SPECTEROPS TROOPERS

Analyzing and Executing ADCS Attack Paths with BloodHound

Permalink to this deck: https://bit.ly/4csKVjc

PS C:\> Get-Speakers | %{Get-SpeakerInfo}

Jonas Bülow Knudsen

Product Architect @ SpecterOps

@Jonas_B_K

Andy Robbins

Principal Product Architect @ SpecterOps

@_wald0

Agenda

- ADCS Attack Path Discovery, Analysis, and Execution
  - ESC1
  - ESC3
  - ESC5
  - ESC13
- Visualizing and Auditing the ADCS LDAP Hierarchy
- Practical Remediation Strategies and Examples

ESC1

ESC1 Cert Template

Enterprise CA

Domain Controller

Alice

Bob

ESC1 Cert Template

Enterprise CA

Domain Controller

“Please issue an ESC1 certificate to me. My subject alternative name is **bob@contoso.local**”

Alice

Bob

ESC1 Cert Template

Enterprise CA

Domain Controller

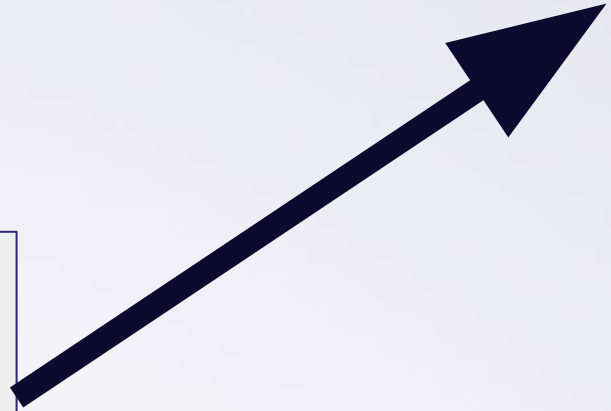
Alice

Bob

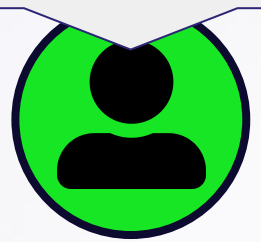
ESC1 Cert Template

Enterprise CA

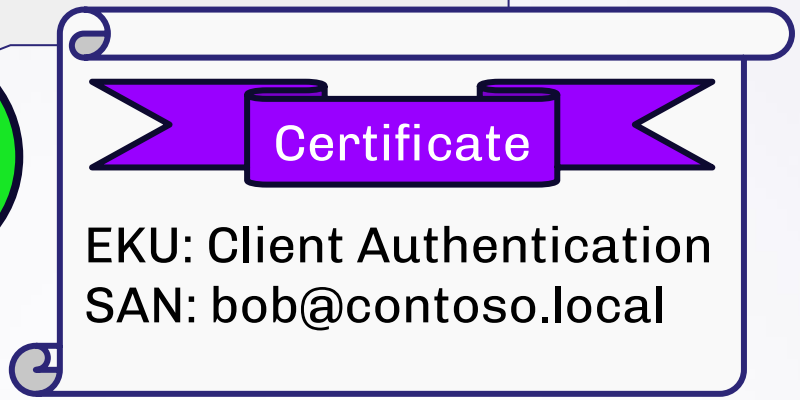
Domain Controller



"Please issue a TGT to me for **bob@contoso.local**. This certificate will serve as my credential for that user."



Alice



Bob

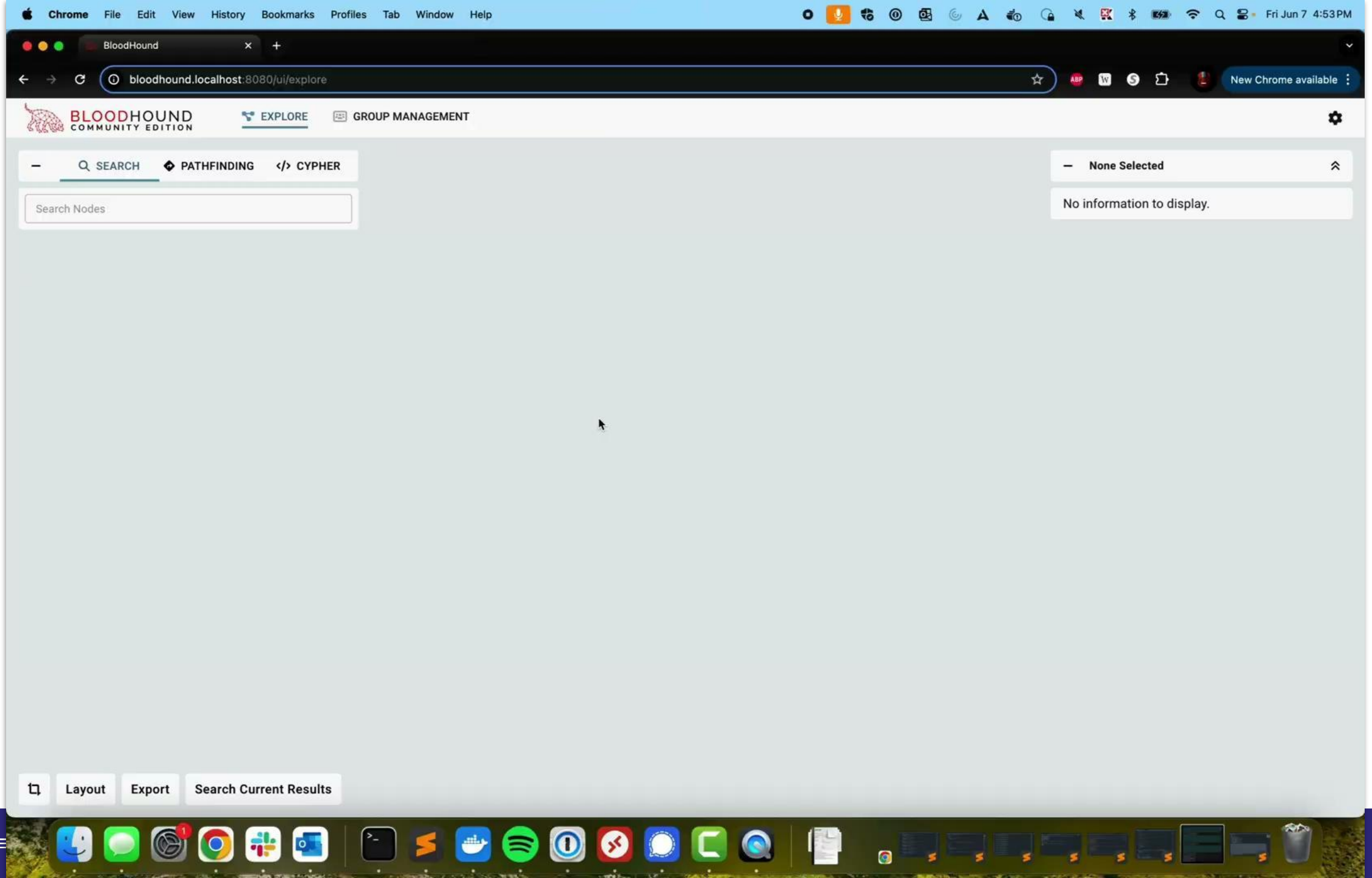
ESC1 Cert Template

Enterprise CA

Domain Controller

Alice

Bob


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri Jun 7 4:53 PM
BloodHound
bloodhound.localhost:8080/ui/explore
New Chrome available
BLOODHOUND COMMUNITY EDITION
EXPLORE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
Search Nodes
None Selected
No information to display.
Layout
Export
Search Current Results

ESC3

EnrollmentAgent

User

Enterprise CA

Domain Controller

ESC3 - Abuse of Enrollment Agent Permissions

Alice

Bob

EnrollmentAgent

User

Enterprise CA

Domain Controller

Alice

Bob

EnrollmentAgent

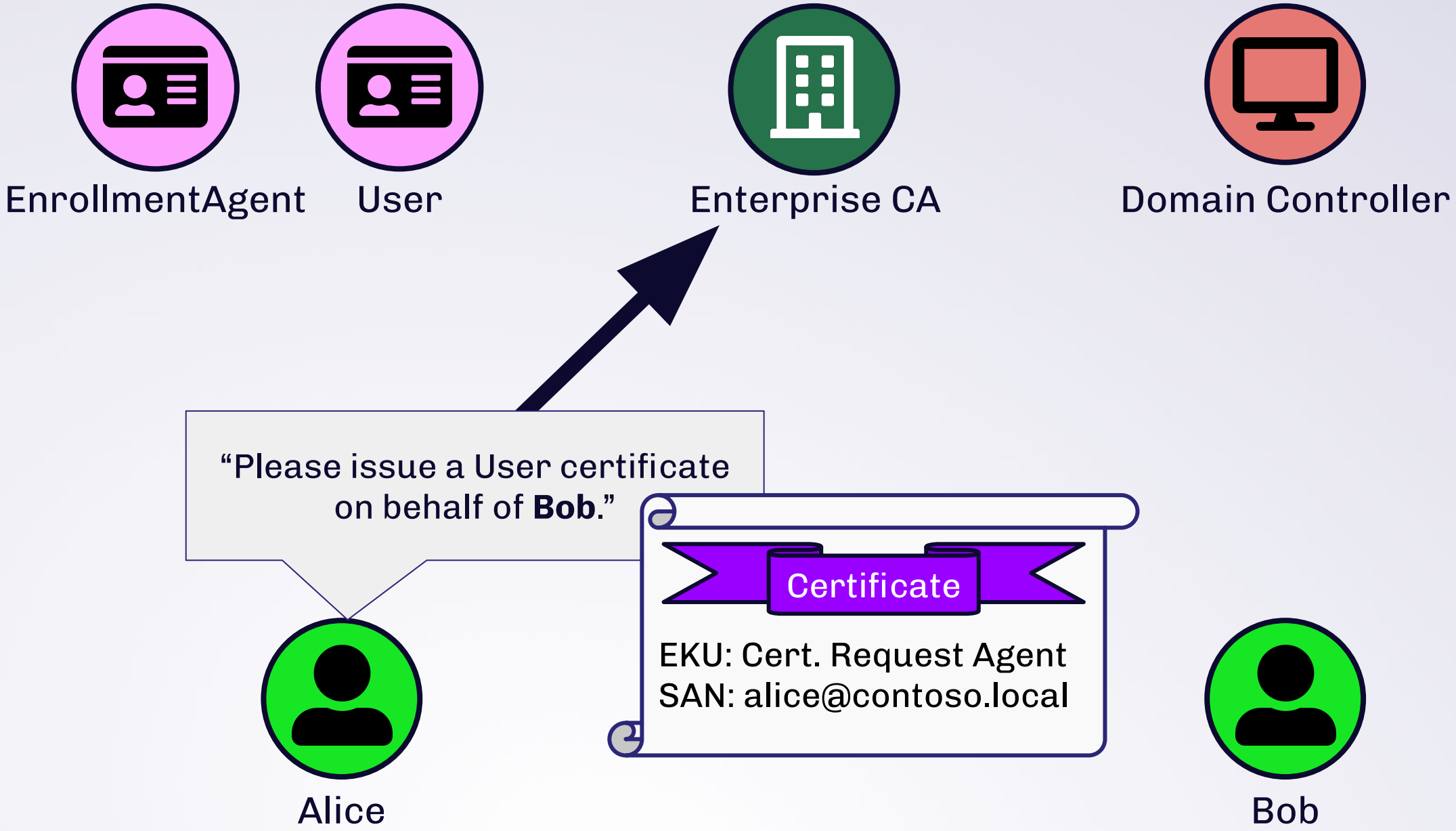
User

Enterprise CA

Domain Controller

Alice

Bob


EnrollmentAgent
User
Enterprise CA
Domain Controller
“Please issue a User certificate on behalf of **Bob**.”
Certificate
EKU: Cert. Request Agent
SAN: alice@contoso.local
Alice
Bob

EnrollmentAgent

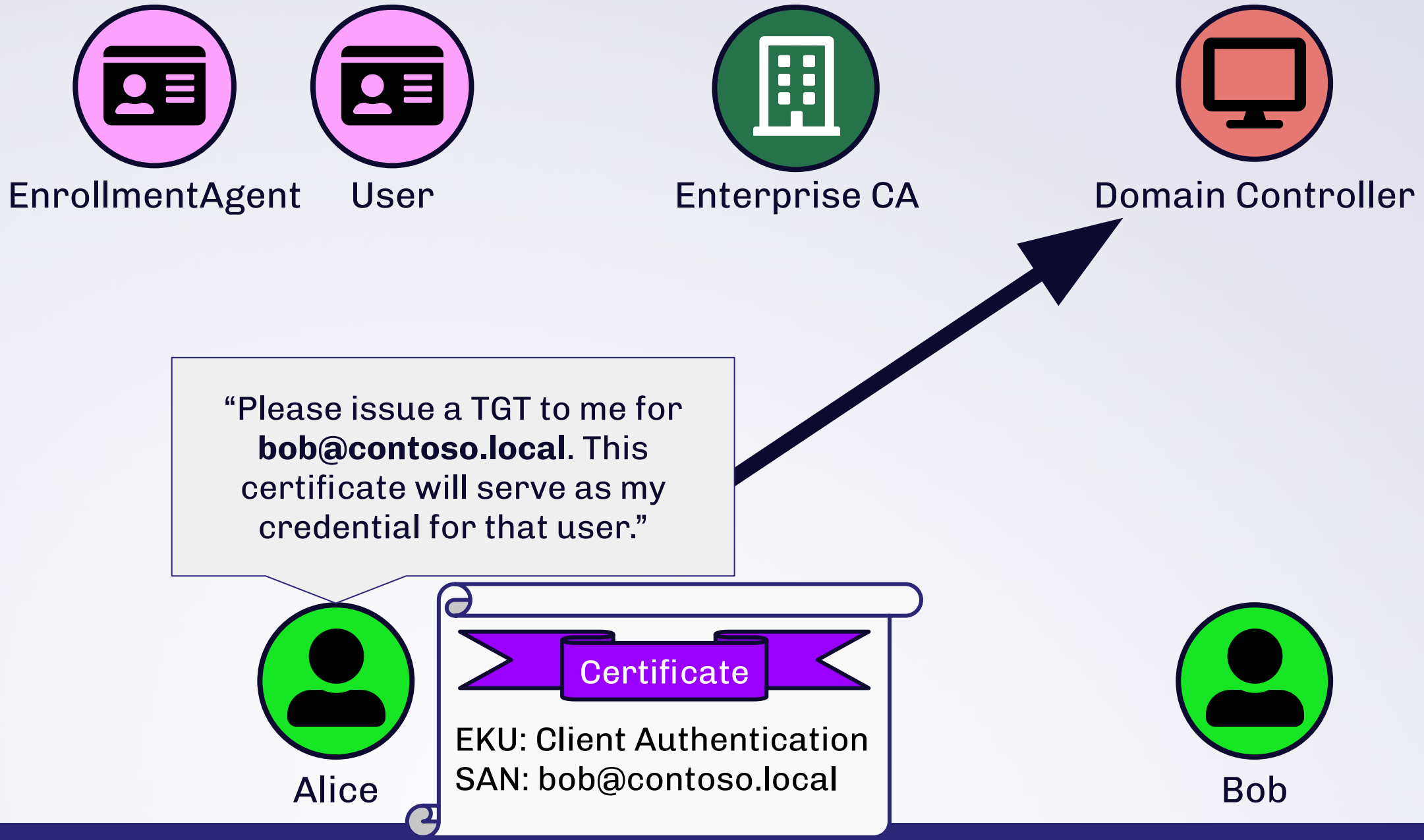
User

Enterprise CA

Domain Controller

Alice

Bob


EnrollmentAgent
User
Enterprise CA
Domain Controller
“Please issue a TGT to me for **bob@contoso.local**. This certificate will serve as my credential for that user.”
Alice
Certificate
EKU: Client Authentication
SAN: bob@contoso.local
Bob

