



Continuous C&A: Minimize Risk with Agents and Associations



Presented to:
NLIT Summit 2007
June 10-13, 2007

Ryan Alldredge
Computer Scientist
Enterprise Architecture & Data Provisioning
Lawrence Livermore National Laboratory



University of California



This work was performed under the auspices of the U.S. Department of Energy by the University of California
Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.



Agenda



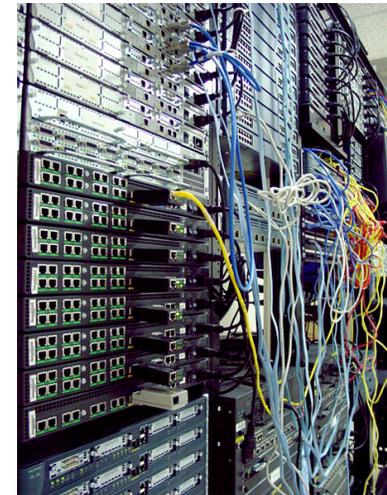
- **Problem Statement**
- Definitions
- Reconciliation Service Design
- Making Associations
- Calculating C&A Compliance
- Reporting
- Questions



Problem Statement



- System management tools provide excellent insight into system health, configuration, and security posture.
- However, there is not a single software package that is suitable for all situations or use cases
 - PCs (Win, Mac, UNIX, Linux)
 - Servers (Win, Mac, UNIX, Linux)
 - Printers
 - Network Infrastructure
 - Blackberry





Problem Statement



- At LLNL, we currently utilize the following; many of which have been extended to answer various Certification & Accreditation (C&A) questions.

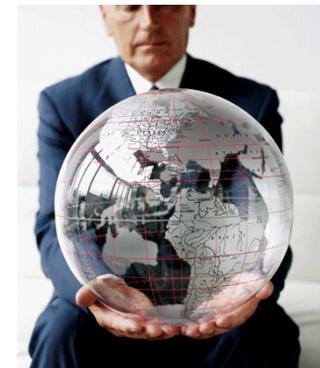




Problem Statement



- **This is all great, each class of device is typically supported by a different team who specializes in that area.**
- **But what about an enterprise-wide view of the whole system?**
 - **You could run six reports and correlate the data to Configuration Items (CI).**
 - By the time you finish, the security landscape has likely changed several times over.
 - **You could store each agent's internal ID with the CI.**
 - ID could change if agent is re-installed
 - Difficult to integrate new management suites
 - If different agents return different results, which do you trust?
 - **You could implement a Reconciliation Service.**





Problem Statement



- **The CIO launched the CMDB initiative in FY06.**
- **He desired a single source of truth about our networks to prove we are in compliance and understand the state of our computing environment.**
- **Unclassified requires a similar level of rigor as classified.**
 - **We couldn't afford 10x more ISSO's.**
- **Should be able to answer the following questions rapidly, repeatable, and accurately:**
 - **What systems are on our network? Are they properly configured?**
 - **What security vulnerabilities do they have?**
 - **Where are the systems?**
 - **What information do the systems process and store?**
 - **Who authorizes access to the information on these systems?**
 - **What systems do foreign nationals use?**
 - **Etc.**





Agenda



- Problem Statement
- **Definitions**
- Reconciliation Service Design
- Making Associations
- Calculating C&A Compliance
- Reporting
- Questions



Definitions



- **Reconciliation Service** – merges disparate datasets from management suites and other apps into a single, controlled set, utilizing metadata to eliminate overlap and conflicts
- **Certification & Accreditation (C&A)** – process mandated by the Federal Information Systems Management Act of 2002
- **Configuration Management Database (CMDB)** – a repository of information related to all the components of an information system
- **Configuration Item (CI)** – any component of an IT infrastructure that is under the control of configuration management
- **Agent** – client-side software that interacts with system management suites (LANDesk, Microsoft SMS, etc.)
- **Association** – a foreign key stored on each registered operating system record, linking to a dataset of reconciled data



Agenda



- Problem Statement
- Definitions
- **Reconciliation Service Design**
- Making Associations
- Calculating C&A Compliance
- Reporting
- Questions



Reconciliation Service Design



- **We chose to build our own, based on concepts found in industry white papers.**
 - Implemented in Java and PL/SQL
 - DBMS is Oracle 10g Release 2
- **Could also be purchased as part of a commercial CMDB.**
- **Requirements:**
 - Allow the addition or subtraction of data sources, columns, and precedence levels without coding changes.
 - Keep track of source system at the attribute level.
- **The database schema contains the following tables:**
 - 4 metadata tables
 - 1 key persistence table
 - 1 reconciled dataset table
 - Various value standardization mapping tables



