



DII COE WINDOWS NT KERNEL

8 July 99

Command Center Development Group
Jet Propulsion Laboratory
David DeVey



Agenda



- Introduction/Background
- Common Data Store
- Installation Process
- Process Management
- Account Management
- Differences between UNIX and NT
- Technical Tidbits
- Questions



Introduction/Background



- This presentation assumes attendance at the DII COE 4.x Developer's Technical Exchange Meeting
 - Meeting held 13-15 April in Washington DC
 - Discussed Changes to COEInstaller, CDS, APM, et cetera.
- NT DII COE Kernel 3.x vs. 4.x
 - Previous (3.x) version was simply comprised of the COEInstaller only
 - DII COE Kernel emphasizes cross-platform solutions to common problems such as installation
 - Major gain in COE 4.x kernel is in cross-platform systems admin.



Introduction/Background (Cont.)



- The DII COE Kernel has been built for Windows NT Version 4.0
 - Service Pack 4
 - Caution:
 - Service Pack 5 - currently testing at DISA.
 - For Intel Platforms only (no PowerPC or DEC Alpha version)
 - Latest deliverable supported only NT Workstation, not Server.
 - Plans are to release support for NT Server in next delivery.



Introduction/Background (Cont.)



- Functionality available now on Windows NT
 - Common Data Store (CDS)
 - Segment Installation
 - COEInstaller
 - Enterprise-wide Account Management
 - Accounts & Profile Management
 - Accounts can be added across the Administrative Domain
 - Process Management
 - In line with DII COE on UNIX
 - Increased Security
 - Meets DISA guidelines for increased security



Common Data Store (CDS)



- OLE Structured Storage, a set of Component Object Model (COM) interfaces.
- OLE Compound Files - Microsoft's implementation of these interfaces.
- The DII Windows NT host implementation of the Common Data Store (CDS) is achieved through the use of OLE Compound Files.
- CDS can be thought of as the “registry” for the COE Kernel and is located in a set of structured storage files on the NT platform.



Common Data Store (CDS) (Cont.)



- CDS storages:
 - Local Host - segments loaded, local users, groups, and profiles.
 - Local Host Private - Secure information about the local host such as authentication keys, and password policies.
 - Master Host - “administrative domain”-wide information. This information is NOT distributed about the administrative domain. This info is served by the Master APM Server only.
 - User - Information specific to the user account such as profiles.
 - User Private - Secure information specific to the user account.



Common Data Store (CDS) (Cont.)



- User and User Private storages are created unique to each account on the local machine when the account is accessed the first time.



Installation Process



- COEInstaller is the primary tool for loading DII COE Segments
 - COEInstaller handles identifiable \$DIRECTIVES found in the IRTS (3.1)



Installation Process (cont)



- Populates CDS with process launch information.
- Lays down necessary segment specific files under the \h directory on the boot partition.
- Populates HKLM\SOFTWARE\COE registry sub-key with segment specific information.
- Notifies Master APM Server of the installation.



Audit Logging



- Start/Programs/Administrative Tools (Common)/Event Viewer - accesses the event log viewer NT application.
- Audit logging is sent to the application event log under the COEKERNEL source.
 - COE Kernel platform neutral Java clients
 - COE Kernel platform DLLs
 - COEKERNEL service



Audit Logging (Cont.)



- Must be logged into an account that has Administrator privilege to view the application event log on the local host machine.
- COEKERNEL source entries - Refer to it often!



Process Management



- Supported processes:
 - Boot Processes
 - Session Processes
 - Session-exit Processes
 - Background Processes
 - Run-Once Processes



Process Management (Cont.)



- Boot Processes
 - Launched at machine boot time
 - Launched as SYSTEM principal
 - Some non-interactive WindowStation, and non-active Desktop.
 - Process information stored in CDS
 - CDS is populated from the SegInfo key word \$BOOT
 - Start and Stop - available through the Services dialog applied to COEKERNEL.exe service.
 - Caveat: Windows NT 4.0 Process Management
 - Services dialog Pause and Continue - implemented together as effectively a restart of all boot processes.
 - Boot services are an extension of the COEKERNEL service.



