

Polaris Under the Hood

Prepared by: Wes Osborn

Overview

Client Communication

Kerberos Authentication

SQL Profiler

SIP Service

!! WARNING !!

Help -> About

Where to start

About Polaris



Polaris Integrated Library System

Version 4.1R2 Build 1036

© 1997-2013 Polaris Library Systems

All rights reserved.

Application Server: [PRODAPP/POLARIS](#)

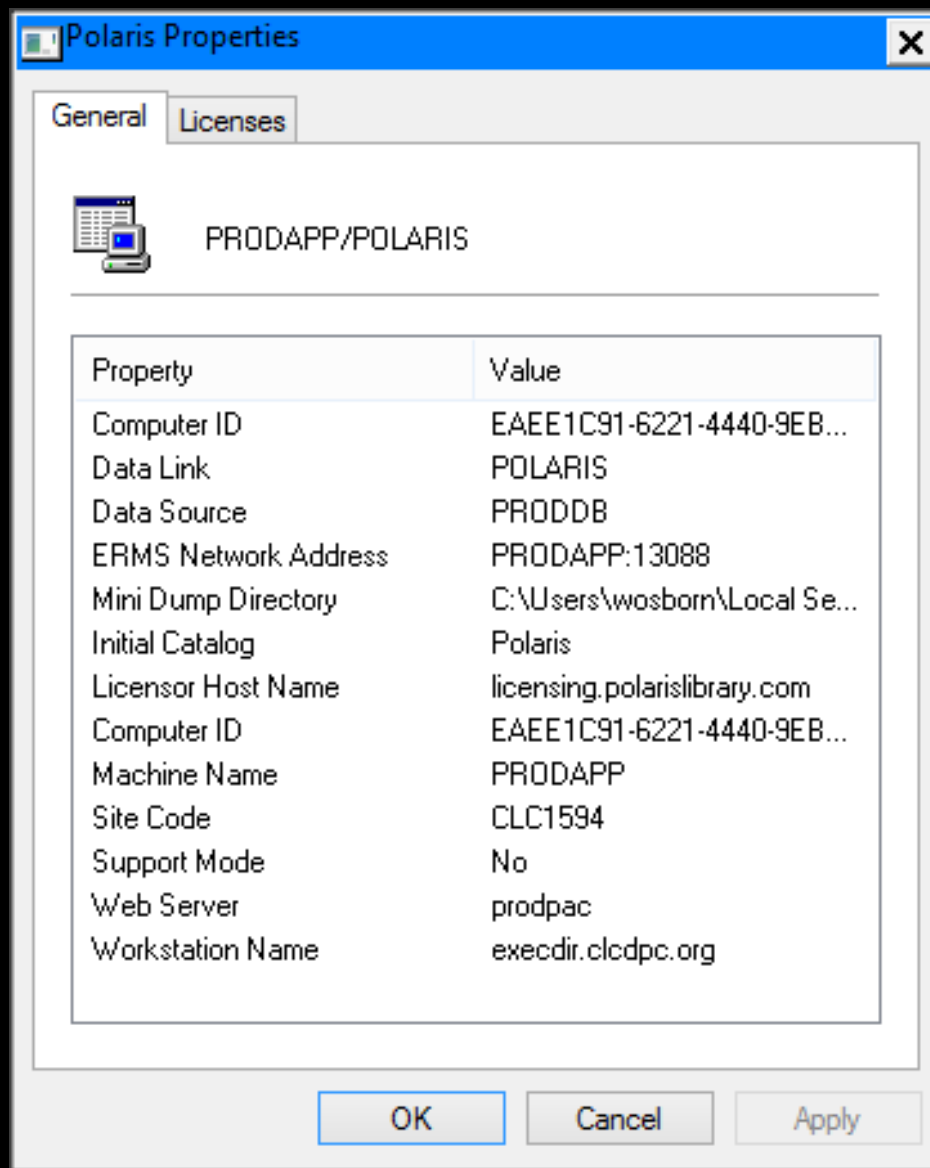
Polaris User: wosborn@dcdpc.org

Polaris Branch: CLC Electronic Library

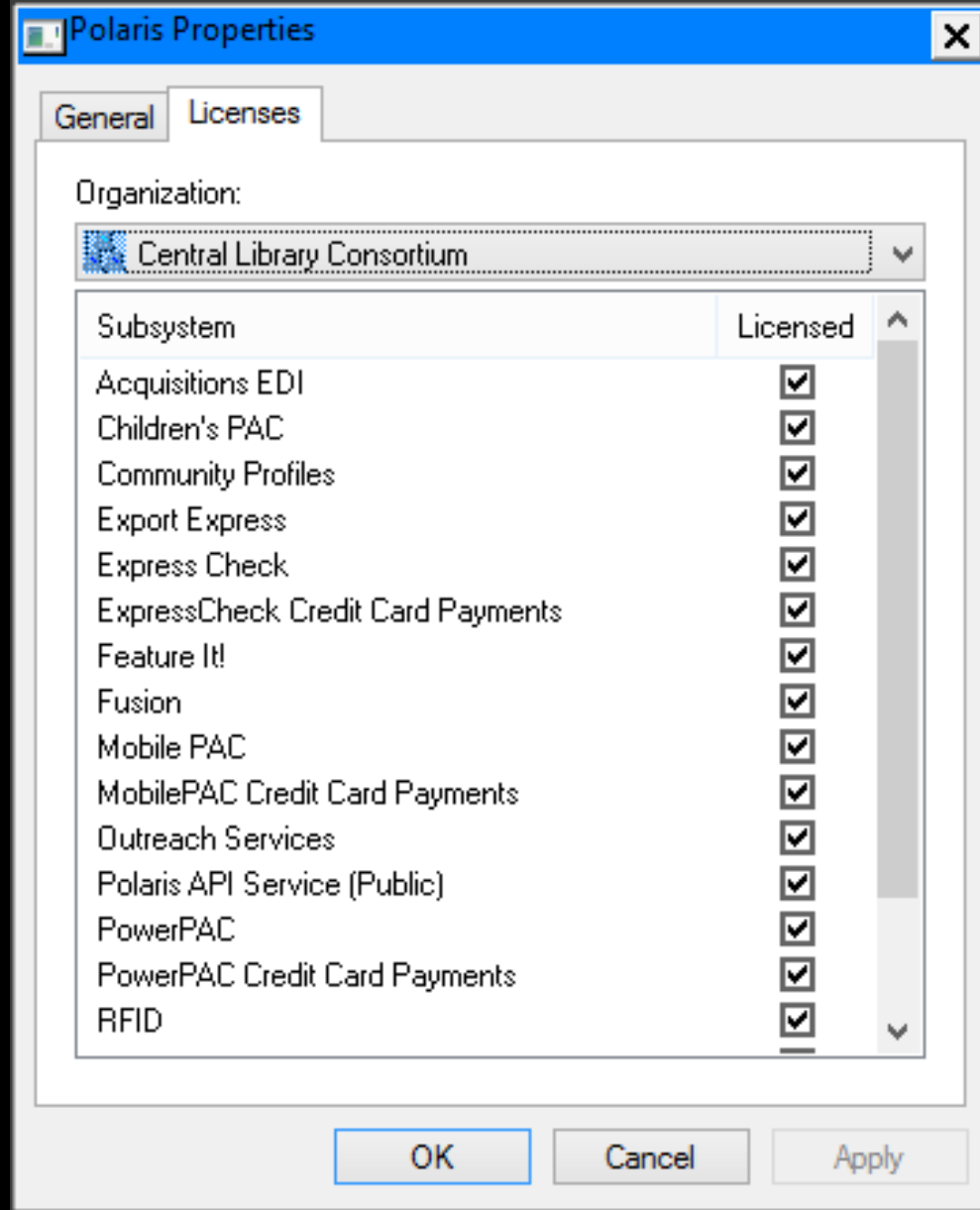
Polaris Workstation: execdir.dcdpc.org

OK

Click on the Application Server “link”



