



Ingham Intermediate
School District
A Regional Educational Service Agency

PowerShell – You’re Using It, Right?

- **Name:** Chris Thomas
- **Title:** Desktop Engineer
- **Organization:** Ingham Intermediate School District
- **Email:** cthomas@inghamisd.org
- **Twitter:** [@AutomateMyStuff](https://twitter.com/AutomateMyStuff)
- **Past Presentations:** <https://github.com/chrisATAutomatemystuff/Presentations>

PowerShell – You're Using It, Right?

PowerShell has the ability to help save you time and effort while also providing you consistent results and documented processes. Find those annoying manual tasks you or your staff do and come learn how you can start to remove some of that manual effort for automated tasks.

We'll cover some fundamentals, but try to spend the majority of the time focusing on real-world examples of how we use PowerShell at our organization to make our lives easier.

Who Am I?

- 22+ Years In K12 Technology
 - Intern, Technician, Coordinator, Engineer
- Lifelong Learner
 - [/r/sysadmin](#), [/r/k12sysadmin](#), RSS feeds
- Relentlessly Inquisitive
 - Let's Ask The [WinAdmins Community](#)
- Problem Solver
 - Professional [Googler](#)
- Voracious Reader
 - [learn.microsoft.com/en-us/docs/](#)
- Community Minded
 - [MAEDS](#), [MISCUG](#), [WMISMUG](#)
- Past Presentations
 - [github.com/chrisATautomatemystuff/Presentations](#)
- [#ImpostorSyndromeBeDamned](#)

There's a struggle to it and that's normal

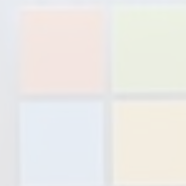
Don Jones: "If you're not willing to play a little bit you'll probably not be successful at PowerShell."

Jeffrey Snover: "I'm a Distinguished Engineer, I'm the Lead Architect with Windows Server and System Center Datacenter, and I invented the dang thing and still there's a struggle to it and that's normal."

Windows PowerShell Unplugged with Jeffrey Snover & Don Jones

TechEd North America 2014 • (1hr 16min • quotes @ 3:15)

<https://www.youtube.com/watch?v=qVIPNsAkJxM>



Microsoft

Shell: the command interpreter that is used to pass commands to the operating system

ISE: the Integrated Scripting Environment is an application where you can run, test, and debug scripts in a single GUI with tab completion, syntax coloring, selective execution, and context-sensitive help

Cmdlet: a task-oriented command that is typically used to return a .NET Framework object to the next command in the pipeline

Variable: a name given to stored information, e.g. \$users, \$IWishYouHadAStrongPassword, \$x

Vocabulary 01

Parameter: input values or arguments used by the cmdlet or script to make it more dynamic

Named:

```
PS C:\>  
PS C:\> Get-ChildItem -Path $env:USERPROFILE\AppData\Local\Temp -Filter *.exe
```

Positional:

```
PS C:\>  
PS C:\> Get-ChildItem $env:USERPROFILE\AppData\Local\Temp *.exe
```

Switch:

```
PS C:\>  
PS C:\> Get-ChildItem -Path $env:USERPROFILE\AppData\Local\Temp -Filter *.exe -Recurse
```

Object: a representation of something with methods to take actions against it and properties to access information stored within it

Vocabulary 02

Objects - The Bicycle Example

Property

Something about the object

- Wheel Size
- Tire Pressure
- Height
- Gears
- Color
- Speed
- Price

Method

Something you can do with or to the object

- Pedal
- Brake
- Change Gear
- Repair
- Re-inflate Tire



Array: a data structure that serves as a collection of multiple items. You can iterate over the array or access individual items using an index

Function: a command or series of commands grouped to run together

Module: a set of related Windows PowerShell functionalities, grouped together as a convenient unit (usually saved in a single directory)

Script Module: a file (.psm1) that contains PowerShell code for functions, variables and more

Binary Module: a .NET Framework assembly (.dll) that contains compiled code

Dynamic Module: a module that only exists in memory (Import-PSSession)

Vocabulary 03

Pipeline (|): a method to send the results of the preceding command as input to the next command

\$_: "the current object in the pipeline", or "this", or \$PSItem

Alias: shortcut to a command, cmdlet or function

Vocabulary

04

Comment: You can type a comment symbol (#) before each line of comments, or you can use the (<#) and(#>) symbols to create a comment block

Escape Character: the grave-accent (`) is a continuation character if used at end of line or displays literal value of a string / variable

Command History: <up arrow> or <down arrow> and Get-History

Vocabulary 05

A inexperienced and/or ignorant or unskilled person. Especially used in computer games.



Exploratory Learning For N00bs

- New-Item -Path C:\MAEDS
- Set-Location -Path C:\MAEDS

<SHOCKED PIKACHU>

- Get-ChildItem
- Remove-Item -Path C:\MAEDS
- New-Item -Path C:\MAEDS -ItemType Directory
- Set-Location -Path C:\MAEDS
- Get-ChildItem

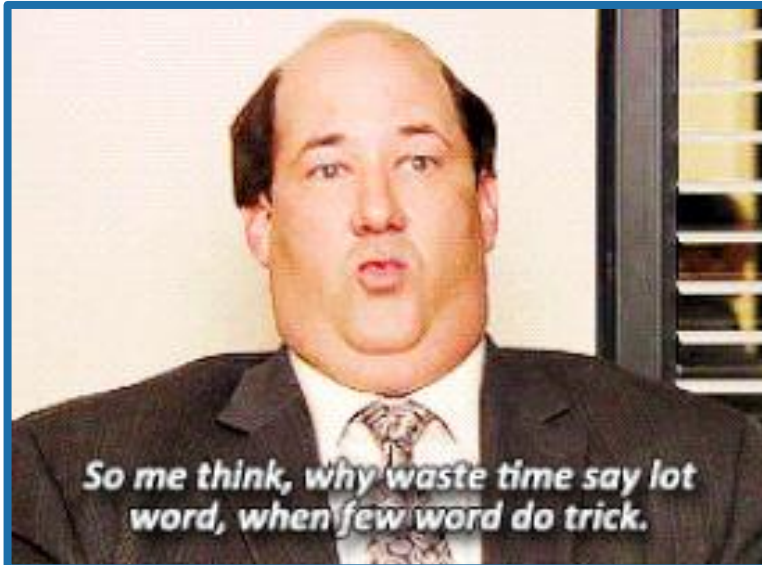
In Information Technology and specifically Computer Science, the term "[Grey beard](#)" or "[Greybeard](#)" is used as a [droll](#), sarcastic way to describe any person who is older. Typically, a [Grey Beard](#) in IT will be very specific about methodology and have well-reasoned arguments about why the methods they are using are superior to current ideas and methods. Many times, they're not wrong!

