is already installed).

Run `tcpdump` as follows:

```
tcpdump -s 0 -w plexcel.pcap ! port ssh
```

Perform the operation of interest and press `Ctrl-C` to stop the capture. A file `plexcel.pcap` should be created in the current directory. This file may be examined with Wireshark (freely downloadable) or sent to IOPLEX Software support for analysis.

> Note: It is preferred that the capture only be allowed to run for the shortest time possible so as to isolate the traffic of interest.

Obtaining a Packet Capture on the Windows Client

Install the XP Support Tools from CD-ROM as described in the following KB article:

http://support.microsoft.com/kb/306794/EN-US/

Run cmd.exe and then netcap.exe /? to see if it was installed properly.

> Note: If you have multiple network interfaces look at the end of the output of netcap.exe for the list of adapters. If the one your HTTP traffic is on is not primary you will need to specify /N:<number> where number is the numeric value for that adapter so make a note of that value.

Reboot XP. This is important because the OS can cache information about Kerberos authentication failures (even if you log off and back on). We want to be absolutely certain that there is no cached information that would otherwise be recorded in the capture.

Once rebooted, run a cmd.exe prompt and run netcap.exe as illustrated here (adding the /N:<number> if you need to specify a particular adapter):

```
C:\tmp>netcap /c:plexcel.cap
```

This will start to write network packets to the named file plexcel.cap in the current directory.

Now launch IE and try to visit page that triggers the problem being diagnosed. Press the space bar in the cmd.exe window to stop the capture.

> Note: It is preferred that the capture only be allowed to run for the shortest time possible so as to isolate the traffic of interest. Similarly it is preferred that no other programs run between the time XP is rebooted and the capture is recorded.

Appendix D: Running Apache in the GNU Debugger (gdb)

If Apache is not starting and nothing is being logged in either the Plexcel or Apache log files, something could be crashing during initialization. To detect this scenario and determine the source of the error, the operator can run Apache within the GNU Debugger. The following is a description of this procedure.

Install the gdb package and run the commands in bold shown below (substituting the path to httpd if necessary):

```
# gdb /usr/sbin/httpd<enter>
GNU gdb 6.4
Copyright 2005 Free Software Foundation, Inc.
<skip output>
(gdb) run -X<enter>
(no debugging symbols found)
(no debugging symbols found)
(no debugging symbols found)
<hit enter to skip output>
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread -1214200128 (LWP 4133)]
0xb70344ae in some_function()
(gdb) bt<enter>
<cryptic "backtrace" here>
```

If Apache is in fact crashing, you should see something like "SIGSEGV, Segmentation fault" as shown above. GDB should then present a (gdb) prompt into which running the "bt" command will emit a "backtrace" which, if interpreted correctly, can reveal the source of the error.

Please contact support@ioplex.com if you discover a crash bug in Plexcel.