A wealth of information



Check if addon product isn't working

Client Communication

Client Communication

Complex

Try monitoring with Wireshark

Uses App Server specified in client

Can be separated from DB server

New App servers need registered in
the database

Client Communication

API Calls = ERMS port 13088

Z39.50 = ERMS port 210

Direct DB calls = SQL port 1433

Authentication = Kerberos port 88

COM+ API Calls = TCP High ports

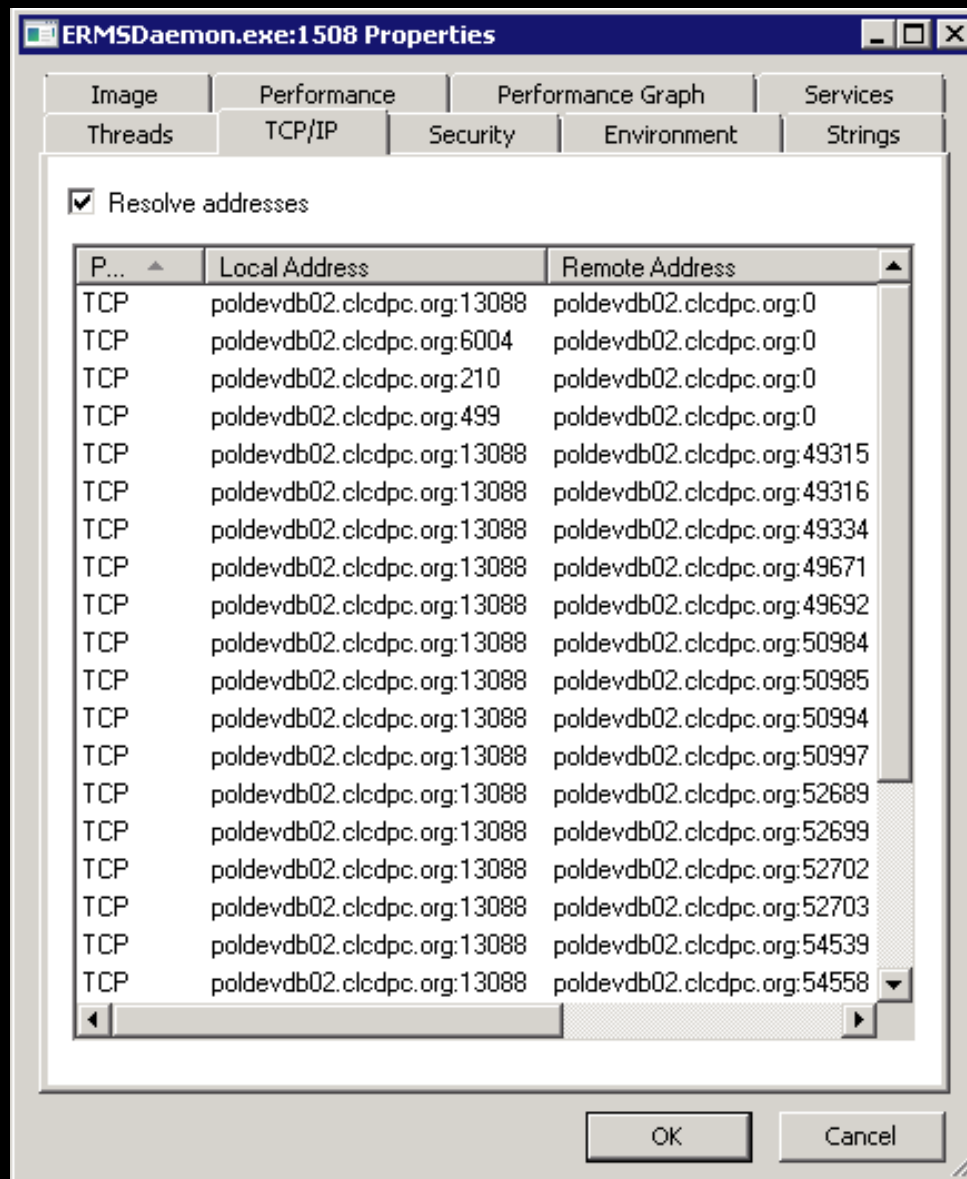
Process Explorer - Sysinternals: www.sysinternals.com [CLCDPC\wosborn]