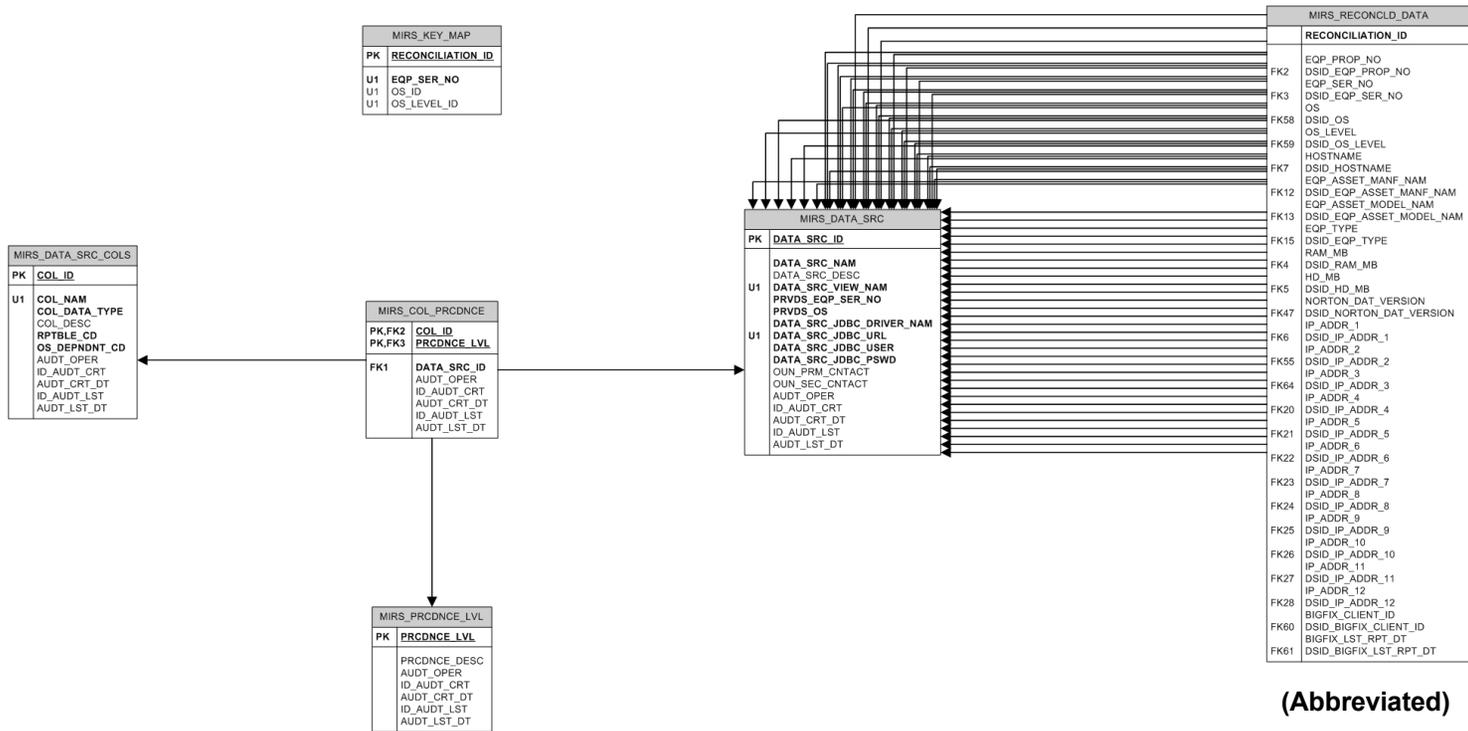
ORACLE



Reconciliation Service Design



- Core ERD





Reconciliation Service



- **Every table, except the reconciled dataset table, utilizes triggers to keep track of the who, what, and when**
 - **Columns include**
 - AUDT_OPER – (i.e., insert, update, delete)
 - ID_AUDT_CREATE – who created the record originally
 - AUDT_CREATE_DT – when they did it
 - ID_AUDT_LST – who touched it last
 - AUDT_LST_DT – when they did it
- **These tables also have shadows that we call the journal tables, and suffix with “_jn”**
 - **Can be used to reconstruct the configuration at a point in time**



Reconciliation Service Design



- **Data Source Table**
 - **Where you register system management tools and other applications**
 - **Provide the name of the database view**
 - **Provide connection information**
 - Could be local or remote
 - We chose to support Oracle and SQL Server connections via JDBC, but could be extended easily
 - **Provide developer contact info**

MIRS_DATA_SRC	
PK	DATA_SRC_ID
	DATA_SRC_NAM
	DATA_SRC_DESC
U1	DATA_SRC_VIEW_NAM
	PRVDS_EQP_SER_NO
	PRVDS_OS
	DATA_SRC_JDBC_DRIVER_NAM
U1	DATA_SRC_JDBC_URL
	DATA_SRC_JDBC_USER
	DATA_SRC_JDBC_PSWD
	OUN_PRM_CNCTACT
	OUN_SEC_CNCTACT
	AUDT_OPER
	ID_AUDT_CRT
	AUDT_CRT_DT
	ID_AUDT_LST
	AUDT_LST_DT



