RSA enVision™
Windows Agentless Collection Troubleshooting

RSA Security Inc.
200 Lowder Brook Drive, Suite 2000
Westwood, MA 02090
U.S.A.
781.375.9000

Windows Agentless Collection Troubleshooting

Overview of Windows Collection Process

The NIC Windows Service allows the envision system to retrieve Windows logs from remote Windows systems without installing any third-party software (agentless Windows). You can also use third-party Windows collection applications to collect the Windows events. See Envision Help for third-party windows collection

The NIC Windows Service converts these messages into syslog events and sends them via shared memory to the NIC Collector Service. The NIC Windows Service tracks which events were read by event log type and by system so that old log information is not re-polled.

By default, the NIC Windows Service polls 3 NIC log files types (Application, System, Security,) (Directory Service, DNS Server, File Replication Service are available but not set as a default). You can select the log types to poll and the event polling interval and filter criteria for each type. You can add custom log files for any windows application. For more info see Envision Help for "Manage Windows Logs"

You can add an unlimited number of windows devices to the NIC Windows Service (however, you are limited by your license to the number of devices that you can collect from).

The WIN gauge on the Dashboard displays the cumulative number of events collected from all connected Windows Systems.

In a multiple appliance site, the NIC Windows Service runs on the LC and RC appliances

Overview of Configuration steps

1. Verify Pre-requisites for network communication on client and server
2. Step by Step Example of setting up one Agentless Client
3. Verification of configuration via the Envision GUI interface
   (Only required if you can't see devices under manage monitored devices screen in Envision GUI)
4. Verification of communication using Wintool utility
   (Only required if you can't see devices under manage monitored devices screen in Envision GUI)
5. Verification of User access rights for proper event retrieval using Runeventvieweras utility
   (Only required as a debugging step if logs indicate device access issues)

Windows Pre-requisites

1. Client for Microsoft Networks is enabled(Client / Server)
   (On the LAN interface or the interface you are collecting from. See Appendix "MS Client")
2. File and Print Sharing for Microsoft Networks enabled(Client / Server)
   (On the LAN interface or the interface you are collecting from. See Appendix "File and Print Sharing")
3. Remote Registry Service running (Windows 2000 – 2003)
   (On enVision collector / Designated for collection windows machine)
4. Remote Registry Service running under Local System acct (Windows2003)
5. Netbios over TCP required only for NT 4 and Bulk Add feature in Envision
   (On the LAN interface or the interface you are collecting from, on AS / LC. See Appendix "Netbios")
6. Lan Card Binding order
   (On the LAN interface or the interface you are collecting from on the envision Collector.
   See Appendix "Binding Order")
7. Ports used for Windows collection
   (See Appendix "Ports Used for Windows Collection")

Windows Troubleshooting Tools — Where Found

1. Wintool.exe — e:\envision\bin – folder
   (To be run on an HA or LC, RC node)
2. Runeventvieweras.exe — e:\envision\bin – folder
   (To be run on an HA or LC, RC node)
3. StartISQL.cmd — e:\envision\database\cmd – folder
   (To only be used with support over the phone or via a webex. See Apendix "ISQL")

Step by Step Example

(On the Client you want to collect logs from)

1. Verify Client for Microsoft Networks is enabled(MS Client)
2. Verify File and Print Sharing for Microsoft Networks enabled(File and Print Sharing)
3. Verify Remote Registry Service running (Windows 2000 – 2003)
4. Verify Remote Registry Service running under Local System acct (Windows2003)

(On the Envision Server)

5. Within Envision GUI go to Overview Tab -> System Configuration ->Services -> Device Services -> Windows Service -> Manage Windows Service.
   a. Click on Add and create an entry.
   b. Select the domain where this machine resides from the dropdown list.

Notes: If the domain is not on the list the GUI will popup automatically a screen to add the domain.
The account that you use to add this domain must have Domain Admin privileges. On an LS system the changes are made on the AS1 server and it will take up to 3 min to populate to the end LC… the NIC Windows Service is sensitive to database changes and will restart it self if there are any new changes.

c. Add the IP address of the machine you want to collect logs from.

d. Check off the enabled box.

e. Click the apply button to save this entry.

6. Within Envision GUI go to Overview Tab -> System Configuration ->Services -> Device Services -> Windows Service -> Manage Windows Logs:

   a. Verify the specific logs you want are checked by default, If not select your preferances..

   b. Verify the "Adaptive polling Range" meet your requirements, If not select your preferances.

   c. When all changes have been made Click Apply.

   d. Restart the Nic Windows service.

   e. Allow 4 to 5 min and then verify under Manage Monitored devices your device is listed.

Verification of GUI configuration

1. Within Envision GUI go to Overview Tab -> System Configuration ->Services -> Device Services -> Windows Service -> Manage Windows Domains. Is there an entry for the domain in which the machines you are trying to gather logs from listed?

   a. If windows domain is not listed Click on Add,

   b. Select the Domain from the drop down Menu. (When configuring the Windows Domain make sure you use a user that has Domain admin privileges(required))

      i. If windows domain does not show up in drop down list attempt the following.

      ii. Go to the desktop of the envision server and open up "My Network Connections" and browse for the domain.

      iii. If you can't browse for the domain you may have a network issue. This issue should be resolved first before proceeding.

      iv. You can also manually type in the domain if it doesn't show up but underlying network issues may cause event collection problems.

   c. If using an Authentication server it must be defined before envision is able to use it. To define the Authentication server do the following:

      i. Within Envision GUI go to Overview Tab -> System Configuration -> Users -> Manage Authentication Servers.

         1. Click Add

         2. Enter the fully qualified Hostname of the Auth server

         3. Choose LDAP of SSL (default) or Choose LDAP over port 389

2. Within Envision GUI go to Overview Tab -> System Configuration ->Services -> Device Services -> Windows Service -> Manage Windows Service. Is there an entry for the windows machine in question?
    a. If not Click on Add and create an entry.
    b. Select the domain where this machine resides from the dropdown list.
    c. Add the IP address of the machine you want to collect logs from.
    d. Check off the enabled box.
    e. Click the apply button to save this entry.
    f. Restart the Nic Windows service.
    g. To perform a bulk add procedure, enVision requires that the Windows NetBIOS over TCP/IP be enabled and your DNS resolution name options be set correctly. For more information review the help file. Search for “Required LAN Settings for NIC Windows Service”
3. Within Envision GUI go to Overview Tab -> System Configuration ->Services -> Device Services -> Windows Service -> Manage Windows Logs:
    a. Is “Used by default” checked off for the expected logs?
        i. If not Click on the specific logs you want by default.
    b. Does the “Adaptive polling Range” meet your requirements
        i. If not modify the range for your requirements
    c. When all changes have been made Click Apply.
4. Within Envision GUI go to Overview Tab -> System Configuration –> Devices -> Manage Monitored Devices.
    a. Is there an entry for the windows machine in question? If not Perform the following from a command prompt:

Verification of Communication (Wintool.exe)

i. At the cmd prompt change to the e:\envision\bin folder. Type the following cmd:
wintool -e "show summary; show threads; show list nd 10000" > ..\logs\%COMPUTERNAME%_windows.txt

ii. This will generate a log under e:\envision\logs folder with the envision host name_windows.txt. Open this file up with notepad:

iii. Examples of a log file:

(See the wintool appendix for more info)

1. (1) WAITING 10.10.30.10 Security Microsoft Windows 2000 (900 +) Tue Feb 20 17:22:30 2007 (No new events) (Normal)
2. (2) UNRESPONSIVE 10.10.30.190 Security Microsoft Windows XP (3600 ~) Tue Feb 20 18:07:35 2007 (OpenEventLog failed: A required privilege is not held by the client.) (Improper access rights)
3. (3) DISABLED 10.10.30.118 System (84600 ~) Wed Feb 21 11:37:51 2007 (Unabled to connect to registry: 5 Access is denied.) (remote registry service not running / Improper access rights)

b. Under manage monitored devices is the Analyze Box checked off for the detected windows server?

i. If not,

1. Check the box
2. Click Analyze. Without this box you can not analyze any reporting data for this machine

Verification of Proper rights (Runeventvieweras.exe)

5. Using windows explorer:

a. Go to e:\envision\bin folder and run the application runeventvieweras.exe.

b. Enter an account and password that has admin rights (same account you setup under “Manage Windows Domains”).

c. Click on the Event Viewer folder.

d. Click on the Action menu.

e. Select “Connect to remote computer” from the drop down list.

f. Type in the IP of the server.

g. Click OK. If it connects try and open each of the logs. If you can view log information this account has the proper access rights.

Appendix:
Wintool Options w/ descriptions

Using wintool.exe

Overview

The wintool executable is used to debug the windows collection processes. It connects directly to a winprocess.exe instance (using named pipes) and lets you see real-time statistics about the current state of collection. The wintool executable must be run on the same box as the winprocess executable you are trying to debug. The wintool executable can be run interactively, or non-interactively in script-mode (using *–e*).

Wintool.exe supports the following command-line arguments,

-h	displays help information
-d <domain>	specify to which winprocess.exe to connect
-e “commands”	run *commands* in script-mode (instead of interactive)

In interactive mode, if no domain was specified, on the command line (using *–d*) then a list of known domains (from the windowsServiceDomainConfig table) is displayed. Type the number corresponding to the domain and press return to begin the interactive session. If only one domain is configured then the interactive session begins immediately connected to that domain. You cannot run in interactive mode against multiple domains at the same time.

In script-mode, if no domain is specified, the given commands will be run against all domains found. You can only specify one domain on the command line. The result of the commands is output to stdout. You can specify multiple commands to run by separating them by semicolons. For example, `wintool –e "show threads; show polling"` will execute *show threads* and then *show polling* for each domain.

Commands

All are available in both script and interactive modes. In the examples section the output from each command it shown and explained.

- `show summary`

  Displays a summary of the states of the log files for the domain.

- `show threads`

  Displays status information about the collection threads.

- `show polling`

  Displays status information about the logs currently being polled.

- `show list ( nd | nq | hd | hq | iq ) N`

  Displays the top N logs from the list specified,

  - nd, normal priority logs
  - nq, normal priority log queue
  - hd, high priority logs
  - hq, high priority log queue
  - iq, inactive log queue (logs in disabled or unresponsive state)

  In general, you will run `show list nd 50`, to show the top 50 logs in the normal priority list. If you specify N larger than the number of logs all logs will be returned.

- `filter [(+|-)(P|Q|W|U|D)]`

  Used to change the results for `show list`. Without an argument it displays the current filter setting. Using `filter -D` filters out disabled log files; likewise, `filter +D` will show disabled log files. `P` for polling; `Q` for queued; `W` for waiting; `U` for unresponsive; and `D` for disabled.

- `show entry ( id N | ip a.b.c.d )`

  Displays details about a specific log file, or a specific IP address. The display includes a history of each polling attempt.

- `Reset [nextTimeToRun]`

  Resets the next-time-to-run value for all log files to the current time. This will cause all log files to be polled as soon as possible..

Examples

show summary

```
Threads:            15
Inactive threads:    2

High: (0)
        Polling      0
        Queued       0
        Waiting      0 (late: 0)
        Unresponsive 0
        Disabled     0


Normal: (351)
        Polling      15
        Queued       18
        Waiting      125 (late: 0)
        Unresponsive 51
        Disabled     142

89187 log files polled in 47884.03 seconds.  (1.863 polls per second / 0.537 seconds per poll)
```

The first two lines show the number of each type of threads available to the winprocess. Inactive threads are used exclusively for log files in the disabled or unresponsive state. The next two sections are a count of the log files by state in each of the priorities. Currently, the UI does not enable you to set a log file to the high priority. The number in parenthesis after the priority the total number of logs. The count of “late” logs are those logs in the waiting state that are past due to be moved to the Queued state (but cannot because the queue is full). The last line aggregate number of polls and collection time.

show threads

```
Thread Information:

        ( 0)      Collection  =>  processing (344) 192.168.1.50, System
        ( 1)      Collection  =>  processing (320) 192.168.1.24, System
        ( 2)      Collection  =>  processing (315) 192.168.1.22, Application
        ( 3)      Collection  =>  waiting for object
        ( 4)      Collection  =>  processing (317) 192.168.1.22, System
        ( 5)      Collection  =>  processing (323) 192.168.1.25, System
        ( 6)      Collection  =>  processing (302) 192.168.1.155, System
        ( 7)      Collection  =>  processing (343) 192.168.1.50, Application
        ( 8)      Collection  =>  waiting for object
        ( 9)      Collection  =>  waiting for object
        (10)      Collection  =>  processing (321) 192.168.1.25, Application
        (11)      Collection  =>  processing (300) 192.168.1.155, Application
        (12)      Collection  =>  processing (305) 192.168.1.160, Application
        (13)      Collection  =>  waiting for object
        (14)      Collection  =>  processing (304) 192.168.1.160, System
        (15)        Inactive  =>  waiting for object
        (16)        Inactive  =>  waiting for object
```

The first column (in parenthesis) is the thread id number. Each thread displays its thread type ("Collection" or "Inactive”—inactive threads are used only for logs marked as disabled or unresponsive) and their status. In general this will be "waiting for object", indicating that the thread is waiting to be notified that there is work to do, or “processing” the given log file.