File Options View Process Find Users Help

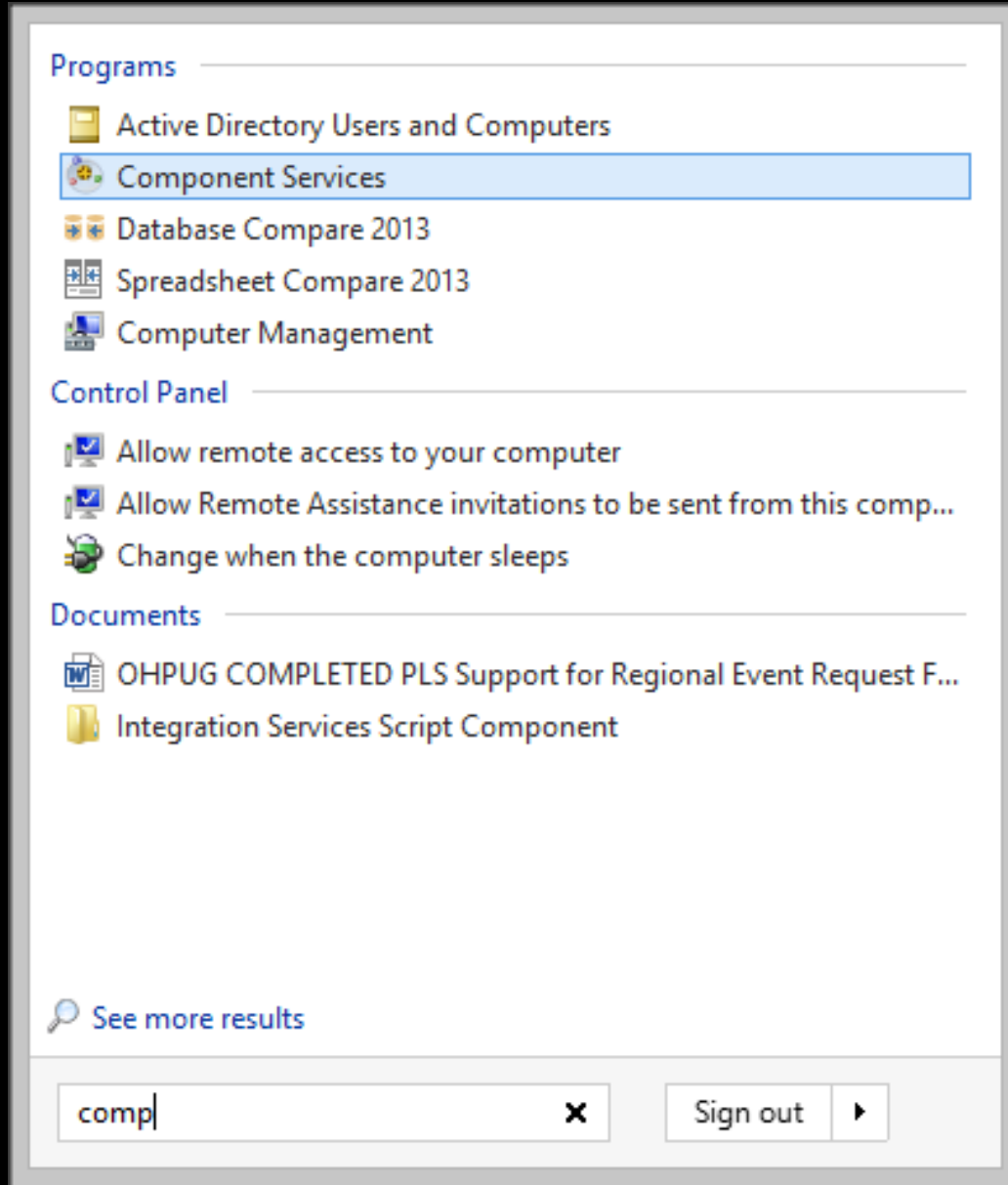
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
7zFM.exe	< 0.01	5,076 K	12,816 K	5540	7-Zip File Manager	Igor Pavlov
ccSvcHst.exe	0.01	26,988 K	18,096 K	2480	Symantec Service Framework	Symantec Corporation
ccSvcHst.exe	< 0.01	6,264 K	5,264 K	2036	Symantec Service Framework	Symantec Corporation
conhost.exe	< 0.01	1,540 K	3,388 K	2868		
csrss.exe	< 0.01	2,988 K	5,452 K	520		
csrss.exe	< 0.01	2,200 K	4,304 K	584		
csrss.exe	0.01	3,256 K	6,548 K	2520		
dllhost.exe	< 0.01	6,152 K	14,200 K	3792	COM Surrogate	Microsoft Corporation
dllhost.exe		8,232 K	15,564 K	9120		
dwm.exe		2,032 K	4,604 K	5304	Desktop Window Manager	Microsoft Corporation
ERMSD aemon.exe	< 0.01	2,189,696 K	229,792 K	1508	ERMSD aemon	Polaris Library Systems
explorer.exe	0.02	44,308 K	64,480 K	5356	Windows Explorer	Microsoft Corporation
inetinfo.exe		14,212 K	20,664 K	1572	Internet Information Services	Microsoft Corporation
Interrupts	0.03	0 K	0 K		n/a Hardware Interrupts and DPCs	
LogonUI.exe		9,100 K	16,144 K	940		
lsass.exe		21,652 K	29,492 K	676	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		3,676 K	6,872 K	684		
mqsvc.exe		8,368 K	9,772 K	1712	Message Queuing Service	Microsoft Corporation
msdtc.exe	< 0.01	4,156 K	8,936 K	2964	Microsoft Distributed Transa...	Microsoft Corporation
MsDtsSrvr.exe		106,656 K	25,488 K	1596	SQL Server Integration Servi...	Microsoft Corporation
perfmon.exe	0.18	14,964 K	24,204 K	10940		
PolarisILS.exe	0.04	48,328 K	63,508 K	5252	Polaris ILS Application Comp...	Polaris Library Systems
procexp.exe		2,996 K	7,880 K	10644	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.13	16,128 K	23,864 K	6624	Sysinternals Process Explorer	Sysinternals - www.sysinter...
psr.exe	< 0.01	14,160 K	26,564 K	5508		
rdpclip.exe		2,796 K	7,272 K	5140	RDP Clip Monitor	Microsoft Corporation
ReportingServicesService.exe	0.01	448,044 K	339,180 K	2052	Reporting Services Service	Microsoft Corporation
services.exe		7,068 K	12,940 K	668		
SIPService.exe	< 0.01	12,016 K	17,600 K	2020	Polaris ILS Application Comp...	Polaris Library Systems
Smc.exe	< 0.01	17,596 K	9,052 K	3736	Symantec CMC Smc	Symantec Corporation
smss.exe		732 K	1,392 K	428		

CPU Usage: 0.63% Commit Charge: 76.23% Processes: 57 Physical Usage: 73.53%

Find out more using ProcessExplorer



ERMS Daemon Properties

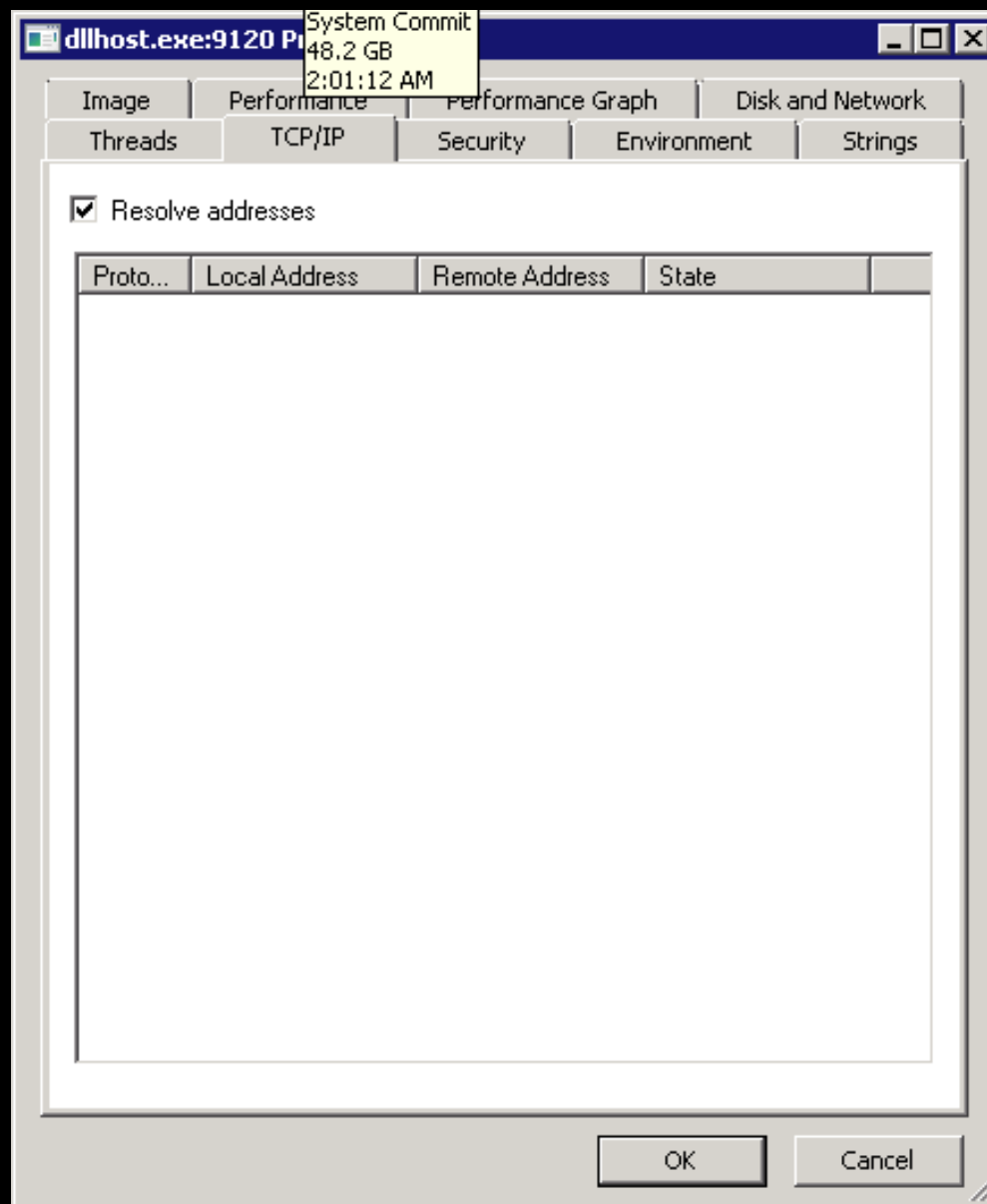


Launch management on AppServer

The image shows a screenshot of the Windows Task Manager application. The window title is "Task Manager". The menu bar includes "File", "Action", "View", "Window", and "Help". The toolbar contains various icons for navigation and actions. The left pane shows the "Console Root" tree with "Running Processes" selected. The right pane displays a table of running processes.

