OU GPO

OU SQL SRV01 SRV02 OU SQL_Server HR OU HR

GPO OU GPO OU GPO GPO

OU

OU:

```
Get-DomainOU -Properties Name
```

```
beacon> powershell get-domainou -properties name
[*] Tasked beacon to run: get-domainou -properties name
[+] host called home, sent: 361 bytes
[+] received output:
#< CLIXML

name
----
Domain Controllers
Groups
Web Server
```

3 OU 2 PROD OU

```
beacon> powershell get-domainou -domain prod.raven-med.local -properties name
[*] Tasked beacon to run: get-domainou -domain prod.raven-med.local -properties name
[+] host called home, sent: 437 bytes
[+] received output:
#< CLIXML

name
----
Domain Controllers
Groups
Assets
SQL Server
File Server
Web Server
```

SQL Server

```
beacon> powershell get-domainou -domain prod.raven-med.local -identity "SQL Server"
[*] Tasked beacon to run: get-domainou -domain prod.raven-med.local -identity "SQL Server"
[+] host called home, sent: 453 bytes
[+] received output:
#< CLIXML


usncreated            : 29442
name                  : SQL Server
gplink                : [LDAP://cn={44A64ADE-70E1-4F92-B4DF-09B01AADC296},cn=policies,cn=system,DC=prod,DC=raven-med,DC
                        =local;0]
whenchanged           : 1/29/2023 12:36:02 AM
objectclass           : {top, organizationalUnit}
usnchanged            : 29465
dscorepropagationdata : {1/29/2023 12:37:59 AM, 1/29/2023 12:28:45 AM, 1/29/2023 12:28:35 AM, 1/29/2023 12:28:35 AM...}
distinguishedname     : OU=SQL Server,OU=Assets,DC=prod,DC=raven-med,DC=local
ou                    : SQL Server
whencreated           : 1/29/2023 12:28:35 AM
instancetype          : 4
objectguid            : cf42d795-db43-4e7d-ba06-d641da10937e
objectcategory        : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=raven-med,DC=local
```

OU

```
Get-DomainOU -domain prod.raven-med.local -identity "SQL Server" | %{Get-DomainComputer -SearchBase $_.distinguishedname -Properties Name}
```

PROD SQL Server OU SRV01

```
beacon> powershell Get-DomainOU -domain prod.raven-med.local -identity "SQL Server" | %{Get-DomainComputer -SearchBase $_.distinguishedname -Properties Name}
[*] Tasked beacon to run: Get-DomainOU -domain prod.raven-med.local -identity "SQL Server" | %{Get-DomainComputer -SearchBase $_.distinguishedname -Properties Name}
[+] host called home, sent: 653 bytes
[+] received output:
#< CLIXML

name
----
SRV01
```

GPO

GPO

```
Get-DomainGPO -Properties DisplayName
```

```
beacon> powershell get-domaingpo -properties  displayname
[*] Tasked beacon to run: get-domaingpo -properties  displayname
[+] host called home, sent: 385 bytes
[+] received output:
#< CLIXML

displayname
-----------
Default Domain Policy
Default Domain Controllers Policy
DebugRemoval
```

GPO DebugRemoval

```
beacon> powershell get-domaingpo -identity DebugRemoval
[*] Tasked beacon to run: get-domaingpo -identity DebugRemoval
[+] host called home, sent: 381 bytes
[+] received output:
#< CLIXML


usncreated               : 25983
displayname              : DebugRemoval
gpcmachineextensionnames : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
whenchanged              : 1/29/2023 12:45:38 AM
objectclass              : {top, container, groupPolicyContainer}
gpcfunctionalityversion  : 2
showinadvancedviewonly   : True
usnchanged               : 25996
dscorepropagationdata    : 1/1/1601 12:00:00 AM
name                     : {B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
flags                    : 0
cn                       : {B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
gpcfilesyspath           : \\white-bird.local\SysVol\white-bird.local\Policies\{B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
distinguishedname        : CN={B21C9CAF-5C08-4F24-BDE3-26D18CB01143},CN=Policies,CN=System,DC=white-bird,DC=local
whencreated              : 1/29/2023 12:41:24 AM
versionnumber            : 2
instancetype             : 4
objectguid               : 1a9e3fab-4c81-4c54-b709-58e4ef0f4ecf
objectcategory           : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=white-bird,DC=local
```