show polling

```
Normal:
        (  331)    192.168.1.29      Security Microsoft Windows Server 2003 => ProcessEventRecord(14707)
        (  343)    192.168.1.50   Application          Microsoft Windows XP => ProcessEventRecord(43470)
        (   44)    10.10.15.121   Application          Microsoft Windows XP => ProcessEventRecord(38621)
        (   57)    10.10.20.128   Application        Microsoft Windows 2000 => ReadEventLog(894)
```

```
(   42)    10.10.15.121        System          Microsoft Windows XP => ProcessEventRecord(17990)
(   59)    10.10.20.128        System       Microsoft Windows 2000 => GetNumberOfEventLogRecords
(   92)    10.10.30.172        System       Microsoft Windows 2000 => ProcessEventRecord(1157)
(  265)   192.168.1.118      Security       Microsoft Windows 2000 => ProcessEventRecord(675988)
(   14)   10.10.100.114        System          Microsoft Windows XP => ProcessEventRecord(10190)
(  308)    192.168.1.18      Security Microsoft Windows Server 2003 => ProcessEventRecord(9642586)
(  309)    192.168.1.18      Security Microsoft Windows Server 2003 => OpenEventLog
(  115)    10.10.30.195      Security       Microsoft Windows 2000 => ProcessEventRecord(841627)
(  242)   192.168.1.103        System          Microsoft Windows XP => ProcessEventRecord(24990)
(   12)   10.10.100.114   Application          Microsoft Windows XP => ReadEventLog(1584)
(   48)    10.10.15.124   Application          Microsoft Windows XP => ProcessEventRecord(1)
```

This shows a list of the logs in the polling state. If any log files were high priority there would be a second list. The number in parenthesis is the log id number, which is assigned at configuration time and uniquely tied to the log file for the duration of the winprocess execution. Next is displayed information about the log: the IP address, log name, OS type and file the status of the polling. You will mainly see logs in the ProcessEventRecord(X), where X is the record number currently being processed.

show list nd 32

```
(  329)       POLLING    192.168.1.28      Security Microsoft Windows Server 2003 (   30 - ) Fri Feb 10 09:58:42 2006 (Ok)
(  250)       POLLING   192.168.1.106      Security       Microsoft Windows 2000 (   30 ~ ) Fri Feb 10 09:58:43 2006 (Ok)
(   24)       POLLING    10.10.15.107   Application         Microsoft Windows XP (  120 - ) Fri Feb 10 09:58:46 2006 (Ok)
(  208)       POLLING    10.10.31.188      Security       Microsoft Windows 2000 (   30 - ) Fri Feb 10 09:58:47 2006 (Ok)
(  226)       POLLING    10.10.31.203      Security         Microsoft Windows XP (   30 - ) Fri Feb 10 09:59:00 2006 (Ok)
(  229)       POLLING    10.10.31.254      Security Microsoft Windows Server 2003 (   30 - ) Fri Feb 10 09:59:02 2006 (Ok)
(  311)       POLLING    192.168.1.19        System Microsoft Windows Server 2003 (  210 - ) Fri Feb 10 09:59:04 2006 (Ok)
(  179)       POLLING     10.10.30.69        System         Microsoft Windows XP (  150 - ) Fri Feb 10 09:59:06 2006 (Ok)
(  346)       POLLING    192.168.1.52   Application Microsoft Windows Server 2003 (  150 - ) Fri Feb 10 09:59:06 2006 (Ok)
(  185)        QUEUED     10.10.30.78        System       Microsoft Windows 2000 (  240 - ) Fri Feb 10 09:59:08 2006 (Ok)
(  218)        QUEUED    10.10.31.195   Application         Microsoft Windows XP (  300 + ) Fri Feb 10 09:59:09 2006 (Ok)
(  165)        QUEUED     10.10.30.61   Application         Microsoft Windows XP (  180 - ) Fri Feb 10 09:59:16 2006 (Ok)
(  217)        QUEUED    10.10.31.195        System         Microsoft Windows XP (  300 ~ ) Fri Feb 10 09:59:19 2006 (Ok)
(  231)        QUEUED     10.10.31.35   Application         Microsoft Windows XP (  300 + ) Fri Feb 10 09:59:20 2006 (Ok)
(   91)        QUEUED    10.10.30.172      Security       Microsoft Windows 2000 (   30 - ) Fri Feb 10 09:59:20 2006 (Ok)
(   61)        QUEUED     10.10.30.10      Security Microsoft Windows Server 2003 (   30 - ) Fri Feb 10 09:59:22 2006 (Ok)
(  140)       WAITING     10.10.30.34        System         Microsoft Windows XP (  120 - ) Fri Feb 10 09:59:24 2006 (Ok)
(    2)       WAITING    10.10.10.252        System       Microsoft Windows 2000 (  210 - ) Fri Feb 10 09:59:25 2006 (Ok)
(  257)       WAITING   192.168.1.113        System         Microsoft Windows XP (  120 - ) Fri Feb 10 09:59:25 2006 (Ok)
(  326)       WAITING    192.168.1.27      Security       Microsoft Windows 2000 (   30 + ) Fri Feb 10 09:59:29 2006 (No new events)
(  289)       WAITING   192.168.1.134      Security       Microsoft Windows 2000 (   30 + ) Fri Feb 10 09:59:29 2006 (No new events)
(  196)       WAITING    10.10.31.142      Security       Microsoft Windows 2000 (   30 + ) Fri Feb 10 09:59:29 2006 (No new events)
(  232)       WAITING     10.10.31.35      Security         Microsoft Windows XP (   30 + ) Fri Feb 10 09:59:30 2006 (Ok)
(  265)       WAITING   192.168.1.118      Security       Microsoft Windows 2000 (   30 - ) Fri Feb 10 09:59:30 2006 (Ok)
(  319)  UNRESPONSIVE    192.168.1.24      Security Microsoft Windows Server 2003 ( 3600 ~ ) Fri Feb 10 10:52:50 2006 (GetNumberOfEventLogRecords or
GetOldestEventLogRecord failed)
(   73)  UNRESPONSIVE     10.10.30.12      Security       Microsoft Windows 2000 ( 3600 ~ ) Fri Feb 10 10:54:59 2006 (OpenEventLog failed: The RPC se
unavailable.)
(   63)  UNRESPONSIVE     10.10.30.11      Security       Microsoft Windows 2000 ( 3600 ~ ) Fri Feb 10 10:54:59 2006 (OpenEventLog failed: The RPC se
unavailable.)
(   81)  UNRESPONSIVE     10.10.30.16   Application Microsoft Windows Server 2003 ( 3600 ~ ) Fri Feb 10 10:54:59 2006 (OpenEventLog failed: Access is
denied.)
(   83)  UNRESPONSIVE     10.10.30.16        System Microsoft Windows Server 2003 ( 3600 ~ ) Fri Feb 10 10:54:59 2006 (OpenEventLog failed: Access is
denied.)
(   18)      DISABLED    10.10.15.101   Application                              (84600 ~ ) Fri Feb 10 16:22:19 2006 (Unable to connect to registry:
network path was not found.)
(   19)      DISABLED    10.10.15.101      Security                              (84600 ~ ) Fri Feb 10 16:22:19 2006 (Unable to connect to registry:
network path was not found.)
(   10)      DISABLED   10.10.100.113      Security                              (84600 ~ ) Fri Feb 10 16:21:58 2006 (Unable to connect to registry:
network path was not found.)
```

This is a list of the top 32 logs on in the normal directory (“nd”). You will see that they are sorted by next time to run. The first number (in parenthesis is the log id, and then follows the state, IP, log name and OS type of the log file. The next number (also in parenthesis) is the current polling interval in seconds. The sign after it indicates the last direction the adaptive algorithm moved the interval: + means it increase, - that it decreased, and ~ that remained unchanged. After the next time to run is the status of the last poll. As you can see above, for logs that failed the error that caused the failure is displayed.