Name	Executable ...	Process ID	Paused	Recy...	NT S...
Polaris.4.1R2...	dllhost.exe	9120	No	No	No
System Applic...	dllhost.exe	3792	No	No	Yes

Find Polaris PID



ProcessExplorer Polaris COM Service

SQLQuery2.sql - p...CDPC\wosborn (65))* X SQLQuery1.sql - p...CDPC\wosborn (58))*

```
exec polaris.dwishowentries 'appserver'
```

100 % <

Results Messages

	EntryID	CommonName
1	2409	devpac02
2	2408	poldevdb02

Finding registered app servers

Adding a new app server

Find PolarisSupport folder on server

Run server setup process

Choose ERMS and Application setup

Run this stored procedure:

```
exec dwinewappserver  
'DBHostName', 'Polaris',  
'AppServerHostName'
```

Client Side: PING.EXE

“Normal” Ping uses ICMP

ICMP Packets can be dropped or
delayed

May tell you if server is powered on
but service may not be running

Time to find something new

C:\

C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.2.9200]

(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping prodapp

Pinging prodapp.clcdpc.org [192.168.144.170] with 32 bytes of data:

Reply from 192.168.144.170: bytes=32 time<1ms TTL=127

Reply from 192.168.144.170: bytes=32 time<1ms TTL=127

Reply from 192.168.144.170: bytes=32 time<1ms TTL=127

Reply from 192.168.144.170: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.144.170:

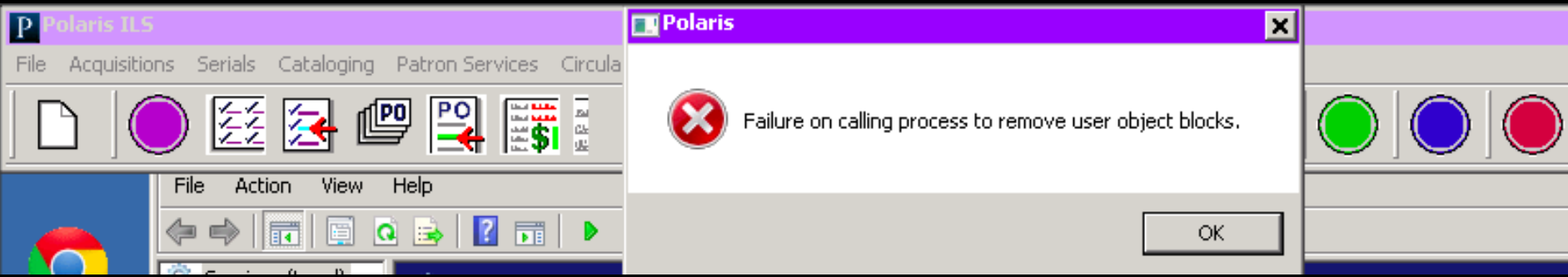
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>

Pinging App Server works



But client won't connect

Client Side: TCP Ping

Two Options:

<http://go.clcoho.org/psping>

<http://go.clcoho.org/tcping>

Mimics a client attempting TCP
connection to server on service port

Ideally run from CLIENT with issue

```
C:\Windows\system32\cmd.exe

C:\Users\wosborn\Downloads>tcping poldevdb02 13088

Probing fe80::2432:b2bc:cba5:44dd:13088/tcp - Socket is not connected (10057) -
time=2011.496ms
Probing fe80::2432:b2bc:cba5:44dd:13088/tcp - Socket is not connected (10057) -
time=2007.834ms
Probing fe80::2432:b2bc:cba5:44dd:13088/tcp - Socket is not connected (10057) -
time=2000.176ms
Probing fe80::2432:b2bc:cba5:44dd:13088/tcp - Socket is not connected (10057) -
time=2011.829ms

Ping statistics for fe80::2432:b2bc:cba5:44dd:13088
    4 probes sent.
    0 successful, 4 failed.
Was unable to connect, cannot provide trip statistics.

C:\Users\wosborn\Downloads>_
```

By default hostname check is IPv6

```
C:\Windows\system32\cmd.exe

C:\Users\wosborn\Downloads>tcping 192.168.144.80 13088

Probing 192.168.144.80:13088/tcp - Port is open - time=3.353ms
Probing 192.168.144.80:13088/tcp - Port is open - time=0.242ms
Probing 192.168.144.80:13088/tcp - Port is open - time=0.224ms
Probing 192.168.144.80:13088/tcp - Port is open - time=0.241ms

Ping statistics for 192.168.144.80:13088
    4 probes sent.
    4 successful, 0 failed.
Approximate trip times in milli-seconds:
    Minimum = 0.224ms, Maximum = 3.353ms, Average = 1.015ms

C:\Users\wosborn\Downloads>
```