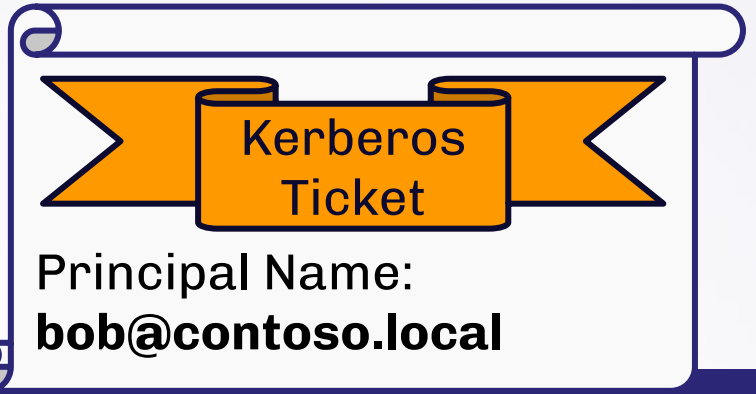
EnrollmentAgent

User

Enterprise CA

Domain Controller

Alice

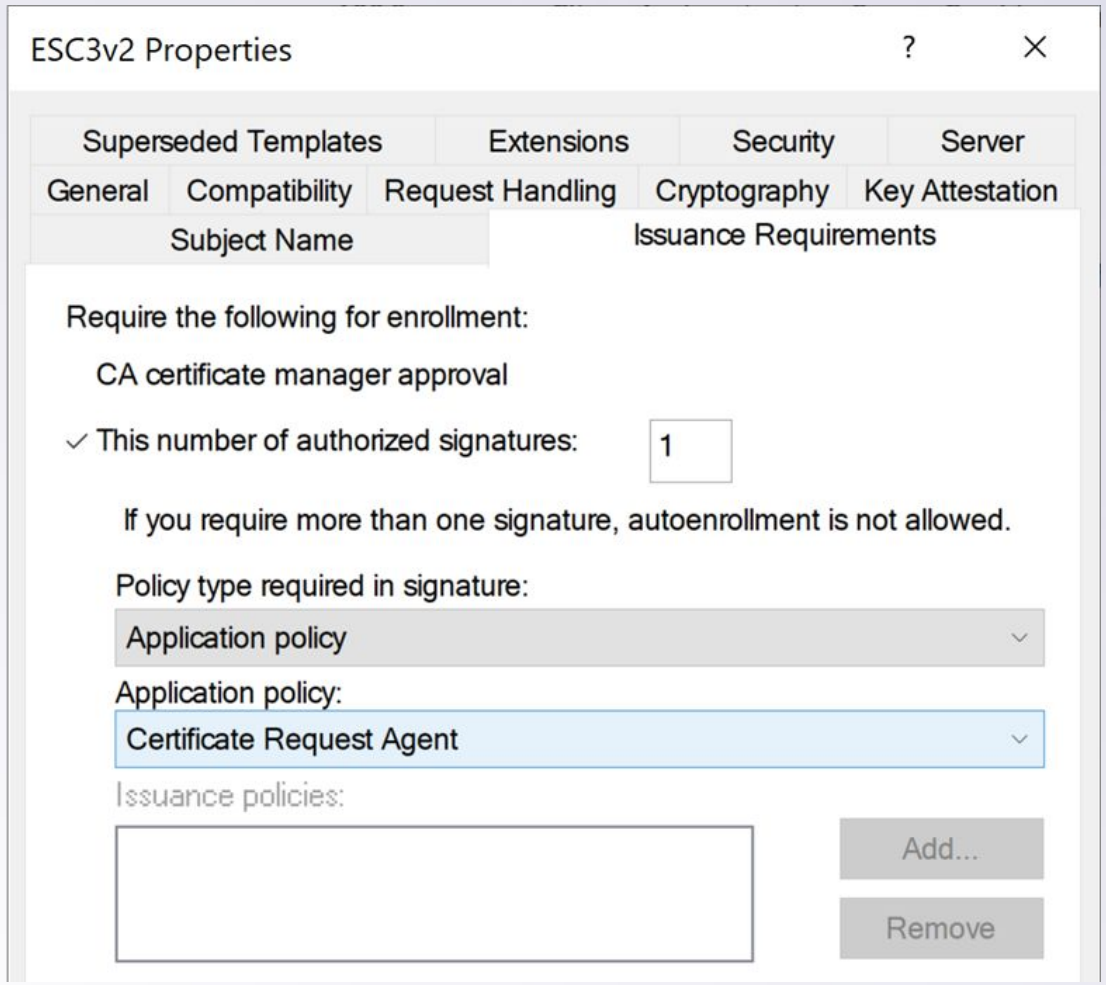


Bob

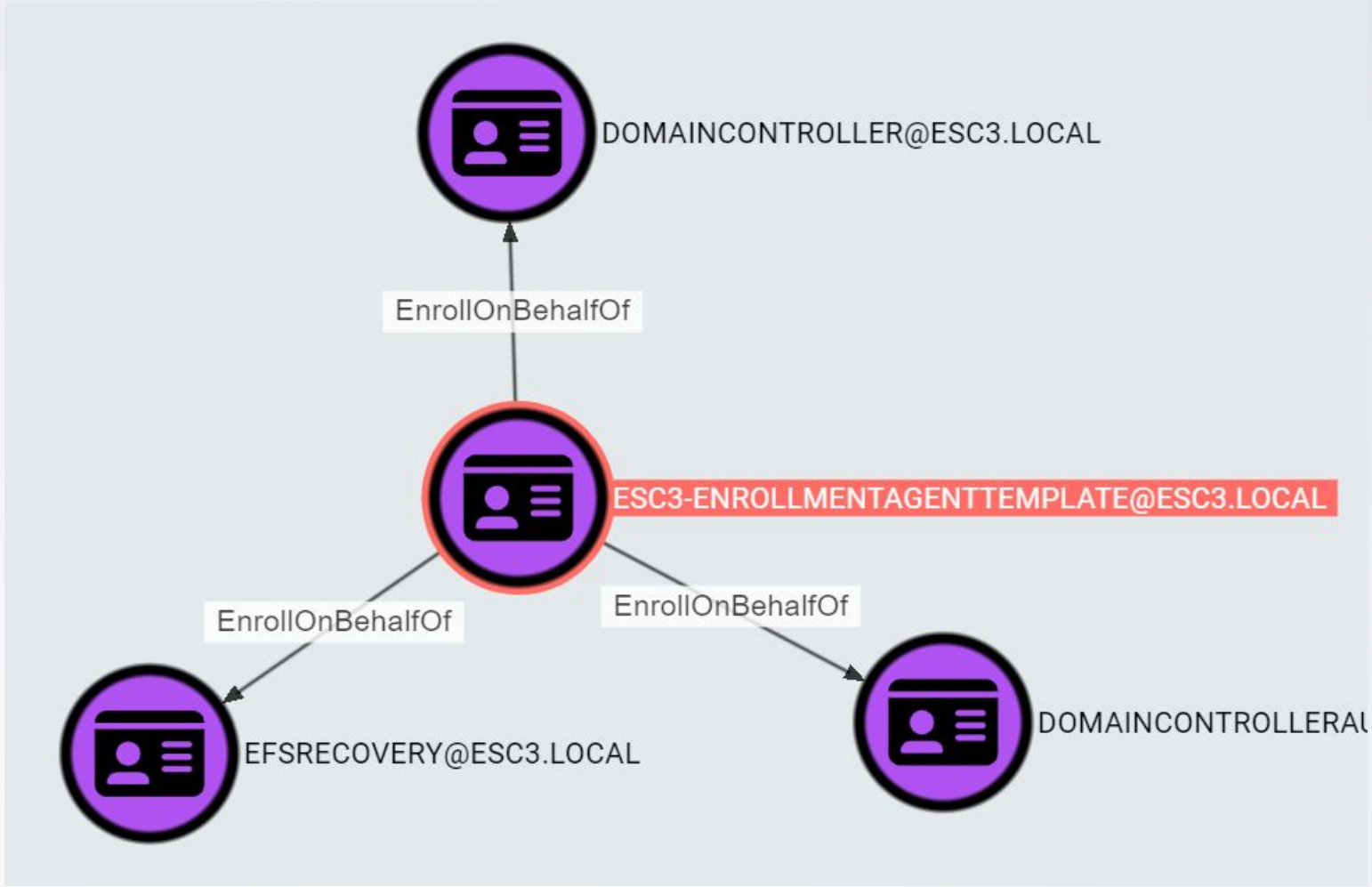
ESC3 - What is an Enrollment Agent

- *Certificate Request Agent* EKU (1.3.6.1.4.1.311.20.2.1) → Enrollment Agent
- Can enroll on behalf of other principals in templates:
  - Schema version 1
  - Schema version 2+ with the Certificate Request Agent EKU required as Application Policy

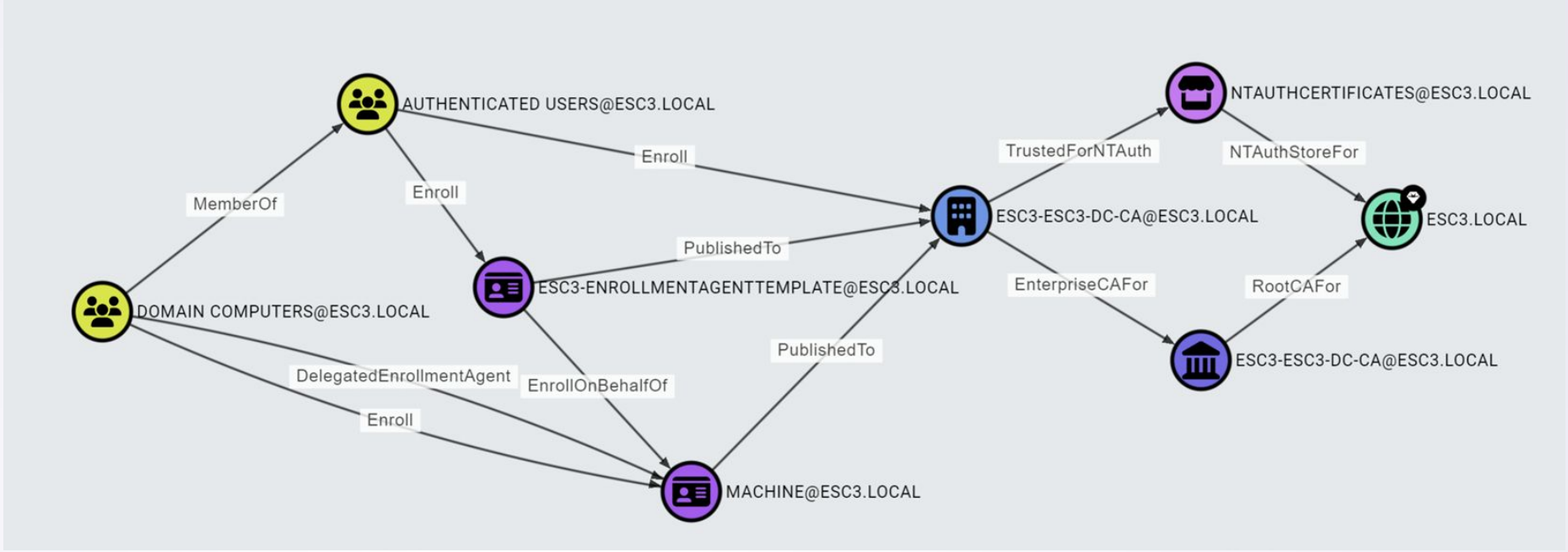
https://posts.specterops.io/adcs-attack-paths-in-bloodhound-part-2-ac7f925d1547



ESC3 - Enrollment Agents in BloodHound



ESC3 - Enrollment Agents in BloodHound



ESC5

ESC5

LDAP object manipulation

Abuses the mechanics of AD and ADCS, combined with abusable privileges to impersonate any principal in AD.

An attractive backdoor

The numerous combinations of privileges that can enable ESC5 make this escalation primitive particularly difficult to manually discover.

Enables escalation from DA to EA

Due to a quirk in Configuration naming context replication, ESC5 enables turning DA in any domain into EA at the forest root.

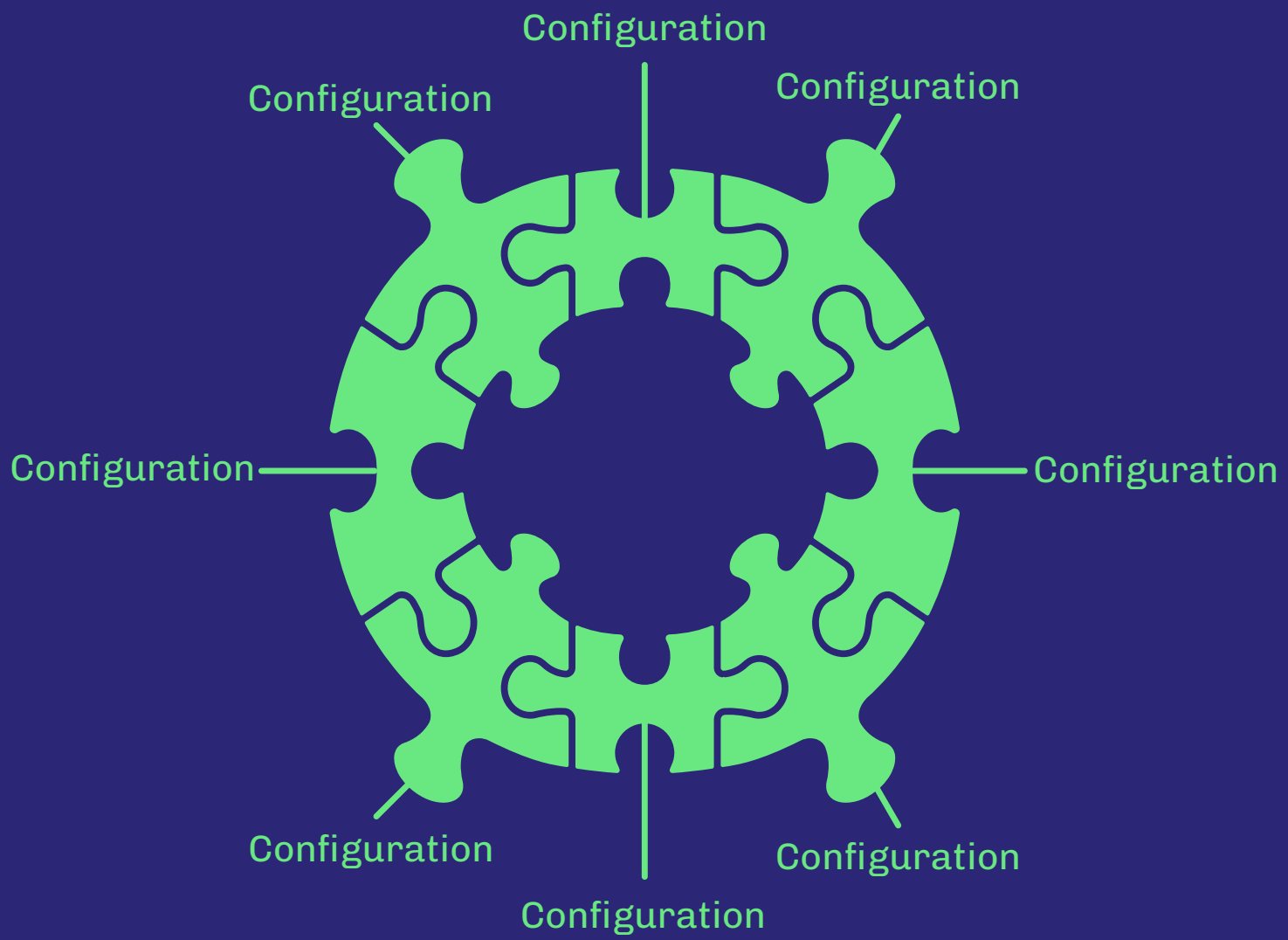
Two Families of ESC5

Modify existing ADCS objects

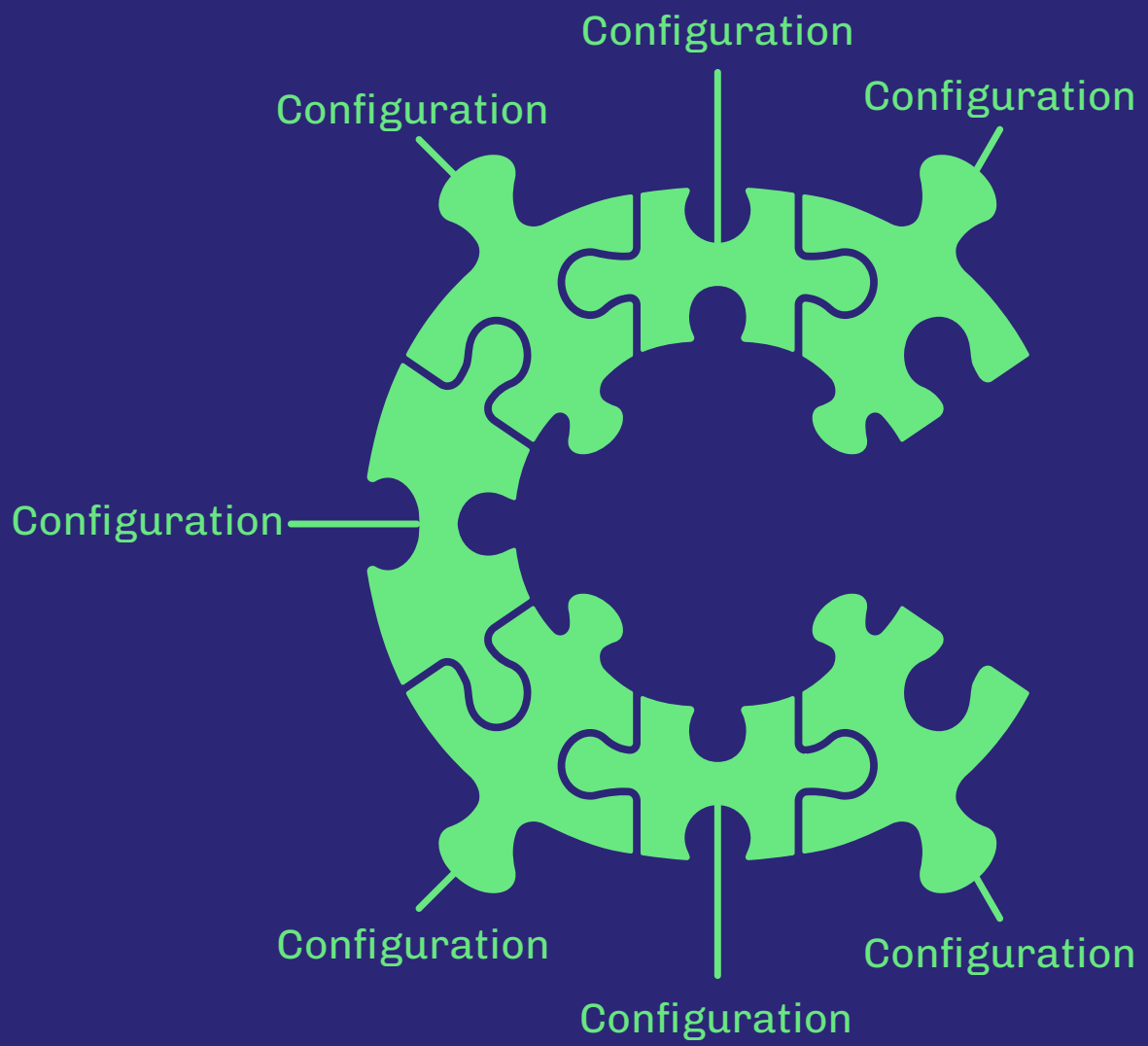
- ADCS is already installed and configured.
- A principal can combine existing configurations and privileges to create for themselves the ability to impersonate other principals.