Exploratory Learning For Greybeards

- mkdir c:\maeds
- cd c:\maeds
- dir
- cd..
- rm maeds

<PYSCH you just learned POSH>


- Get-Help mkdir
- Get-Help cd
- Get-Help dir
- Get-Help rm





Get-Command

- Get-Command -Module *<moduleName>*
 - Get-Command -Verb Get
 - Get-Command -Verb Get -Noun P*
 - Get-Command Get-P*
 - Get-Command Get-P* -Module Microsoft.PowerShell.Utility
 - Get-Command Get-P* -Module Microsoft.PowerShell.Management
-



Get-Help

- Get-Help *<cmdlet>* -Examples
 - Get-Help *<cmdlet>* -Full
 - Get-Help *<cmdlet>* -ShowWindow
 - Get-Help *<cmdlet>* -Online
 - Get-Help *<cmdlet>* | Clip
-



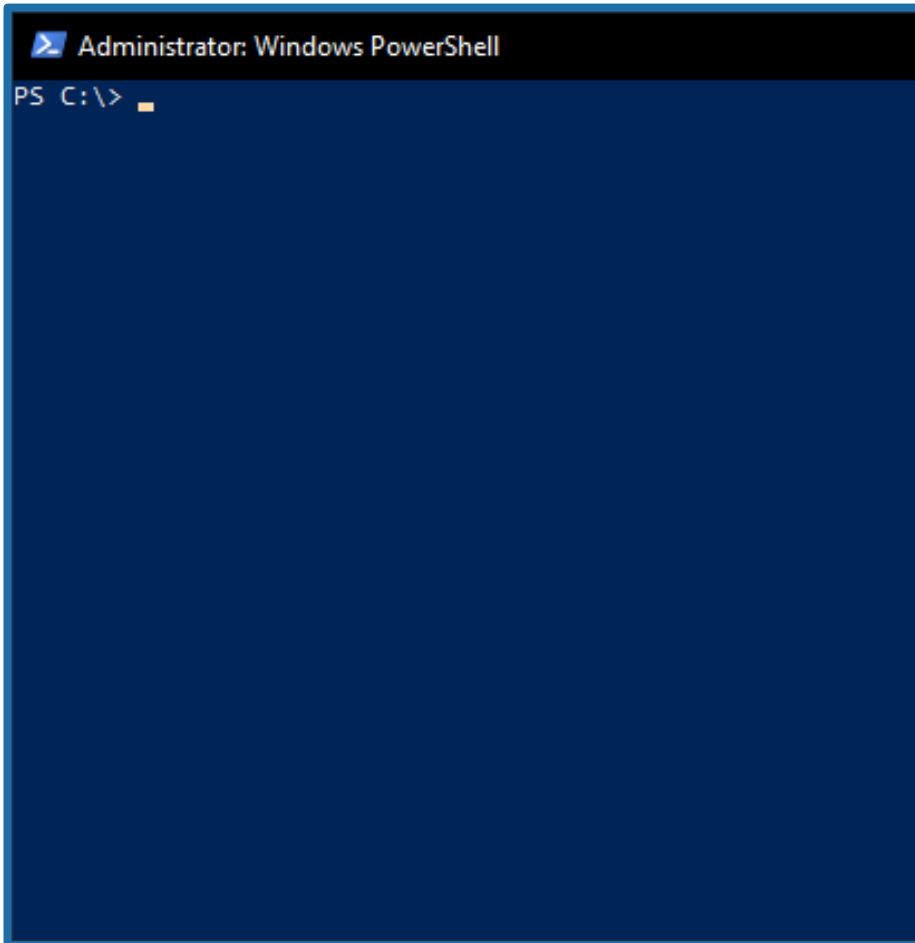
Get-Member

- `<cmdlet> | Get-Member`
 - **Caveat**
 - `Get-ADUser cthomas | Get-Member`
- vs.
- `Get-ADUser cthomas -Properties * | Get-Member`
-



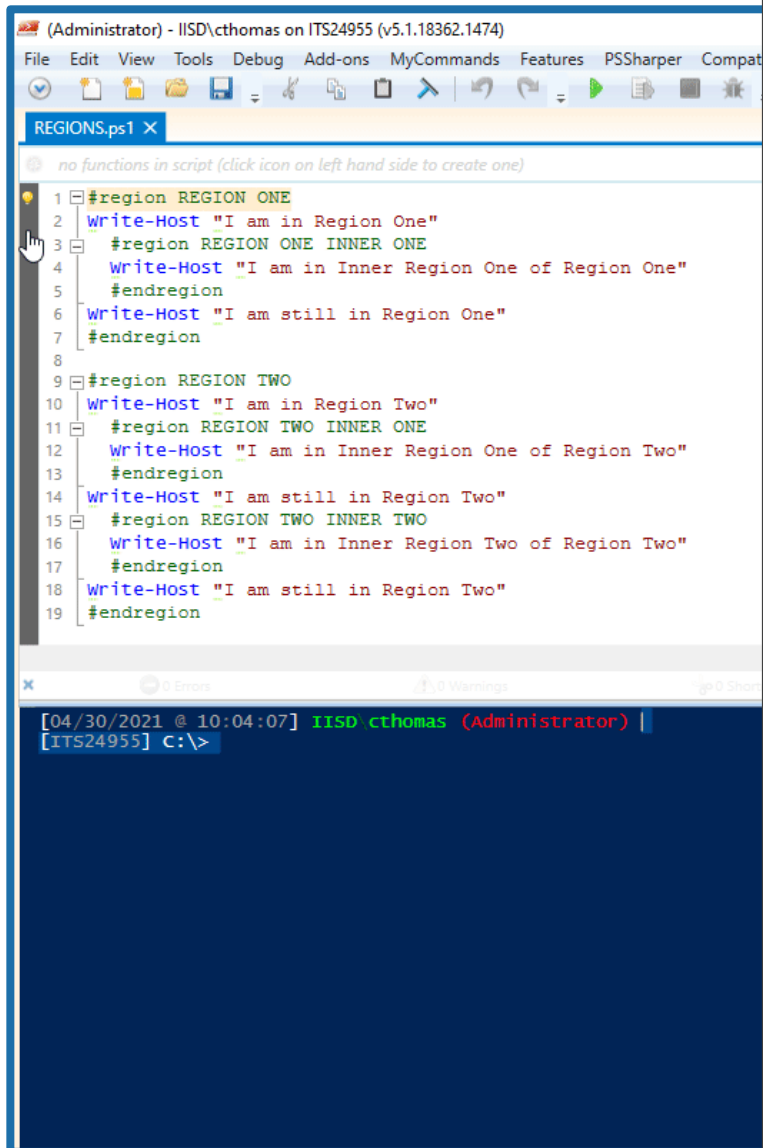
Get-Module

- Get-Module
 - Get-Module -ListAvailable
 - \$session_DC1 = New-PSSession -ComputerName V-DC1
 - Get-Module -PSSession \$session_DC1 -ListAvailable
-