Reconciliation Service Design



- **Data Source Columns Table**
 - Register SQL column names that are to be included
 - Provide column data type (VARCHAR2, NUMBER, DATE)
 - Indicate if there could be multiple values (Repeatable)
 - Example: IP and MAC addresses
 - Indicate if the column is “OS Dependent”
 - Example: If the machine is multi-boot, the hostname will vary based on OS. The hostname is “OS Dependent”
 - The building location is the same for both OS instances, therefore building is not “OS Dependent”
 - **Must also add columns to Reconciled dataset table.**

MIRS_DATA_SRC_COLS	
PK	COL ID
U1	COL_NAM COL_DATA_TYPE COL_DESC RPTBLE_CD OS_DEPNENT_CD AUDT_OPER ID_AUDT_CRT AUDT_CRT_DT ID_AUDT_LST AUDT_LST_DT



Reconciliation Service Design



- **Precedence Level Table**

- **Define acceptable values and their meanings**

- Example: 1, 2, 3, 4, 5 (one has the highest precedence)

- Will need one precedence level per source system providing the same column

- Sources can't share the same precedence level

- Leaving gaps is recommended. Easier to change order later.

MIRS_PRCDNCE_LVL	
PK	<u>PRCDNCE_LVL</u>
	PRCDNCE_DESC AUDT_OPER ID_AUDT_CRT AUDT_CRT_DT ID_AUDT_LST AUDT_LST_DT



Reconciliation Service Design



- **Column Precedence Table**
 - **Define the precedence of the various data sources at the column level.**
 - Example: For building, trust Sunflower Assets over LANDesk if they differ
 - For MAC Address, trust Opsware Network over Sunflower Assets if they differ
 - **Many-to-Many relationship between columns and precedence levels.**

MIRS_COL_PRCDNCE	
PK,FK2	<u>COL_ID</u>
PK,FK3	<u>PRCDNCE_LVL</u>
FK1	DATA_SRC_ID AUDT_OPER ID_AUDT_CRT AUDT_CRT_DT ID_AUDT_LST AUDT_LST_DT



Reconciliation Service Design



- **Key Map Table**

- **Used for reconciled dataset primary key persistence**

- We truncate the reconciled dataset daily, rather than compare

- **The primary key (Reconciliation ID) represents a composite of columns, that when found in multiple data sources, can be assumed to be running on the same OS instance**

- We chose Serial Number, Operating System, and Operating System Level (version)

- In our experience, users who run the same OS and version, use virtualization technology that provides a different S/N

- Could be made more strict, but matches would decrease

MIRS_KEY_MAP	
PK	<u>RECONCILIATION_ID</u>
U1	EQP_SER_NO
U1	OS_ID
U1	OS_LEVEL_ID



Reconciliation Service Design



- **Reconciled Data Table**

- **Contains the dataset produced by the Reconciliation Service.**
- **Each column defined in the Data Source Columns table must exist here, along with a corresponding “DSID” column.**
 - Names could be made generic, but it is less confusing to use actual names.
- **Columns that were defined as “repeatable” must exist here (denormalized) for the max number of repeats defined.**
- **Our production table contains over 150+ columns. Oracle has a limit of 1000.**