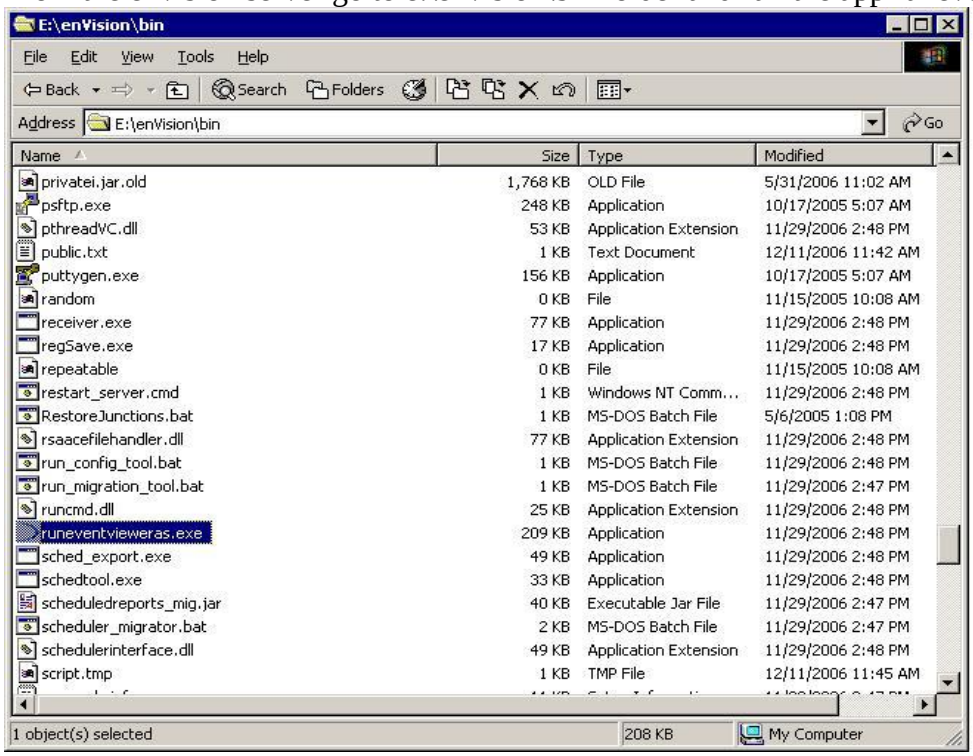
show entry id 24

```
(   24)       POLLING    10.10.15.107                Application         Microsoft Windows XP (  120 + ) Fri Feb 10 10:03:24 2006 (Ok)
         Fri Feb 10 05:19:29 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 1.634 seconds 0.000 real eps (stable) OpenEventLog failed: The
RPC server is unavailable.
         Fri Feb 10 06:20:08 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 1.200 seconds 0.000 real eps (stable) OpenEventLog failed: The
RPC server is unavailable.
         Fri Feb 10 07:20:28 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 1.367 seconds 0.000 real eps (stable) OpenEventLog failed: The
RPC server is unavailable.
         Fri Feb 10 08:20:59 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 1.382 seconds 0.000 real eps (stable) OpenEventLog failed: The
RPC server is unavailable.
         Fri Feb 10 09:21:02 2006 33 events (191.303 eps) 5000 bytes (28985.274 Bps) 0.173 seconds 0.000 real eps (up) Ok
         Fri Feb 10 09:26:00 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 0.008 seconds 0.001 real eps (up) No new events
         Fri Feb 10 09:31:08 2006 0 events (0.000 eps) 0 bytes (0.000 Bps) 0.013 seconds 0.001 real eps (up) No new events
         Fri Feb 10 09:36:17 2006 4169 events (6556.624 eps) 662144 bytes (1041359.822 Bps) 0.636 seconds 0.001 real eps (down) Ok
         Fri Feb 10 09:41:27 2006 3902 events (3684.569 eps) 620212 bytes (585651.994 Bps) 1.059 seconds 0.070 real eps (down) Ok
         Fri Feb 10 09:46:10 2006 4500 events (3013.972 eps) 713944 bytes (478179.376 Bps) 1.493 seconds 0.135 real eps (down) Ok
         Fri Feb 10 09:50:13 2006 2446 events (2375.778 eps) 393616 bytes (382315.753 Bps) 1.030 seconds 0.209 real eps (down) Ok
         Fri Feb 10 09:53:32 2006 1729 events (1190.897 eps) 266768 bytes (183743.878 Bps) 1.452 seconds 0.248 real eps (down) Ok
         Fri Feb 10 09:56:46 2006 3756 events (3559.165 eps) 597868 bytes (566536.390 Bps) 1.055 seconds 0.276 real eps (down) Ok
         Fri Feb 10 09:59:27 2006 4500 events (5154.102 eps) 713944 bytes (817720.061 Bps) 0.873 seconds 0.337 real eps (down) Ok
         Fri Feb 10 10:01:24 2006 21 events (21.134 eps) 3260 bytes (3280.801 Bps) 0.994 seconds 0.410 real eps (up) Ok
```

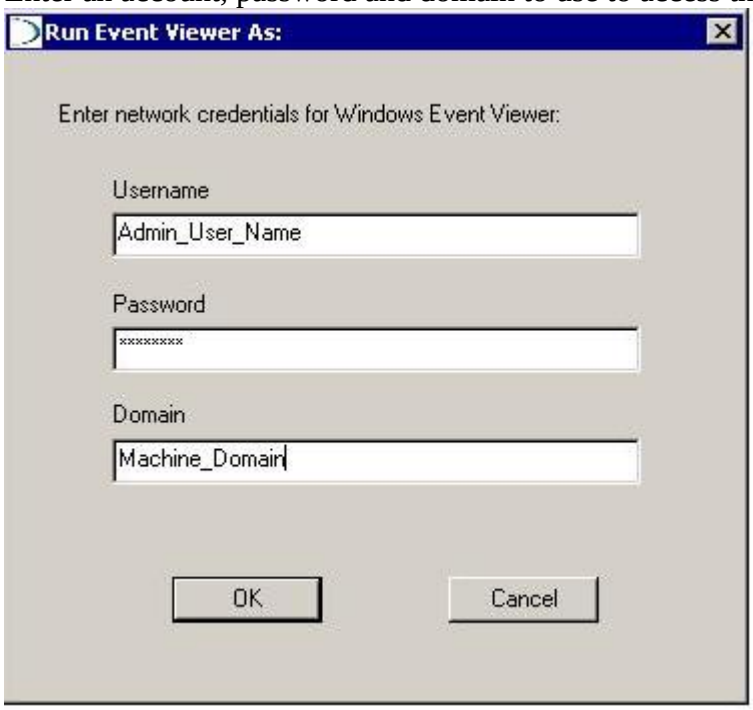
This lists all of the information for a given log file (or all of the log files for an IP address). The first line is the same data as returned by “show list”. The following lines show the historical polling information for that log file, including number of events/bytes retrieved, the time spent polling the log, and EPS information. The real eps value at the end is calculated by the total number of events read from the log over the real difference in clock time. The first eps value is eps from the remote log to the windows collection service. The “up”, “down”, “stable” indicates what modification was made to the polling interval as a result of that poll. And the poll status is give at the end of the line. In the above example you can see that the box was unavailable during the early morning hours and came back online between the 8:20 and 9:21 polls.