Tab Expansion

- new-adu<TAB>
- New-ADUser -<TAB>
 - <TAB> to advance through parameters
 - or
 - <SHIFT+TAB> to go back to a previous parameter
- New-ADUser -<CTRL + SPACE>
 - <ARROW KEYS> + <SPACE> to select appropriate parameter

The screenshot shows the IISD console interface. At the top, the title bar reads "(Administrator) - IISD\cthomas on ITS24955 (v5.1.18362.1474)". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, MyCommands, Features, PSSharper, and Compat. Below the menu is a toolbar with various icons. The main window displays a PowerShell script named "REGIONS.ps1". The script contains two regions: "REGION ONE" and "REGION TWO". Each region contains an inner region and a "Write-Host" command. The script is as follows:

```
1 #region REGION ONE
2 Write-Host "I am in Region One"
3 #region REGION ONE INNER ONE
4 Write-Host "I am in Inner Region One of Region One"
5 #endregion
6 Write-Host "I am still in Region One"
7 #endregion
8
9 #region REGION TWO
10 Write-Host "I am in Region Two"
11 #region REGION TWO INNER ONE
12 Write-Host "I am in Inner Region One of Region Two"
13 #endregion
14 Write-Host "I am still in Region Two"
15 #region REGION TWO INNER TWO
16 Write-Host "I am in Inner Region Two of Region Two"
17 #endregion
18 Write-Host "I am still in Region Two"
19 #endregion
```

The bottom of the console shows a command prompt window with the text "[04/30/2021 @ 10:04:07] IISD cthomas (Administrator) | [ITS24955] C:\>".

Regions

- Separate code into collapsible sections
- <CTRL> + M to collapse/expand all regions
- Collapsing regions only affects readability, not runability

Command Syntax

SYNTAX

```
New-ADUser [-Name] <String> [-AccountExpirationDays <Int32>] [-AuthenticationPolicySilo <ADAuthenticationPolicySilo>] [-CompoundIdentitySupported <Boolean>] [-EmployeeNumber <String>] [-Enabled <Boolean>] [-KerberosEncryptionType {None | DES | RC4 | AES128 | AES256} <Hashtable>] [-OtherName <String>] [-PassThru <Boolean>] [-ProfilePath <String>] [-SamAccountName <String>] [-Title <String>] [-TrustedForDelegation <Boolean>]
```

- <command-name> -<Required Parameter Name> <Required Parameter Value>
- [-<Optional Parameter Name> <Optional Parameter Value>]
- [-<Optional Switch Parameters>]
- [-<Optional Parameter Name>] <Required Parameter Value>

SYNTAX

```
Add-ADGroupMember [-Identity] <ADGroup> [-Members] <ADPrincipal>
```

Splatting

- Remove the need for horizontal scrolling
- Remove the need for backticks (or troubleshooting forgotten backticks...)
- Cleaner look to the script

```
1 Import-Module ActiveDirectory
2
3 #region Import File Locations
4 $students = Import-Csv C:\scripts\students_import.csv
5 #endregion
6
7 foreach ($student in $students){
8
9 #region Student Variable Definitions
10     $FN = $student.FN
11     $LN = $student.LN
12     $NAME = $FN + " " + $LN
13     $YOG = $student.YOG
14     $SAM = $student.SN
15     $TEMPPWD = (ConvertTo-SecureString -AsPlainText "IWishYouHad8DigitPasswo
16     $INSECUREPWD = $student.PWD
17     $SECUREPWD = (ConvertTo-SecureString $INSECUREPWD -Force)
18     $UPN = $SAM + "@<DOMAIN NAME>"
19     $EMAIL = $SAM + "@<DOMAIN NAME>"
20     $PATH = "OU=" + $YOG + ",OU=StudentAccounts,OU=UserAccounts,DC=<DOMAIN N
21     $GROUP = "U_All_" + $YOG + "Students"
22 #endregion
23
24 $newUserSplat = @{
25     Name = $NAME
26     DisplayName = $NAME
27     GivenName = $FN
28     Surname = $LN
29     SamAccountName = $SAM
30     UserPrincipalName = $UPN
31     EmailAddress = $EMAIL
32     AccountPassword = $TEMPPWD
33     CannotChangePassword = $true
34     PasswordNeverExpires = $true
35     Path = $PATH
36     PassThru = $null
37 }
38
39 #region Active Directory Student Provisioning
40     New-ADUser @newUserSplat | Enable-ADAccount
41
42     Add-ADGroupMember -Identity $GROUP -Members $SAM
43
44     Set-ADAccountPassword -Identity $SAM -Reset -NewPassword $SECUREPWD
45 #endregion
46 }
```