Full ADCS Bootstrap

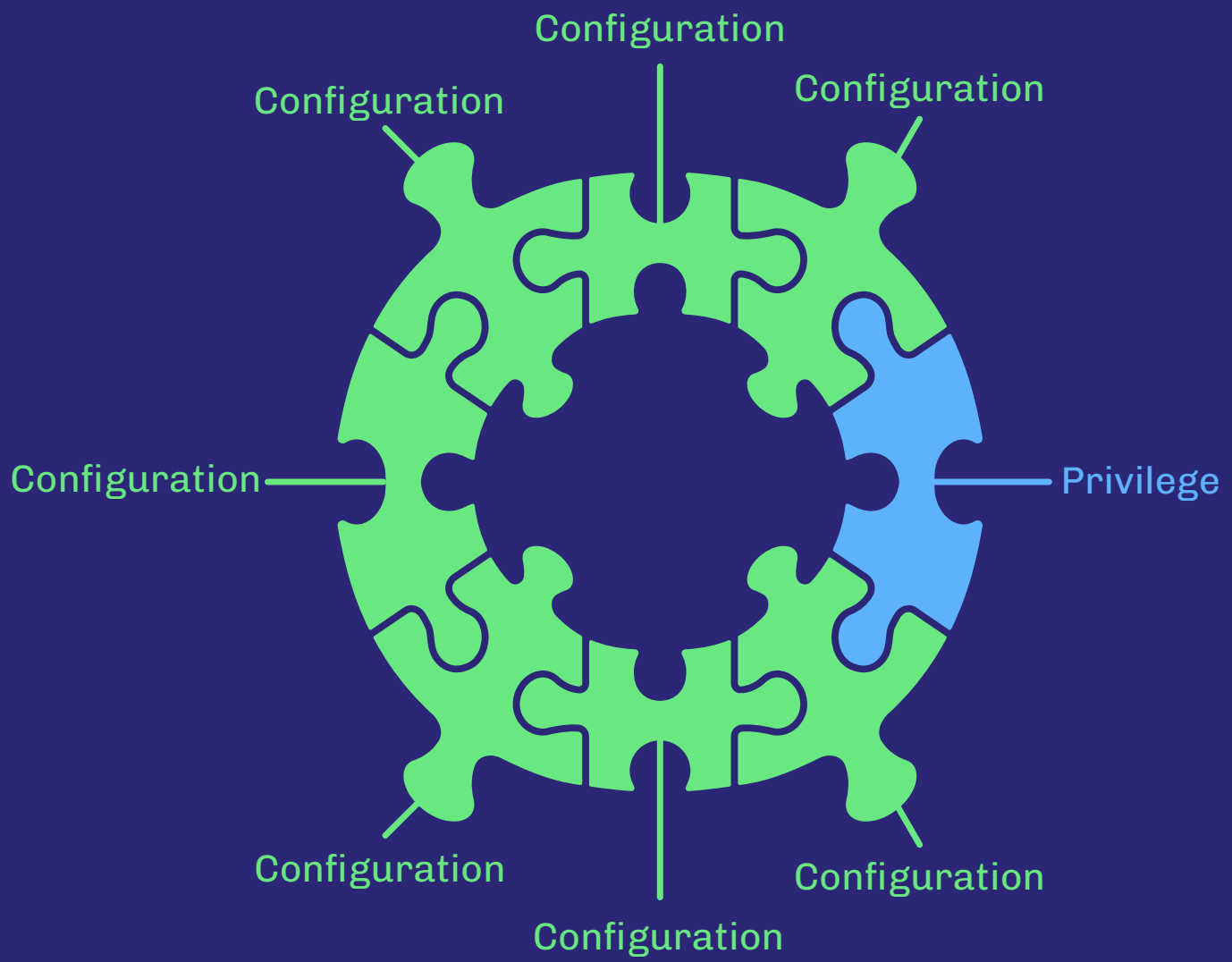
- ADCS is not installed nor configured.
- A principal has the privileges needed to create and configure specific objects in the Configuration naming context, such that a functional ADCS environment emerges.


Configuration
Configuration
Configuration
Configuration
Configuration
Configuration
Configuration
Configuration

ESC1

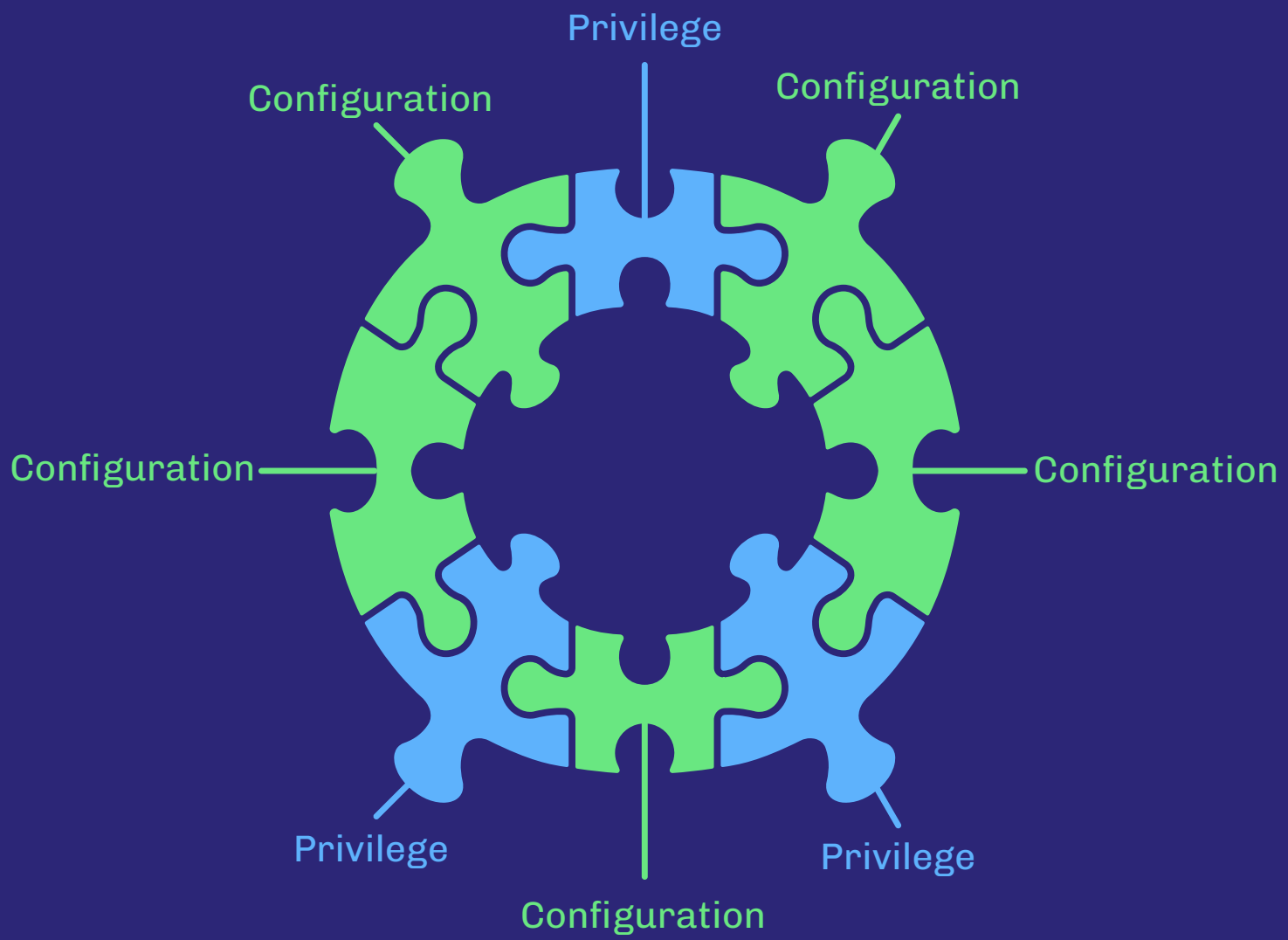

Configuration
Configuration
Configuration
Configuration
Configuration
Configuration
Configuration

≠ ESC1

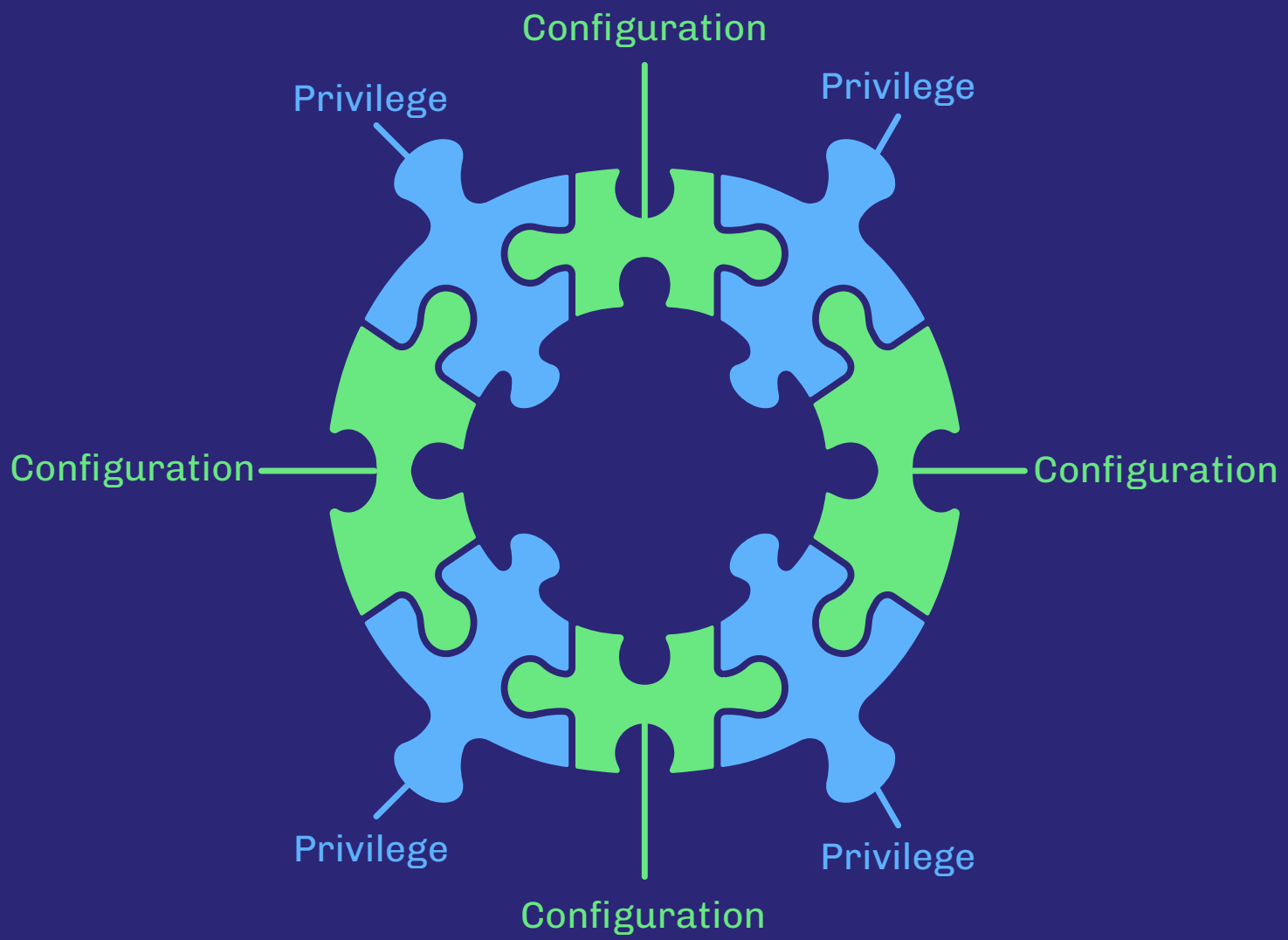

Configuration
Configuration
Configuration
Configuration
Privilege
Configuration
Configuration
Configuration