Runeventvieweras.exe Screenshots

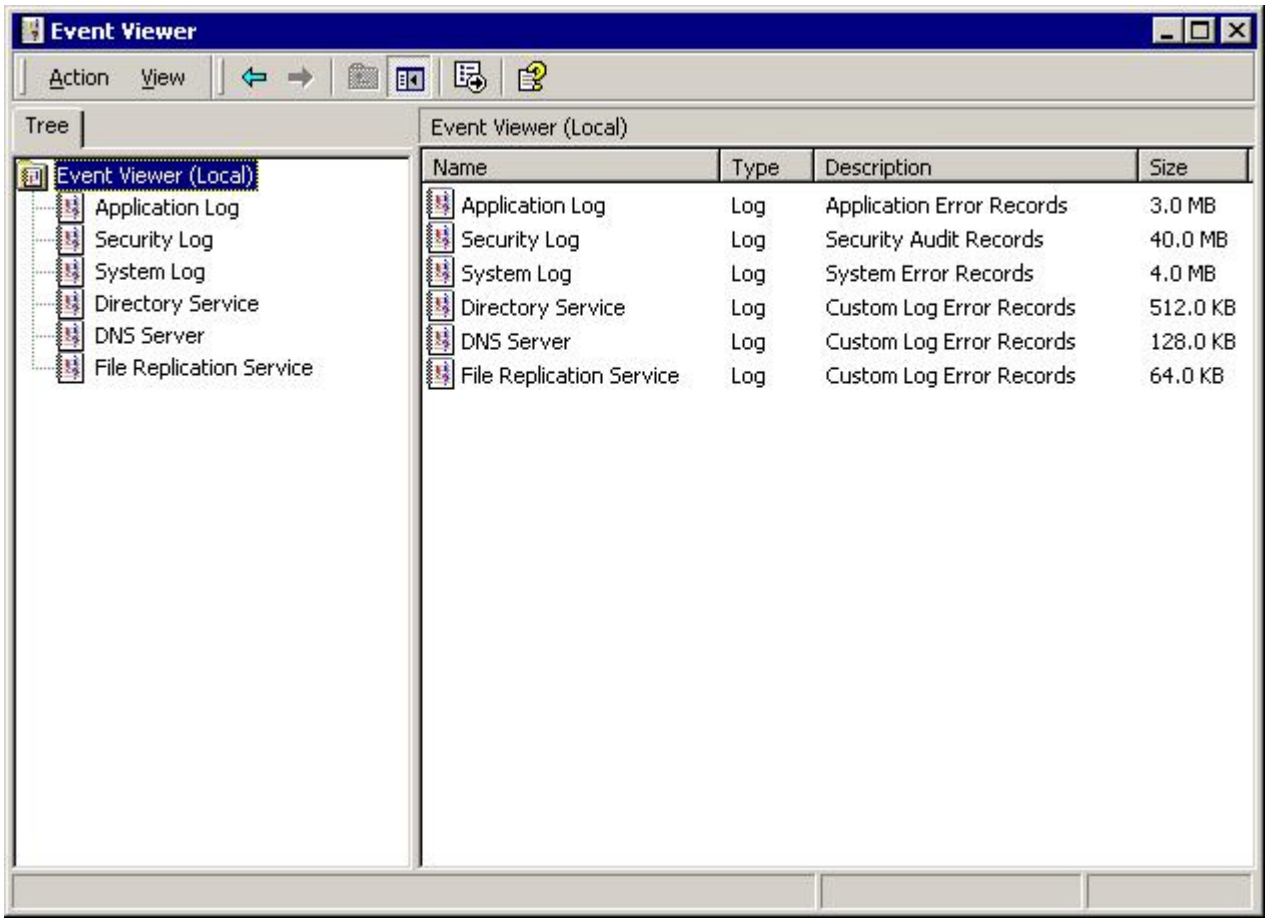
From the envision server go to e:\envision\bin folder and run the app runeventvieweras.exe



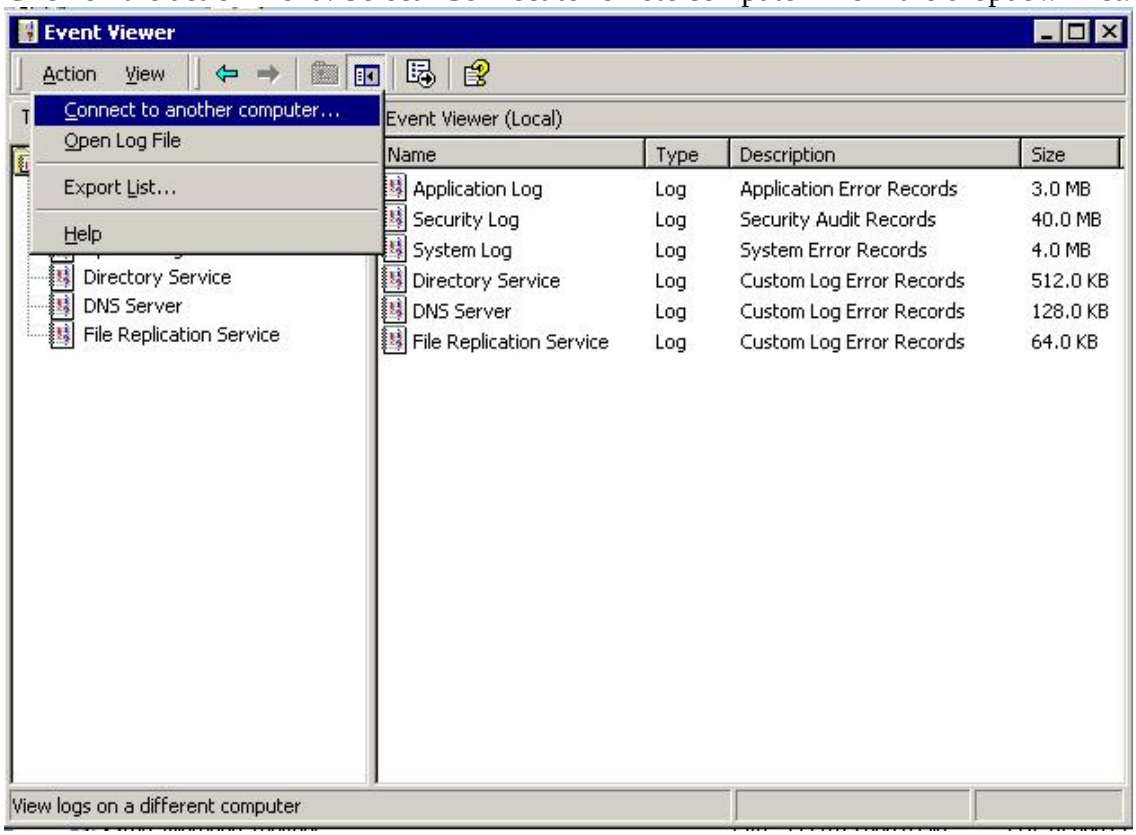
Enter an account, password and domain to use to access the remote registry of the windows machine.