PowerShell Profile

- If you don't have a \$profile, create one and get going!
- `if (! (Test-Path $Profile)) { New-Item -Type File -Path $Profile -Force }`
- `powershell_ise $profile`

```
Microsoft.PowerShellISE_profile.ps1 X
Roll-Rick
701 "Never gonna give you up, never gonna let you down",
702 "Never gonna run around and desert you",
703 "Never gonna make you cry, never gonna say goodbye",
704 "Never gonna tell a lie and hurt you"
705
706 Invoke-Command -ComputerName $ComputerName -ArgumentList (,$Rick)
707 Param ([String[]]$Rolling)
708 [Reflection.Assembly]::LoadWithPartialName('System.Speech') |
709 $Speech = New-Object System.Speech.Synthesis.SpeechSynthesizer
710 ForEach ($Verse in $Rolling)
711 {
712     $Command = {msg * "$Verse"}
713     $Command | Invoke-Expression
714     $Speech.Speak($Verse)
715     Sleep 1
716 }
717 }
718 }
719
720 #requires -Module ActiveDirectory
721 #Import-Module ActiveDirectory -EA Stop
722
723 Function Get-AccountLockoutStatus {...}
836
837 function QueryRdpConnections {...}
865
866 #endregion
867
868 #region PSDrives
869 New-PSDrive -Name sccm -PSProvider FileSystem -Root '\\
870 New-PSDrive -Name staging -PSProvider FileSystem -Root '\\
871 #endregion
872
873 #cleanup my o365 sessions
874 Register-EngineEvent PowerShell.Exiting -SupportEvent -Action {...}
881
882 #TAKE ME HOME
883 Set-Location 'C:\'
884
885 #GET OUT OF MY FACE
886 Clear-Host
887
888 $intro = @"
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2660
2661
2662
2663
2664
2665
2666
2667
2668
2669
2670
2671
2672
2673
2674
2675
2676
2677
2678
2679
2680
2681
2682
2683
2684
2685
2686
2687
2688
2689
2690
2691
2692
2693
2694
2695
2696
2697
2698
2699
2700
2701
2702
2703
2704
2705
2706
2707
2708
2709
2710
2711
2712
2713
2714
2715
2716
2717
2718
2719
2720
2721
2722
2723
2724
2725
2726
2727
2728
2729
2730
2731
2732
2733
2734
2735
2736
2737
2738
2739
2740
2741
2742
2743
2744
2745
2746
2747
2748
2749
2750
2751
2752
2753
2754
2755
2756
2757
2758
2759
2760
2761
2762
2763
2764
2765
2766
2767
2768
2769
2770
2771
2772
2773
2774
2775
2776
2777
2778
2779
2780
2781
2782
2783
2784
2785
2786
2787
2788
2789
2790
2791
2792
2793
2794
2795
2796
2797
2798
2799
2800
2801
2802
2803
2804
2805
2806
2807
2808
2809
2810
2811
2812
2813
2814
2815
2816
2817
2818
2819
2820
2821
2822
2823
2824
2825
2826
2827
2828
2829
2830
2831
2832
2833
2834
2835
2836
2837
2838
2839
2840
2841
2842
2843
2844
2845
2846
2847
2848
2849
2850
2851
2852
2853
2854
2855
2856
2857
2858
2859
2860
2861
2862
2863
2864
2865
2866
2867
2868
2869
2870
2871
2872
2873
2874
2875
2876
2877
2878
2879
2880
2881
2882
2883
2884
2885
2886
2887
2888
2889
2890
2891
2892
2893
2894
2895
2896
2897
2898
2899
2900
2901
2902
2903
2904
2905
2906
2907
2908
2909
2910
2911
2912
2913
2914
2915
2916
2917
2918
2919
2920
2921
2922
2923
2924
2925
2926
2927
2928
2929
2930
2931
2932
2933
2934
2935
2936
2937
2938
2939
2940
2941
2942
2943
2944
2945
2946
2947
2948
2949
2950
2951
2952
2953
2954
2955
2956
2957
2958
2959
2960
2961
2962
2963
2964
2965
2966
2967
2968
2969
2970
2971
2972
2973
2974
2975
2976
2977
2978
2979
2980
2981
2982
2983
2984
2985
2986
2987
2988
2989
2990
2991
2992
2993
2994
2995
2996
2997
2998
2999
3000
3001
3002
3003
3004
3005
3006
3007
3008
3009
3010
3011
3012
3013
3014
3015
3016
3017
3018
3019
3020
3021
3022
3023
3024
3025
3026
3027
3028
3029
3030
3031
3032
3033
3034
3035
3036
3037
3038
3039
3040
3041
3042
3043
3044
3045
3046
3047
3048
3049
3050
3051
3052
3053
3054
3055
3056
3057
3058
3059
3060
3061
3062
3063
3064
3065
3066
3067
3068
3069
3070
3071
3072
3073
3074
3075
3076
3077
3078
3079
3080
3081
3082
3083
3084
3085
3086
3087
3088
3089
3090
3091
3092
3093
3094
3095
3096
3097
3098
3099
3100
3101
3102
3103
3104
3105
3106
3107
3108
3109
3110
3111
3112
3113
3114
3115
3116
3117
3118
3119
3120
3121
3122
3123
3124
3125
3126
3127
3128
3129
3130
3131
3132
3133
3134
3135
3136
3137
3138
3139
3140
3141
3142
3143
3144
3145
3146
3147
3148
3149
3150
3151
3152
3153
3154
3155
3156
3157
3158
3159
3160
3161
3162
3163
3164
3165
3166
3167
3168
3169
3170
3171
3172
3173
3174
3175
3176
3177
3178
3179
3180
3181
3182
3183
3184
3185
3186
3187
3188
3189
3190
3191
3192
3193
3194
3195
3196
3197
3198
3199
3200
3201
3202
3203
3204
3205
3206
3207
3208
3209
3210
3211
3212
3213
3214
3215
3216
3217
3218
3219
3220
3221
3222
3223
3224
3225
3226
3227
3228
3229
3230
3231
3232
3233
3234
3235
3236
3237
3238
3239
3240
3241
3242
3243
3244
3245
3246
3247
3248
3249
3250
3251
3252
3253
3254
3255
3256
3257
3258
3259
3260
3261
3262
3263
3
```

```

1 + $sqlQuery = @"..."@
189
190 $inven = Invoke-Sqlcmd -ServerInstance "..." -Database "..." -Query $sqlQuery
191
192 $inven | Export-Csv -Path C:\scripts\devices w primary users $(Get-Date -Format MMddyy).csv -NoTypeInformation