=

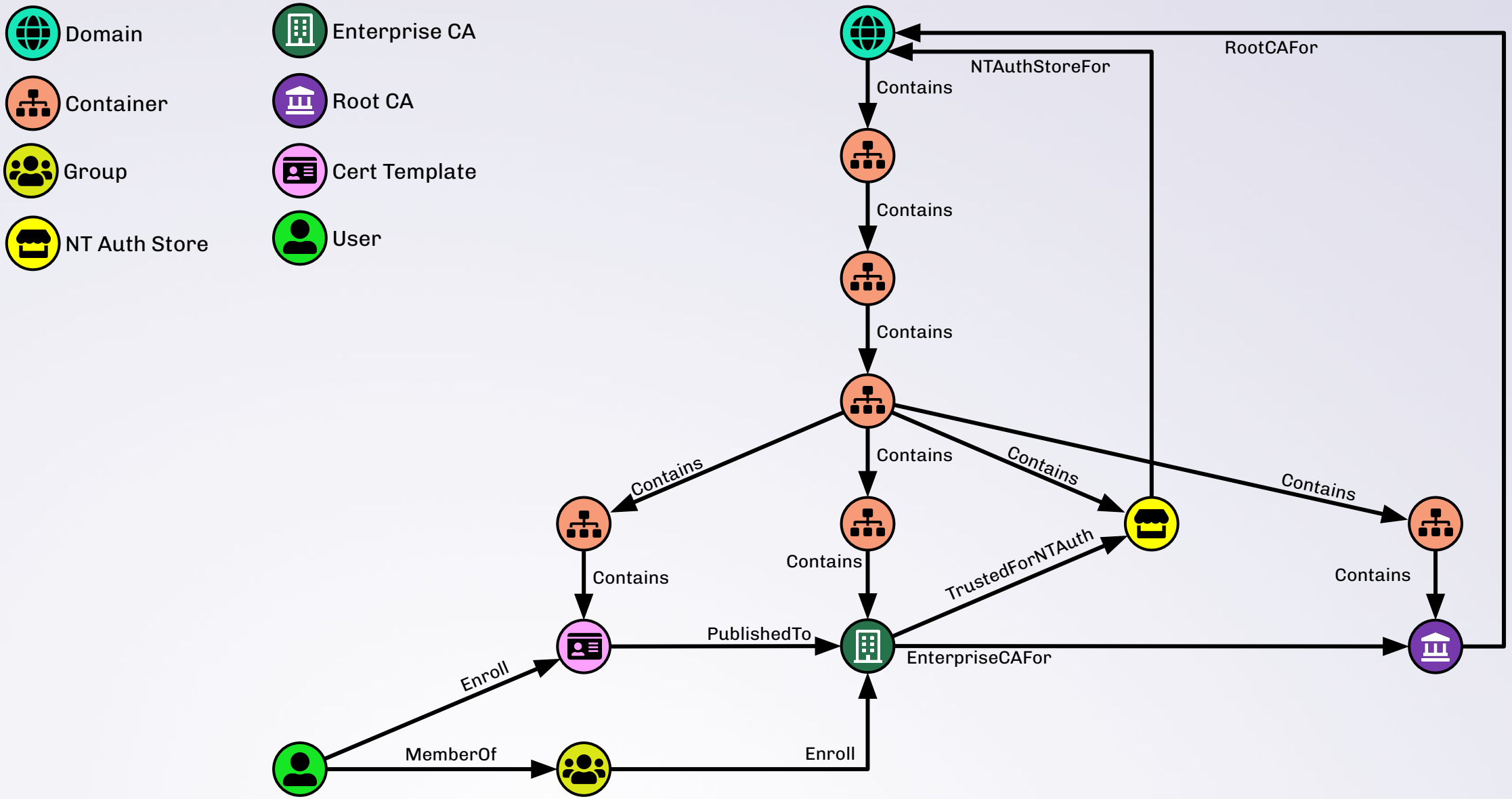
ESC5

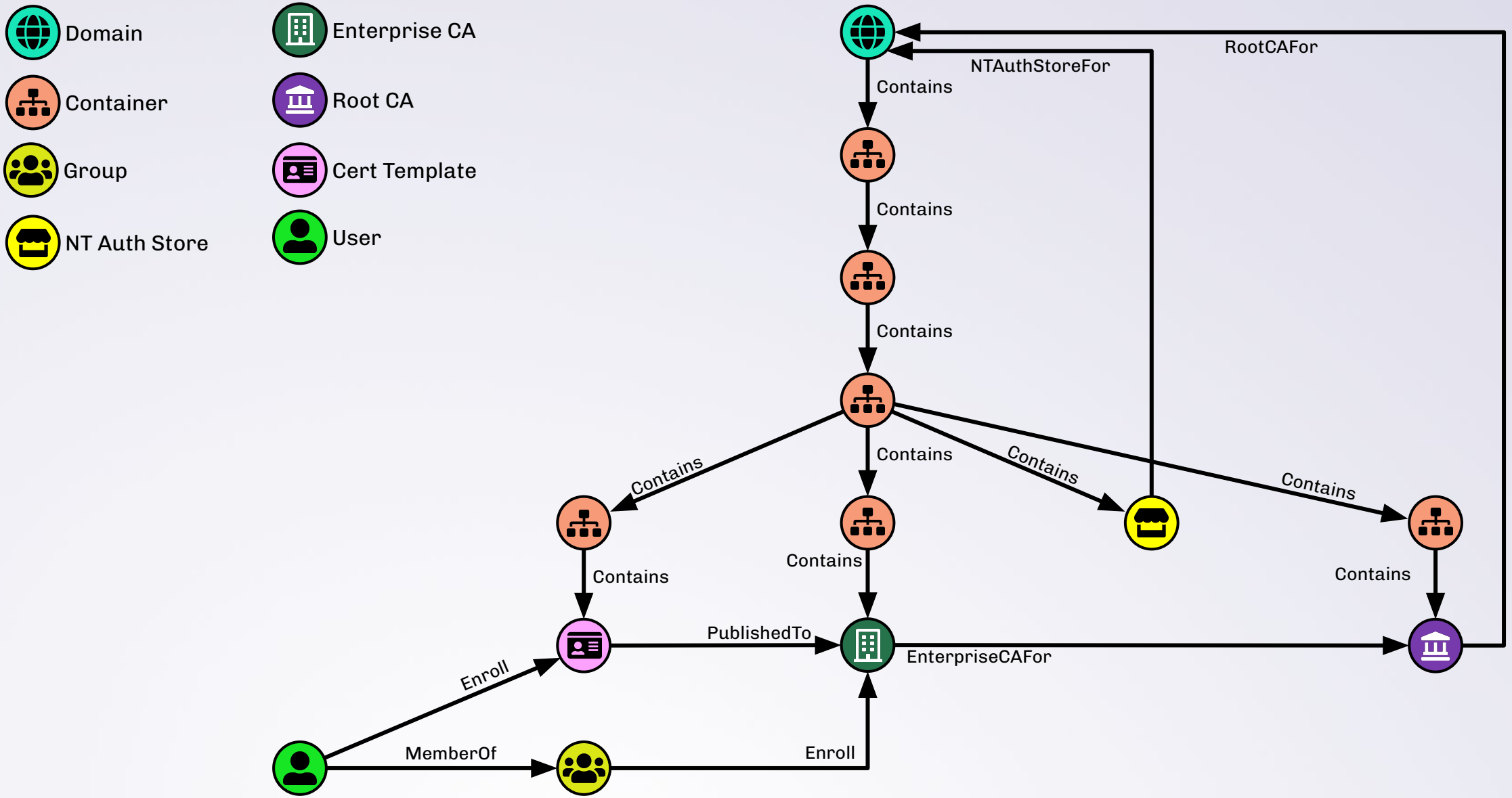

Privilege
Configuration
Configuration
Configuration
Configuration
Privilege
Privilege
Configuration

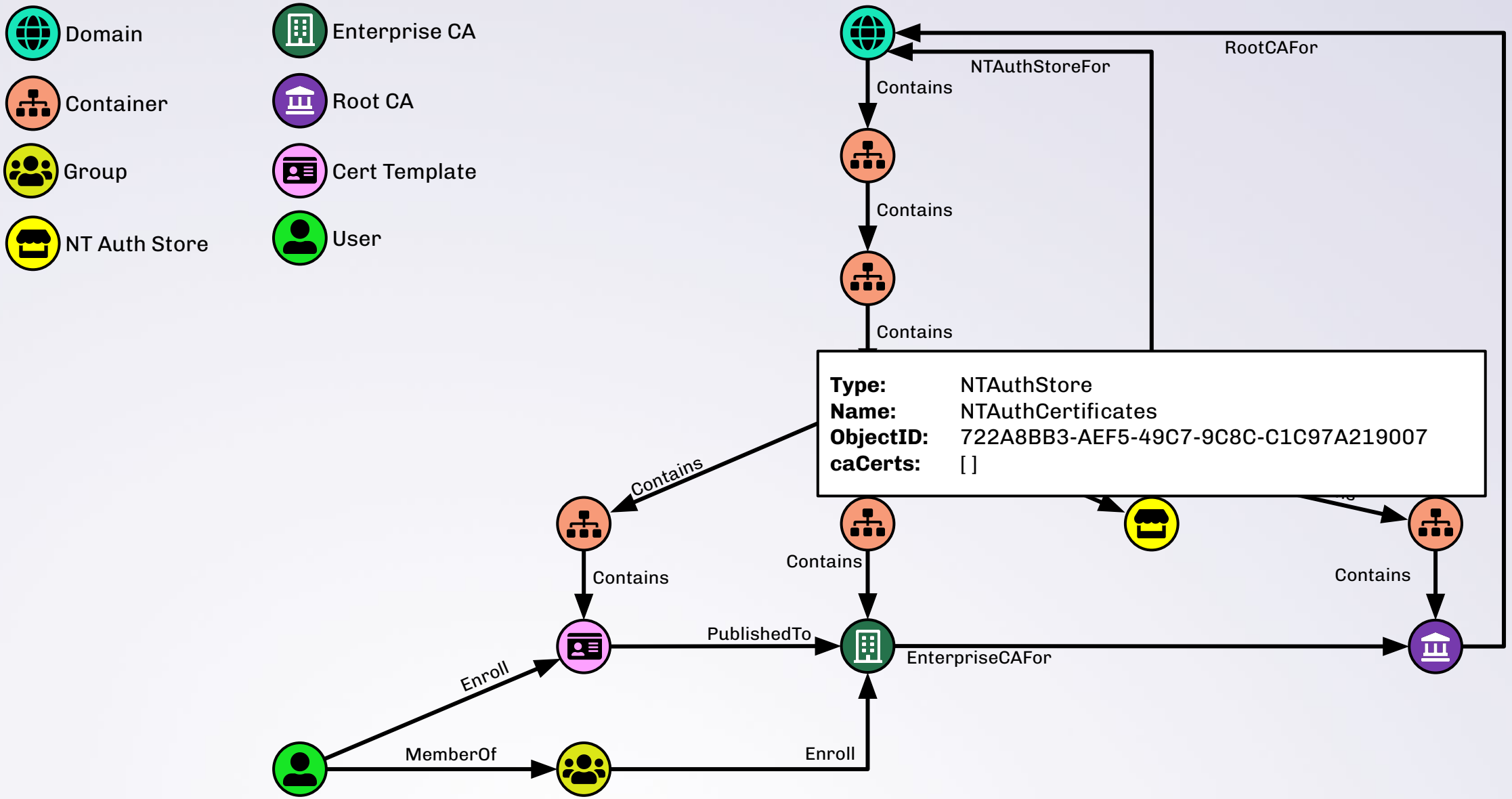
ESC5

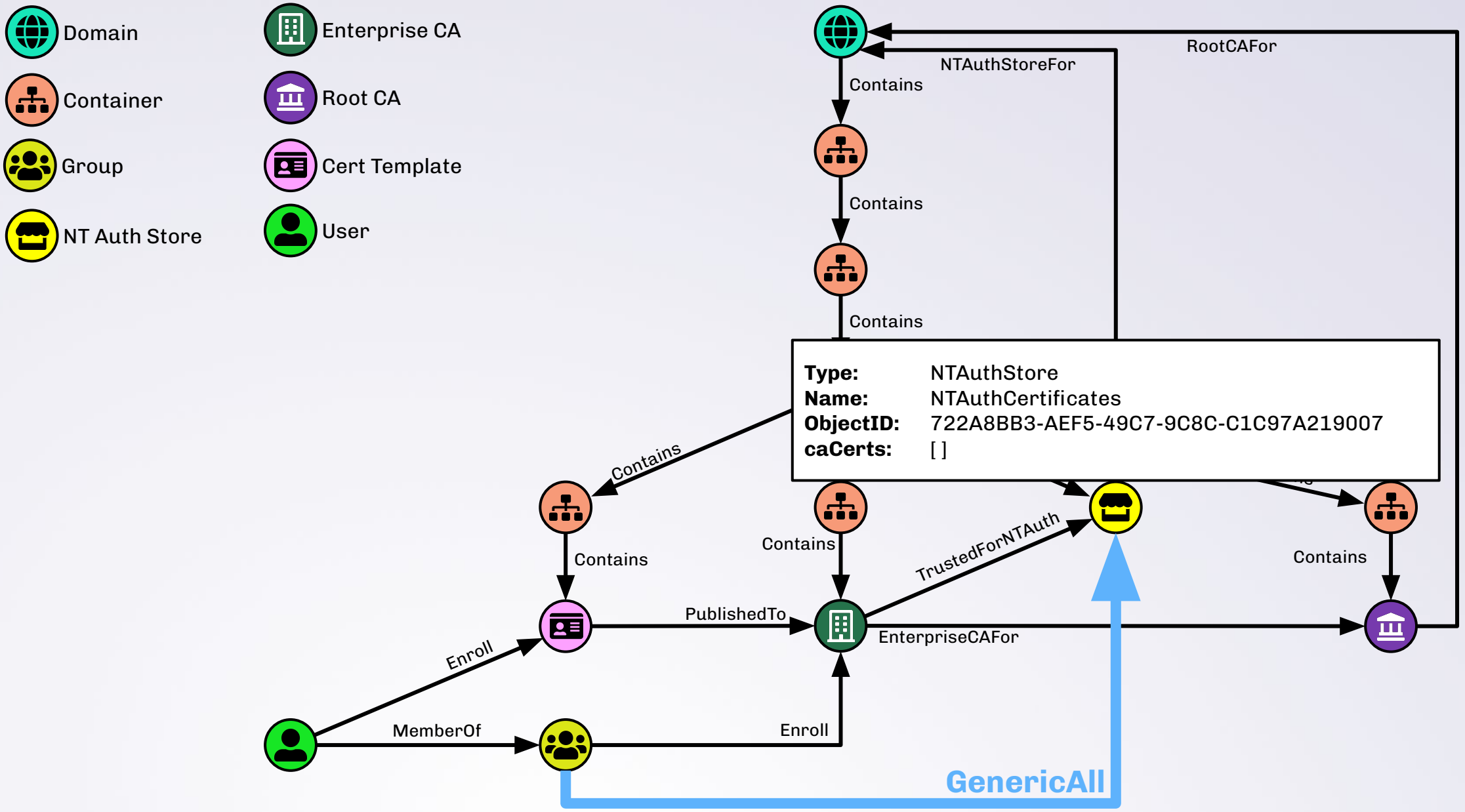

Configuration
Privilege
Privilege
Configuration
Configuration
Privilege
Privilege
Configuration

