Not too long ago I wrote a quick post on how easy it is to gather information from AD. As a case in point example I provided a script to gather all the disabled user accounts which are still assigned Lync IDs. In this script I take it one step further and provide a full blown Active Directory reporting script which can be produced with any non-privileged domain user account.

Version Information

1.8 - 02/28/2014

- New GUI wrapper (both as a ps1 and an exe)!

1.7 - 02/19/2014

- New save/load functionality! With a switch you can export all collected data to xml for later report processing.
- Fixed domain user priveleged report to show lastlogontimestamp as 'never' in html report
- Added change notification attribute to site link report section
- Small modification to Format-HTMLTable function to catch errors when processing empty tables
- Fixed issue with domain report count of passwords set to never expire.

1.6.1 - 01/15/2014

- Removed superfluous skipdomainreport and skipforestreport paramenters
- Swapped out Colorize-Table with Format-HTMLTable. This means pretty HTML reports on older systems where the Linq assemblies are not available.
- Minor fixes.

1.6 - 01/10/2014

- Added registered NPS devices
- Added registered DHCP devices
- Added domain registered print devices
- Added SCCM servers and sites
- Added wrapper parameters to entire script with some most used options for directly running the script from a powershell prompt.
- Added ability to prompt for input for all major global variables.
- Fixed verbose calling for priv groups and users
- Updated lastlogontimestamp for user export normalization to show never logged in instead of a date from the 1600's.
- Added date translation for account expiration in account normalization.
- Updated ad gathering functions to account for inability to connect to domain and silently exit.
- Slight rearrangement of report sections.

1.5 - 11/26/2013

- Added the parameter ForceAnonymous along with the code to force anonymous authentication when sending email reports

1.4.0 - 11/21/2013

- Fixed site connections destiniation server output flaw
- Fixed errors occuring when subnets have no sites
- Fixed a number of other errors and bugs related to my prior addition of Get-ADPathName.
- Fixed issues where phantom domains exist in topology

1.3.0: 11/17/2013

- Fixed DC count issue
- Some formatting changes
- Added detection for newer versions of exchange schemas
- Changed logic for exchange role detection for 2013 to provide accurate results
- Fixed linq issues when running on windows 2012 servers
- Stopped using builtin -split for ldap paths in favor of a custom function called Get-ADPathName
- Added function for resolving msRTCSIP-PrimaryHomeServer to the user's lync pool name in the CSV export of all users
- More changes to the base functions (more error handling and such)

1.2.0: 11/10/2013

- Added site summary section
- Added Exchange Federations section
- Fixed some code for when no subnets/sites are returned.
- Fixed site options section (I think)
- Changed 'AllowEmptyReport' Section element to saner name of 'ShowSectionEvenWithNoData'
- Commented out write-verbose statements for the report generation portions
- Added timer in the forest data collection routine (as it was taking way too long to process), found that pulling all properties in the Search-AD function was a real drag so I manually defined all the properties gathered where needed. Should speed things up considerably.
- Fixed recycle bin detection
- Prettied up the DC report section to better show FSMO roles and GCs
- Changed the trusts attribute detection to be an enumeration instead of a switch
- Mild changes to the base report generation functions.

1.1.0: 11/02/2013

- Added domain level reporting
- Added AD Integrated Zone information to forest reports
- Added GPO information to forest reports
- Fixed a ton of Powershell V2 related issues

1.0.1: 10/23/2013

- Removed duplicate FSMO role reporting
- Added RID utilization statistics
- Added site links section
- Added DFSR section
- Changed the lync config container output (if found) to be either system or configuration.

1.0.0: 10/20/2013

- Initial release

Features

To create the output I repurposed my server asset reporting script. This means several output methods are baked right in.

New I've wrapped the entire script up in one easy to use set of parameters which includes the most common output formats and types of reports you may want to create. All of the prior reporting formats are still available to those who are determined though (I've setup custom sections you can use just for such a purpose). There is also an option for prompting at the console for all of the optional output such as the diagrams and user data exports.

- Report Containers/Types
  - Documentation – Currently the only format for this type of report. This returns all data gathered in the report.
- HTML Templates
  - DynamicGrid – A heavily modified CSS layout
  - EmailFriendly – A basic layout
- Saved Report Layout
  - Individual – Each asset saves as its own file
  - One big report – Only a single report will be generated no matter which option you choose.
- Saved Report File Format
  - HTML
  - PDF
- Email Reports (HTML only)
- Export all data to individual worksheets within Excel

Optionally, three diagrams can be created when this script is run. One for domain trusts, another for site replication connections, and a third for site adjacencies. By default the diagram source text file and a png file will get created in the directory which you run the script.