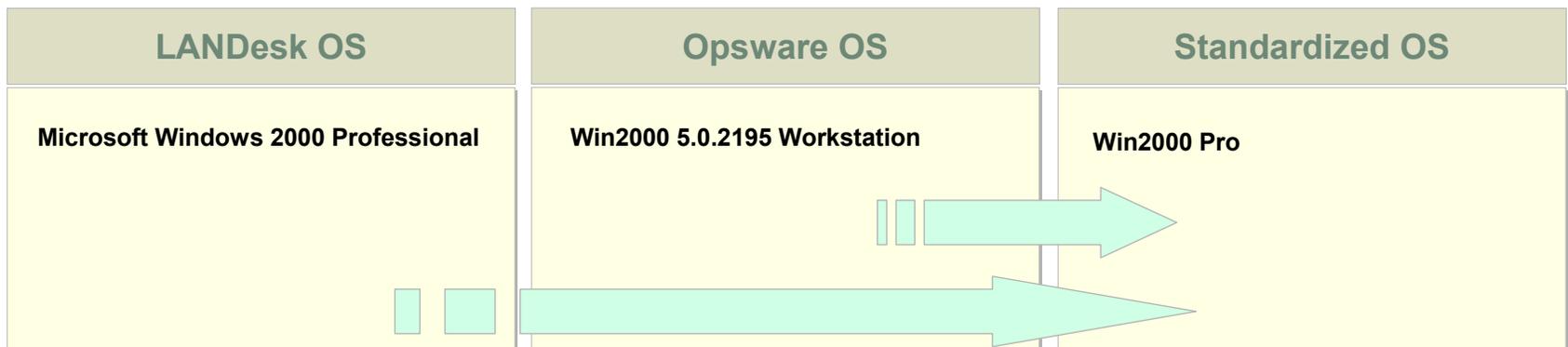
MARK_RECONCILED_DATA	
RECONCILIATION_ID	
FK01	EQP_PROP_NO
FK02	DSID_EQP_PROP_NO
FK03	EQP_SER_NO
FK04	DSID_EQP_SER_NO
FK05	OS
FK06	OS_LEVEL
FK07	DSID_OS_LEVEL
FK08	HOSTNAME
FK09	DSID_HOSTNAME
FK10	EQP_ASSET_NAME
FK11	DSID_EQP_ASSET_NAME
FK12	EQP_ASSET_NAME
FK13	DSID_EQP_ASSET_NAME
FK14	EQP_TYPE
FK15	DSID_EQP_TYPE
FK16	MAN_M8
FK17	DSID_MAN_M8
FK18	HD_M8
FK19	DSID_HD_M8
FK20	REPORTING_DAT_VERSION
FK21	DSID_REPORTING_DAT_VERSION
FK22	IP_ADDR_1
FK23	DSID_IP_ADDR_1
FK24	IP_ADDR_2
FK25	DSID_IP_ADDR_2
FK26	IP_ADDR_3
FK27	DSID_IP_ADDR_3
FK28	IP_ADDR_4
FK29	DSID_IP_ADDR_4
FK30	IP_ADDR_5
FK31	DSID_IP_ADDR_5
FK32	IP_ADDR_6
FK33	DSID_IP_ADDR_6
FK34	IP_ADDR_7
FK35	DSID_IP_ADDR_7
FK36	IP_ADDR_8
FK37	DSID_IP_ADDR_8
FK38	IP_ADDR_9
FK39	DSID_IP_ADDR_9
FK40	IP_ADDR_10
FK41	DSID_IP_ADDR_10
FK42	IP_ADDR_11
FK43	DSID_IP_ADDR_11
FK44	IP_ADDR_12
FK45	DSID_IP_ADDR_12
FK46	BIOPK_CLIENT_ID
FK47	DSID_BIOPK_CLIENT_ID
FK48	BIOPK_LIST_SPT_DT
FK49	DSID_BIOPK_LIST_SPT_DT



Reconciliation Service Design



- **Data Standardization**
 - **Different management suites can report values in different formats and precision.**
 - **Computers manufactured at different times can have several variations of the manufacturer's name.**
 - Example: Dell, Dell Computer Corporation, Dell Inc.
 - **We handle this problem at the database view layer, via mapping tables.**
 - **Standardized values make searching simple.**





Reconciliation Service Design



- **Known Quality Issues**

- **Values that participate in the service should either be:**

- Valid

- Null

- **Non-valid values should be nulled or converted**

- Example: Not all machines return a valid serial number

- '00000000'

- 'To Be Filled By O.E.M.'

- 'SYS-1234567890'

- Handled through the view, or pre-processing





Reconciliation Service Design



- **Special Considerations**
 - **Client re-installs can generate new internal id's in the management suite databases.**
 - Makes it difficult to recognize multi-boot vs. re-install
 - **You should physically remove abandoned entries occasionally, or virtually remove them on the fly.**
 - We look for the maximum “last report date” for our composite key attributes, through the view's where clause.
 - **How long should you trust this data since it last reported?**

```
Windows XP Home Edition Setup

A new partition for Windows XP has been created on
15360 MB Disk 0 at Id 0 on bus 0 on atapi (MBR).
This partition must now be formatted.

From the list below, select a file system for the new partition.
Use the UP and DOWN ARROW keys to select the file system you want,
and then press ENTER.

If you want to select a different partition for Windows XP,
press ESC.

Format the partition using the NTFS file system (Quick)
Format the partition using the FAT file system (Quick)
Format the partition using the NTFS file system
Format the partition using the FAT file system

ENTER=Continue  ESC=Cancel
```



Agenda

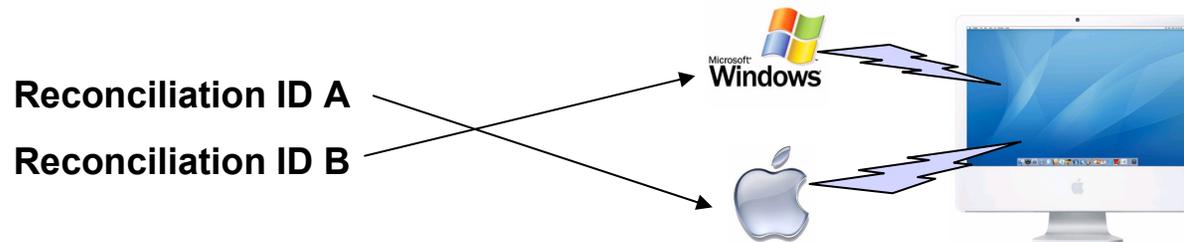


- Problem Statement
- Definitions
- Reconciliation Service Design
- **Making Associations**
- Calculating C&A Compliance
- Reporting
- Questions