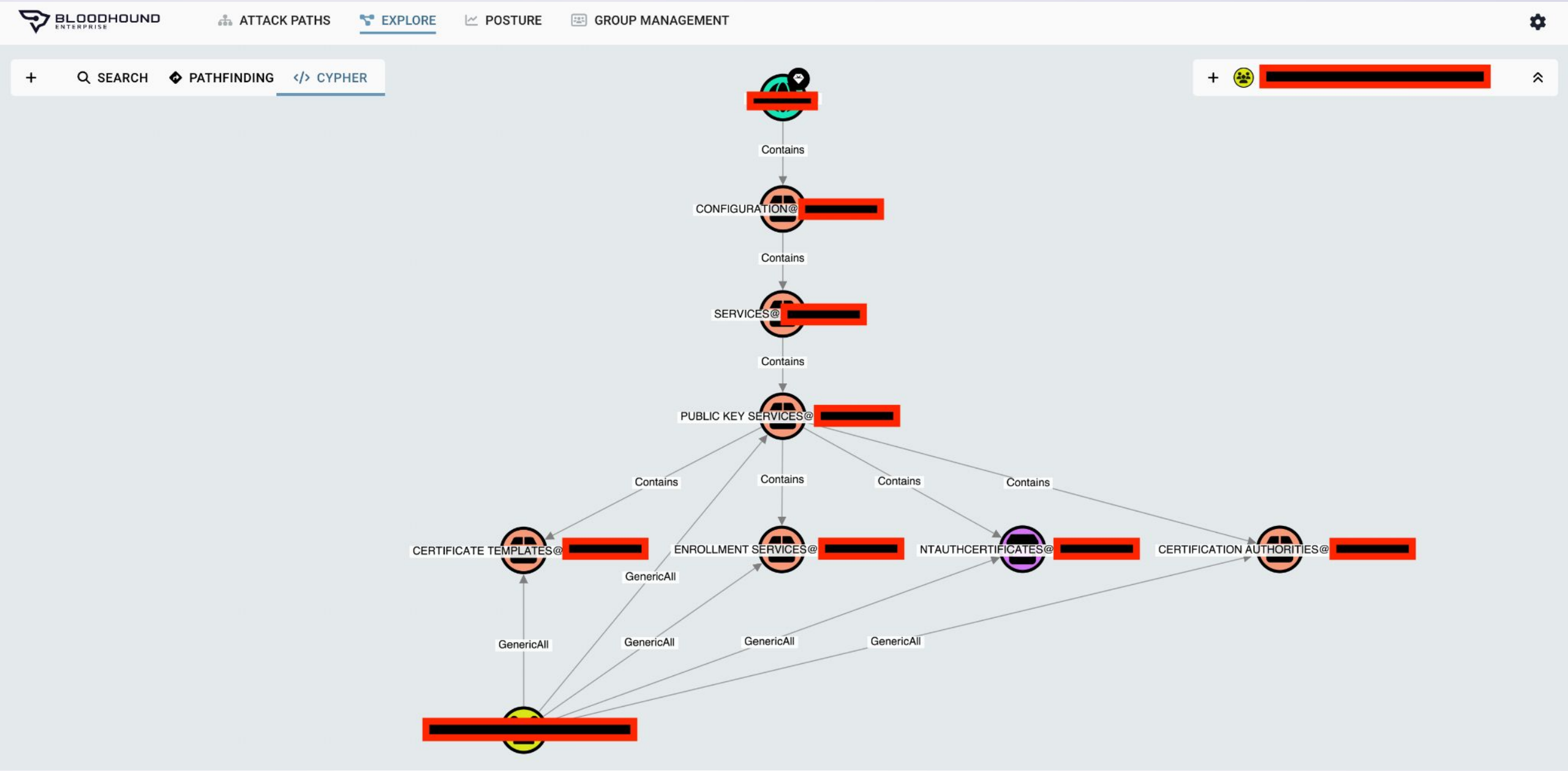
ESC5

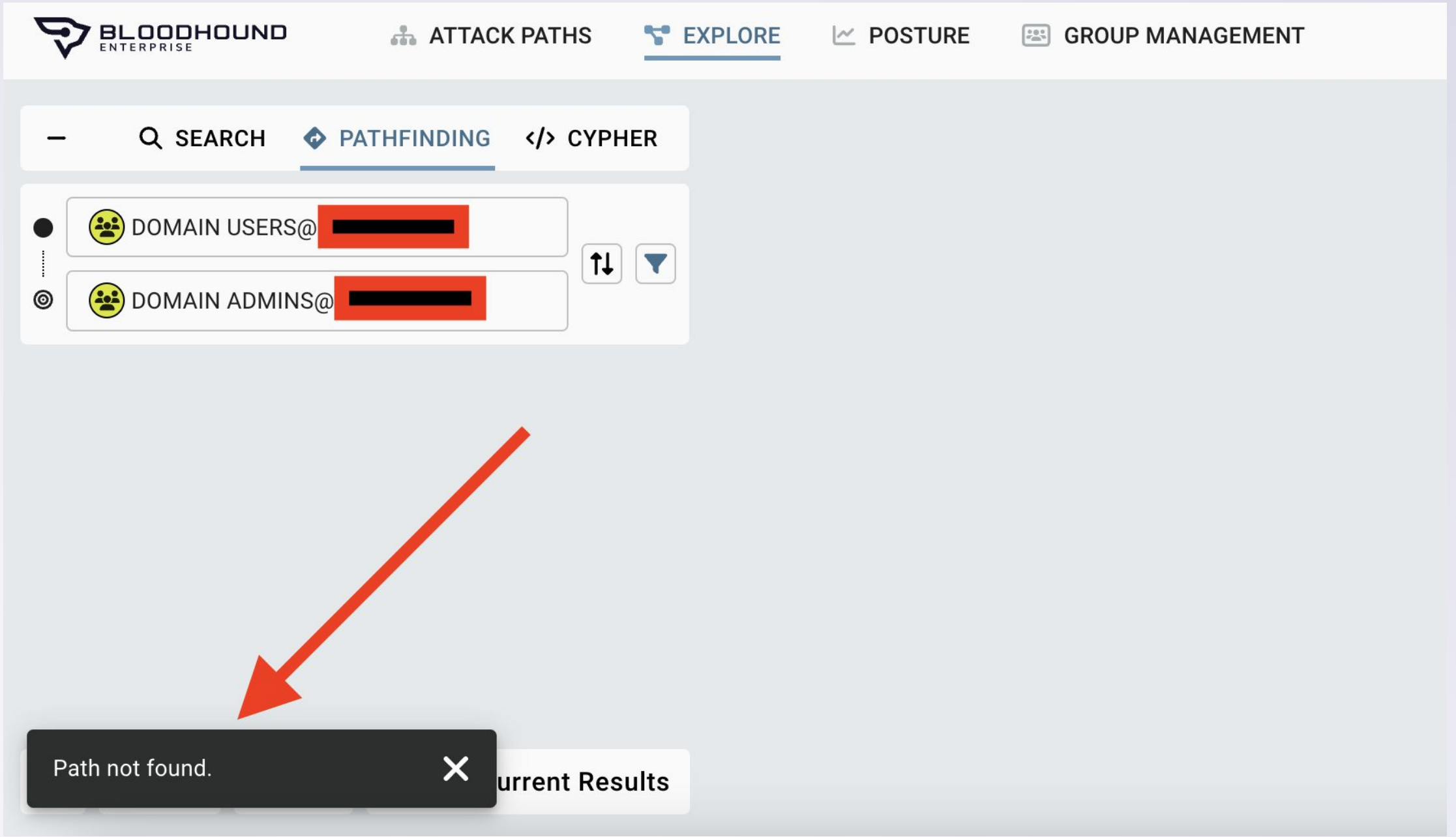

Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
RootCAFor
NTAuthStoreFor
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
TrustedForNTAuth
PublishedTo
EnterpriseCAFor
Enroll
MemberOf
Enroll

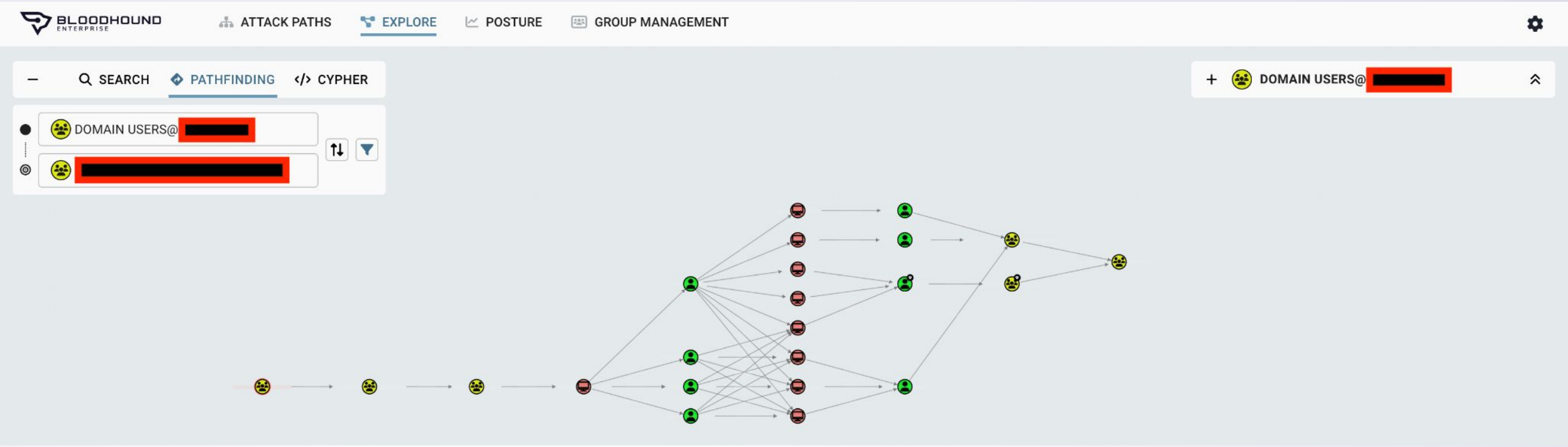

Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
RootCAFor
NTAuthStoreFor
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains
PublishedTo
EnterpriseCAFor
Enroll
MemberOf
Enroll

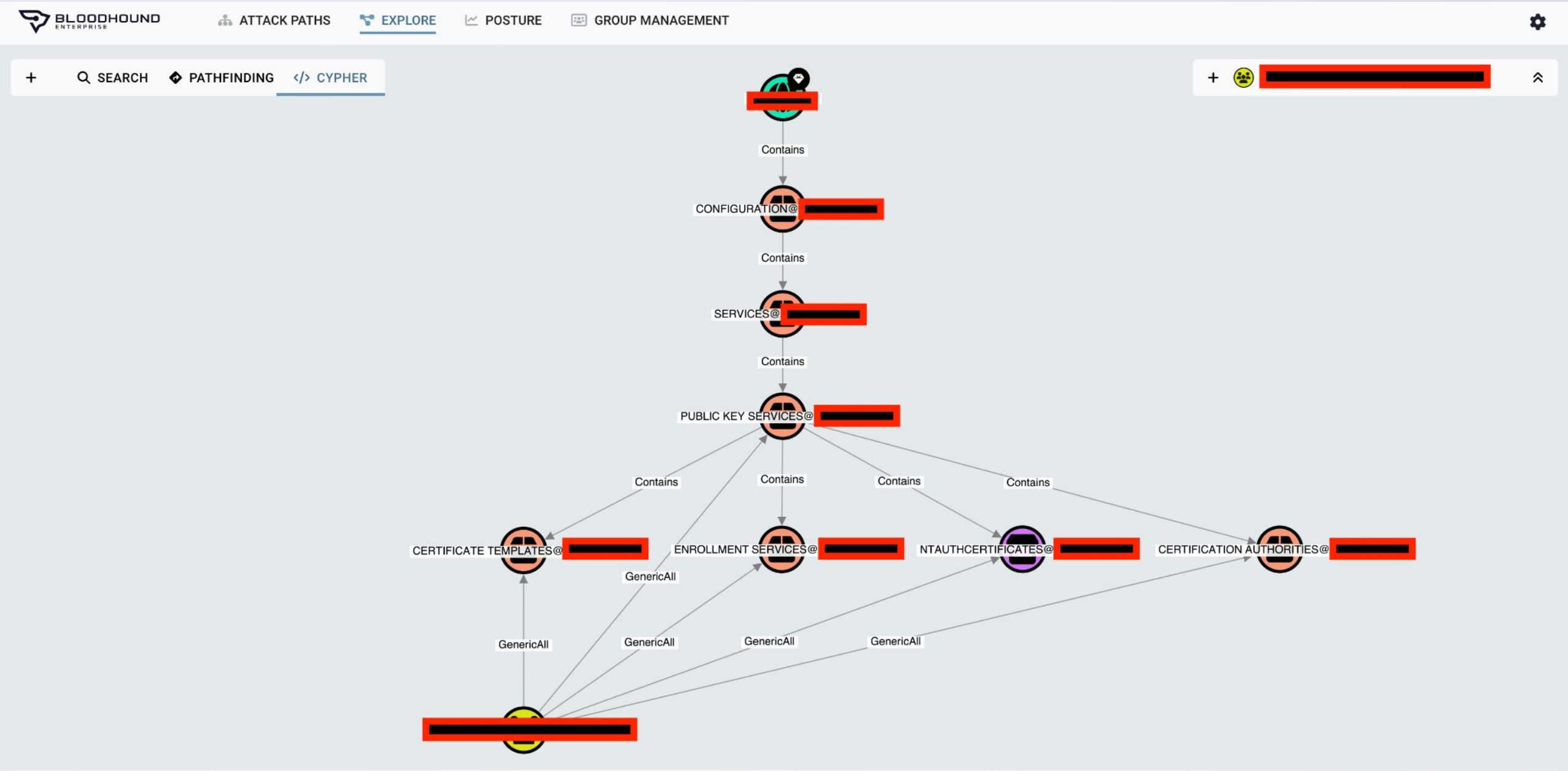

Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
RootCAFor
NTAuthStoreFor
Contains
Contains
Contains
Contains
Type: NTAuthStore
Name: NTAuthCertificates
ObjectID: 722A8BB3-AEF5-49C7-9C8C-C1C97A219007
caCerts: [ ]
Contains
Contains
Contains
Contains
PublishedTo
EnterpriseCAFor
Enroll
MemberOf
Enroll

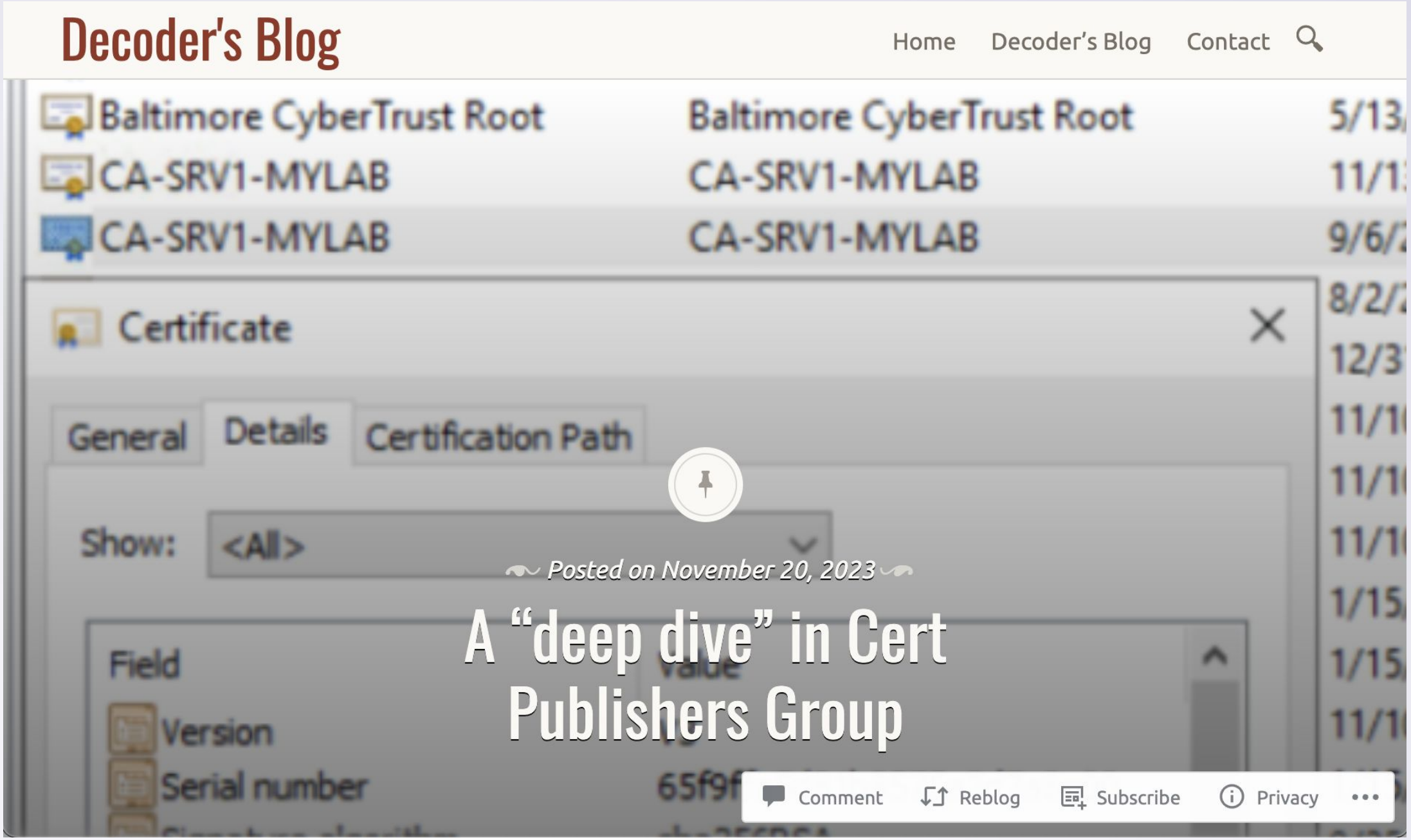

Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
RootCAFor
NTAuthStoreFor
Contains
Contains
Contains
Contains
Type: NTAuthStore
Name: NTAuthCertificates
ObjectID: 722A8BB3-AEF5-49C7-9C8C-C1C97A219007
caCerts: [ ]
Contains
Contains
Contains
Contains
TrustedForNTAuth
PublishedTo
EnterpriseCAFor
Enroll
MemberOf
Enroll
GenericAll

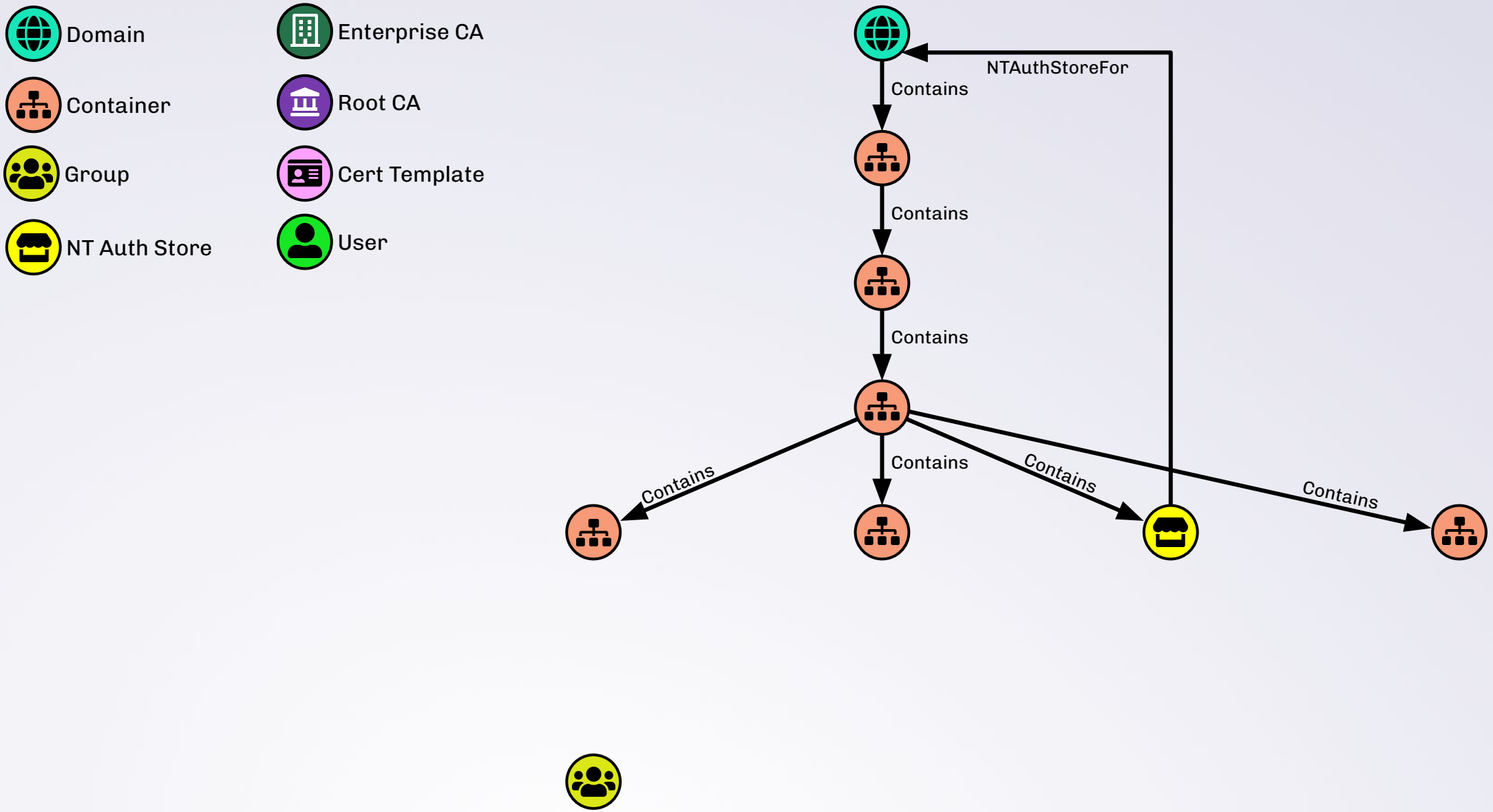

BLOODHOUND ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
Contains
CONFIGURATION@
Contains
SERVICES@
Contains
PUBLIC KEY SERVICES@
Contains
Contains
Contains
Contains
CERTIFICATE TEMPLATES@
ENROLLMENT SERVICES@
NTAUTHCERTIFICATES@
CERTIFICATION AUTHORITIES@
GenericAll
GenericAll
GenericAll
GenericAll
GenericAll

