ZENworks Windows Agent Troubleshooting

Indumathi B & Ingo Engels

18 November 2015

About us

- Indumathi B
  - ZENworks Windows Agent Core Developer in Rapid Response Team
- Ingo Engels
  - ZENworks Backline Support Engineer

Collecting general agent debug information

- Set debug log level
- Collect debug information with the command:
  - `zac zeninfo`

-> `%tmp%\zeninfo-<date>.zip`

- For Endpoint Security Management and Full Disk Encryption a Diagnostic Package can be created.

Agent Install

- PreAgentPkg_Agent.exe
  - Command line options:
    - q (no reboot prompt)
    - x (no reboot)
    - k (registration key)
    - Z (ZESM install information)
    - v (verbose logging)
  - Defaults to Location Awareness Lite

-> `%windir%\novell\zenworks\bin\ZPA.status`

Agent Configuration

- ZENworks Agent Configuration in ZENworks Control Center
- Windows Registration values
  Mostly documented at:
  https://www.novell.com/documentation/zenworks114/zen11_sys_registry_keys/

Agent Registration

- %zenworks_home%\conf\initial-web-service
- %zenworks_home%\bin\conninfo.dat
- zac reg (-g)
- zac unr
  - -s (local only)
  - -f (force)
  - -a (asynchronous)
- New with ZeUS since 11.4:
  - %zenworks_home%\pstore\ZeUSStore

-> zmd-messages.log

Agent Self Defense

- Protects only Endpoint Security Management part:
  - Using Windows Task Manager to terminate any Endpoint Security Agent processes.
  - Stopping or pausing any Endpoint Security Agent services.
  - Removing critical files and registry entries. If a change is made to any registry keys or values associated with the Endpoint Security Agent, the registry keys or values are immediately reset.
  - Disabling NDIS filter driver binding to adapters.
- Configurable through ZENworks Agent Configuration settings or Security Settings Policy

Location Awareness

- Location Detection is always done in Endpoint Security Management agent component
- ‘Full’ Mode:
  - ESM Agent binds 2 drivers to each network adapter configuration:
    - Novell ZENworks Wireless Location Awareness
    - Novell ZENworks Location Awareness
  - Active network configuration change detection
- ‘Lite’ Mode only effective without ESM:
  - Driverless OS triggered passive network configuration change detection

-> `C:\ProgramData\Novell\ZES\Logs\`

System Update

- Traditional: System Update Content downloads through ZENworks Agent

-> `zmd-messages.log`

- ZeUS (ZENworks Update Service) - New with 11.4:

-> `%zenworks_home%\ZeUS\`

- Disable use of ZeUS

-> `HKLM\Software\Novell\ZCM: EnableTraditionalUpdate (Reg_SZ):True`

- Zenupdater

-> `%zenworks_home%\logs\system-update\<System Update GUID>\system-update.log`

Agent Refreshes

- System Start

-> Intial Refresh after agent service startup

- Partial Refresh

-> Mainly Policy data, no Bundle data processed but gets all assignment on first run

- General Refresh

-> Everything but on first refresh no assignments

- UIRefresh

- Random Time to Wait

Reading zmd-messages.log

- Agent service start :

```
[DEBUG] [09/23/2015 08:00:09.402] [1684] [ZenworksWindowsService] [8] [] [InitZMD] [] [Start Init] [] [] [] [ZENworks Agent]
-> 1684: Agent Service process ID
-> 8: Agent Thread
-> InitZMD: Agent Module Name
```

- User Login gets prepared:

```
[DEBUG] [09/23/2015 08:02:05.552] [1684] [ZenworksWindowsService] [11] [] [RemotingService] [] [ZENCreateSession entered] [] [] []
[ZENworks Agent]
[DEBUG] [09/23/2015 08:02:05.552] [1684] [ZenworksWindowsService] [11] [] [RemotingService] [] [ZENCreateSession calling
EnsureSession with ID:  787959] [] [] [] [ZENworks Agent]
-> 787959: Session ID of logged-in User
-> 999 is always the Device Session ID
```