Making Associations

- **Configuration Items are manually registered.**
 - This authorizes their access to the network
 - DNS entries are made
- **Operating System instances are also manually registered.**
 - Multiples are supported (multi-boot, virtualization)
- **Associations are automatic.**
 - Data from the reconciled dataset table is associated to the appropriate OS instance by the Reconciliation ID
 - Occurs daily, before C&A is calculated





Making Associations



- CI Registration

Equipment - Windows Internet Explorer

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#).

Logout

Home | C & A | **Equipment** | IP Management | Reports | Roles | Security | Help | Wizard

Search | Add | Bulk Change | SpeedLoad

CMDB Equipment Search

Official User Name DOE # MAC Address
Primary, SysMgr or Custodian Exact Match Exact Match. All other fields ignored if MAC entered

Building Serial # IP Address
Matches first part of building Exact Match Can use % as wildcard (eg 128.115.254.%)

DNS Name Security Plan Equipment Type
Matches first part of host name Select Security Plan Equipment Type

Total Number of Entries: 0

DNS Name	IP Address	Status	Type	Manufacturer (Model)	DOE #	Serial #	Building	Custodian	SysMgr	Primary User	Personal	Prop	Sec	Plan
No rows yet.														

Home | C & A | **Equipment** | IP Management | Reports | Roles | Security | Help | Wizard | Logout

Internet | Protected Mode: On | 100%

*simulated data



Making Associations



- **CMDB Software tab**
 - **Single-boot desktop, running BigFix and LANDesk**

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#). [Logout](#)

Home | C & A | **Equipment** | IP Management | Reports | Roles | Security | Help

Search | Add | Bulk Change | SpeedLoad

Equipment: (ID 86392) (DOE # 0923342) (Serial # 7VWIW23) nliit2007-1.lni.gov

Operating System	Version	Computer Name
WinXP Pro	SP2	nliit2007-1
None		

Associated Data (What is this?)

OS: WinXP Pro
OS Version: SP2
Computer Name: nliit2007-1

OS Sanctioned:
OS Version Sanctioned:
Accounts Managed:
Backups:
Banner OK:
Event Logging:
Anti-Virus:

Security Configuration: None
Auth Configuration: None
Patching: None
Source: Manual

WinXP Pro
SP2
nliit2007-1
LANDESK
LANDESK
BIGFIX
LABIMAGE
AD
LANDESK
LANDESK
BigFix(2007-05-21), LanD

Responsible Manager:
System Manager:

Potentials that were auto-detected.
Associations occur automatically every night. If this is a new machine, it will be associated tonight. The most common reason that associations do not occur is that the serial # that the tool is reporting differs from that in Sunflower. If you have a machine that needs to be corrected, please send mail to cmdb-help@lists.lni.gov.

Error on page. Internet | Protected Mode: On 100%

*simulated data



Making Associations



- **CMDB Software tab**
 - **Dual-boot desktop, running LANDesk**

The screenshot shows a web application interface for equipment management. At the top, there's a navigation bar with tabs for EQUIPMENT, SOFTWARE, NETWORK, SECURITY PLAN, ACCOUNT, HISTORY, SUMMARY, ADVANCED, and HELP. Below this is a table with columns for Operating System, Version, and Computer Name. Two rows are visible, representing a dual-boot system: RHEL WS4 and WinXP Pro. Below the table is an 'Associated Data' section with various configuration options and checkboxes. A blue box highlights a message at the bottom: 'Potentials that were auto-detected. WinXP Pro SP2 nlit2007-3 LanDesk Serial number match. Associated with another entry.'

Operating System	Version	Computer Name
1 RHEL WS4		nlit2007-2
2 WinXP Pro		nlit2007-3

Associated Data (What is this?)

OS: RHEL WS4
OS Version:
Computer Name: nlit2007-2
OS Sanctioned:
OS Version Sanctioned:
Accounts Managed:
Backups:
Banner OK:
Event Logging:
Anti-Virus:
Security Configuration: None
Auth Configuration: None
Patching: None
Source: Manual
Update

Responsible Manager:
System Manager:

Potentials that were auto-detected.
WinXP Pro SP2 nlit2007-3 LanDesk Serial number match. Associated with another entry.

*simulated data



Agenda



- Problem Statement
- Definitions
- Reconciliation Service Design
- Making Associations
- **Calculating C&A Compliance**
- Reporting
- Questions



Calculating C&A Compliance



- Each Configuration Item, that is a C&A Reportable Device (CARD), must be assigned to a FISMA enclave.