Check with IPv4 address

Kerberos Authentication

Kerberos Authentication

Authentication happens frequently

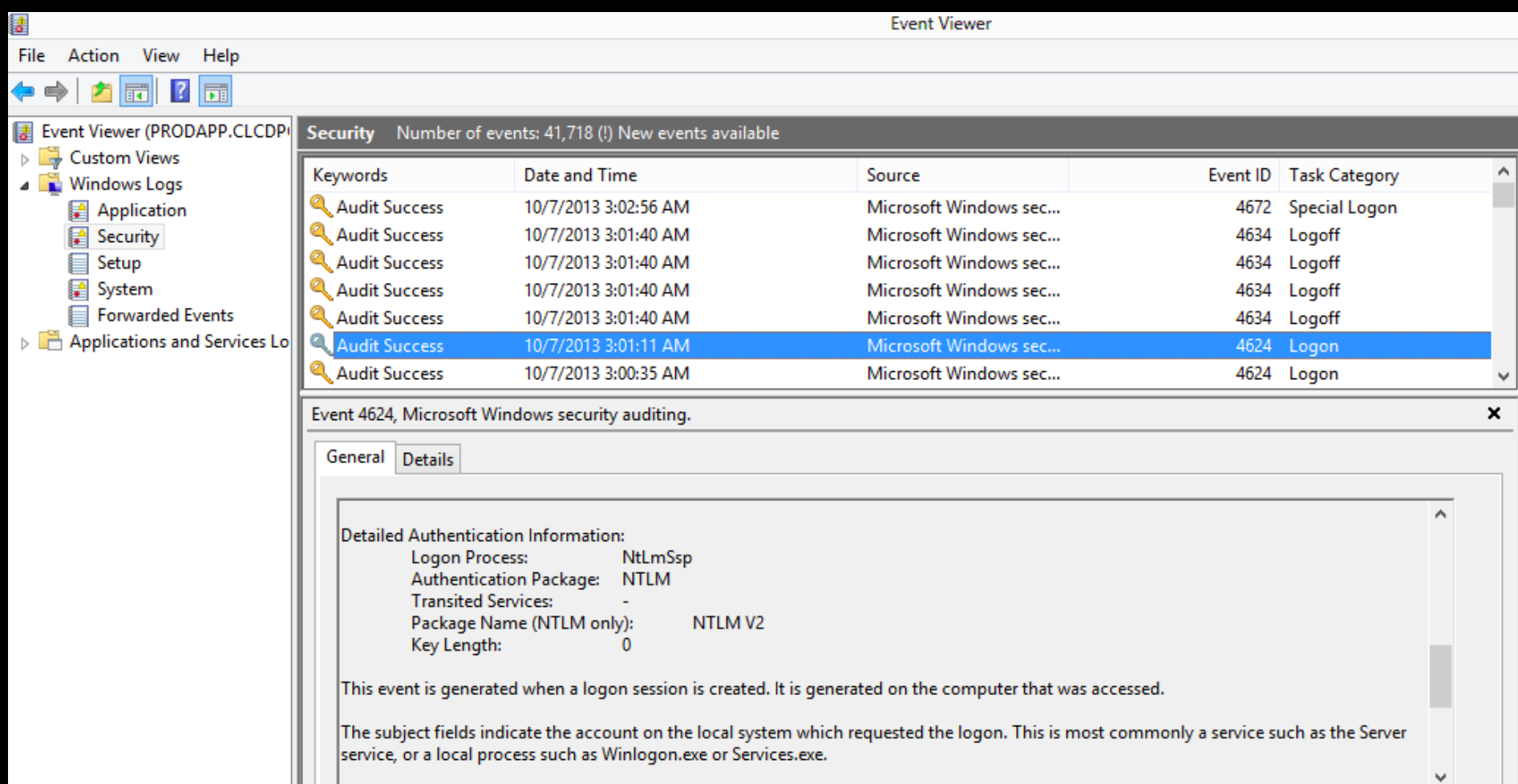
NTLM is the fallback

Kerberos requires

2008r2+ Forest/Domain Level

Windows 7 Clients

Kerberos Forest Search Order



The screenshot shows the Windows Event Viewer application. The left-hand pane displays the navigation tree with 'Security' selected under 'Windows Logs'. The main pane shows a list of security events. The event with ID 4624 and task category 'Logon' is highlighted. Below the list, the details for event 4624 are shown, including a 'Detailed Authentication Information' section with the following values:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/7/2013 3:02:56 AM	Microsoft Windows sec...	4672	Special Logon
Audit Success	10/7/2013 3:01:40 AM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/7/2013 3:01:40 AM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/7/2013 3:01:40 AM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/7/2013 3:01:40 AM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/7/2013 3:01:11 AM	Microsoft Windows sec...	4624	Logon
Audit Success	10/7/2013 3:00:35 AM	Microsoft Windows sec...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General | Details

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM
- Transited Services: -
- Package Name (NTLM only): NTLM V2
- Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

App Server Event Viewer - NTLM

Security Number of events: 41,718 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/6/2013 4:11:34 PM	Microsoft Windows sec...	4624	Logon
Audit Success	10/6/2013 4:11:34 PM	Microsoft Windows sec...	4624	Logon
Audit Success	10/6/2013 4:11:34 PM	Microsoft Windows sec...	4624	Logon
Audit Success	10/6/2013 4:11:33 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/6/2013 4:11:33 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/6/2013 4:11:33 PM	Microsoft Windows sec...	4634	Logoff
Audit Success	10/6/2013 4:11:32 PM	Microsoft Windows sec...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

Network Information:

Workstation Name:
Source Network Address: 192.168.34.36
Source Port: 54212

Detailed Authentication Information:

Logon Process: Kerberos
Authentication Package: Kerberos

App Server Event Viewer - Kerberos

C:\Windows\system32\cmd.exe

```
#14> Client: wosborn @ CLCDPC.ORG
Server: cifs/prodapp.clcdpc.org @ CLCDPC.ORG
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canoni
calize
Start Time: 10/2/2013 12:12:51 <local>
End Time: 10/2/2013 21:47:28 <local>
Renew Time: 10/4/2013 14:47:18 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DC02.clcdpc.org

#15> Client: wosborn @ CLCDPC.ORG
Server: RestrictedKrbHost/prodapp @ CLCDPC.ORG
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canoni
calize
Start Time: 10/2/2013 12:12:51 <local>
End Time: 10/2/2013 21:47:28 <local>
Renew Time: 10/4/2013 14:47:18 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DC02.clcdpc.org

C:\Windows\system32>
```

Also run *klist* from client

SQL Profiler

SQL Profiler

Installed as part of SQL Management Tools

Runs locally or remotely

Shows all the “chatter” happening on the SQL server

Simple to use, hard to interpret



File Edit View Replay Tools Window Help

New Trace... Ctrl+N

Open ▶

Close Ctrl+F4

Save Ctrl+S

Save As ▶

Properties...

Templates ▶

Run Trace

Pause Trace

Stop Trace

Export ▶

Import Performance Data...

Exit

Starting a trace

Connect to Server

Microsoft®
SQL Server® 2012

Server type: Database Engine

Server name: poldevdb02

Authentication: Windows Authentication

User name: CLCDPC\wosbom

Password:

Remember password

Connect Cancel Help Options >>

Logging into server to trace

Trace Properties

General | Events Selection

Trace name:

Trace provider name:

Trace provider type: version:

Use the template:

Save to file:

Set maximum file size (MB):

Enable file rollover

Server processes trace data

Save to table:

Set maximum rows (in thousands):

Enable trace stop time:

Run

Cancel

Help

Using default trace parameters

EventClass	TextData	ApplicationName	NTUserName
SQL:BatchStarting	SELECT CarrierID, CarrierName FROM ...	PolarisILS/P...	
SQL:BatchCompleted	SELECT CarrierID, CarrierName FROM ...	PolarisILS/P...	
RPC:Completed	exec sp_executesql N'SELECT PatronC...	PolarisILS/P...	
RPC:Completed	exec sp_executesql N'SELECT Polaris...	PolarisILS/P...	
RPC:Completed	exec Polaris.Circ_LoadPatronAddress...	PolarisILS/P...	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...	
RPC:Completed	exec Polaris.ORS_GetPatron @nPatronID=34030	PolarisILS/P...	
Audit Logout		PolarisILS/P...	
RPC:Completed	exec sp_reset_connection	PolarisILS/P...	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...	
RPC:Completed	declare @p11 nvarchar(2047) set @p...	PolarisILS/P...	
Audit Logout		PolarisILS/P...	
RPC:Completed	exec sp_reset_connection	PolarisILS/P...	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...	
RPC:Completed	declare @p11 nvarchar(2047) set @p...	PolarisILS/P...	
Audit Logout		PolarisILS/P...	
RPC:Completed	exec sp_reset_connection	PolarisILS/P...	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...	
RPC:Completed	declare @p11 nvarchar(2047) set @p...	PolarisILS/P...	

exec Polaris.ORS_GetPatron @nPatronID=34030

Opening patron record - Step 1

SQL Server Profiler - [Untitled - 1 (poldevdb02)]

File Edit View Replay Tools Window Help

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Reads	Writes	Duration
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...		polaris				
RPC:Completed	declare @p5 int set @p5=2 declare...	PolarisILS/P...		polaris	0	120	0	
Audit Logout		PolarisILS/P...		polaris	0	258	0	
RPC:Completed	exec sp_reset_connection	PolarisILS/P...		polaris	0	0	0	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...		polaris				
RPC:Completed	declare @p11 nvarchar(2047) set @p...	PolarisILS/P...		polaris	0	8	0	
Audit Logout		PolarisILS/P...		polaris	0	266	0	
RPC:Completed	exec sp_reset_connection	PolarisILS/P...		polaris	0	0	0	
Audit Login	-- network protocol: LPC set quote...	PolarisILS/P...		polaris				
RPC:Completed	declare @p5 int set @p5=2 declare...	PolarisILS/P...		polaris	16	5755	0	
RPC:Completed	exec sp_executesql N'SELECT Name, S...	PolarisILS/P...		polaris	0	4	0	
SQL:BatchStarting	SELECT LanguageID, LanguageDesc FRO...	PolarisILS/P...		polaris				
SQL:BatchCompleted	SELECT LanguageID, LanguageDesc FRO...	PolarisILS/P...		polaris	0	2	0	
SQL:BatchStarting	SELECT DeliveryOptionID, DeliveryOp...	PolarisILS/P...		polaris				
SQL:BatchCompleted	SELECT DeliveryOptionID, DeliveryOp...	PolarisILS/P...		polaris	0	9	0	
SQL:BatchStarting	SELECT CarrierID, CarrierName FROM ...	PolarisILS/P...		polaris				
SQL:BatchCompleted	SELECT CarrierID, CarrierName FROM ...	PolarisILS/P...		polaris	0	7	0	
RPC:Completed	exec sp_executesql N'SELECT PatronC...	PolarisILS/P...		polaris	0	36	0	
RPC:Completed	exec sp_executesql N'SELECT Polaris...	PolarisILS/P...		polaris	0	31	0	

```

exec sp_executesql N'SELECT PatronCodeID, PCodeDescription, OrganizationID, DeliveryOptionID, BranchName, Barcode, Gender, Birthdate,
NameFirst, NameLast, NameMiddle, NameSuffix, NameTitle, PhoneVoice1, Phone1CarrierID, PhoneVoice2, Phone2CarrierID, PhoneVoice3,
Phone3CarrierID, PhoneFAX, EmailAddress, AltEmailAddress, Password, EntryDate, ExpirationDate, AddrCheckDate, UpdateDate,
StatisticalClassID, RegistrationDate, LanguageID, FormerID, ReadingList, CollectionExempt, User1, User2, User3, User4, User5, CreatorID,
ModifierID, SystemBlocks, LastActivityDate, ExcludeFromOverdues, DeletionExempt, ExcludeFromHolds, ExcludeFromBills, EmailFormatID,
EnablesMS, EReceiptoptionID, TxtPhoneNumber FROM Polaris.ViewPatronRegistration WITH (NOLOCK) WHERE PatronID = @P1',N'@P1 int',34030