- User Login starts:

```
[DEBUG] [09/23/2015 08:02:09.966] [1684] [ZenworksWindowsService] [11] [] [RemotingService] [] [ZENLogin entered] [] [] [] [ZENworks
Agent]
```

- A refresh starts:

```
[DEBUG] [09/23/2015 08:02:11.308] [1684] [ZenworksWindowsService] [11] [iengels] [RefreshMgr] [] [(Thread=11; SessionId=787959;
RefreshType=PartialRefresh) ProcessRefresh entered] [] [] [] [ZENworks Agent]
```

- Refresh triggers a module:

```
[DEBUG] [09/23/2015 08:02:11.392] [1684] [ZenworksWindowsService] [11] [iengels] [RefreshMgr] [] [(Thread=11; SessionId=787959;
RefreshType=PartialRefresh) Calling Refresh Handler: Assignment Manager Module] [] [] [] [ZENworks Agent]
```

- Module Refresh concludes:

```
[DEBUG] [09/23/2015 08:02:11.651] [1684] [ZenworksWindowsService] [11] [iengels] [RefreshMgr] [] [(Thread=11; SessionId=787959;
RefreshType=PartialRefresh) Finished Refreshing Assignment Manager Module: 259 ms] [] [] [] [ZENworks Agent]
```

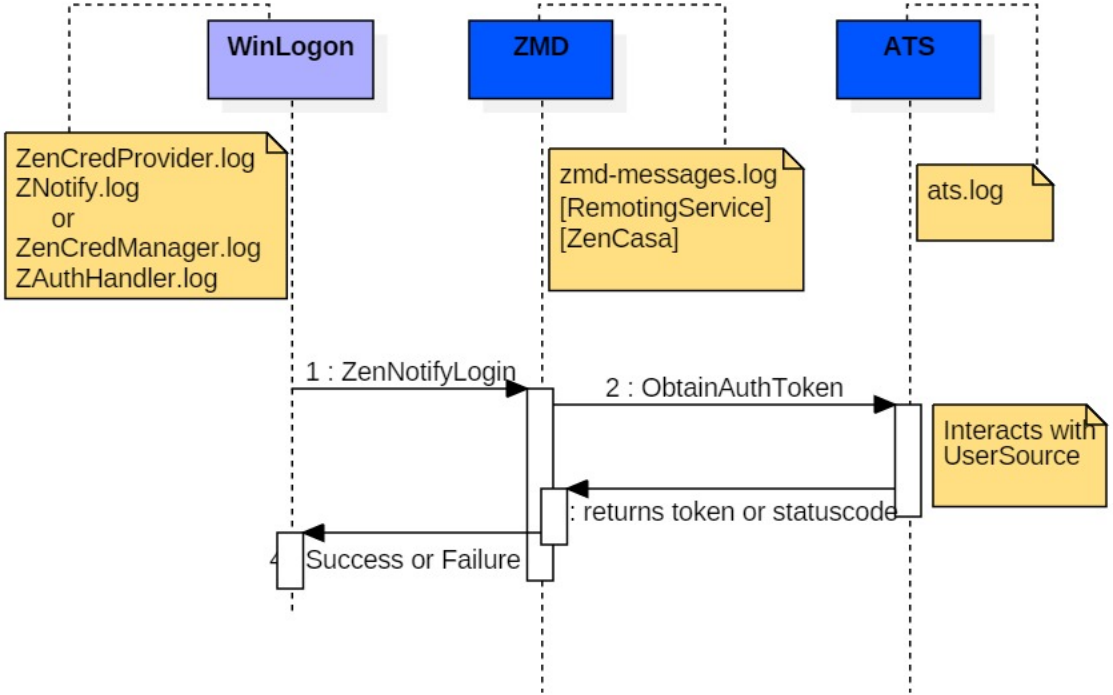
- A refresh concludes:

```
[DEBUG] [09/23/2015 08:02:11.727] [1684] [ZenworksWindowsService] [11] [iengels] [RefreshMgr] [] [(Thread=11; SessionId=787959;
RefreshType=PartialRefresh) ProcessRefresh exited: 0,718 seconds] [] [] [] [ZENworks Agent]
```