Process Management (cont)



- Session Processes
 - Launch
 - Immediately upon login or -
 - Upon assumption through the COE Profile Selector application.
 - Launched as interactive user principal
 - Interactive user's token acquired and used to launch session/session-exit processes under that principal.
 - Coclass/interface CLSID_Logon/IID_Ilogon served up by COEKERNEL service called by COELOGON client using RPC_C_IMP_LEVEL_IMPERSONATE.
 - Session process information stored in CDS
 - CDS is populated from the SegInfo key word \$SESSION
 - Shutdown
 - Interactive-session termination (logoff) or -
 - Explicitly by the interactive user
 - Normal process termination



Process Management (cont)



- Session-Exit Processes
 - Launch
 - Immediately upon Interactive-session termination (logoff) or
 - System shutdown.
 - Upon de-assumption through the COE Profile Selector application.
 - Launched as interactive user principal
 - Interactive user's token acquired and used to launch session/session-exit processes under that principal.
 - Coclass/interface CLSID_Logon/IID_Ilogon served up by COEKERNEL service called by COELOGON client using RPC_C_IMP_LEVEL_IMPERSONATE.
 - Session process information stored in CDS
 - CDS is populated from the SegInfo key word \$SESSIONEXIT
 - Shutdown
 - Explicitly by the interactive user
 - Normal process termination



Process Management (cont)



- Session-Exit Processes (cont.)
 - Interactive Session Termination (Logoff)
 - COEKERNEL service uses a hidden window created in the Interactive Window Station of the Active Desktop -
 - WM_QUERY_ENDSESSION
 - WM_ENDSESSION
 - Answers FALSE to WM_QUERY_ENDSESSION
 - Launches SESSION-EXIT processes under the interactive-user's current profile set.
 - When all SESSION-EXIT processes have terminated only then is logoff action taken.
 - System Shutdown By Interactive User
 - Same as the description for Logoff above with one caveat
 - Results in logoff only - requiring interactive user to issue 2nd shutdown command.
 - This situation results from the NT 4.0 logoff/shutdown message sequence.



Process Management (cont)



- Background Processes
 - Launched once only, immediately upon 1st user login.
 - Launched as SYSTEM principal.
 - Some non-interactive WindowStation, and non-active Desktop.
 - Process information stored in CDS
 - CDS is populated from the SegInfo key word \$BACKGROUND
 - Shutdown
 - Reboot
 - Normal process termination



Process Management (cont)



- Run-Once Processes
 - Launched once only, immediately upon 1st boot after COE Kernel installation.
 - Launched as SYSTEM principal.
 - Some non-interactive WindowStation, and non-active Desktop.
 - Process information stored in CDS
 - CDS is populated from the SegInfo key word \$RUN_ONCE
 - Shutdown
 - Reboot
 - Normal process termination



Account Management



- Account Management is through Accounts & Profile Manager (APM)
 - Cross platform solution to APM administration
 - Java client - platform neutral.
 - Create/Modify/Delete Windows NT Accounts/Groups **from** any machine within the “Administrative Domain” (definition required) **on** any machine within the Administrative Domain!
 - All APM configuration information stored in CDS
 - Accounts are created/modified/deleted from the NT O/S using Win32 NETAPI



Account Management (cont)



- Account Management is through Accounts & Profile Manager (APM)
 - Backdoor APM not supported or recognized under COE Kernel
 - Users created through USER MANAGER or the command line will NOT be displayed within APM Client.
 - Leave profile management (as related to kernel and installed apps) to COE Kernel as well.
 - COE Kernel APM provides enterprise-wide account management.
 - Security-related information (e.g. passwords) held as usual by the Windows NT Local Security Authority.
 - “Global” or “Domain” Account/Group support currently under integration test at JPL.



Differences Between UNIX & NT



- UNIX uses Icons as primary means of launching, NT uses the Start menu on the active desktop.
- Handling of Accounts between UNIX and NT
 - Global Accounts - accomplished through Microsoft Windows Network domains under NT and through NIS+ domains on Solaris.
 - UIDs do not apply on NT.



Differences Between UNIX & NT (Cont.)



- Handling of Groups between UNIX and NT
 - Global Groups - accomplished through Microsoft Windows Network domains under NT and through NIS+ domains on Solaris.
 - GIDs do not apply on NT.
- How are passwords handled
 - NT passwords are validated using LogonUser.
 - It turns out you need a privileged process to perform the validation
 - SE_TCB_NAME
 - APM Server - boot process running as SYSTEM principal.



Differences Between UNIX & NT (Cont.)



- Environmental Variable Support
 - No support for NT environment variables - \$ENVIRONMENT
- No System Administrator (SA) Tool Support On NT
 - Examples of Unix SA tools:
 - Setting system time
 - Disk mount facilities
- Installer \$DIRECTIVES not supported on NT
 - \$PERIODIC



Technical Tidbits



- Internet Explorer 4.0 installation conflicts with the Kernel
 - Programs located in the startup directory do not start on login. This was a problem with the Active Desktop which was removed from IE 5.0. Thus far, IE 5.0 looks good.
- Service Pack 4.0 Problem
 - RPC breaks.
 - IE 3 & 5 do not appear to have this same problem.



Questions/Comments



- Check the newsgroup
- For problems, submit a GSPR
- For enhancements, submit a GSPR



Background - Security



- Out of the scope of this discussion.
- Mitre has NT security research results.