```

Opening patron record - Step 2

SQL Profiler - Client Debug

Find stored procedure “called” when
executing in client

Attempt to execute procedure
manually w/SQL Management

Execute OK = Client Bug (Bad)

Execute Fail = Procedure Bug

SQL Profiler - Deconstruction

Determine Stored Procedure called
so you can create a batch process

Batch remove erroneous fines

Figure out what process is running so
you can try to speed it up

```
exec polaris.polaris.ors_getpatron
```

100 % <

SQL Manager, call up stored procedure

The screenshot shows the SQL Server Enterprise Manager interface. The 'Query' menu is open, and the 'Display Estimated Execution Plan' option is highlighted. The background shows a query window with the following text:

```
SQLQuery2.sql - p
exec pole
```

Below the query window, the execution results are displayed:

Query 1: Query cost (relative to the batch): 0%
exec polaris.polaris.ors_getpatron

Query 2: Query cost (relative to the batch): 100%
polaris.polaris.ors_getpatron

The execution plan for Query 2 is shown, consisting of two operations:

- Stored Procedure (Cost: 0%)
- SET ON/OFF (Cost: 0%)

A status bar at the bottom indicates: Query executed successfully.

Display Execute Plan

The screenshot shows the SQL Server Enterprise Manager interface. The top menu bar includes File, Edit, View, Query, Project, Debug, Tools, Window, and Help. The toolbar contains various icons for file operations and execution. The main window displays three tabs for SQL queries: 'SQLQuery3.sql - p...CDPC(wosborn (58))', 'SQLQuery2.sql - p...CDPC(wosborn (62))', and 'SQLQuery1.sql - p...CDPC(wosborn (58))'. The active query contains the following T-SQL code:

```
exec polaris.dbo.clc_custom_changeduedate
```

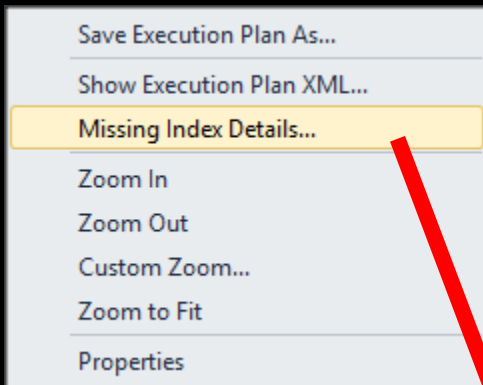
Below the query editor, the 'Messages' and 'Execution plan' tabs are visible. The 'Messages' tab shows the following output:

Query 1: Query cost (relative to the batch): 0%
exec polaris.dbo.clc_custom_changeduedate
Missing Index (Impact 98.2631): CREATE NONCLUSTERED INDEX [<Name of Missing Index, sysname,>] ON [Polaris].[ItemCheckouts] ([OrganizationID]) INCL...

Query 2: Query cost (relative to the batch): 99%
polaris.dbo.clc_custom_changeduedate
Missing Index (Impact 98.2631): CREATE NONCLUSTERED INDEX [<Name of Missing Index, sysname,>] ON [Polaris].[ItemCheckouts] ([OrganizationID]) INCL...

The execution plan shows a 'Stored Procedure' node with a cost of 0% and an 'ASSIGN' node with a cost of 0%. A yellow banner at the bottom of the messages pane states: 'Query executed successfully.' The status bar at the bottom indicates the server is 'Ready', the current location is 'poldevdb02 (10.50 SP2) | CLCDPC(wosborn (58) | Polaris', and the execution time is '00:00:00 | 0 rows'. The status bar also shows 'Ln 1 Col 42 Ch 42 INS'.

An index would help this part of the SP



```
/*  
Missing Index Details from SQLQuery3.sql - poldevdb02.Polaris (CLCDPC\wosborn (58))  
The Query Processor estimates that implementing the following index could improve the query cost by 98.2631%.  
*/  
  
/*  
USE [Polaris]  
GO  
CREATE NONCLUSTERED INDEX [<Name of Missing Index, sysname,>]  
ON [Polaris].[ItemCheckouts] ([OrganizationID])  
INCLUDE ([CreatorID])  
GO  
*/
```

Right click on the Missing Index...

Do NOT DO IT!