```

| B | C | D | I | J | K | R | S | T | AA | AB |
|------|--------|-----------|-------------------------|---------------|-----------------|-----------------------|--------------|-------------------------|--------------------------|--------------------------------|
| Name | ADSite | User Name | Model | Serial Number | BIOSDate | Last Reboot Date/Time | Install Date | Last Hardware Inventory | Windows Updates Scan Tim | Windows Updates Last Error Cod |
| EO | | | Latitude 3520 | FPCBRG3 | 9/12/2021 0:00 | Oct 3 2022 9:53AM | 8/8/2022 | 10/3/2022 | 8/22/2022 18:41 | -2016410110 |
| EO | | | Latitude 5490 | BRWKQN2 | 8/27/2018 0:00 | Oct 18 2022 7:44AM | 7/5/2022 | 10/18/2022 | 8/30/2021 14:35 | -2147467259 |
| EO | | | Latitude 7490 | 3RLPHR2 | 7/12/2018 0:00 | Oct 12 2022 1:35PM | 6/30/2022 | 10/18/2022 | | -2147467259 |
| EO | | | Latitude 7420 | DL6G6G3 | 7/12/2022 0:00 | Oct 3 2022 9:38AM | 8/1/2022 | 10/18/2022 | 2/25/2022 17:21 | -2147467259 |
| EO | | | Latitude 7275 | FBX2M72 | 7/9/2016 0:00 | Oct 3 2022 9:38AM | 8/1/2022 | 10/18/2022 | 4/26/2021 11:06 | -2147467259 |
| ER | | | Latitude 7275 | FBX2M72 | 7/9/2016 0:00 | Oct 17 2022 8:02AM | 12/9/2021 | 10/17/2022 | 4/26/2021 11:06 | -2147467259 |
| ER | | | Latitude E7470 | G2CVKC2 | 8/20/2018 0:00 | Oct 17 2022 8:02AM | 12/9/2021 | 10/17/2022 | 10/2/2022 18:01 | -2147023890 |
| ER | | | Latitude E7470 | G2CVKC2 | 8/20/2018 0:00 | Oct 17 2022 7:43AM | 1/8/2022 | 10/18/2022 | 10/2/2022 18:01 | -2147023890 |
| ER | | | OptiPlex 7060 | DD6M7X2 | 11/1/2018 0:00 | Oct 3 2022 7:54AM | 1/21/2022 | 10/17/2022 | 3/29/2021 14:05 | -2147467259 |
| ER | | | OptiPlex 7060 | DF0M7X2 | 11/1/2018 0:00 | Oct 18 2022 10:37AM | 2/25/2022 | 10/18/2022 | 4/12/2021 12:09 | -2147467259 |
| ER | | | OptiPlex 7060 | DF3Q7X2 | 11/1/2018 0:00 | Oct 6 2022 2:40PM | 9/30/2022 | 10/6/2022 | 3/18/2021 16:26 | -2147467259 |
| ER | | | Latitude 3410 | B1T8303 | 7/17/2020 0:00 | Sep 26 2022 12:44PM | 7/25/2022 | 9/26/2022 | 10/4/2022 16:08 | -2145123264 |
| ER | | | HP EliteDesk 800 G1 SFF | MXL4291XSZ | 5/9/2017 0:00 | Oct 17 2022 7:03AM | 1/14/2022 | 10/18/2022 | 11/17/2020 18:23 | -2147467259 |
| GR | | | Latitude E6440 | DSGQQ72 | 10/9/2018 0:00 | Oct 17 2022 7:31AM | 8/9/2022 | 10/18/2022 | 9/26/2022 17:05 | -939523078 |
| GR | | | OptiPlex 7060 | DCNN7X2 | 11/1/2018 0:00 | Oct 8 2022 3:29PM | 4/22/2021 | 10/18/2022 | | -2147467259 |
| GR | | | OptiPlex 7060 | DDMK7X2 | 11/1/2018 0:00 | Sep 29 2022 1:12PM | 6/29/2020 | 10/17/2022 | 3/11/2021 20:14 | -2147467259 |
| GR | | | Latitude 5520 | 5B7F1B3 | 7/4/2022 0:00 | Oct 10 2022 10:23AM | 8/23/2019 | 10/18/2022 | | -2147467259 |
| GR | | | HP EliteDesk 800 G1 SFF | MXL4291XNG | 12/17/2013 0:00 | Oct 3 2022 7:35AM | 1/7/2022 | 10/18/2022 | | -2147467259 |
| GR | | | HP EliteDesk 800 G1 SFF | MXL4291XQN | 12/17/2013 0:00 | Oct 12 2022 8:23AM | 1/10/2022 | 10/18/2022 | 9/13/2021 16:14 | -2147467259 |
| | | | | | | Oct 3 2022 8:20AM | 1/7/2022 | 10/18/2022 | | -2147467259 |
| | | | | | | Oct 17 2022 8:23AM | 7/25/2022 | 10/18/2022 | | -2147467259 |

Hardware Inventory

[SQL Queries](#)

[Invoke-Sqlcmd](#)

[Export-Csv](#)

```
function New-HomeFolder ($homeDrivePath, $samAccountName)
{
    $domainName = "iisd"

    #CREATE HOME DIRECTORY
    New-Item -Path $homeDrivePath -ItemType Directory -Force

    #APPLY PERMISSIONS TO HOME FOLDER
    $identityReference = $domainName + '\' + $samAccountName
    $filesystemAccessRights = [System.Security.AccessControl.FileSystemRights]::Modify
    $inheritanceFlags = [System.Security.AccessControl.InheritanceFlags]::ContainerInherit -bor [System.Security.AccessControl.InheritanceFlags]::ObjectInherit
    $propagationFlags = [System.Security.AccessControl.PropagationFlags]::None
    $accessControl = [System.Security.AccessControl.AccessControlType]::Allow
    $accessRulesplat = $identityReference, $filesystemAccessRights, $inheritanceFlags, $propagationFlags, $accessControl
    $accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule $accessRulesplat
    $homeDirectoryACL = Get-Acl $homeDrivePath
    $homeDirectoryACL.AddAccessRule($accessRule)
    Set-Acl -Path $homeDrivePath -AclObject $homeDirectoryACL
}
```

Managing Home Drives

[New-Item](#)

[Get-Acl](#)

[Set-Acl](#)

PowerShell App Deployment Toolkit (PSADT)

W

- Co
- Se
- Pre
- Pre
- Cu
- Pre
- Ex
- SO
- Ov
- Re
- Go
- Ac

PowerShell App Deployment Toolkit Variables

Toolkit Name

\$appDeployToolkitName
\$appDeployMainScriptFriendlyName
\$scriptInfo
\$appDeployMainScriptVersion
\$appDeployMainScriptMinimumConfigVersion
\$appDeployMainScriptDate
\$appDeployMainScriptParameters

Datetime and Culture

\$currentTime
\$currentTimeTime
\$currentTimeDate
\$currentTimeZoneBias
\$culture
\$currentLanguage
\$currentUILanguage

Environment Variables

\$envHost
\$envShellFolders
\$envAllUsersProfile
\$envAppData
\$envArchitecture
\$envCommonProgramFiles
\$envCommonProgramFilesX86
\$envCommonDesktop
\$envCommonDocuments
\$envCommonStartMenuPrograms
\$envCommonStartMenu
\$envCommonStartUp
\$envCommonTemplates
\$envComputerName
\$envComputerNameFQDN
\$envHomeDrive
\$envHomePath

\$envHomeShare
\$envLocalAppData
\$envLogicalDrives
\$envProgramFiles
\$envProgramFilesX86
\$envProgramData
\$envPublic
\$envSystemDrive
\$envSystemRAM
\$envSystemRoot
\$envTemp
\$envUserCookies
\$envUserDesktop
\$envUserFavorites
\$envUserInternetCache
\$envUserInternetHistory
\$envUserMyDocuments
\$envUserName
\$envUserProfile
\$envUserSendTo
\$envUserStartMenu
\$envUserStartMenuPrograms
\$envUserStartUp
\$envSystem32Directory
\$envWinDir

Domain Membership

\$isMachinePartOfDomain
\$envMachineWorkgroup
\$envMachineAddDomain
\$envLogonServer
\$envMachineDomainController
\$envMachineDNSDomain
\$envUserDNSDomain
\$envUserDomain

Operating System

\$envOS
\$envOSName
\$envOSServicePack
\$envOSVersion
\$envOSVersionMajor
\$envOSVersionMinor
\$envOSVersionBuild
\$envOSVersionRevision
\$envOSProductType
\$isServerOS
\$isDomainControllerOS
\$isWorkStationOS
\$envOSProductTypeName
\$is64Bit
\$envOSArchitecture

Current Process Architecture

\$is64BitProcess
\$psArchitecture

PowerShell And CLR (.NET) Versions

\$envPSVersionTable
\$envPSVersion
\$envPSVersionMajor
\$envPSVersionMinor
\$envPSVersionBuild
\$envPSVersionRevision
\$envCLRVersion
\$envCLRVersionMajor
\$envCLRVersionMinor
\$envCLRVersionBuild
\$envCLRVersionRevision
Permissions/Accounts
\$currentProcessToken
\$currentProcessSID

