EXACT IDENTITY

XID

Daren Roberts

March 2019

ver 318.7

Presenter

EXACT IDENTITY

- XID software author
  - Company founder
- Consultant/Developer Novell (now NetIQ) Identity Management suite since 2003.
  - Began with Novell DirXML 1.1a
  - Work today with NetIQ Identity Manager 4.7..
- SailPoint Developer BeanShell - IIQ 5.5, 6.x, 7.0..

EXACT IDENTITY

Concepts

Product Fit

EXACT IDENTITY

- XID is more collaborative than competitive to SailPoint/NetIQ/Oracle/Quest/CyberArk etc.

- Development driven for the need to ensure data readiness was not an issue when the main IDM/IAM solution (SailPoint, Quest, NetIQ, Oracle, CyberArk, Microsoft etc.) went live.

XID Application Concepts

EXACT IDENTITY

- XID is designed to analyse data at a fixed point in time. This is achieved by gathering extracts of data in LDIF, CSV or XML formats and creating a model of the production system.

- XID also remains abstracted from production systems for the following reasons:
  - Complexity in obtaining account(s) to access data directly.
  - Difficulty in obtaining the appropriate authorisation level to extract all relevant data.
  - Live data changes during processing can create a variant in the result set.
  - Potential performance and/or operational impact to live systems upon extraction.
  - XID processes an agreed data set sanctioned by the data owner.

- Minimal Infrastructure Required
  - Runs on a PC as standard user; no additional software is required.
  - Can run from a network share, USB or local drive.

EXACT IDENTITY

Demo

New Project

New Project

EXACT IDENTITY

- Create New Project.
  - Customer: Test Co
  - Project No: 323
  - Project Name: TestCo_IAM_Project
  - Path: Auto
  - Output File Delimiter: , (Window List Separator setting).
    Note: Enter ‘#9’ without quotes for a ‘tab’ delimiter.

Applications

EXACT IDENTITY

- eDir
  - Name: IAMeDir1
- SAP
  - Name: IAMSAP1
- AD
  - Name: IAMAD1
- Generic
  - Name: IAMunix1

Edit App – eDir

EXACT IDENTITY

- eDir
  - Input File: ‘xtcoidvault.csv’ LDIF
  - Schema Template: XID_Test_Project_1_IDV_sch.xml
  - Security: loginDisabled false
  - LDAP
    - Base: OU=USERS,O=XIDTESTCO
    - User|Active: OU=ACTIVE,OU=USERS,O=XIDTESTCO
    - Inactive: OU=INACTIVE,OU=USERS,O=XIDTESTCO

Edit App – SAP

EXACT IDENTITY

- SAP
  - Input File: ‘xtcosap.csv’ CSV
  - Schema Template: XID_Test_Project_1_SAP2_sch.xml
  - Security: Employment Status Active
  - Special Account Mask : *Blog*

Edit App – AD

EXACT IDENTITY

- AD
  - Input File: ‘HX_AD1.csv’ CSV
  - Schema Template: HX_Test_1_322_HXAD1_sch.xml
  - Security: userAccountControl 512
  - Aux: **hx_ad_entitlements1.txt**

Edit App – Unix

EXACT IDENTITY

- Unix
  - Input File: **hx_unixpasswd.txt**
    - Input Type: UNIX : ; N N
  - Schema Template: HX_Test_1_322_HXunix1_sch.xml
  - Group:
    - CRLF
    - Entity Input: **hx_unixgroup.txt**
    - Input Type: UNIX : , N N
  - Aux: **hx_unix_entitlements1.txt**

Match

EXACT IDENTITY

- SAP

  App1: workforceID App: Employee Number
- AD

  App1: workforceID App: EmployeeID
- Unix

  App1: cn App: name

Business Rules

EXACT IDENTITY

- App1(eDir)->SAP

App1	App	App1 -> App	App -> App1	Merge Authority
givenName	First Name	ignore	sync	App
sn	Last Name	ignore	sync	App
l	location	ignore	sync	App
title	Position Title	ignore	sync	App
ou	Org Unit	ignore	sync	App
mail	Email Address	sync	ignore	App1
telephoneNumber	TEL_NUMBER	ignore	sync	App
mobile	MOB_NUMBER	sync	sync	App1