Why NOT to add an Index

Could break a future upgrade

Could take up a LOT of disk space

Might not actually speed up the query
or process

Test the index on your dev/test
system and then suggest to Polaris

Learn more cool stuff about SQL

<http://www.brentozar.com/>

SIP Server

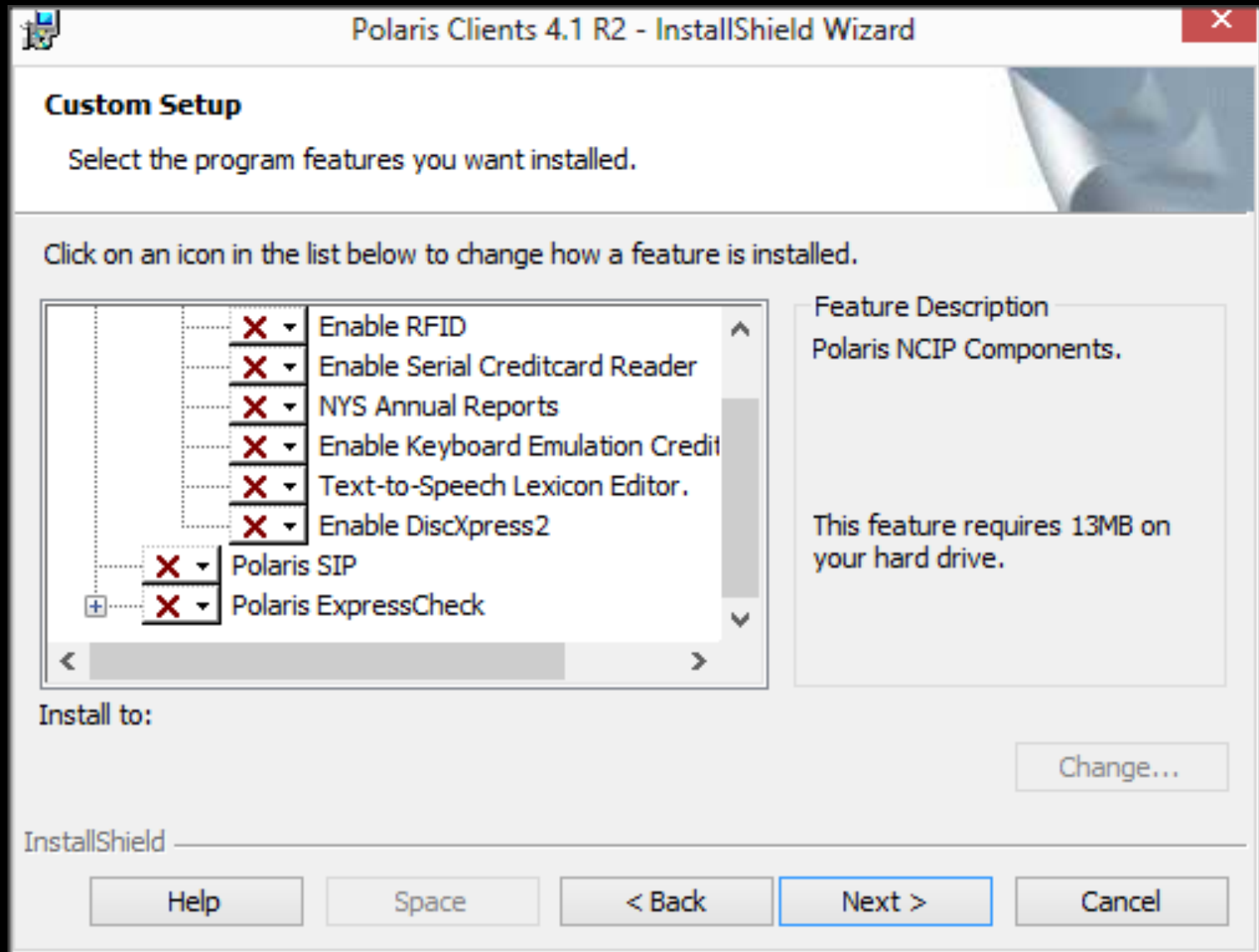
SIP Server

Operates as a client to the Polaris database

Part of Polaris client install package

32-bit but CPU hungry

Watch log file growth



Installs through client process

0.48%
0.32% procexp64.exe:5420
3:49:44 AM

Performance Graph Services

Threads TCP/IP Security Environment Strings

Resolve addresses

F ^	Local Addr...	Remot...	State	Service	▲
TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5001	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5002	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5003	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5004	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5005	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5006	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5007	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5008	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5009	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5010	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5011	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5012	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5013	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5014	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5015	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5016	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5017	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5018	0.0.0.0:0	LISTENING	Polaris SIP	
TCP	0.0.0.0:5019	0.0.0.0:0	LISTENING	Polaris SIP	

OK Cancel

Can check with ProcessExplorer

Debugging SIP

Use TCPing to check SIP ports

Check SIP Logs

C:\ProgramData\Polaris\4.1R2\Logs\SIP

Dumping SIP Service Binary

CLC SIP Testing Tool

Dumping SIP Service

SIP Service is a compiled binary

Source code isn't accessible

But the “plain text” within the EXE
can be revealed

Google: McAfee BinText

**The hold satisfies
conundrum**

Administration Explorer - System - Central Library Consortium - Polaris

File Edit Help

Administration Explorer - System

Parameters

Acquisitions / Serials Patron Services Cataloging PAC Notification

SelfCheck Unit Request Credit Card Payment

Parameter	Value
Checkin screen message: Item checkin ok (status was CL...	Item Claimed Returned.
Checkin screen message: Item checkin ok (status was IN)	Successful Check-in.
Checkin screen message: Item checkin ok (status was IN-...	Successful Bindery to In.
Checkin screen message: Item checkin ok (status was IN-...	Successful In-Process to In.
Checkin screen message: Item checkin ok (status was IN-...	Successful In-Repair to In.
Checkin screen message: Item checkin ok (status was IN-...	Successful In-Transit to In.
Checkin screen message: Item checkin ok (status was MI...	Successful Missing to In.
Checkin screen message: Item checkin ok (status was UN...	Successful Unavailable to In.
Checkin screen message: Item checkin ok - held (status ...	Successful hold for:
Checkin screen message: Item checkin ok.	Item checkin ok.
Checkout printer message: Item is not already checked out.	Item is not already checked o
Checkout printer message: Internal error occurred.	Internal error occurred.
Checkout printer message: Invalid patron password.	Invalid patron password.
Checkout printer message: Item checkout ok (by forced ...	Item checkout ok (by forced

For Help, press F1

Wosborn NUM

Sys Admin SIP Message Options



Edit Tool

Language Options

Product:

- ✓ PowerPAC
- ExpressCheck
- Inbound Telephony
- Outbound Telephony
- Notices
- ILL
- Polaris Fusion

Organization:

sortium

Language 1:



Language 2:



Limit Options

Specific string ID

String contains:

Only show cus

- Acquisitions Exchange
- Mobile PAC
- ERMSPortal
- Receipts
- ContentXChange

Load Strings

Nothing in Language Editor

Hardcoded, we think...



BinText 3.0.3

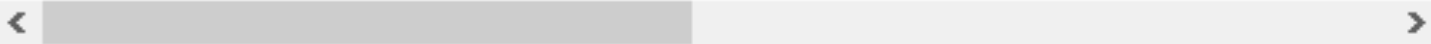


Search | Filter | Help

File to scan

Advanced view

File pos	Mem pos	ID	Text
----------	---------	----	------



Ready

BinText

Locate SIP Service Binary



Search | Filter | Help

File to scan: C:\Program Files (x86)\Polaris\4.1R2\Bin\SIPService.exe

Browse

Go

Advanced view

Time taken : 1.313 secs Text size: 52696 bytes (51.46K)

File pos	Mem pos	ID	Text
U 0000000890E8	00000048A8E8	0	Patron has too many total claims, not allowed to ren
U 000000089178	00000048A978	0	Patron has too many claims, not allowed to renew; p
U 000000089200	00000048AA00	0	Patron has lost items, not allowed to renew; port %d
U 000000089280	00000048AA80	0	Patron has verify borrower block, not allowed to ren
U 000000089310	00000048AB10	0	Patron has collection agency block, not allowed to
U 0000000893A8	00000048ABA8	0	Patron has free text block, not allowed to renew; pc
U 000000089430	00000048AC30	0	Patron has stop code that is not allowed to renew; p
U 0000000894B8	00000048ACB8	0	Patron code not allowed to renew; port %d from %s
U 000000089520	00000048AD20	0	Renewals are not allowed when book is 'out' to anc
U 0000000895C0	00000048ADC0	0	Item reached its renewal limit.
U 000000089608	00000048AE08	0	Item reached its renewal limit; port %d from %s
U 000000089668	00000048AE68	0	This item satisfies a hold for another Patron.
U 0000000896C8	00000048AEC8	0	This ItemID: %d satisfies a hold for a different Patrc

Ready

AN: 1374

UN: 1118

RS: 2

satisfies

Find

Save

BinText

Click Go -> Enter query -> Click Find



Search | Filter | Help

File to scan C:\Program Files (x86)\Polaris\4.1R2\Bin\SIPService.exe

Browse

Go

Advanced view

Time taken : 1.313 secs

Text size: 52696 bytes (51.46K)

ext

```
or retrieving Current Claims Count; port %d from %s
or retrieving Held Items Count.
atron has free text blocks.
atron has free text blocks; port %d from %s
or retrieving Free Text Blocks Count.
or retrieving Blocks Count.
atron Info - Printing Outstanding Fines...
rocessPatronInformationMessage is converting the username(%s) to barcode(%s); port %d from %s
o end item; port %d from %s
o start item; port %d from %s
atron Information Message: The message is too short to process the fixed fields; port %d from %s
;SELECT OrganizationID, TCPIPPortNumber FROM Polaris.Polaris.SIPServicePorts WITH (NOLOCK)
is executable is not running as an NT Service. In order to send the message to quit, click the OK butt
```

Ready

AN: 1374

UN: 1118

RS: 2

select

Find

Save

BinText

We can also see SQL being called

CLC SIP Testing Tool

SIP Finger Pointing

3rd Party Vendor

SIP Sys Admin Setting

SIP Bug

No readily available tools to
impersonate a SIP client

Introducing...