\$processNTAccount
\$processNTAccountSID
\$isAdmin
\$isLocalSystemAccount
\$isLocalServiceAccount
\$isNetworkServiceAccount
\$isServiceAccount
\$isProcessUserInteractive
\$localSystemNTAccount
\$sessionZero

Script Name and Script Paths

\$scriptPath
\$scriptName
\$scriptFileName
\$scriptRoot
\$invokingScript
\$scriptParentPath

App Deploy Script Dependency Files

\$appDeployLogoIcon
\$appDeployLogoBanner
\$appDeployConfigFile
\$appDeployToolkitDotSourceExtensions
\$xmlConfigFile
\$configConfigVersion
\$configConfigDate

Script Directories

\$dirFiles
\$dirSupportFiles
\$dirAppDeployTemp

Script Naming Convention

\$appVendor
\$appName

\$appVersion
\$appLang
\$appRevision
\$appArch
\$installTitle
\$installName

Executables

\$exeWusa
\$exeMsiexec
\$exeSchTasks

Regex Patterns

\$msiProductCodeRegexPattern

Registry Keys

\$regKeyApplications
\$regKeyLotusNotes
\$regKeyAppExecution
\$regKeyDeferHistory

COM Objects

\$shell
\$shellApp

Log File

\$logName
\$logTempFolder
\$configToolkitLogDir
\$disableScriptLogging
\$revertScriptLogging

Script Parameters

\$deployAppScriptParameters
\$appDeployMainScriptParameters
\$appDeployExtScriptParameters

Logged On Users

\$loggedOnUserSessions
\$usersLoggedOn
\$currentLoggedOnUserSession
\$currentConsoleUserSession
\$runAsActiveUser

Miscellaneous

\$dpiPixels
\$runningTaskSequence
\$isTaskSchedulerHealthy
\$invalidFileNameChars
\$useDefaultMsi

Mailbox Forwarding / Inbox Rules Auditing

- `Get-Mailbox -Identity cthomas@inghamisd.org | Select-Object -Property *forward*`
- `Get-InboxRule -Mailbox cthomas@inghamisd.org -IncludeHidden | Select-Object -Property name,description,enabled,redirectto,movetofolder,forwardto | Format-List`
- `Get-InboxRule -Mailbox cthomas@inghamisd.org -IncludeHidden | Select-Object -Property name,description,enabled,redirectto,movetofolder,forwardto | Where-Object -FilterScript {$_.redirectto -ne $null -or $_.forwardto -ne $null}`

Mailbox Size Audits & Modifications

- `Get-MailboxFolderStatistics -Identity cthomas@inghamisd.org -FolderScope Inbox | Select-Object -Property name,foldersize,itemsinfolder`
- `Get-Mailbox -Identity cthomas@inghamisd.org | Select-Object -Property *quota*`
- `Set-Mailbox -Identity cthomas@inghamisd.org -IssueWarningQuota 90GB -ProhibitSendQuota 95GB -ProhibitSendReceiveQuota 99GB`

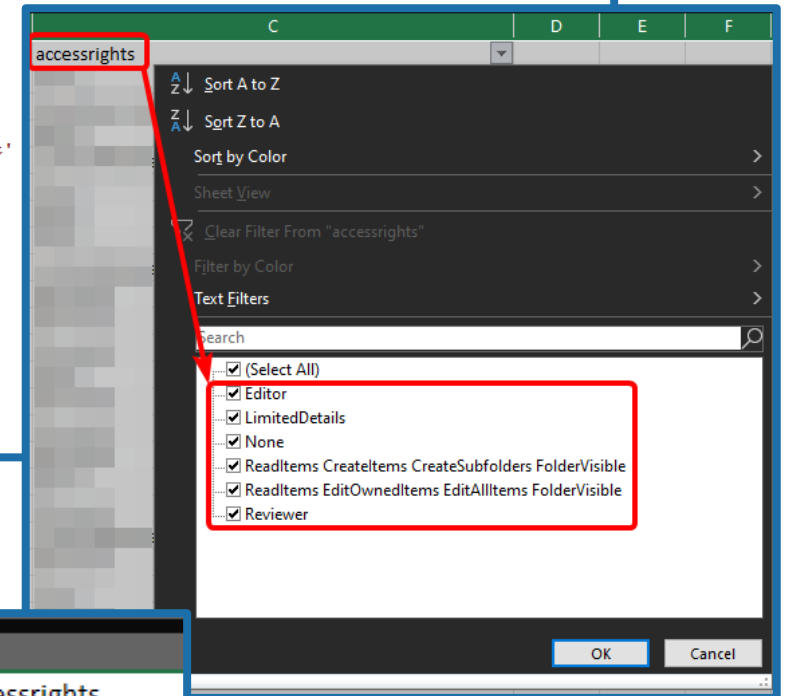
Calendar Permission Audit

```
1 $staffmailboxes = Get-Mailbox -ResultSize Unlimited | Where-Object -FilterScript {$_.userprincipalname -like "*@inghamisd.org"}
2 |
3 $cachedmailboxes = $staffmailboxes
4 $array = @()
5
6 foreach ($staffmailbox in $cachedmailboxes)
7 {
8     $staffmailbox.UserPrincipalName
9     $nonstandardcalendarpermissions = Get-MailboxFolderPermission -Identity "$($staffmailbox.userprincipalname):\Calendar" -User 'Default'
10     "AvailabilityOnly"}
11
12 foreach ($nonstandardcalendarpermission in $nonstandardcalendarpermissions)
13 {
14     $nonstandardobject = New-Object -TypeName PSObject
15     $nonstandardobject | Add-Member -MemberType NoteProperty -Name userprincipalname -Value $staffmailbox.UserPrincipalName
16     $nonstandardobject | Add-Member -MemberType NoteProperty -Name foldername -Value $nonstandardcalendarpermission.FolderName
17     $nonstandardobject | Add-Member -MemberType NoteProperty -Name accessrights -Value $nonstandardcalendarpermission.AccessRights
18     $array += $nonstandardobject
19 }
```

iisd (Get-Date -Format MMddyy).csv -NoTypeInformation



| | A | B | |
|----|-------------------------|-----------|--------------|
| 1 | userprincipalname | foldernan | accessrights |
| 16 | Super Nintendo Chalmers | Calendar | Owner |