Business Rules

EXACT IDENTITY

- App1->AD

App1	App	App1 -> App	App -> App1	Merge Authority
givenName	givenName	sync	ignore	App1
sn	sn	sync	ignore	App1
l	l	sync	ignore	App1
title	title	sync	ignore	App1
ou	Department	sync	ignore	App1
mail	mail	ignore	sync	App
telephoneNumber	telephoneNumber	sync	sync	App1

Business Rules

EXACT IDENTITY

- App1->Generic (Unix)

App1	App	App1 -> App	App -> App1	Merge Authority
cn	GECOS	sync	sync	App1

EXACT IDENTITY

Demo

Reporting

Reporting

EXACT IDENTITY

- All parallel
- AD Self
- Unix Self
- eDir, SAP & AD cascade

Summary Report

EXACT IDENTITY

XID Reports

Summary Report 323:TestCo_IDM_Project

Matching and Orphans — App1 (P) to App (S) -> | <- App (S) to App1 (P)

App	Accounts	In scope	Match->	Orphan->	<-Match	<-Orphan
HXeDir1	56	56				
HXSap1	56	56	54	2	54	2
HXAD1	54	54	54	2	54	0
HXunix	5	5	3	53	3	2

Business Rules - App1 (P) to App (S) -> matched

App	Description	Issues	Accnts Impacted
HXeDir1	HXeDir1 core data overwrite by HXSap1	1	
HXSap1	HXSap1 core data overwrite by HXeDir1	1	
Totals	->	2	2
HXeDir1	HXeDir1 core data overwrite by HXAD1	1	
HXAD1	HXAD1 core data overwrite by HXeDir1	19	
Totals	->	20	20
HXeDir1	HXeDir1 core data overwrite by HXunix	0	
HXunix	HXunix core data overwrite by HXeDir1	3	
Totals	->	3	3

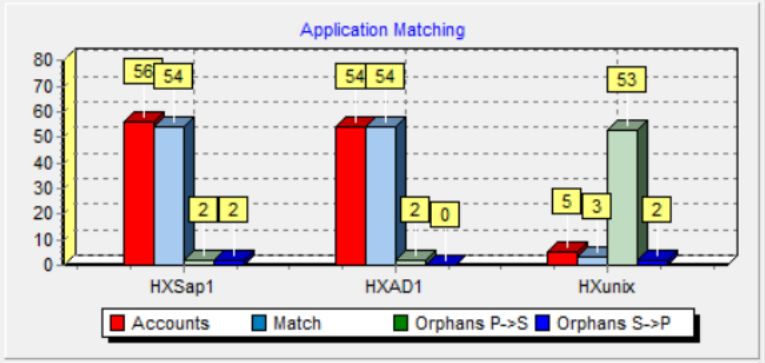
General

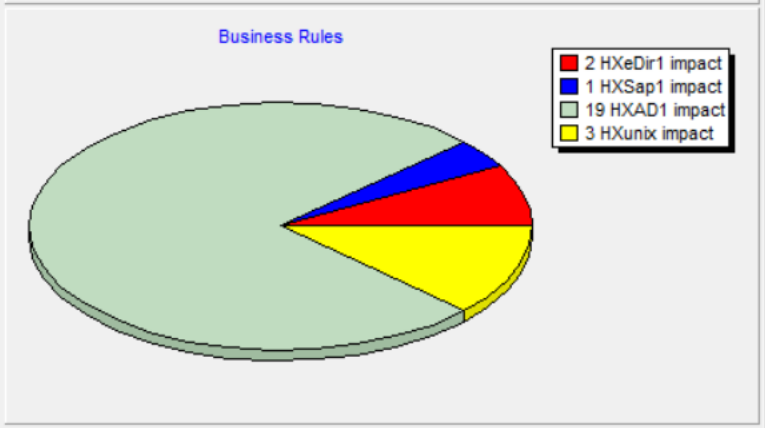
App	Account Control Discrepancy	Impacted	Detailed Items
HXeDir1	Inactive in HXeDir1 but active in HXSap1	1	1
HXeDir1	Inactive in HXeDir1 but active in HXAD1	1	1
HXAD1	Active in HXeDir1 but inactive in HXAD1	1	1

