OU GPO

 OU SQL
 SRV01
 SRV02
 OU SQL_Server
 HR
 OU HR

 GPO
 OU
 GPO
 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</pre>
```

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</pre>
```

SQL Server

```
<u>beacon</u>> 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
                      : SQL Server
name
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
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...}
                      : OU=SQL Server, OU=Assets, DC=prod, DC=raven-med, DC=local
distinguishedname
                      : SQL Server
ou
whencreated
                      : 1/29/2023 12:28:35 AM
instancetype
objectguid
                      : cf42d795-db43-4e7d-ba06-d641da10937e
                      : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=raven-med,DC=local
objectcategory
```

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

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</pre>
```

GPO DebugRemoval

```
<u>beacon</u>> 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
                           [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
gpcmachineextensionnames :
whenchanged
                            1/29/2023 12:45:38 AM
objectclass
                           {top, container, groupPolicyContainer}
gpcfunctionalityversion
showinadvancedviewonly
                           True
usnchanged
                           25996
                            1/1/1601 12:00:00 AM
dscorepropagationdata
                           {B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
name
flags
cn
                           {B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
                            \white-bird.local\SysVol\white-bird.local\Policies\{B21C9CAF-5C08-4F24-BDE3-26D18CB01143}
gpcfilesyspath
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
instancetype
                           1a9e3fab-4c81-4c54-b709-58e4ef0f4ecf
objectguid
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

GPO OU

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

RROASPPL GPO File Server OU OUfile01

```
<u>beacon</u>> powershell get-domainou -gplink "6CBEAF1A-9C1D-4FEA-A0A8-4D4053996030" -domain prod.raven-med.local
[*] Tasked beacon to run: get-domainou -gplink "6CBEAF1A-9C1D-4FEA-A0A8-4D4053996030" -domain prod.raven-med.local
[+] host called home, sent: 517 bytes
[+] received output:
#< CLIXML
                          : 29445
: File Server
usncreated
name
gpLink
                            [LDAP://cn={6CBEAF1A-9C1D-4FEA-A0A8-4D4053996030},cn=policies,cn=system,DC=prod,DC=raven-med,DC
                            =local;0]
whenchanged
                            1/29/2023 12:31:46 AM
                          : {top, organizationalUnit}
: 29456
objectclass
usnchanged
dscorepropagationdata : {1/29/2023 12:37:59 AH, 1/29/2023 12:29:17 AM, 1/29/2023 12:29:11 AM, 1/29/2023 12:28:45 AH...}
distinguishedname
                          : OU=File Server,OU=Assets,DC=prod,DC=raven-med,DC=local
                            File Server
ou
                            1/29/2023 12:28:45 AM
whencreated
instancetype
                          : 4
objectguid
                          : 4004d6cd-2728-415b-b9c1-363fb2a81686
                          : CN=Organizational-Unit, CN=Schema, CN=Configuration, DC=raven-med, DC=local
objectcategory
```

```
beacon> powershell Get-DomainOU -domain prod.raven-med.local -identity "File Server" | %{Get-DomainComputer -SearchBase $_.distinguishedname -Properties Name}
[*] Tasked beacon to run: Get-DomainOU -domain prod.raven-med.local -identity "File Server" | %{Get-DomainComputer -SearchBase $_.distinguishedname -Properties Name}
[+] host called home, sent: 653 bytes
[+] received output:
#< CLIXML
name
----
FILEO1
```

BloodHound OU GPO

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