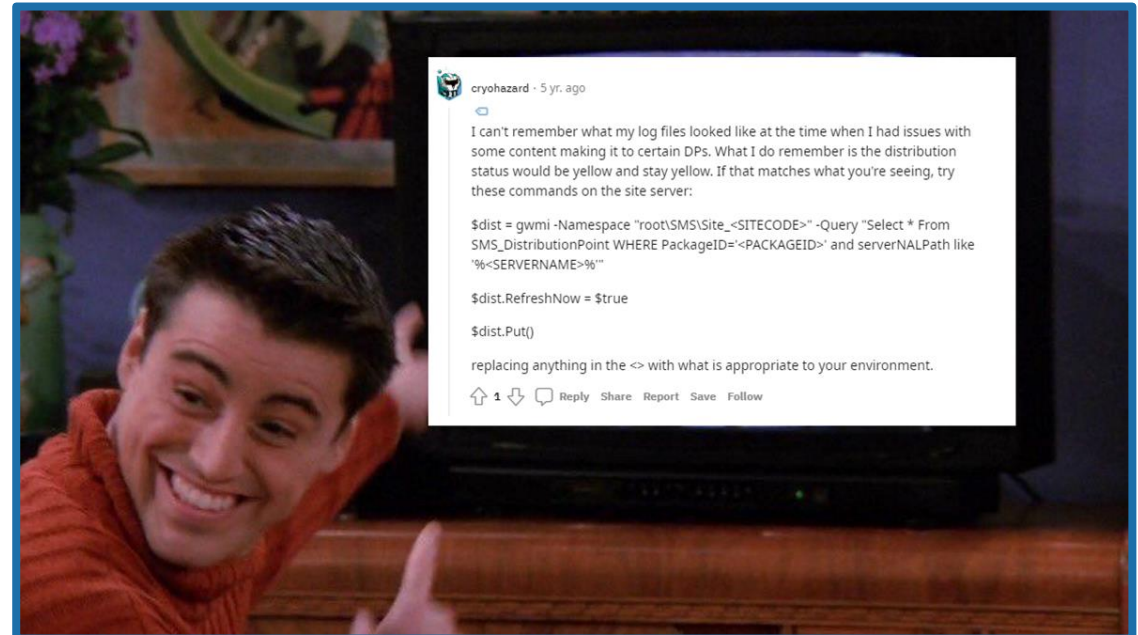


ConfigMgr – Content Issues

```
$dist = gwmi -Namespace "root\SMS\Site_<SITECODE>" -Query "SELECT * FROM SMS_DistributionPoint WHERE  
PackageID='<PACKAGEID>' AND serverNALPath LIKE '%<SERVERNAME>%'"
```

```
$dist.RefreshNow = $true
```

```
$dist.Put()
```



ConfigMgr – DP Issues Post IPU

- <https://smsagent.blog/2020/10/19/real-world-notes-in-place-os-upgrade-on-server-2012-r2-configmgr-distribution-points/>

Anyway, I'm documenting here what I did to fix it and the scripts I used.

To fix the broken ConfigMgr client I did the following:

1. Compile the mof file %program files%\Microsoft Policy Platform\ExtendedStatus.mof
2. Stop any ccmrepair.exe or ccmsetup.exe process so they don't hinder step 3
3. Run the 'Configuration Manager Health Evaluation' scheduled task (ccmeval.exe) a couple of times. This will self-remediate the WMI issues.

To fix the broken DP role:

1. Compile the mof file ..\SMS_DP\$\sms\bin\smsdpprov.mof (this restores the missing WMI namespace)
2. Query the ConfigMgr database to find the list of packages distributed to the distribution point
3. Run some PowerShell code to restore the packages as instances in the root\SCCMDB:SMS_PackagesInContLib WMI class
4. Run the Content Validation scheduled task to revalidate the content and remove any errors in the console

For the latter, I don't take any credit in my script below as I simply used and expanded something I found [here](#). Note both scripts must be run as administrator and the second script requires read access to the ConfigMgr database.

ConfigMgr/M365 Licensing Reconciliation

```
1 $SqlQuery = @"
31
32 $devices = [System.Collections.ArrayList](Invoke-Sqlcmd -ServerInstance " -Database " -Query $SqlQuery)
33
34 $devices | Measure-Object
35
36 foreach ($device in $devices)
37 {
38   $hostname = $device.NetBios_Name0
39   $domain = $device.User_Domain0
40   $username = $device.User_Name0
41
42   switch ($domain)
43   {
44     {
45       $domainName = ' '
46       $members = Get-ADGroupMember -Server -Identity '0365_A1_Faculty' | Select-Object -ExpandProperty SamAccountName
47     }
48     {
49       $domainName = ' '
50       $members = Get-ADGroupMember -Server -Identity '0365_A1_Faculty' | Select-Object -ExpandProperty SamAccountName
51     }
52     {
53       $domainName = ' '
54       $members = Get-ADGroupMember -Server -Identity '0365_A1_Faculty' | Select-Object -ExpandProperty SamAccountName
55     }
56     {
57       $domainName = ' '
58       $members = Get-ADGroupMember -Server -Identity '0365_A1_Faculty' | Select-Object -ExpandProperty SamAccountName
59     }
60     {
61       $domainName = ' '
62       $members = Get-ADGroupMember -Server -Identity '0365_A1_Faculty' | Select-Object -ExpandProperty SamAccountName
63     }
64     default { $domainName = 'INVESTIGATE' }
65   }
66
67   if ($domainName -ne 'INVESTIGATE')
68   {
69     $domainController = (Get-ADDomain -Identity $domainName).PDCemulator
70
71     Write-Host "Checking on $username from $domainName"
72
73     $aduser = Get-ADUser -Server $domainController -Identity $username
74
75     if ($aduser.Enabled -eq $false)
76     {
77       Write-Host "$username is disabled." -ForegroundColor Red
78     }
79
80     if ($members -contains $aduser.SamAccountName)
81     {
82       Write-Host "$username from $domain is in A1 and should likely be licensed as they are a primary user on $hostname." -ForegroundColor Cyan
83     }
84   }
85 }
```

checking on from from
 from is in A1 and should likely be licensed as they are a primary user on .
checking on from from

Print Server Management

- `Invoke-Command -ComputerName <SERVERNAME> -ScriptBlock {Stop-Service -Name Spooler -Force}`
- `Invoke-Command -ComputerName <SERVERNAME> -ScriptBlock {Remove-Item C:\Windows\System32\spool\PRINTERS*.>*`
- `Invoke-Command -ComputerName <SERVERNAME> -ScriptBlock {Start-Service -Name Spooler}`

<TOO MUCH TO REMEMBER!>

- `function Reset-Spooler`
- `{`
- `Param([Parameter(Mandatory=$true)]$PrintServerFQDN)`
- `Invoke-Command -ComputerName $PrintServerFQDN -ScriptBlock {Stop-Service -Name Spooler -Force}`
- `Invoke-Command -ComputerName $PrintServerFQDN -ScriptBlock {Remove-Item C:\Windows\System32\spool\PRINTERS*.*`
- `Invoke-Command -ComputerName $PrintServerFQDN -ScriptBlock {Start-Service -Name Spooler}`
- `}`