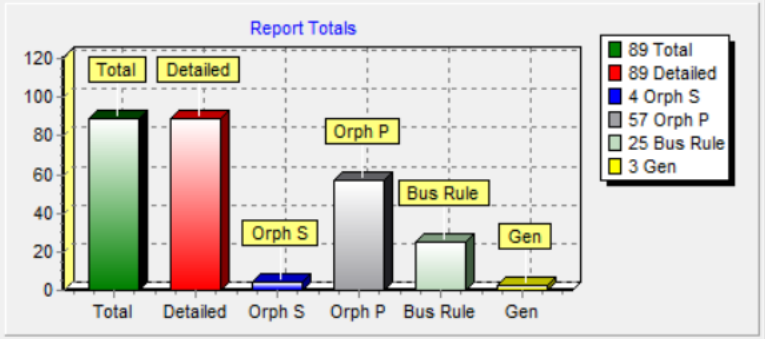
Discrepancy Totals

Report Section	Description	Sub Total	Detailed Total
App Matching	Orphan accounts: App1 -> App	57	57
System Matching	Orphan accounts: App -> App1	4	4
Business Rules	Data Flow	25	25
General	Account Control	3	3

p:170606065359 Totals - Issues: 89 Detailed Report: 89







Save
Print
OK
Cancel

Summary Self Report

EXACT IDENTITY

- AD

XID Reports - Self

Summary Report - Self

323:TestCo_IDM_Project

Self Statistics

App	Item	Value	Item	Value
HXAD1	Total Accounts: 54	In Scope: 54		
HXAD1	Number of Groups Belonged To	2		
HXAD1	Users with Managers	53	Users without Managers	1
HXAD1	Non Dormant Users	0		
HXAD1	Dormant Users Old Last Logon	2	Dormant Users Never Logged On	52
HXAD1	Disabled Users	1	Elevated Privileged Users	107

- Unix

XID Reports - Self

Summary Report - Self

323:TestCo_IDM_Project

Self Statistics

App	Item	Value	Item	Value
HXunix	Total Accounts: 5	In Scope: 5		
HXunix	Number of Groups Belonged To	3		
HXunix	Users with Managers	0	Users without Managers	0
HXunix	Non Dormant Users	0		
HXunix	Dormant Users Old Last Logon	0	Dormant Users Never Logged On	0
HXunix	Disabled Users	0	Elevated Privileged Users	4

Detailed Reports

EXACT IDENTITY

Match

RowID	Operation	Directive	Filter	App1 attr	App1 attr1	App1 attr2	App1 attr3	App1 attr4	App1 attr5	App2 attr3	App2 attr4	App2 attr5	Description
A	Match	HXeDir1 ->	match A-B	cn=SmithJ,ou=A	10000001	SmithJ	10000001	James	Smith	10000001	James	Smith	Matched on HXeDir1 workforceID to HXSap1 Employee Number
A	Match	HXeDir1 ->	match A-B	cn=JohnsonJ,ou	10000002	JohnsonJ	10000002	John	Johnson	10000002	John	Johnson	Matched on HXeDir1 workforceID to HXSap1 Employee Number
A	Match	HXeDir1 ->	match A-B	cn=WilliamsM,c	10000003	WilliamsM	10000003	Mary	Williams	10000003	Mary	Williams	Matched on HXeDir1 workforceID to HXSap1 Employee Number

Orphans

RowID	Operation	Directive	Filter	App1 attr1	App1 attr2	App1 attr3	App1 attr4	App1 attr5	App1 attr6	App2 attr1	App2 attr2	App2 attr3
A	Orphan	HXeDir1 ->	match A-B	cn=Blogma	30000065	BlogmanF	30000065	Fred	Blogman	No match HXeDir1 to HXAD1		
A	Orphan	HXeDir1 ->	match A-B	cn=Brown	BrownR	BrownR	10000004	Robert	Brown	No match HXeDir1 to HXunix		
A	Orphan	HXeDir1 ->	match A-B	cn=JonesP	JonesP	JonesP	10000005	Patricia	Jones	No match HXeDir1 to HXunix		