To actually generate the diagrams you will need graphviz's dot.exe executable which can be downloaded and installed here. Or here is a portable version of the application you can try utilizing. All you need is for the dot.exe file to work correctly to generate your diagram. You may have to modify this script to use the appropriate path to the executable if you use the portable version of graphviz.

Report Data

I've included only items which can be gathered from Active Directory with a regular user account and without any special AD modules. This is what has been added thus far:

Forest Level Audit Report

- Forest Information
  - Forest Summary
    - Name/Functional Level
    - Domain/Site/DC/GC/Exchange/Lync/Pool counts
  - Forest Features
    - Tombstone Lifetime
    - Recycle Bin Enabled
    - Lync AD Container
  - Exchange Servers
    - Organization/Administrative Group/Name/Roles/Site
    - Serial/Product ID
  - Lync
    - Element (Server/Pool)
    - Type (Internal/Edge/Backend/Pool)
    - Name/FQDN

- Site Information
  - Summary
    - Site Name/Location/Domains/DCs/Subnets
  - Details
    - Site Name/Options/ISTG/Links/Bridgeheads/Adjacencies
  - Subnets
    - Subnet/Site Name/Location
  - Site Connections
    - Enabled/Options/From/To
  - Site Links ***new***
    - Name/Replication Interval/Sites
- Domain Information
  - Domains
    - Name/NetBIOS/Functional Level/Forest Root/RIDs Issued/RIDs Remaining ***new***
  - Domain Password Policies
    - Name/NetBIOS/Lockout Threshold/Pass History Length/Max Pass Age/Min Pass Age/Min Pass Length
  - Domain Controllers
    - Domain/Site/Name/OS/Time/IP/GC/FSMO Roles
  - Domain Trusts
    - Domain/Trusted Domain/Direction/Attributes/Trust Type/Created/Modified
  - Domain DFS Shares
    - Domain/Name/DN/Remote Server
  - Domain DFSR Shares ***new***
    - Domain/Name/Content/Remote Servers
  - AD Integrated DNS Zones
  - Group Policy Object Information

Domain Level Audit Report

- Account Statistics (count) 1
  - Total User Accounts
  - Enabled
  - Disabled
  - Locked
  - Password Does Not Expire
  - Password Must Change
- Account Statistics (count) 2
  - Password Not Required
  - Dial-in Enabled
  - Control Access With NPS
  - Unconstrained Delegation

    - Not Trusted For Delegation
    - No Pre-Auth Required

- Group Statistics
    - Total Groups
    - Built-in
    - Universal Security
    - Universal Distribution
    - Global Security
    - Global Distribution
    - Domain Local Security
    - Domain Local Distribution

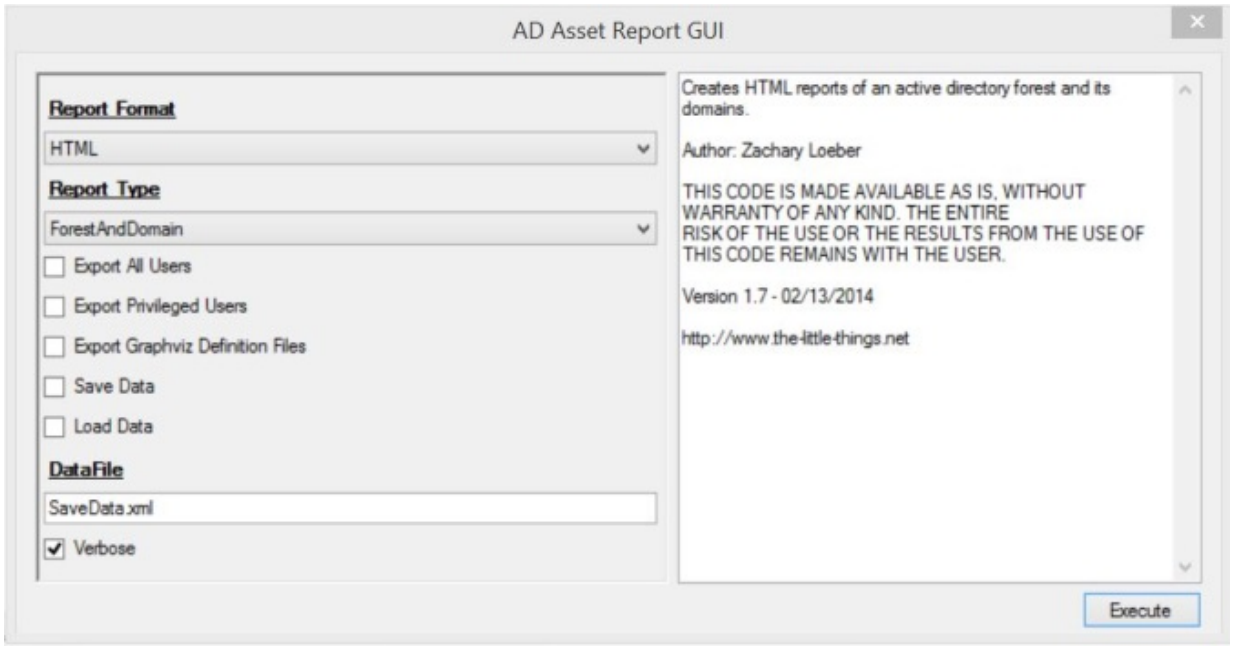
- Privileged Group Statistics
    - Default Priv Group Name
    - Current Group Name (if it were changed)
    - Member Count