LAPS

- `Get-ADComputer -Identity (hostname)`
- `Get-ADComputer -Identity (hostname) | Select-Object -Property *`

<HRMPH>

- `Get-ADComputer -Identity (hostname) -Properties ms-mcs-admpwd`
- `Get-ADComputer -Identity (hostname) - Properties ms-mcs-admpwd | Select-Object -Property ms-mcs-admpwd | Clip`

<WUT?!>

- `Get-ADComputer -Identity (hostname) -Properties ms-mcs-admpwd | Select-Object -ExpandProperty ms-mcs-admpwd | Clip`

PowerShell As 2FA Bypass Vector

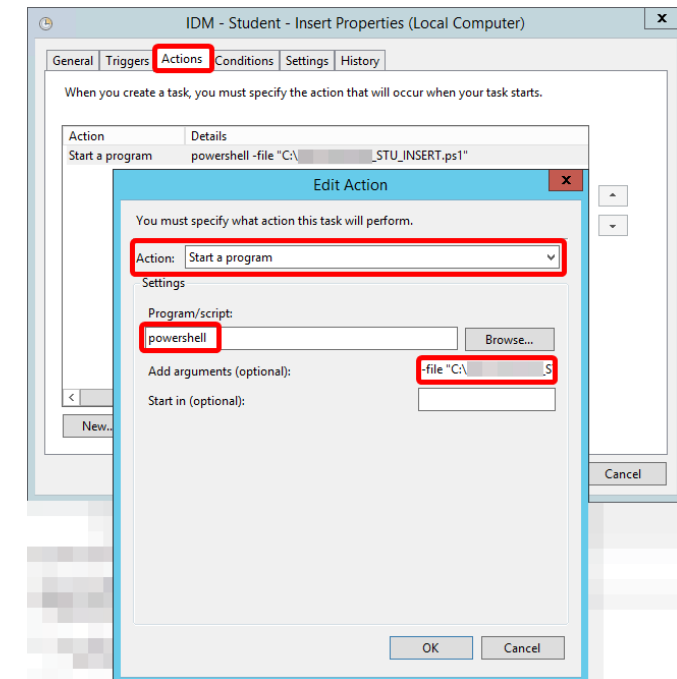
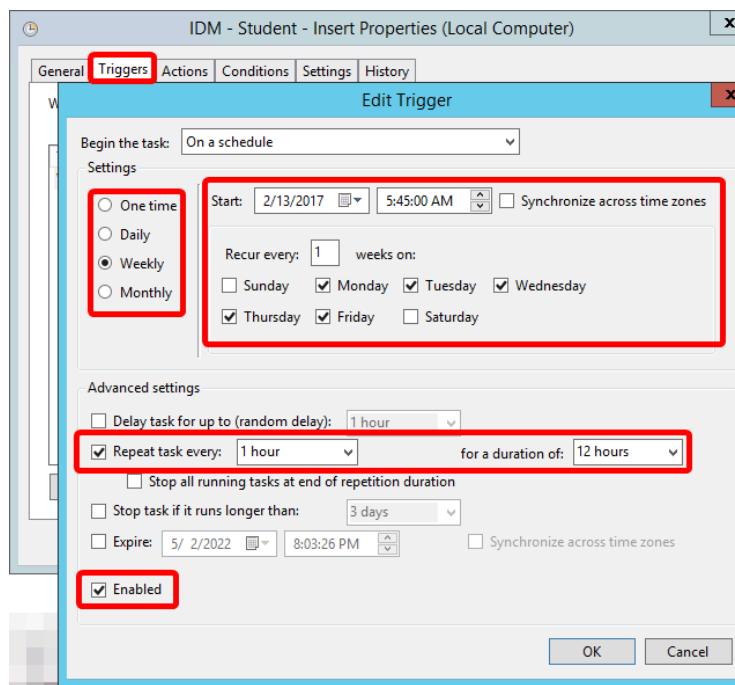
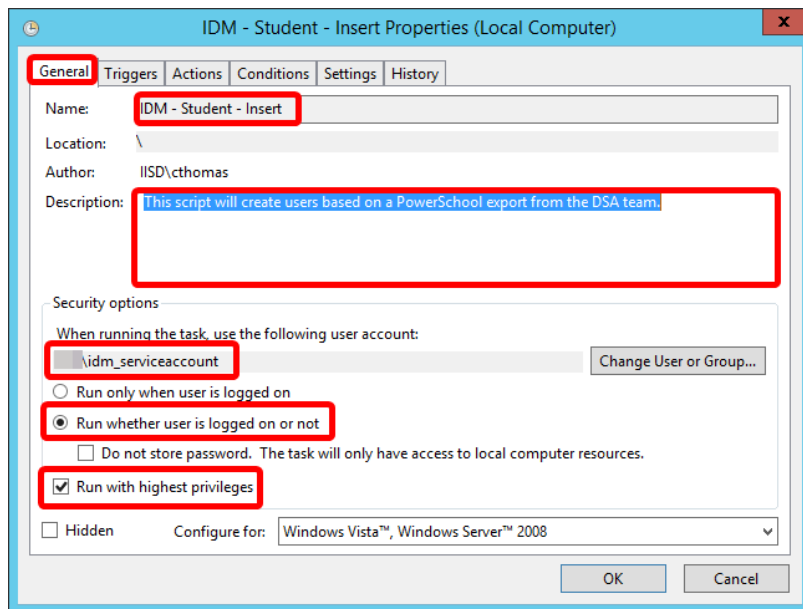
- <https://cybergladius.com/secure-windows-remote-management-from-2fa-bypass/>

Wrap-Up: TLDR

Bypassing 2FA on Windows systems can be done quickly using built-in tools. Our job as Blue Team Defenders is to understand these attacks and build a defense against them. We identified four critical pieces of the WinRM attack and how we can mitigate their risk. Those mitigations are as follows.

1. Limit network access to servers that use WinRM on ports 5985 & 5986 through VLAN Segmentation with ACL rules and Windows Firewalls.
2. Limit password re-use of the local Administrator account.
3. Protect Domain Admin account credentials stored in the system cache.
4. Block Basic User accounts from accessing PowerShell on their systems.

These defenses combined will significantly impede an Attacker from using WinRM against you.



Task Scheduler

Run scripts on-demand until you are comfortable and then schedule them to run automatically so you can focus on other tasks

[How to Schedule PowerShell Script using Task Scheduler](#)

Use a service account with delegated permissions, not Domain Admin, to run your tasks

[Active Directory Delegated Permissions Best Practices](#)

[Delegate AD group management](#)

-- The End --

Ask Questions ...

... then go forth and iterate.

PAST PRESENTATIONS:

<https://github.com/chrisATautomatemystuff/Presentations>