Business Rules Parallel

RowID	App1	Integrated	Filter	App1 attr1	App1 attr2	App1 attr3	App2 attr5	App2 attr6	Description
A	HXeDir1	HXSap1	busruleatt	cn=SmithJ,	10000001	SmithJ	James	Smith	HXeDir1 title:Line Manager will be overwritten by HXSap1 Position Title:Area Manager
A	HXeDir1	HXSap1	Acntctrl	cn=Willian	10000003	WilliamsM	Mary	Williams	Primary App1 Inactive:loginDisabled=TRUE - App Active:Employment Status=ACTIVE
A	HXeDir1	HXSap1	busruleatt	cn=ReedM	10000065	ReedM	Martha	Reed	HXeDir1 mail:Martha.Reedy@xidtestco.com will overwrite HXSap1 Email Address:Martha.Reed@xidtestco.com
A	HXeDir1	HXAD1	Acntctrl	cn=SmithJ,	10000001	SmithJ	James	Smith	Primary App1 Active:loginDisabled=FALSE - App Inactive:userAccountControl=514
A	HXeDir1	HXAD1	busruleatt	cn=SmithJ,	10000001	SmithJ	James	Smith	HXeDir1 title:Line Manager will overwrite HXAD1 title:Line Mgr
A	HXeDir1	HXAD1	Acntctrl	cn=Willian	10000003	WilliamsM	Mary	Williams	Primary App1 Inactive:loginDisabled=TRUE - App Active:userAccountControl=512
A	HXeDir1	HXAD1	busruleatt	cn=Brown	10000004	BrownR	Robert	Brown	HXeDir1 telephoneNumber:020710105 will overwrite HXAD1 telephoneNumber:20710105

Detailed Reports

EXACT IDENTITY

Business Rules Cascade

HXeDir1	HXeDir1	HXeDir1	HXeDir1	HXeDir1	HXeDir1	11-HXeDir1	11-HXeDir1	11-HXeDir1	12-HXeDir1	12-HXeDir1	12-HXeDir1
Primary Sy	Id Attr1	Id Attr2	Id Attr3	Id Attr4	Id Attr5	Auth-title	New-title	title	Auth-mail	New-mail	mail
1-HXeDir1	cn=SmithJ,	10000001	SmithJ	James	Smith	S2-HXSap1	Area Manager	Line Manager			
1-HXeDir1	cn=ReedM	10000065	ReedM	Martha	Reed				S3-HXAD1	Martha.Reed@x	Martha.Reedy@x

Self Detailed Report

Integrated	Filter	App1 attr6	App2 attr1	App2 attr2	App2 attr3	App2 attr4	App2 attr5
IAMAD1	self-account_quiescence	cn=SmithJ,	SmithJ	10000001	James	Smith	Last Logon 3/6/2015 15:16:20 > date cut off - 20160601
IAMAD1	self-no_manager	cn=SmithJ,	SmithJ	10000001	James	Smith	User does not have a manager
IAMAD1	self-acntctrl	cn=SmithJ,	SmithJ	10000001	James	Smith	User NOT enabled:514
IAMAD1	self-entitlement	cn=SmithJ,	SmithJ	10000001	James	Smith	Member of entitlement:xidtestgroup1
IAMAD1	self-account_quiescence	cn=Johnso	JohnsonJ	10000002	John	Johnson	Not logged on null
IAMAD1	self-entitlement	cn=Johnso	JohnsonJ	10000002	John	Johnson	Member of entitlement:xidtestgroup1
IAMAD1	self-entitlement	cn=Johnso	JohnsonJ	10000002	John	Johnson	Member of entitlement:xidtestgroup2
ADunix1	self-entitlement		testuser1	1001		Test User :	Member of entitlement:testunixgroup1
ADunix1	self-entitlement		testuser1	1001		Test User :	Member of entitlement:testunixgroup5
ADunix1	self-entitlement		robedar	1000		robedar	Member of entitlement:testunixgroup1
ADunix1	self-entitlement		robedar	1000		robedar	Member of entitlement:testunixgroup5

Questions & Answers

EXACT IDENTITY

Email: daren.roberts@exactidentity.com