Equipment - Windows Internet Explorer

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#)

Logout

Home | C & A | **Equipment** | IP Management | Reports | Roles | Security | Help

Search | Add | Bulk Change | SpeedLoad

Equipment: (ID 86392) (DOE # 0923342) (Serial # 7VWIW23) nlit2007-1.lnl.gov

ID	Number	Name	Type	Action
414		NLIT Enclave	FISMA	Delete

Assign security plans

None [v] Assign

Potential [Foreign National Plans](#)

Match by DOE #, DNS Name, or IP Address

Contact the [DISSO](#) for more information.

Internet | Protected Mode: On 100%

*simulated data



Calculating C&A Compliance



- **C&A compliance is calculated every morning.**
- **Calculations are greatly simplified when there are only two datasets to worry about.**
- **Calculated by looking at each OS instance's broad category (Windows, Mac, UNIX, Linux) to determine appropriate logic.**
 - **Example: not all categories have an anti-virus requirement**
 - **Some calculations use multiple attributes**
- **Reconciliation Service data is trusted over manual values.**
- **Manual data cannot override Reconciliation Service data.**





Calculating C&A Compliance



- Official calculation in right-hand column
 - Manual Anti-Virus determination didn't override LANDesk

Equipment - Windows Internet Explorer

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#)

Home | C & A | **Equipment** | IP Management | Reports | Roles | Security | Help

Search | Add | Bulk Change | SpeedLoad

Equipment: (ID 86393) (DOE # 0923343) (Serial # YAS389WE) nlit2007-2.lnl.gov nlit2007-3.lnl.gov

Operating System	Version	Computer Name
1 RHEL WS4		nlit2007-2
2 WinXP Pro		nlit2007-3
None		

Associated Data (What is this?)

OS: WinXP Pro	WinXP Pro
OS Version:	SP2
Computer Name: nlit2007-3	nlit2007-3
OS Sanctioned: <input type="checkbox"/>	<input checked="" type="checkbox"/>
OS Version Sanctioned: <input type="checkbox"/>	<input checked="" type="checkbox"/>
Accounts Managed: <input type="checkbox"/>	<input checked="" type="checkbox"/>
Backups: <input type="checkbox"/>	<input checked="" type="checkbox"/>
Banner OK: <input type="checkbox"/>	<input type="checkbox"/>
Event Logging: <input type="checkbox"/>	<input checked="" type="checkbox"/>
Anti-Virus: <input checked="" type="checkbox"/>	<input type="checkbox"/>
Security Configuration: None	LABIMAGE
Auth Configuration: None	AD
Patching: None	LANDESK
Source: Manual	LanDesk(2007-05-21)

Responsible Manager:
System Manager:

Potentials that were auto-detected:
WinXP Pro | SP2 | nlit2007-3 | LanDesk | Already Associated

*simulated data



Calculating C&A Compliance



- Agent was only able to obtain OS and patching data
 - Manual values were accepted for others

Equipment: (ID 86394) (DOE # 0923344) (Serial # 63ESWNH) nlit2007-4.lnl.gov

Operating System	Version	Computer Name
Solaris 10		nlit2007-4
None		

Associated Data (What is this?)

OS: Solaris 10
OS Version:
Computer Name: nlit2007-4

OS Sanctioned:
OS Version Sanctioned:
Accounts Managed:
Backups:
Banner OK:
Event Logging:
Anti-Virus:

Security Configuration: P2022
Auth Configuration: P2022
Patching: None
Source: Manual

Responsible Manager:
System Manager:

Associated Data Table:

Solaris 10	
nlit2007-4	
P2022	CMDB
P2022	CMDB
OPSWARE	OPSWARE
OpsWare(2007-05-21)	

Potentials that were auto-detected.
Associations occur automatically every night. If this is a new machine, it will be associated tonight.
The most common reason that associations do not occur is that the serial # that the tool is reporting differs from that in Sunflower.
If you have a machine that needs to be corrected, please send mail to cmdb-help@lists.lnl.gov.

*simulated data



Agenda

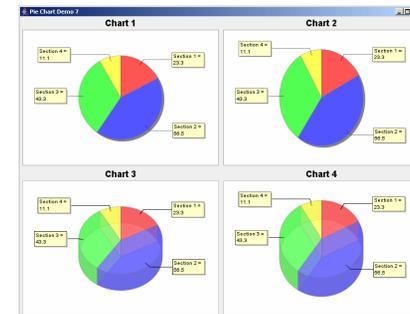


- Problem Statement
- Definitions
- Reconciliation Service Design
- Making Associations
- Calculating C&A Compliance
- **Reporting**
- Questions