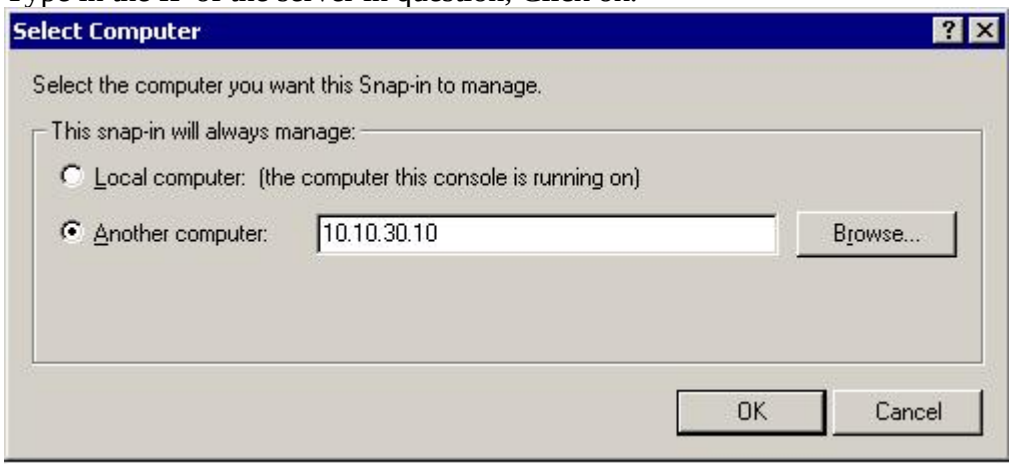
Click on the Event Viewer folder.



Click on the action menu. Select "Connect to remote computer" from the dropdown list.



Type in the IP of the server in question, Click ok.



If it can't connect it is either a network connectivity issue or Authentication issue (Domain\UserName - password) (localmachinename\UserName - password))

If you can connect but when you click on a particular log you get Access denied could be (Authentication / Remote registry service (not running / running under incorrect service account))

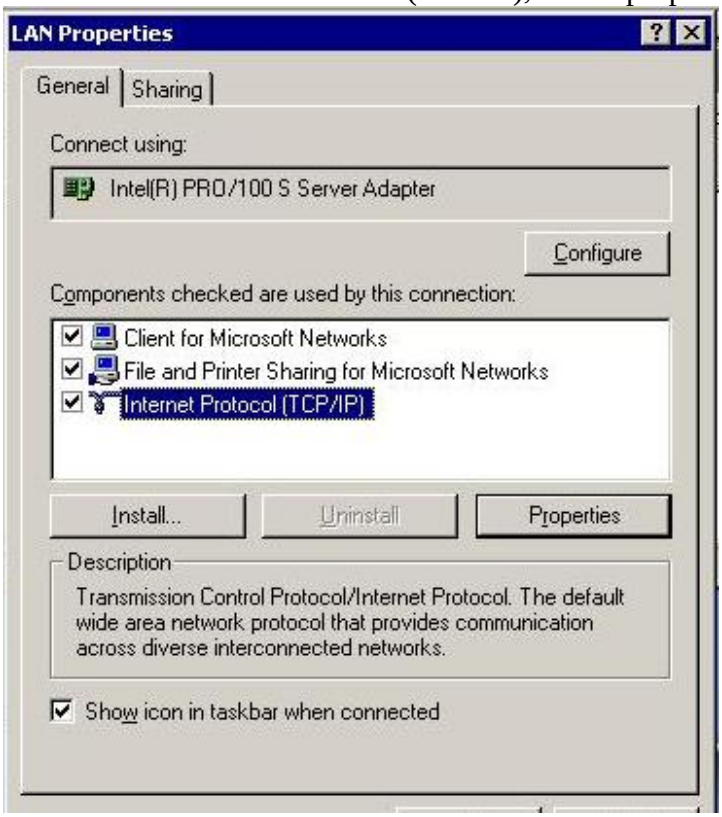
Ports used for Windows Event Collection

TCP 135, 139, 445 and dynamic RPC ports Outbound HA, LC, RC

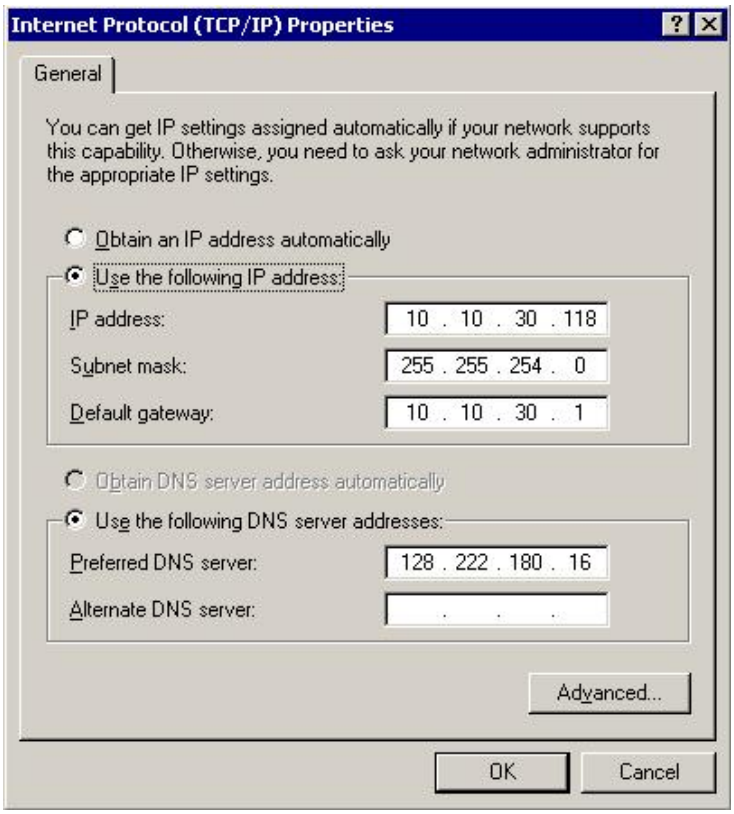
Network Settings and configuration Screenshots

Select the interface you are using to collect logs from and go to the properties page.