- Privileged Group Membership for the following groups
    - Enterprise Admins
    - Schema Admins
    - Domain Admins
    - Administrators
    - Cert Publishers
    - Account Operators
    - Server Operators
    - Backup Operators
    - Print Operators

- Account information for the prior sections:
    - Logon ID
    - Name
    - Password Age (Days)
    - Last Logon Date
    - Password Does Not Expire
    - Password Reversable
    - Password Not Required

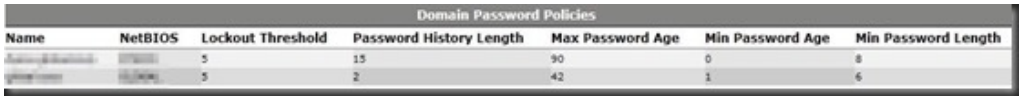
Screenshots

Here are some screenshots of the reports and diagrams which can be created:



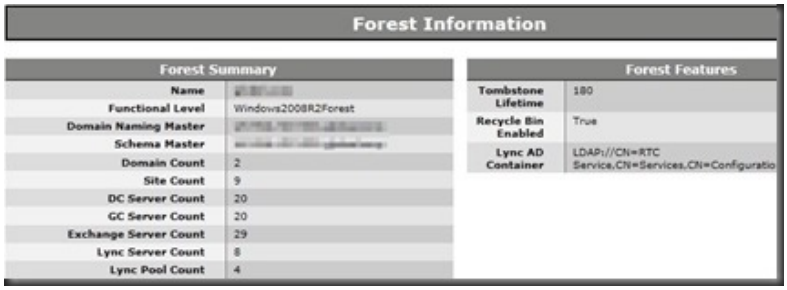
Domains Controllers

Domain	Site	Name	OS	Time	IP	GC	Infra	Naming	Schema	RID	PDC
			Windows Server 2008 R2 Enterprise	10/17/2013 7:45:48 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:45:50 PM		True	False	False	False	False	False
						True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:02 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:04 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:09 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:13 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Standard	10/17/2013 7:46:17 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:17 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:22 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:24 PM		True	True	False	False	True	True
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:26 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:34 PM		True	False	False	False	False	False
			Windows Server 2008 R2 Enterprise	10/17/2013 7:46:36 PM		True	False	True	True	False	False



Domain Password Policies

Name	NetBIOS	Lockout Threshold	Password History Length	Max Password Age	Min Password Age	Min Password Length
		5	15	90	0	8
		5	2	42	1	6



Forest Information

Forest Summary

Name	
Functional Level	Windows2008R2Forest
Domain Naming Master	
Schema Master	
Domain Count	2
Site Count	9
DC Server Count	20
GC Server Count	20
Exchange Server Count	29
Lync Server Count	8
Lync Pool Count	4

Forest Features

Tombstone Lifetime	180
Recycle Bin Enabled	True
Lync AD Container	LDAP://CN=RTC Service,CN=Services,CN=Configuratio