Reporting

- **Several reporting options are available.**
 - **C&A Summary**
 - **C&A Rollup**
 - **C&A Detail**
 - **Dashboards**
 - **Enterprise Reporting Workbench**
- **Allows small problems to be resolved before they become large.**
- **Minimizes risk of system shutdown or compromise.**





Reporting



- C&A Summary
 - Red indicates percentages below minimum

CMDB C & A Summary - Windows Internet Explorer

Home C & A Equipment IP Management Reports Roles Security Help Wizard

C & A Detail C & A Summary Enterprise Reporting Workbench (ERW) Upload

C & A Summary

Security Plan: NLIT Enclave (Select Security Plan) Rollup Report (Select for CSP Rollup Report)

Save to Excel

Number	Description	Count	Total	Percent Of Total	Min Required
1.1.1	Responsible Manager	5	5	100.0	100
1.1.2	Identified System Manager	5	5	100.0	100
2.1.1	Mac OS X auto patching	1	1	100.0	50
2.1.2	Linux Satellite Server patching	1	1	100.0	50
2.1.3	UNIX auto patching	1	1	100.0	50
2.1.4	Windows Anti-Virus running	1	2	50.0	90
2.1.5	Mac OS X Anti-Virus running	1	1	100.0	80
2.2.1	Linux minimum security configuration per P2022	0	1	0.0	80
2.2.2	Unix minimum security configuration per P2022	1	1	100.0	80
2.2.3	Mac Authentication per P2022	1	1	100.0	90
2.2.4	Linux Authentication per P2022	1	1	100.0	90
2.2.5	Unix Authentication per P2022	1	1	100.0	90
4.1.1	System in CMDB	5	5	100.0	90
4.2.1	30 Day Logs	5	5	100.0	80
5.1.1	Login Banner	4	5	80.0	90
6.1.1	Lab approved OS (Win, Mac, Linux, Unix)	5	5	100.0	90
6.1.2	Supported Windows version (XP/2000)	2	2	100.0	70
6.1.3	Supported Mac version (10.3-10.4)	1	1	100.0	70
6.1.4	Supported Linux version	1	1	100.0	90
6.1.5	Supported Unix version	1	1	100.0	90
6.1.6	Windows configuration OK	2	2	100.0	80
6.1.7	Mac configuration OK	1	1	100.0	80
7.1.1	Windows Authentication per P2022	2	2	100.0	50
7.1.2	Windows auto patching	2	2	100.0	50
	Total Number Passed All C&A Requirements	3	5	60.0	0
	Total Number of UNIX	1	5	20.0	0
	Total Number of Linux	1	5	20.0	0
	Total Number of non OS X Macs	0	5	0.0	0
	Total Number of OS X Macs	1	5	20.0	0
	Total Number of Windows	2	5	40.0	0
	Total Number of Other Systems	0	5	0.0	0
	Total Number of OS Instances	5	5	100.0	0

Internet | Protected Mode: On 100%

*simulated data



Reporting



- C&A Rollup
 - Collapses multi-boot into single record

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#).

Home | C & A | Equipment | IP Management | Reports | Roles | Security | Help | Wizard

C & A Summary

Security Plan: NLIT Enclave (Select Security Plan) Rollup Report (Select for CSP Rollup Report) [Help](#)

[Save to Excel](#)

Number	Description	Count	Total	Percent Of Total
1.1.1	Responsible Manager	4	4	100.0
1.1.2	Identified System Manager	4	4	100.0
X	OS Auto patching	4	4	100.0
X	OS Anti-Virus running	3	4	75.0
X	OS minimum security configuration per P2022	3	4	75.0
X	OS Authentication per Lab Policy	4	4	100.0
4.1.1	System in CMDB	4	4	100.0
4.2.1	30 Day Logs	4	4	100.0
5.1.1	Login Banner	3	4	75.0
6.1.1	Lab approved OS (Win, Mac, Linux, Unix)	4	4	100.0
X	OS version OK (XP/2000, MacOS 10.3-10.4, etc)	4	4	100.0
	Total Equipment Count	4	4	100.0
	Total Number of OS Instances	5	5	100.0
	Total Number Passed All C&A Requirements	3	4	75.0
	Total Number of Windows	1	4	25.0
	Total Number of OS X 10.3-10.4 Macs	1	4	25.0
	Total Number of other Macs	0	4	0.0
	Total Number of Linux	0	4	0.0
	Total Number of UNIX	1	4	25.0
	Total Number of Heterogeneous Multi-OS Systems	1	4	25.0
	Total Number of Multi-OS Systems	1	4	25.0
	Total Number of Other Systems	0	4	0.0

Home | C & A | Equipment | IP Management | Reports | Roles | Security | Help | Wizard | Logout

[Privacy & Legal Notice](#)

*simulated data



Reporting



- C&A Detail
 - Used to target failures

Recent requests have prompted Open LabNet to propose a new schedule for DNS pushes in production. For details and a chance to comment, see [link](#).