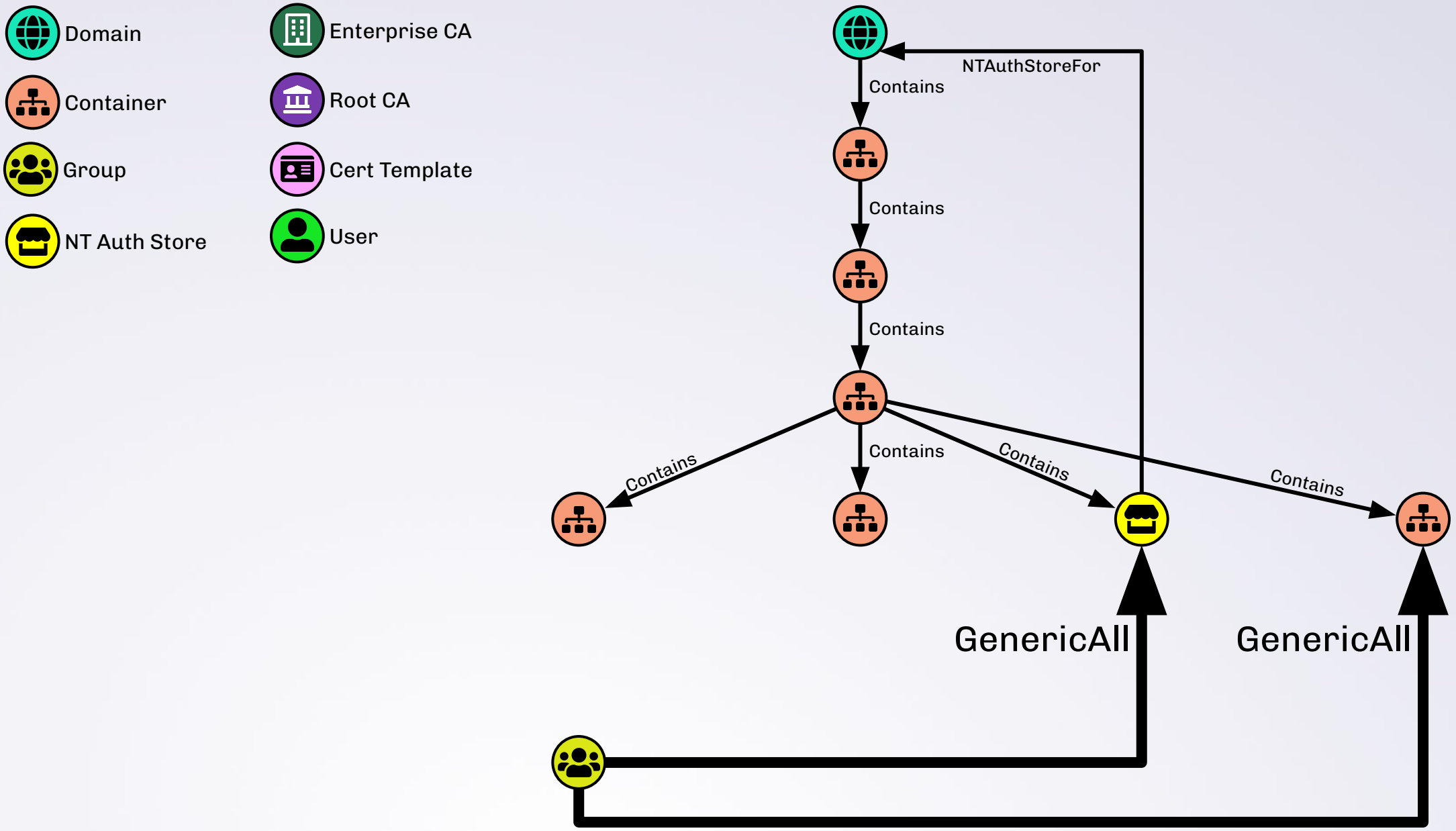

BLOODHOUND
ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
DOMAIN USERS@
DOMAIN ADMINS@
Path not found.
urrent Results

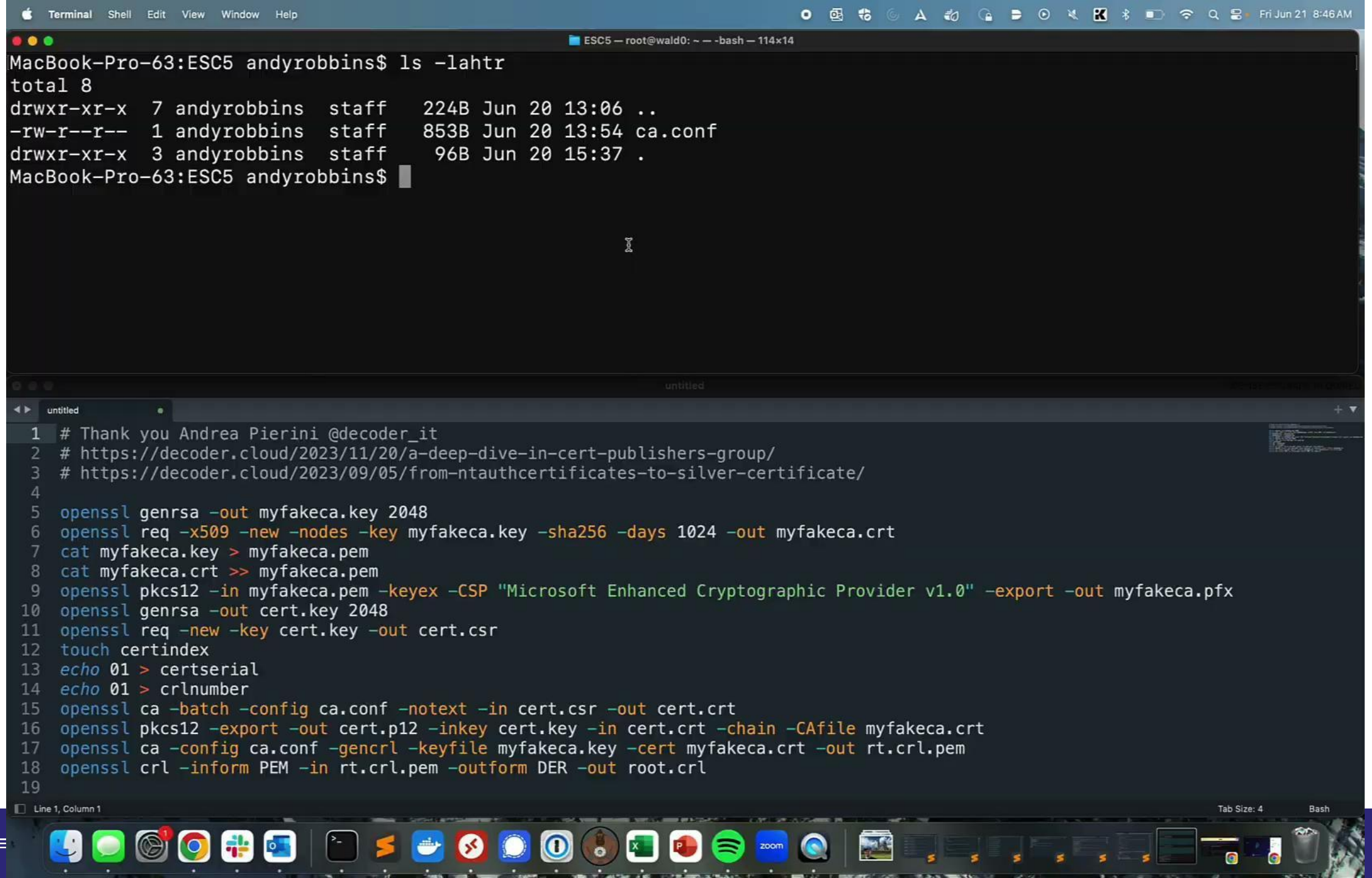

BLOODHOUND
ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
DOMAIN USERS@
DOMAIN USERS@


BLOODHOUND ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
Contains
CONFIGURATION@
Contains
SERVICES@
Contains
PUBLIC KEY SERVICES@
Contains
Contains
Contains
Contains
CERTIFICATE TEMPLATES@
ENROLLMENT SERVICES@
NTAUTHCERTIFICATES@
CERTIFICATION AUTHORITIES@
GenericAll
GenericAll
GenericAll
GenericAll
GenericAll


Decoder's Blog
Home
Decoder's Blog
Contact
Baltimore CyberTrust Root
Baltimore CyberTrust Root
CA-SRV1-MYLAB
CA-SRV1-MYLAB
CA-SRV1-MYLAB
CA-SRV1-MYLAB
Certificate
General
Details
Certification Path
Show:
<All>
Field
Version
Serial number
Posted on November 20, 2023
A "deep dive" in Cert Publishers Group
Comment
Reblog
Subscribe
Privacy

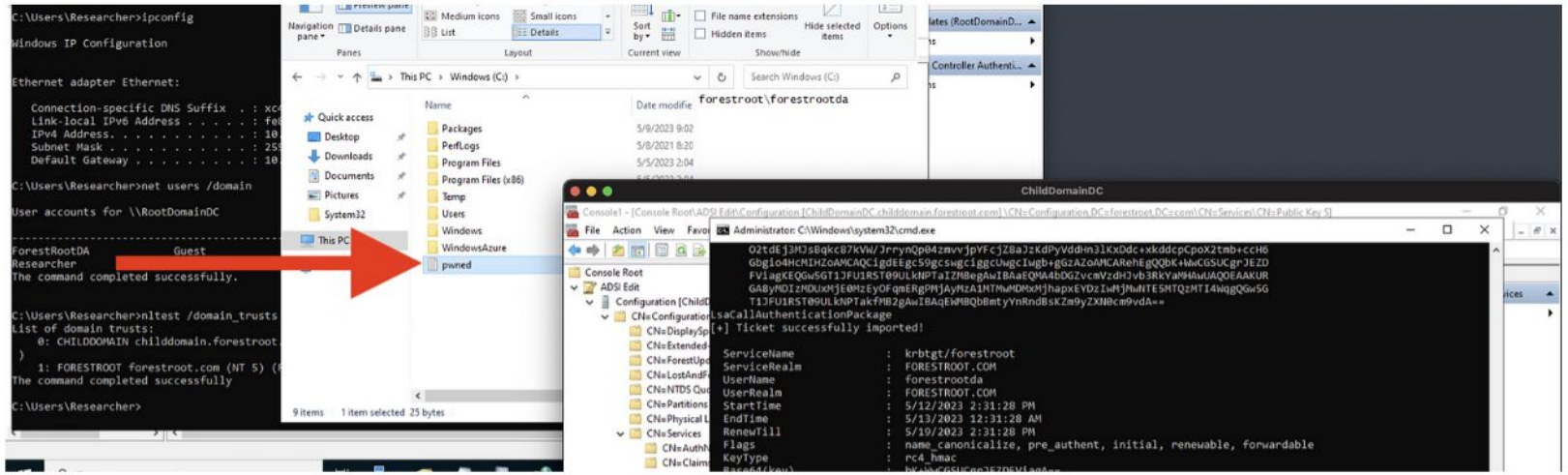

Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
NTAuthStoreFor
Contains
Contains
Contains
Contains
Contains
Contains
Contains
Contains


Domain
Container
Group
NT Auth Store
Enterprise CA
Root CA
Cert Template
User
NTAuthStoreFor
Contains
Contains
Contains
Contains
Contains
Contains
Contains
GenericAll
GenericAll


Terminal Shell Edit View Window Help
Fri Jun 21 8:46 AM
ESC5 — root@wald0: ~ — -bash — 114×14
MacBook-Pro-63:ESC5 andyrobbins$ ls -lahtr
total 8
drwxr-xr-x 7 andyrobbins staff   224B Jun 20 13:06 ..
-rw-r--r-- 1 andyrobbins staff   853B Jun 20 13:54 ca.conf
drwxr-xr-x 3 andyrobbins staff   96B Jun 20 15:37 .
MacBook-Pro-63:ESC5 andyrobbins$
untitled
Thank you Andrea Pierini @decoder_it
https://decoder.cloud/2023/11/20/a-deep-dive-in-cert-publishers-group/
https://decoder.cloud/2023/09/05/from-ntauthcertificates-to-silver-certificate/
openssl genrsa -out myfakeca.key 2048
openssl req -x509 -new -nodes -key myfakeca.key -sha256 -days 1024 -out myfakeca.crt
cat myfakeca.key > myfakeca.pem
cat myfakeca.crt >> myfakeca.pem
openssl pkcs12 -in myfakeca.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out myfakeca.pfx
openssl genrsa -out cert.key 2048
openssl req -new -key cert.key -out cert.csr
touch certindex
echo 01 > certserial
echo 01 > crlnumber
openssl ca -batch -config ca.conf -notext -in cert.csr -out cert.crt
openssl pkcs12 -export -out cert.p12 -inkey cert.key -in cert.crt -chain -CAfile myfakeca.crt
openssl ca -config ca.conf -gencrl -keyfile myfakeca.key -cert myfakeca.crt -out rt.crl.pem
openssl crl -inform PEM -in rt.crl.pem -outform DER -out root.crl
Line 1, Column 1
Tab Size: 4
Bash