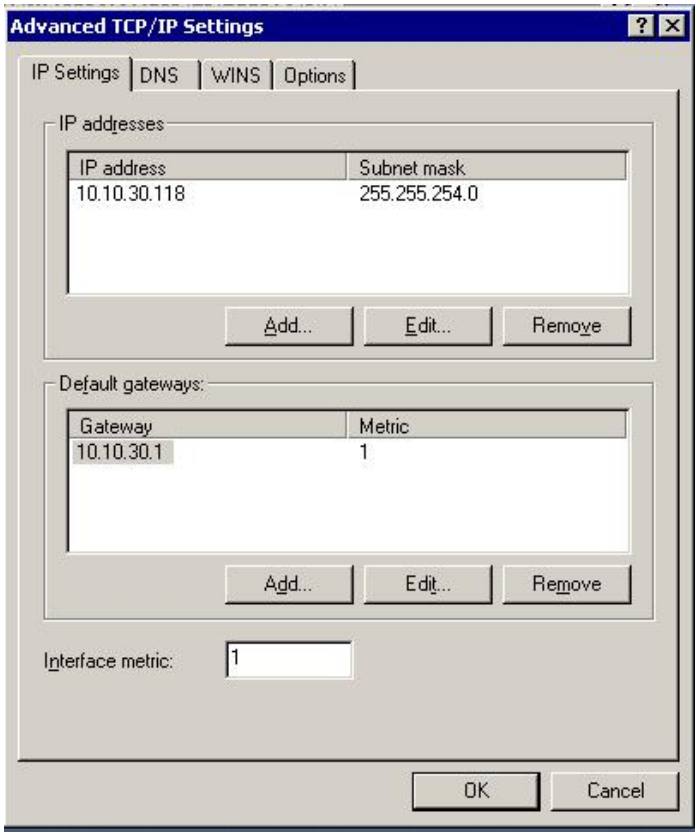
Click on the “Internet Protocol (TCP/IP), Select properties



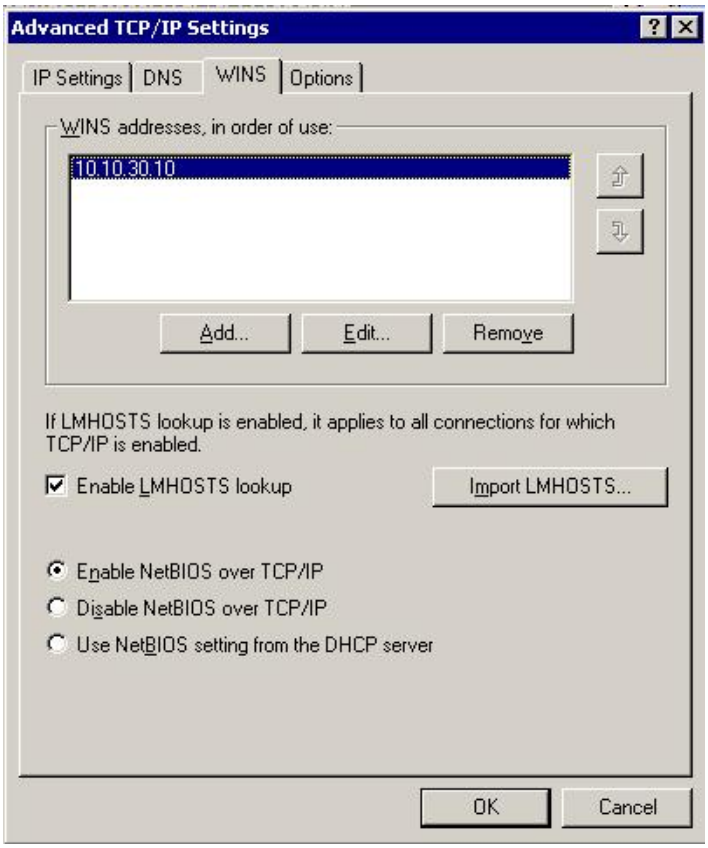
Click on Advanced button



Click on the Wins Tab



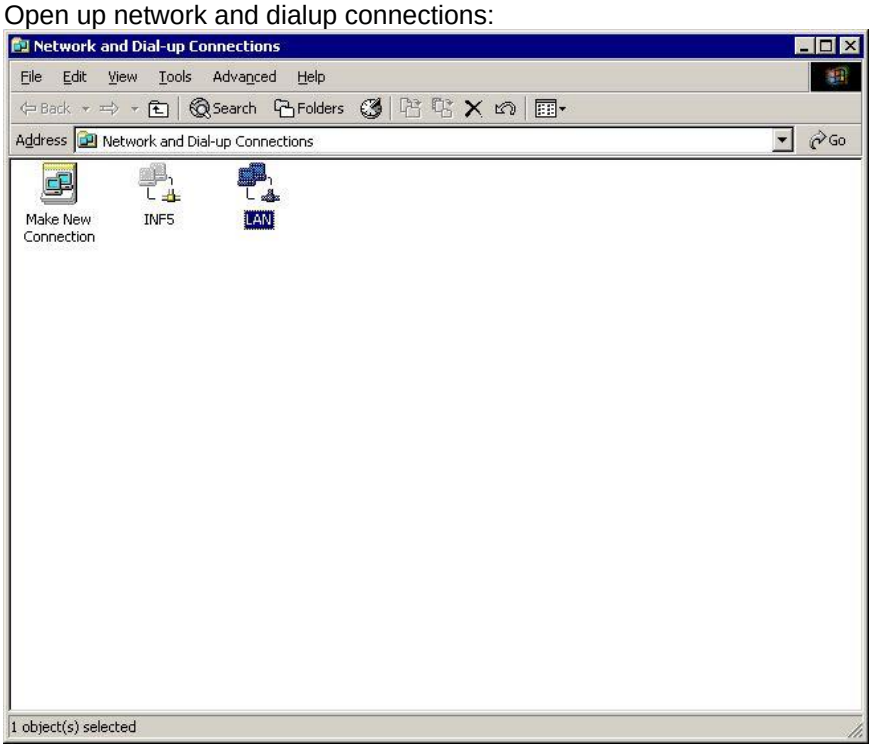
Verify Netbios over TCP is selected, Click Ok



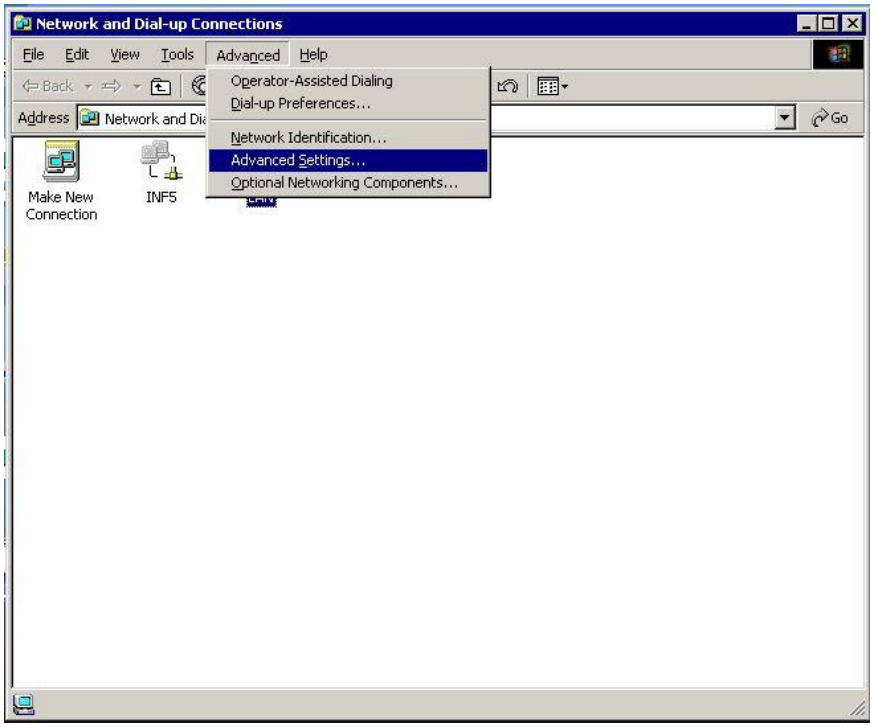
Binding Order:

(Make sure you are on the appliance (Not via terminal services), making these changes will cause you to loose your network connection momentarily)

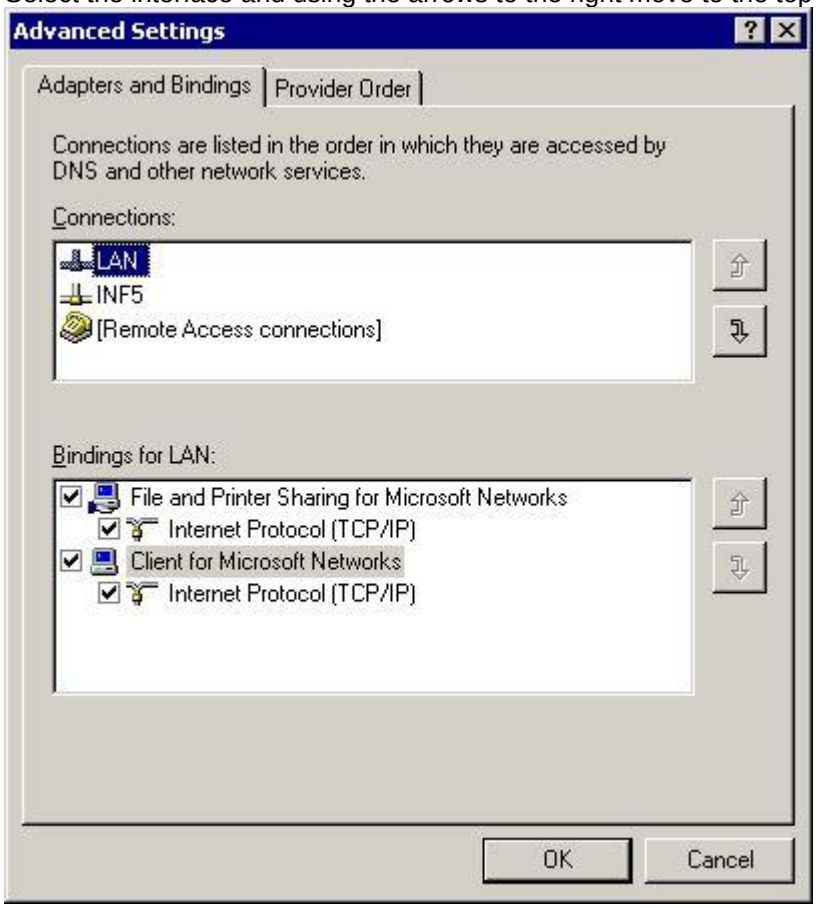
Open up network and dialup connections:



Select the Lan card, Go to the Advanced menu item and select Advanced Settings.

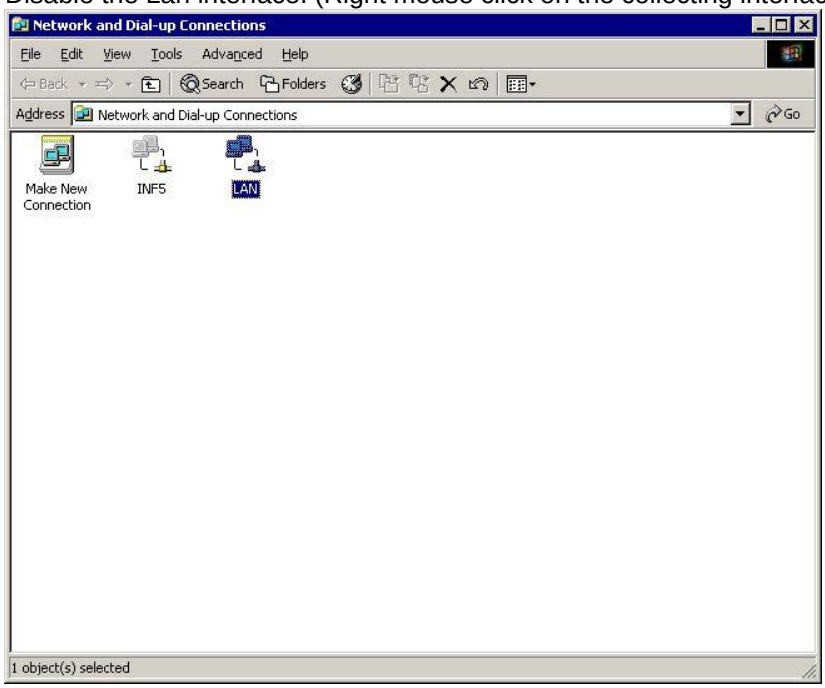


Verify that the Lan interface or the collecting interface is the first one in the list if not make it the first. Select the interface and using the arrows to the right move to the top of the list. Click ok



(Notice the next steps can not be done via terminal service connection!!)

Disable the Lan interface. (Right mouse click on the collecting interface and select Disable)



Re-enable the LAN interface. (Right mouse click on the collecting interface and select Enable)

Verification of Database configuration (ISQL)

(Warning table changes should only be done on the phone or webex session with Technical Spport)

Using windows explorer:
(On the AS and the LC to make sure there are no differences.)

Go to e:\envision\database\cmd folder and run the application StartISQL.cmd. A sql query window will open awaiting your query instructions

Type: “select * from device_list where dtypename=’winevent_nic’” (Hit F5 to execute) This will return a list of all discovered windows machines

i. Does this list include the machines in question? If not Review Steps #1, #2 above under “Verification of GUI configuration”

ii. Are the “States” of all the machines in question listed as “Active”? If not Review Step #2d

iii. Is the “Analyze” box checked for all the machines in question? If not Review Step #4 b

Using windows explorer:

Go to e:\envision\database\cmd folder and run the application StartISQL.cmd. A sql query window will open awaiting your query instructions

Type: “select * from windowsServiceDomainConfig” (Hit F5 to execute) This will return a list of all configured windows domains.

iv. Does this list include all domains in question? If not Review Step #1 above under “Verification of GUI configuration”

v. Are there multiple instances of any of the domains? If so call Technical Support.

Using windows explorer:

Go to e:\envision\database\cmd folder and run the application StartISQL.cmd. A sql query window will open awaiting your query instructions

Type: “select * from windowsServiceClientConfig order by ip” (Hit F5 to execute) This will return a list of all configured windows machines

vi. Does this list include the machines in question? If not Review Step #2 a-g above under “Verification of GUI configuration”

vii. Do all the machines in question have the expected logs “Enabled” box checked? If not Review Step #3 a-c