Home | C & A | Equipment | IP Management | Reports | Roles | Security | Help | Wizard

C & A Detail | C & A Summary | Enterprise Reporting Workbench (ERW) | Upload

C & A Detail

Security Plan: NLIT Enclave | OS Category: [Optional] | Failed C&A: [] | Official Username: [] | Any OUN Associated w/Device: []

Search | Clear Form | Save to Excel

Total Number of Entries: 5

Status	Hostname	Prop #	Serial #	Bldg	Security Plan	Os	OS Category	OS Ver	OS Ver OK	Banner	Logging	Sec Config	Auth	Patched	Anti-Virus	Manufacturer	Sysadmin	User
View	ACTIVE	nlt2007-3	0923343	YAS389WE	B5 R41	NLIT Enclave	WinXP Pro	WINDOWS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	HP (8400)	alldredge2	alldredge2
View	ACTIVE	nlt2007-2	0923343	YAS389WE	B5 R41	NLIT Enclave	RHEL WS4	LINUX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	HP (8400)	alldredge2	alldredge2
View	ACTIVE	nlt2007-5	0923345	ZASDW3U498	B7 R254	NLIT Enclave	Mac OS X	MAC	<input checked="" type="checkbox"/>	APPLE (MACBOOK PRO)	alldredge2	alldredge2						
View	ACTIVE	nlt2007-4	0923344	63ESWNH	B7 R745	NLIT Enclave	Solaris 10	UNIX	<input checked="" type="checkbox"/>	SUN MICROSYSTEMS (FIRE X4500)	alldredge2	alldredge2						
View	ACTIVE	nlt2007-1	0923342	7VWVW23	B9 R1232	NLIT Enclave	WinXP Pro	WINDOWS	<input checked="" type="checkbox"/>	DELL (PRECISION WORKSTATION 370)	alldredge2	alldredge2						

Home | C & A | Equipment | IP Management | Reports | Roles | Security | Help | Wizard | Logout

Privacy & Legal Notice

*simulated data



Reporting



- **Enterprise Reporting Workbench (ERW)**
 - **Provides customizable reporting**
 - User can pick which columns to display
 - User can specify simple or complex search criteria
 - User can choose output type (PDF, Excel, TSV, HTML, etc.)
 - **Once the report is defined, it can be saved and run again in the future.**
 - **Reports can be shared among groups.**
 - **Scheduled batch reporting with Entrust support is coming in July.**





Reporting



- ERW Reports Tree
 - Entry point to create or run reports

The screenshot displays the ERW Enterprise Reporting Workbench Application interface. The browser title is "Available Reports - Windows Internet Explorer". The page header includes the ERW logo, "ENTERPRISE REPORTING WORKBENCH APPLICATION", and a welcome message for Ryan N. Alldredge. Navigation tabs include "Reports", "Batch", "Lookups", "URAs", "Components", "Views", "Groups", and "Web Repo". A "View Filter" dropdown is set to "Enterprise".

The main content area is divided into two panels:

- Available Reports:** A tree view showing a hierarchy of reports. The "CNA Detail" folder is expanded, showing sub-reports like "CNA Overall Failure Detail (Enterprise)", "CNA Overall Failure Summary (Enterprise)", "CNA Overall Success Detail (Enterprise)", and "CNA Overall Success Summary (Enterprise)".
- Report Information:** A panel displaying details for the selected report: "CNA Overall Failure Detail". It shows the owner as "Enterprise", a description, the last update date (6/27/08 3:40:35 PM), and the format. Below this are buttons for "Run", "Edit", "Edit Copy", "Read Only", and "Delete".

At the bottom, there is an "Output Options" section with a dropdown for "Output Type" (set to PDF), a "To Web Repo" checkbox, and input fields for "Output Title", "Email to:", and "Subject:". The footer contains copyright information for Enterprise Architecture and Data Provisioning at Lawrence Livermore National Laboratory.



Reporting



- ERW Format
 - Columns to display on report



Reporting



- ERW Filter
 - Search conditions (where clause)

Filter Information for Report CNA Overall Failure Detail (copy 2)

Filter Name: CNA Overall Failure Detail Filter (copy 2) Output Type: PDF To Web Repo:

Filter Owner: allredge2 Output Title: _____

Domain: CNA Detail Email To: _____

Last Update: _____ Subject: _____

Condition	Prompt	Exclude
<input type="checkbox"/> Data Effective Date = Today	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> and Security Plan Name AMONG	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> and Primary User OUN AMONG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> and DOE Number = exclude	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> and Computer Name = exclude	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> and Building AMONG	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> and Operating System LIKE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> and Overall Pass Flag = F	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> and Equipment Status = ACTIVE	<input type="checkbox"/>	<input type="checkbox"/>



Questions



Q&A

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

Auspices Statement

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.