Lync Elements

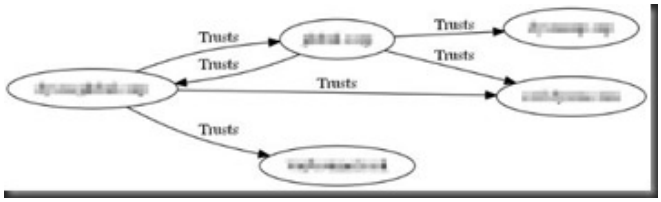
Element	Type	Name	FQDN
Server	Internal		
Server	Internal		
Server	Internal		
Server	Internal		
Server	Internal		
Server	Internal		
Server	Edge		
Server	Backend		
Pool	Pool		
Pool	Pool		

Site Connections

Enabled	Options	From	To
True	IS_GENERATED, OVERRIDE_NOTIFY_DEFAULT		
True	IS_GENERATED, OVERRIDE_NOTIFY_DEFAULT		
True	IS_GENERATED		
True	IS_GENERATED		
True	IS_GENERATED		
True	IS_GENERATED, OVERRIDE_NOTIFY_DEFAULT		
True	IS_GENERATED		

Site Subnets

Subnet	Site Name	Location



Domain Trusts

Domain	Trusted Domain	Direction	Attributes	Trust Type	Created	Modified
		Bidirectional	Intra-Forest Trust	Uplevel (Active Directory)	11/17/2007 10:05:11 AM	9/27/2013 5:07:04
		Bidirectional	0	Uplevel (Active Directory)	4/18/2013 2:46:44 PM	10/16/2013 10:22:1
		Bidirectional	Quarantined Domain (External)	Uplevel (Active Directory)	10/2/2013 2:12:59 PM	10/2/2013 2:22:04
		Bidirectional	Intra-Forest Trust	Uplevel (Active Directory)	11/17/2007 10:01:37 AM	9/27/2013 5:06:36
		Bidirectional	Forest Trust	Uplevel (Active Directory)	2/17/2008 12:03:24 PM	9/27/2013 9:51:36
		Bidirectional	0	Uplevel (Active Directory)	4/18/2013 2:42:48 PM	10/17/2013 6:21:4

Domain DFS Shares

Domain	Name	DN	Remote Server

Domain Statistics

User Account Statistics	
Total User Accounts	
Enabled	
Disabled	
Locked	
Password Does Not Expire	
Password Must Change	

User Account Statistics	
Password Not Required	
Dial-in Enabled	
Control Access With NPS	
Unconstrained Delegation	
Not Trusted For Delegation	
No Pre-Auth Required	

Group Statistics	
Total Groups	
Built-in	
Universal Security	
Universal Distribution	
Global Security	
Global Distribution	
Domain Local Security	
Domain Local Distribution	

Privileged Group Statistics		
Default Name	**Current Name**	**Member Count**
Server Operators	Server Operators	
Account Operators	Account Operators	
Backup Operators	Backup Operators	
Cert Publishers	Cert Publishers	
Domain Admins	Domain Admins	
Enterprise Admins	Enterprise Admins	
Schema Admins	Schema Admins	
Administrators	Administrators	
Print Operators	Print Operators	

Server Operators

Exists only on domain controllers. By default, the group has no members. Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer.

Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
[redacted]	[redacted]	1411	23/10/2013 04:49:35	True	False	False
[redacted]	[redacted]	66	29/10/2013 08:24:16	False	False	False

Backup Operators

By default, the group has no members. Backup Operators can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to the computer and shut it down.

Logon ID	Name	Pwd Age (Days)	Last Logged In	No Pwd Expiry	Pwd Reversable	Pwd Not Req.
[redacted]	[redacted]	4777	28/10/2013 08:12:17	True	False	False
[redacted]	[redacted]	4722	24/10/2013 12:22:53	True	False	False
[redacted]	[redacted]	2683	24/10/2013 03:46:55	True	False	False
[redacted]	[redacted]	2526	14/03/2008 08:57:58	True	False	False
[redacted]	[redacted]	326	31/12/1600 06:00:00	True	False	False
[redacted]	[redacted]	283	23/10/2013 04:40:48	True	False	False
[redacted]	[redacted]	208	31/10/2013 08:00:00	True	False	False
[redacted]	[redacted]	156	03/06/2013 04:34:34	True	False	False
[redacted]	[redacted]	66	29/10/2013 08:24:16	False	False	False