The SIP Testing Tool

From your friends at the CLC

CLC SIP Testing Tool

Easy to use, single click install

Impersonates a SIP Client

Shows both client request and server response messages

Can set Vendor Profiles at login

Customize application defaults

Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

[More info](#)

OK

You will see this when installing on
Windows 8+

SIP Testing Tool

Connection Information SIP Server <input type="text" value="prodsip01"/> SIP Port <input type="text" value="5002"/> AO <input type="text" value="7"/> AP <input type="text" value="GHP"/> <input type="button" value="Connect"/>	Login Information SIP Username <input type="text" value="3MLogin"/> SIP Password <input type="password" value="*****"/> Vendor Profile <input type="text" value=""/> <input type="button" value="Login"/>	Patron Information Barcode <input type="text" value="21870002169440"/> PIN <input type="text" value="1234"/> BP <input type="text" value="1"/> BQ <input type="text" value="5"/> Item Information Barcode <input type="text" value="3000000000123"/>	Fee Information Fee Type <input type="text"/> Payment Type <input type="text"/> Fee Identifier <input type="text"/> Transaction ID <input type="text"/> Payment Amt <input type="text"/>	<input type="button" value="Patron Information"/> <input type="button" value="Item Checkout"/> <input type="button" value="Fee Paid"/> <input type="button" value="Patron Status"/> <input type="button" value="Item Check-in"/> <input type="button" value="Renew All Items"/> <input type="button" value="End Session"/> <input type="button" value="Renew Item"/> <input type="button" value="Item Information"/>
--	--	---	--	--

| |

Connected to prodsip01:5002 | AO = 7 | AP = GHP | VP = |

Main CLC SIP Testing Tool Window

Hostname

Port

AO

AP

SIP Username

SIP Password

Vendor Profile

Patron Barcode

Patron PIN

Item Barcode

Connect on startup

Enable dark theme?

Changing Defaults

SIP Testing Tool

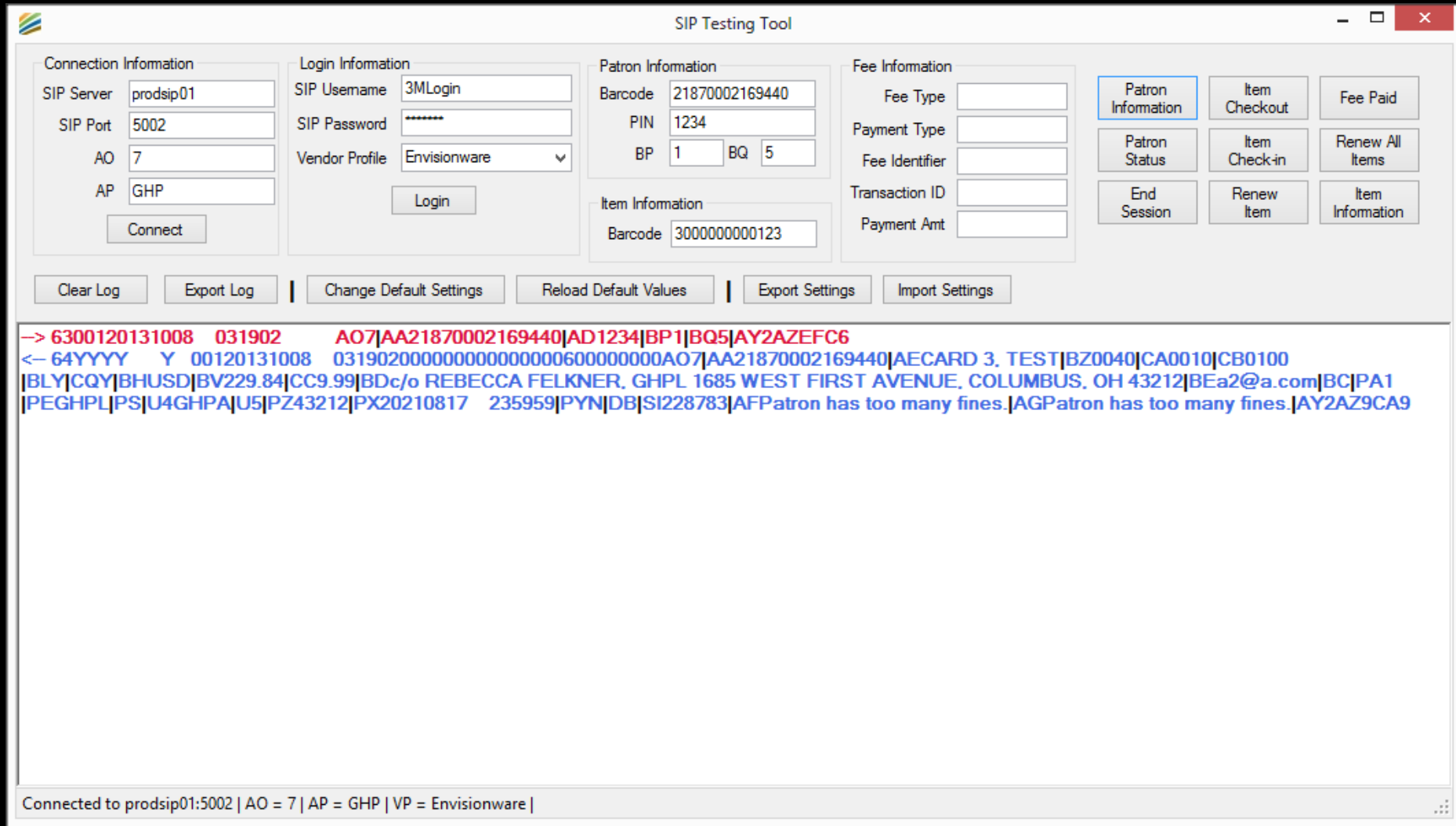
Connection Information SIP Server: <input type="text" value="prodsip01"/> SIP Port: <input type="text" value="5002"/> AO: <input type="text" value="7"/> AP: <input type="text" value="GHP"/> <input type="button" value="Connect"/>	Login Information SIP Username: <input type="text" value="3MLogin"/> SIP Password: <input type="password" value="*****"/> Vendor Profile: <input type="text" value="Envisionware"/> <input type="button" value="Login"/>	Patron Information Barcode: <input type="text" value="21870002169440"/> PIN: <input type="text" value="1234"/> BP: <input type="text" value="1"/> BQ: <input type="text" value="5"/> Item Information Barcode: <input type="text" value="3000000000123"/>	Fee Information Fee Type: <input type="text"/> Payment Type: <input type="text"/> Fee Identifier: <input type="text"/> Transaction ID: <input type="text"/> Payment Amt: <input type="text"/>	<input type="button" value="Patron Information"/> <input type="button" value="Item Checkout"/> <input type="button" value="Fee Paid"/> <input type="button" value="Patron Status"/> <input type="button" value="Item Check-in"/> <input type="button" value="Renew All Items"/> <input type="button" value="End Session"/> <input type="button" value="Renew Item"/> <input type="button" value="Item Information"/>
--	---	--	---	--

| |

```
→ 9300CN3MLogin|CO3MLogin|VPEnvisionware|AY0AZF0A6  
← 941AY0AZDFD
```

Connected to prodsip01:5002 | AO = 7 | AP = GHP | VP = Envisionware |

Logging into SIP Server



SHOW Screenshot tour of testing tool

Available Now

<http://siptool.clcohoio.org/setup.exe>

OR

<http://bit.ly/siptool>

Wes Osborn

<http://go.clcoho.org/pug>

wosborn@clcoho.org

twitter: @wesochuck