Adaptive Agent Components

- User Management
- Image Management
- Bundle Management
- Policy Management
- Patch Management
- Asset Management (Inventory always enabled)
- Remote Management
- Endpoint Security Management
- Full Disk Encryption

User Management



%windir%\system32\ZenCredManager.log:

```
[ZenCredMgr] [] [NPLogonNotify called.]
[ZenCredMgr] [] [NPLogonNotify Store update not required.]
[ZenCredMgr] [] [NPLogonNotify called.]
[ZenCredMgr] [] [NSSCSSetCredential credman successful!.]
[ZenCredMgr] [] [Script string is C:\Windows\system32\ZAuthHandler.exe
-D"WIN-7-SP1-X64" -U"admin" -L"141886" -H"0" ]
```

%tmp%\ZAuthHandler.log:

```
[ZAuthHandler] [] ZenNotifyLogin entered
[ZAuthHandler] [] ZenNotifyLogin calling zenlgn - UserName = admin   Domain= WIN-7-SP1-X64
[ZAuthHandler] [] ZenNotifyLogin Success
```

%windir%\system32\ZenCredentialProvider.log:

```
[ZenCredentialProvider]  []  [CNotify::LocalPreLogonNotify() - Called]
[ZenCredentialProvider]  []  [CNotify::LocalPreLogonNotify() - Returning]
```

%windir%\system32\ZenNotify.log:

```
[ZenNotify]  []  [ZenNotifyLogin entered]  []
[ZenNotify]  []  [ZenNotifyLogin returning 0]
[ZenNotify]  []  [ZENworks user authentication Success]
```

HKLM/Software/Novell/CASA
Key: [SessionID] = Value: ZenCredProvider/CredManager/ZIcon

%zenworks_home%\logs\LocalStore\zmd-messages.log:

```
[ZenworksWindowsService]  [] [RemotingService] [] [ZENIsServerAvailable entered]
[ZenworksWindowsService]  [] [RemotingService] [] [ZENIsServerAvailable returning SUCCESS]

[ZenworksWindowsService]  [] [RemotingService] [] [ZENLogin entered]

[ZenworksWindowsService]  [] [ZenCasa] [] [ObtainAuthToken entered]
[ZenworksWindowsService]  [] [ZenCasa] [] [ObtainSessionTokenFromServer entered]
[ZenworksWindowsService]  [] [ZenCasa] [] [ObtainSessionTokenFromServer returned with code 0]
[ZenworksWindowsService]  [] [ZenCasa] [] [ObtainAuthToken returned with code 0 ]

[Persist credentials @HKLM/Software/Novell/ZCM/ZenLgn/History/Cache/[realm]/metadata]

[ZenworksWindowsService]  [] [RemotingService] [] [ZENStoreCredentials Entered]
[ZenworksWindowsService]  [] [RemotingService] [] [ZENStoreCredentials returning True]
```

[Disconnected Login]

```
[ZenworksWindowsService] [] [RemotingService] [] [ZENIsServerAvailable entered]
[ZenworksWindowsService] [] [RemotingService] [] [No good primary servers..need
```

```
[ZenworksWindowsService] [] [RemotingService] [] [ZENVerifyCache entered]
[ZenworksWindowsService] [] [RemotingService] [] [About to call VerifyCredentials ]
```

%ZENworks_HOME%\share\ats\etc\svc\ Ats.log

[Realm configuration]
[<%ZENworks_HOME%>\share\ats\etc\svc\IAREALMS.XML]

[ATS] [] [(ClientAddr=10.71.55.62)invoke()- NamingException: (LDAP: error code 49 - NDS error: failed authentication (-669))Exception occured while adding connector specified at (XPath: /bci:realms/bci:realm(@id='BLR-SRM-R7S-TREE'))]