GPO PROD GPO PROD GPO AppLocker

```
beacon> powershell get-domaingpo -properties displayname -domain prod.raven-med.local
[*] Tasked beacon to run: get-domaingpo -properties displayname -domain prod.raven-med.local
[+] host called home, sent: 461 bytes
[+] received output:
#< CLIXML

displayname
-----------
Default Domain Policy
Default Domain Controllers Policy
AppLocker
Writable
RunAsPPL
```

AppLocker RunAsPPL

GPO

GPO Web02

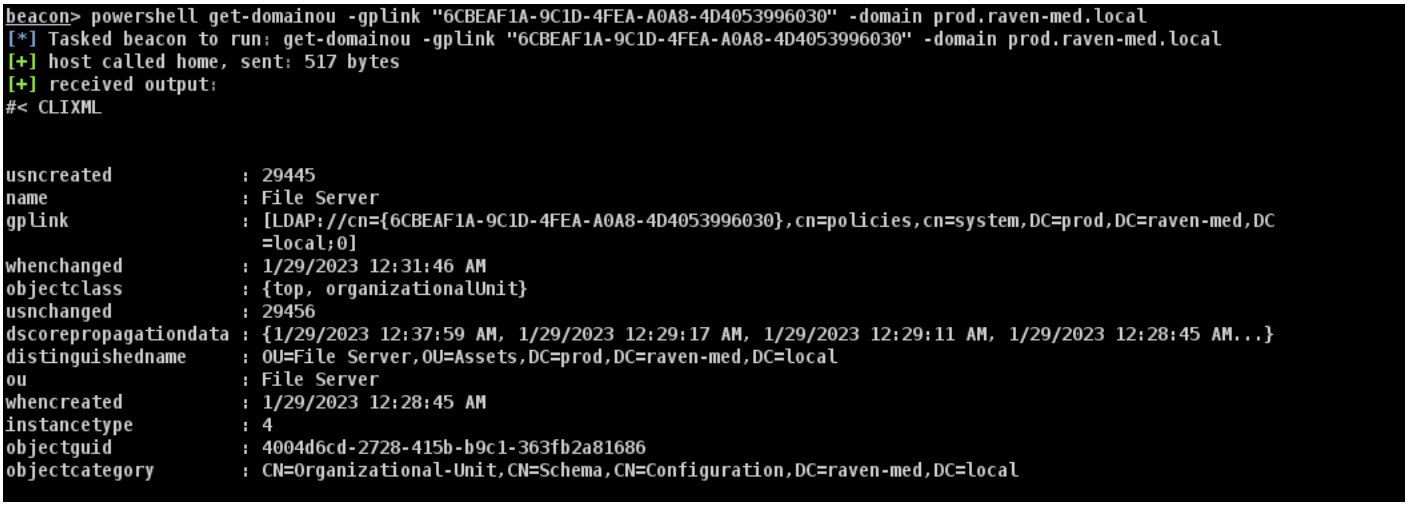
```
beacon> powershell get-netgpo -computername web02 | select displayname
[*] Tasked beacon to run: get-netgpo -computername web02 | select displayname
[+] host called home, sent: 421 bytes
[+] received output:
#< CLIXML

displayname
-----------
DebugRemoval
Default Domain Policy
```

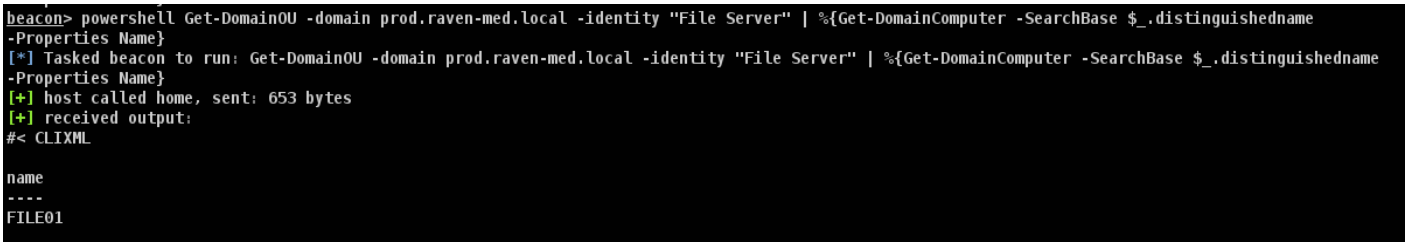
2 GPO Web02

GPO OU

```
Get-DomainOU -gpLink "[GPO Name(   )]"
```

RavenPPL GPO **File Server** OU OU **file01**





BloodHound OU GPO

Revision #5
Created 5 September 2022 03:04:49 by
Updated 30 March 2023 21:43:32 by