[ATS] [] [(ClientAddr=10.71.55.62)invoke()- Reason could be due to LDAP errors: (LDAP: error code 49 - NDS error: failed authentication (-669))Exception occured while adding connector specified at (XPath: /bci:realms/bci:realm(@id='BLR-SRM-R7S-TREE'))]

[ATS] [] [(ClientAddr=10.71.55.62)invoke()- Failed to resolve identity for entity user1]

```
[keystore corrupted:]
%ZENworks_HOME%\share\tomcat\webapps\CasaAuthTokenSvc\WEB-INF\classes\casa_crypto.properties
%ZENworks_HOME%\conf\security\trusted-ats-jks-store]
```

```
[ATS] [] [(ClientAddr=10.71.67.22)Autheticated IdentID:CN=Indu,CN=Users,DC=epm,DC=blr,
          DC=novell,DC=com] [authtoksvc.PwdAuthenticate]
```

```
[ATS] [] [(ClientAddr=10.71.67.22)getSecureTokenUtilObj()- Exception caught, message =
          Keystore was tampered with, or password was incorrect] [authtoksvc.SessionToken]
         [] [] [CASA]
```

```
[ATS] [] [(ClientAddr=10.71.67.22)Constructor()- Failed to obtain secure token util object]
         [authtoksvc.SessionToken] [ATS] [] [(ClientAddr=10.71.67.22)invoke()- Exception:
          java.lang.Exception: SessionToken.Constructor() - Failed to obtain secure token
          util object]
         [authtoksvc.Authenticate] [] [] [CASA]
```

Image Management

- Novell ZENworks ISD Service installed in Windows 7 or newer. In Windows XP ziswin.exe gets launched.
- Updates or restores ZENworks Image Save Data at Windows startup
- The service stops itself after work is finished
- Can be launched after agent install but before reboot e.g. to restore device name
- Configured the

-> `%zenworks_home%\logs\preboot\novell-zisdservice.log`

ZISD can by viewed, edited or cleared with:
`%zenworks_home%\bin\preboot\ziswin.exe`

`ziswin.exe` also allows configuration of the Restore & Collection Mask

Bundle & Policy Management

- Having device related assignment with user account related system access
- Metadata & Schedules through configuration role
- Content
- Windows Explorer integration through nalshell.dll

-> %zenworks_home%\logs\nalshell.txt

-> %zenworks_home%\logs\NSNalWin.txt

-> zmd-messages.log

Patch Management

- ZENworks Core Agent - ‘vehicle’ to transfer patch related configuration & content

-> `zmd-messages.log`

- Heat Software patch agent (analyze.exe & remediate.exe) – Patch install & detection

-> `%zenworks_home%\zpm\debug*.txt`

- Additional patch agent debug information:
  - `<Device GUID>.state` -> Patch Scan result
  - `*plp_result.txt` -> Patch Install result
  - `SnoozeList.xml` -> Patch Scan scheduled for next device boot-up
  - Application Event Log

Asset (Inventory) Management

- Knowledge Base Files Bundles
  - `%zenworks_home%\bin\*.kb`
- Inventory Scan
  - Enable Diagnostic Mode
  - Collector Priority-> only Normal or Idle implemented

  -> `%zenworks_home%\logs\colw32.log`
- Usage Tracking
  - `HKLM\Software\Novell\ZCM\Usage:`
  - `UMUserFullName(Reg_SZ)=0`

    -> Always lowercase user logon id
  - `UMDiagnostic (DWORD)=1`

    -> Debugging
- Scan Results

  -> `%zenworks_home%\work\inventory\*.xml`

Remote Management

- Timesync
- Mirror Driver
- JoinProxy connection
- Configuration through Remote Management policy

-> `zmd-messages.log & winVNC logs`

Endpoint Security Management

- Security Policy Assignment / Effectiveness
  - Location based
  - Zone, Folder, Object
  - Inheritance
- USB devices
- Folder encryption

-> ZESM diag package

Full Disk Encryption

- Preboot Authentication & DMI settings
- Hardware (OPAL) vs. Software Encryption
- Emergency recovery

-> FDE diag package

Q & A