Andy Robbins in Posts By SpecterOps Team Members

May 16, 2023 · 9 min read

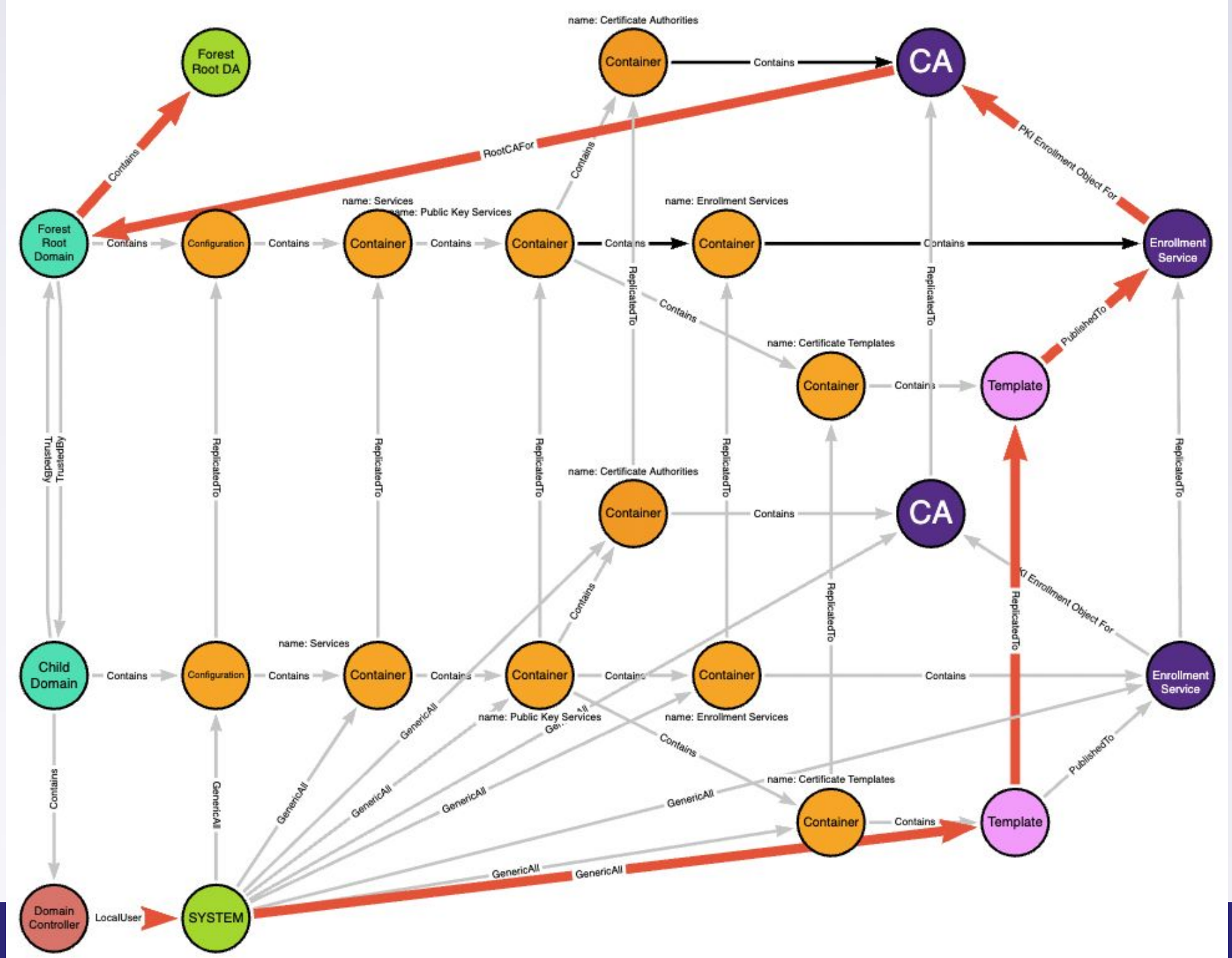


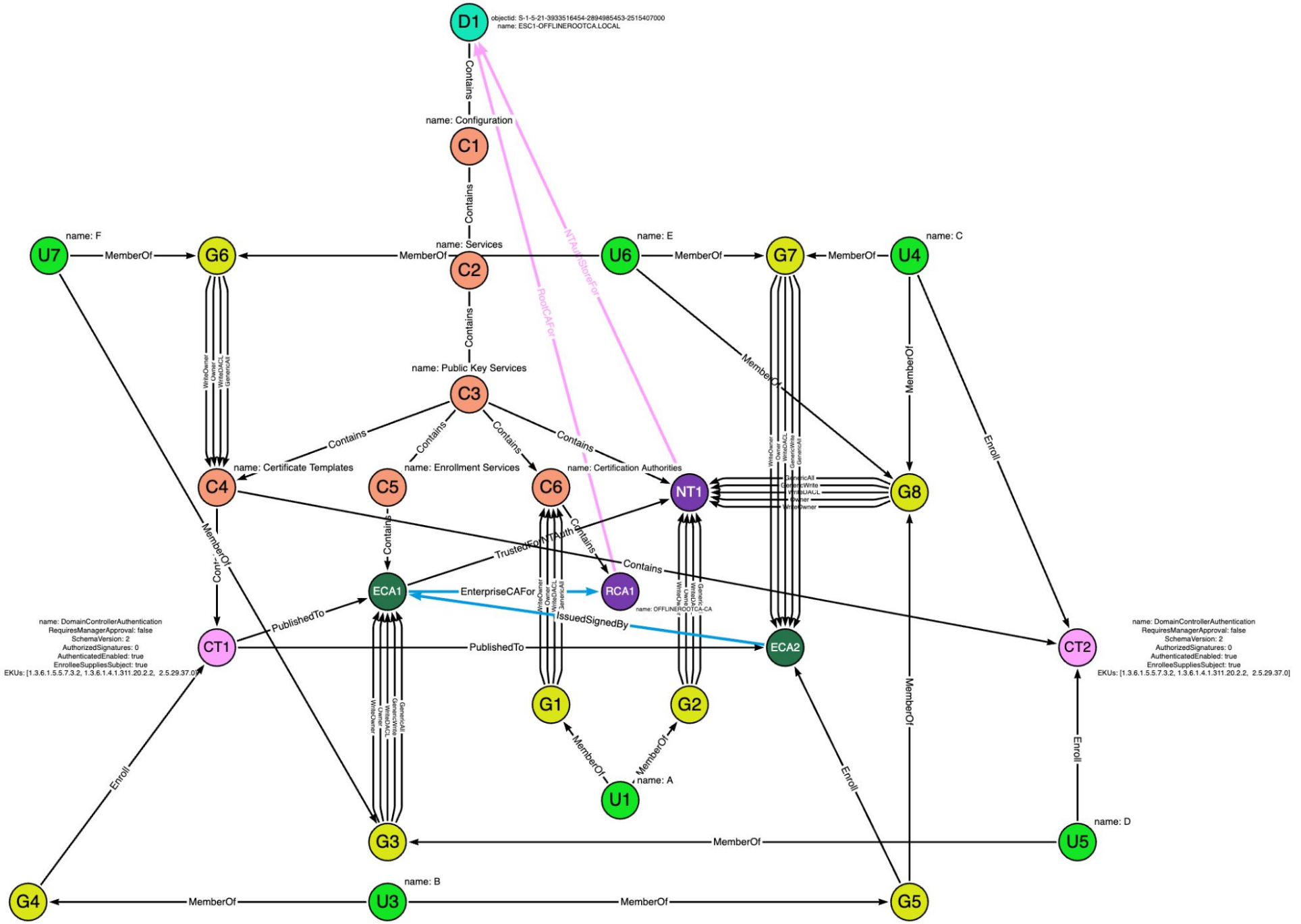
From DA to EA with ESC5

There's a new, practical way to escalate from Domain Admin to Enterprise Admin.

Read more...

59


Forest Root DA
Contains
name: Certificate Authorities
Container
Contains
CA
RootCAFor
PKI Enrollment Object For
Forest Root Domain
Contains
Configuration
Contains
name: Services
Container
Contains
name: Public Key Services
Container
Contains
Container
Contains
name: Enrollment Services
Container
Contains
Enrollment Service
ReplicatedTo
Contains
name: Certificate Templates
Container
Contains
Template
PublishedTo
TrustedBy
ReplicatedTo
name: Certificate Authorities
Container
Contains
CA
Child Domain
Contains
Configuration
Contains
name: Services
Container
Contains
Container
Contains
Container
Contains
Enrollment Service
name: Public Key Services
name: Enrollment Services
GenericAll
Contains
name: Certificate Templates
Container
Contains
Template
PublishedTo
Domain Controller
LocalUser
SYSTEM
GenericAll

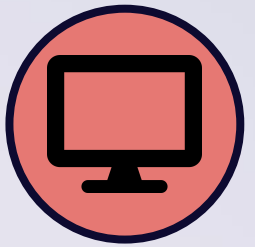

D1
objectid: S-1-5-21-3933516454-2894985453-2515407000
name: ESC1-OFFLINEROOTCA.LOCAL
Contains
name: Configuration
C1
Contains
name: Services
C2
Contains
name: Public Key Services
C3
Contains
Contains
Contains
Contains
name: Certificate Templates
C4
name: Enrollment Services
C5
name: Certification Authorities
C6
NT1
NTAuthStoreFor
RootCAFor
name: F
U7
MemberOf
G6
MemberOf
name: E
U6
MemberOf
G7
MemberOf
name: C
U4
MemberOf
G8
Enroll
WriteOwner
Owner
WriteDACL
GenericAll
GenericWrite
MemberOf
Contains
Contains
TrustedForNTAuth
Contains
Contains
ECA1
EnterpriseCAFor
RCA1
name: OFFLINEROOTCA-CA
PublishedTo
IssuedSignedBy
name: DomainControllerAuthentication
RequiresManagerApproval: false
SchemaVersion: 2
AuthorizedSignatures: 0
AuthenticatedEnabled: true
EnrolleeSuppliesSubject: true
EKUs: [1.3.6.1.5.5.7.3.2, 1.3.6.1.4.1.311.20.2.2, 2.5.29.37.0]
CT1
PublishedTo
ECA2
CT2
name: DomainControllerAuthentication
RequiresManagerApproval: false
SchemaVersion: 2
AuthorizedSignatures: 0
AuthenticatedEnabled: true
EnrolleeSuppliesSubject: true
EKUs: [1.3.6.1.5.5.7.3.2, 1.3.6.1.4.1.311.20.2.2, 2.5.29.37.0]
Enroll
G1
G2
MemberOf
MemberOf
name: A
U1
Enroll
MemberOf
Enroll
G3
MemberOf
name: D
U5
name: B
G4
MemberOf
U3
MemberOf
G5

ESC13

Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA



Domain Controller

ESC13 - Abuse of OID Group Links

Alice

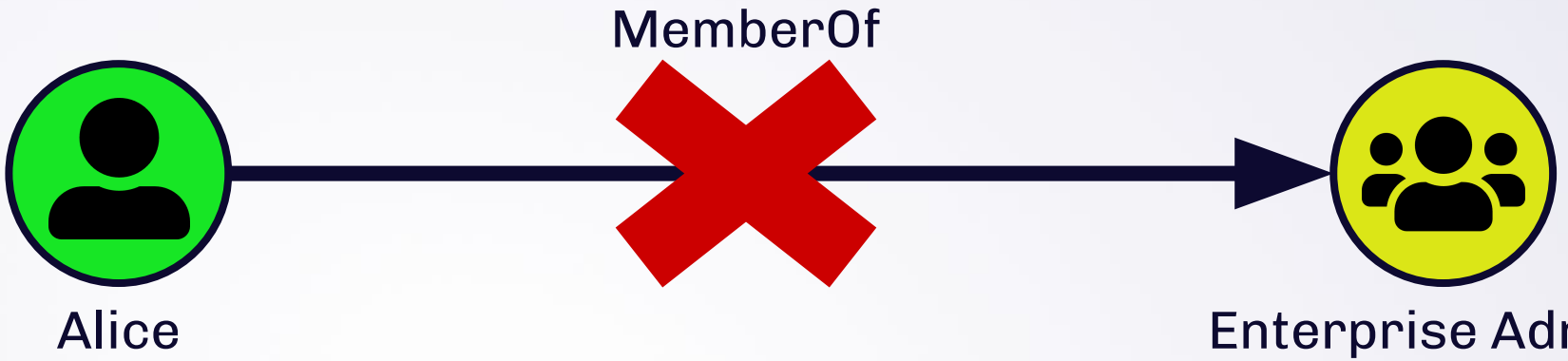
Enterprise Admins

Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA

Domain Controller



Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA

Domain Controller

"Please issue an Enterprise Admins Template certificate to me."

Alice

Enterprise Admins

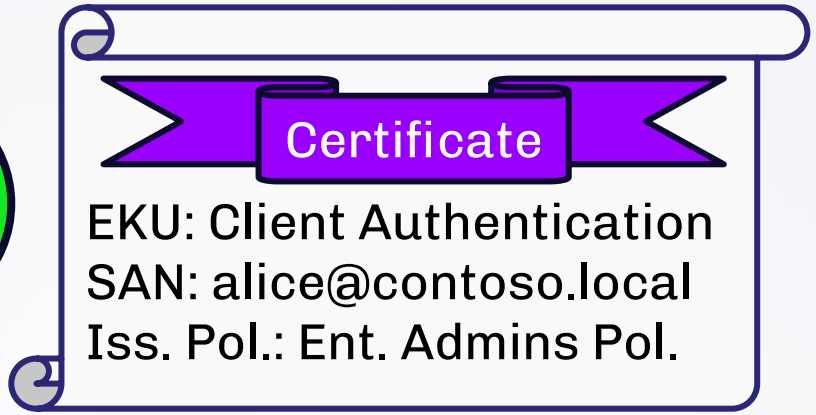
Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA

Domain Controller

Alice



Enterprise Admins

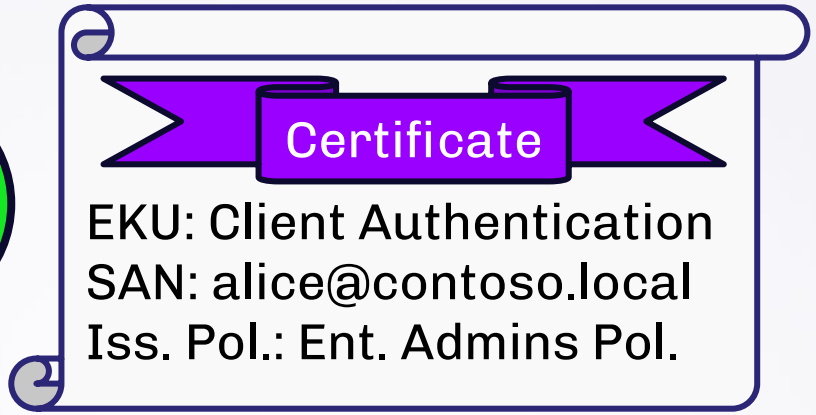
Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA

Domain Controller

Alice



Enterprise Admins

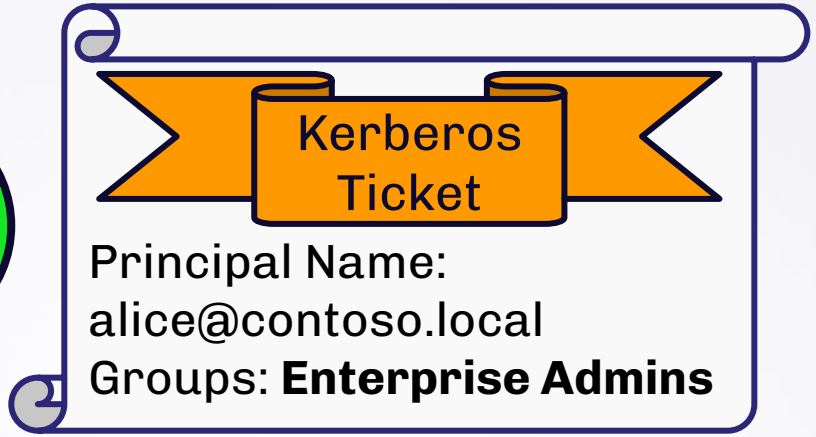
Enterprise Admins Policy

Enterprise Admins Template

Enterprise CA

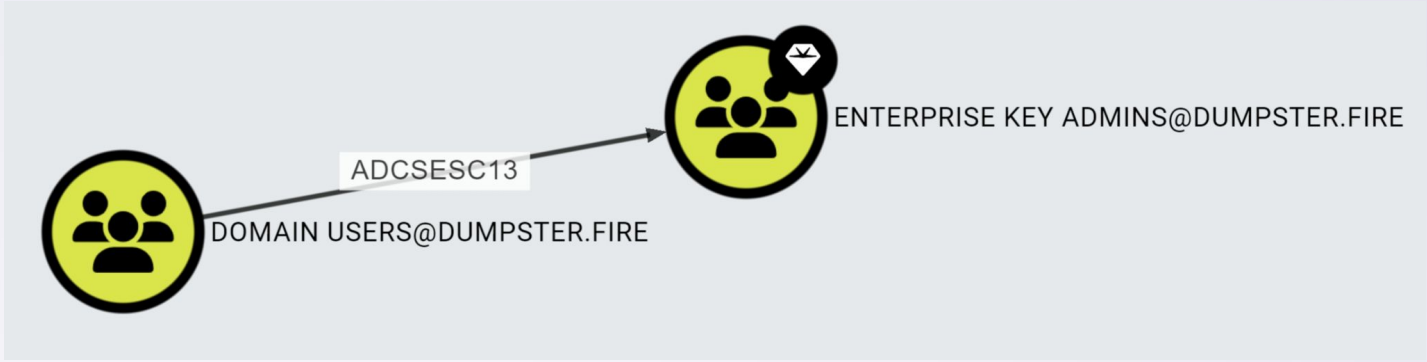
Domain Controller

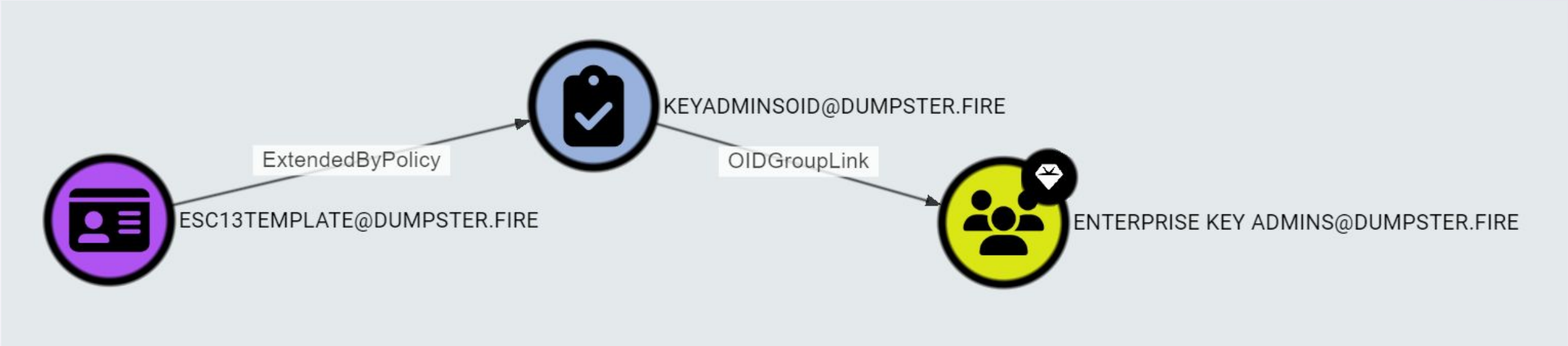
Alice



Enterprise Admins

ESC13 - OID Group Links in BloodHound





https://posts.specterops.io/adcs-esc13-abuse-technique-fda4272fbd53

Visualizing and Auditing the ADCS LDAP Hierarchy

Visualizing and Auditing the ADCS LDAP Hierarchy

Intuitive Understanding

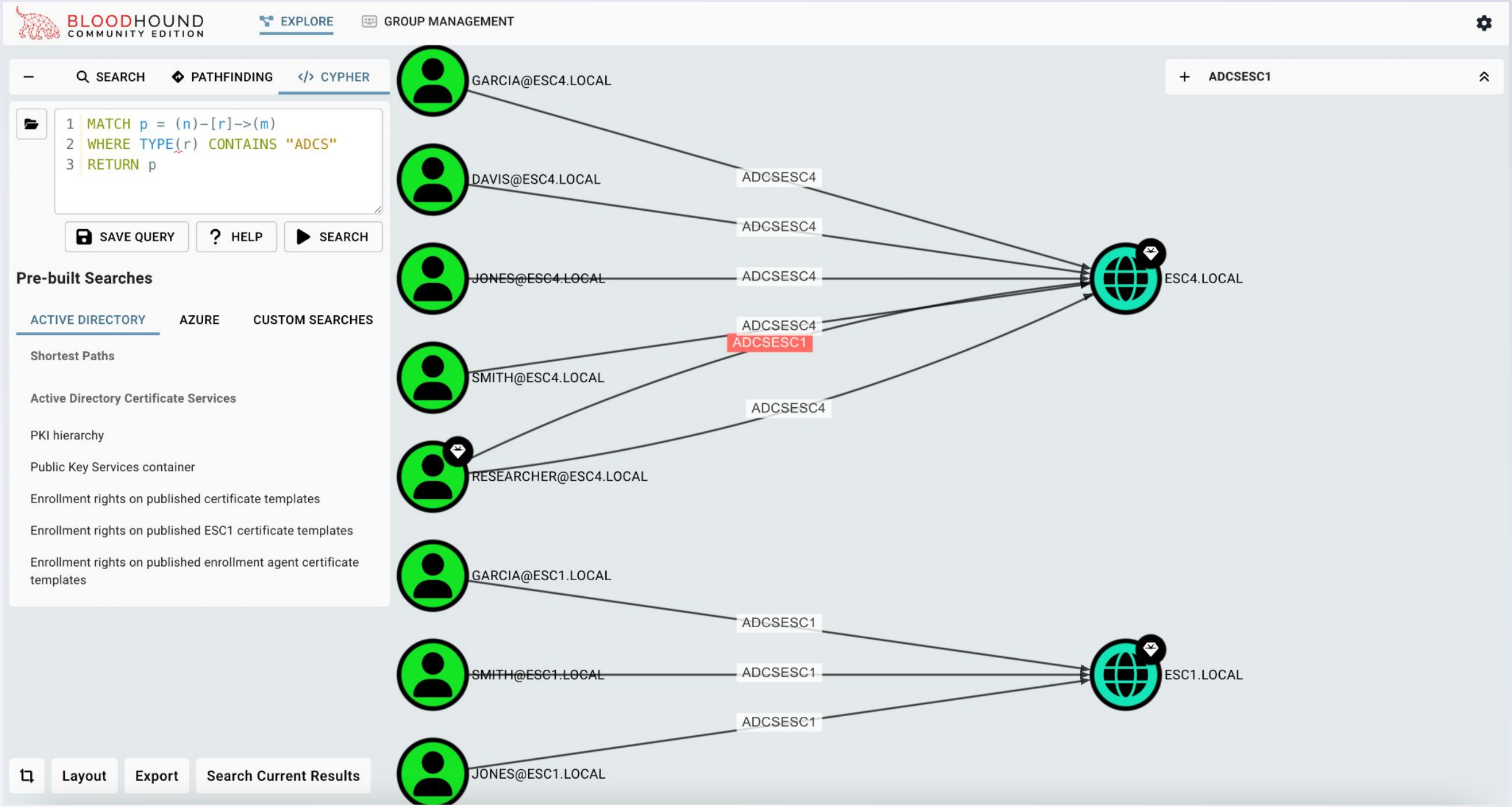
BloodHound provides intuitive visuals that dramatically simplify understanding and communicating the LDAP and PKI hierarchies.

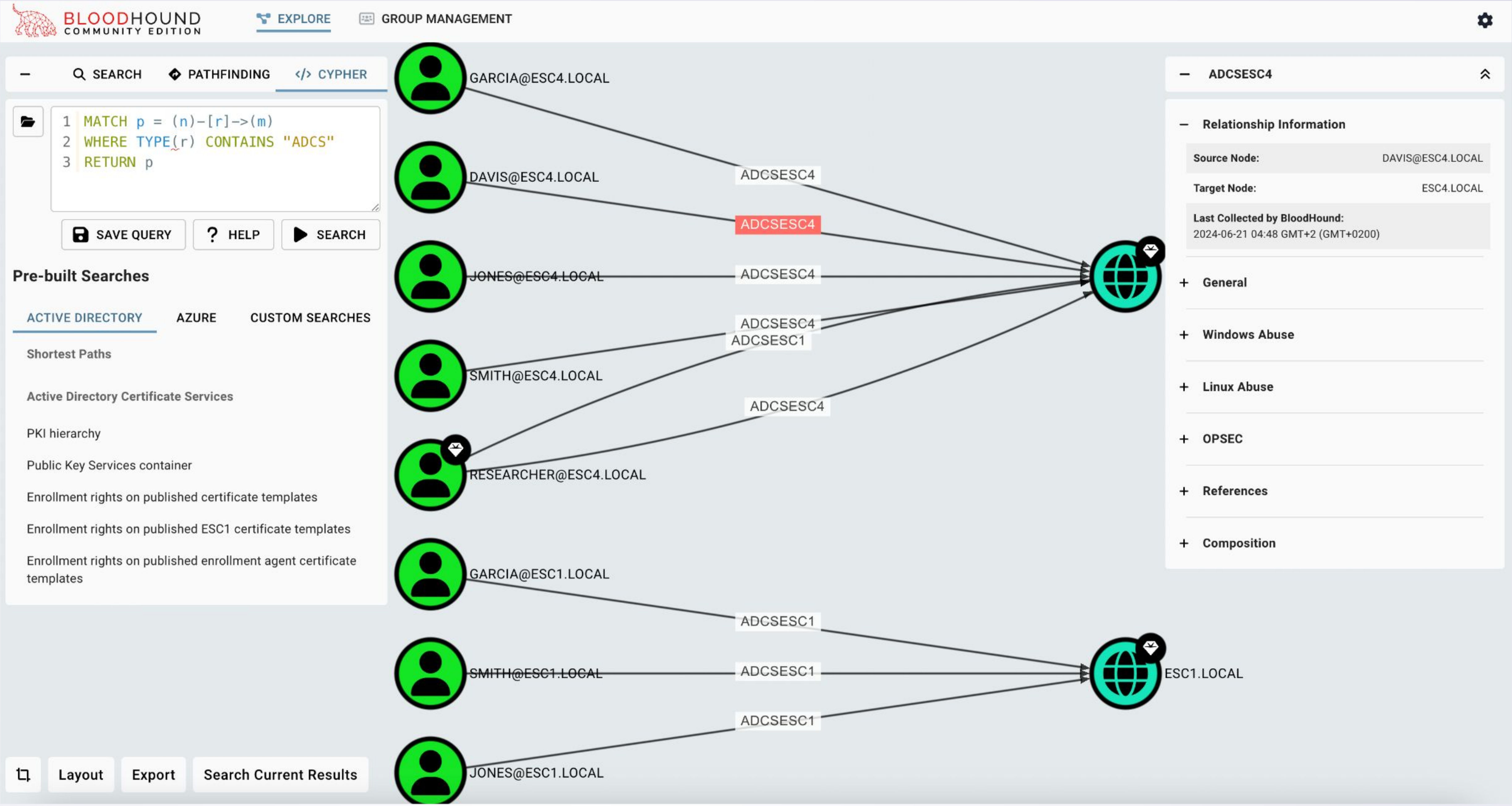
Simple Permissions Auditing

Easily understand which principals have potentially abusable permissions against ADCS objects, even through nested group memberships.

Deliver Better Reports

Auditors and pentesters can use these features to deliver better, more useful reports to their customers.


BLOODHOUND
COMMUNITY EDITION
EXPLORE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
1 MATCH p = (n)-[r]->(m)
2 WHERE TYPE(r) CONTAINS "ADCS"
3 RETURN p
SAVE QUERY
HELP
SEARCH
Pre-built Searches
ACTIVE DIRECTORY
AZURE
CUSTOM SEARCHES
Shortest Paths
Active Directory Certificate Services
PKI hierarchy
Public Key Services container
Enrollment rights on published certificate templates
Enrollment rights on published ESC1 certificate templates
Enrollment rights on published enrollment agent certificate templates
Layout
Export
Search Current Results
ADCSESC1
GARCIA@ESC4.LOCAL
DAVIS@ESC4.LOCAL
JONES@ESC4.LOCAL
SMITH@ESC4.LOCAL
RESEARCHER@ESC4.LOCAL
GARCIA@ESC1.LOCAL
SMITH@ESC1.LOCAL
JONES@ESC1.LOCAL
ADCSESC4
ADCSESC1
ESC4.LOCAL
ESC1.LOCAL


BLOODHOUND
COMMUNITY EDITION
EXPLORE
GROUP MANAGEMENT
SEARCH
PATHFINDING
CYPHER
1 MATCH p = (n)-[r]->(m)
2 WHERE TYPE(r) CONTAINS "ADCS"
3 RETURN p
SAVE QUERY
HELP
SEARCH
Pre-built Searches
ACTIVE DIRECTORY
AZURE
CUSTOM SEARCHES
Shortest Paths
Active Directory Certificate Services
PKI hierarchy
Public Key Services container
Enrollment rights on published certificate templates
Enrollment rights on published ESC1 certificate templates
Enrollment rights on published enrollment agent certificate templates
Layout
Export
Search Current Results
GARCIA@ESC4.LOCAL
DAVIS@ESC4.LOCAL
JONES@ESC4.LOCAL
SMITH@ESC4.LOCAL
RESEARCHER@ESC4.LOCAL
GARCIA@ESC1.LOCAL
SMITH@ESC1.LOCAL
JONES@ESC1.LOCAL
ADCSESC4
ADCSESC4
ADCSESC4
ADCSESC4
ADCSESC1
ADCSESC4
ADCSESC1
ADCSESC1
ADCSESC1
ESC1.LOCAL
ADCSESC4
Relationship Information
Source Node: DAVIS@ESC4.LOCAL
Target Node: ESC4.LOCAL
Last Collected by BloodHound: 2024-06-21 04:48 GMT+2 (GMT+0200)
General
Windows Abuse
Linux Abuse
OPSEC
References
Composition

BLOODHOUND COMMUNITY EDITION

EXPLORE | GROUP MANAGEMENT

SEARCH | PATHFINDING | CYPHER

```
1 MATCH p = (n)-[r]->(m)
2 WHERE TYPE(r) CONTAINS "ADCS"
3 RETURN p
```

SAVE QUERY | HELP | SEARCH

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Shortest Paths

Active Directory Certificate Services

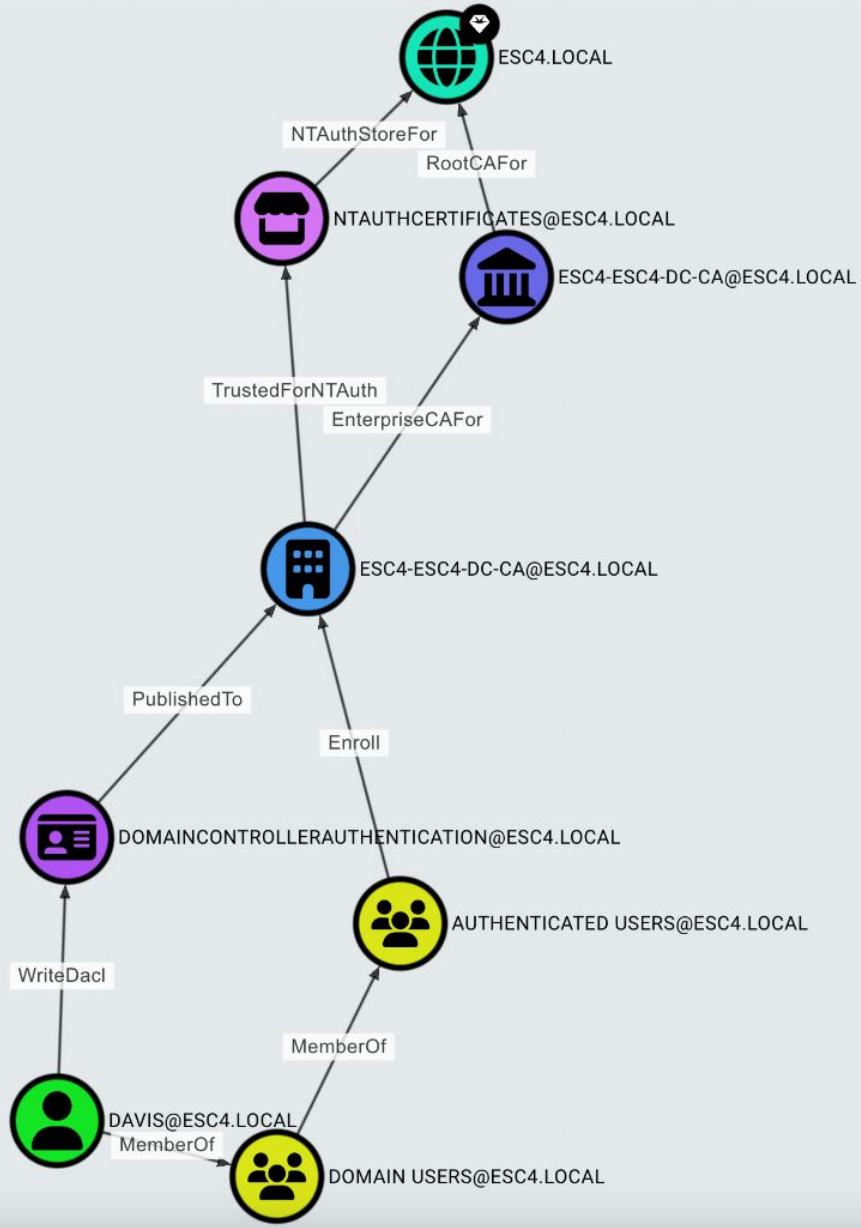
PKI hierarchy

Public Key Services container

Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

Enrollment rights on published enrollment agent certificate templates



Layout | Export | Search Current Results

ADCSESC4

Relationship Information

Source Node:	DAVIS@ESC4.LOCAL
Target Node:	ESC4.LOCAL

Last Collected by BloodHound:
2024-06-21 04:48 GMT+2 (GMT+0200)

+ General

+ Windows Abuse

+ Linux Abuse

+ OPSEC

+ References

Composition

The relationship represents the effective outcome of the configuration and relationships between several different objects. All objects involved in the creation of this relationship are listed here:

- DOMAINCONTROLLERAUTHENTICATIO...
- DOMAIN USERS@ESC4.LOCAL
- DAVIS@ESC4.LOCAL
- ESC4.LOCAL
- AUTHENTICATED USERS@ESC4.LOCAL

BLOODHOUND COMMUNITY EDITION

EXPLORE | GROUP MANAGEMENT

SEARCH | PATHFINDING | CYPHER

```
1 MATCH p = (n)-[r]->(m)
2 WHERE TYPE(r) CONTAINS "ADCS"
3 RETURN p
```

SAVE QUERY | HELP | SEARCH

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Shortest Paths

Active Directory Certificate Services

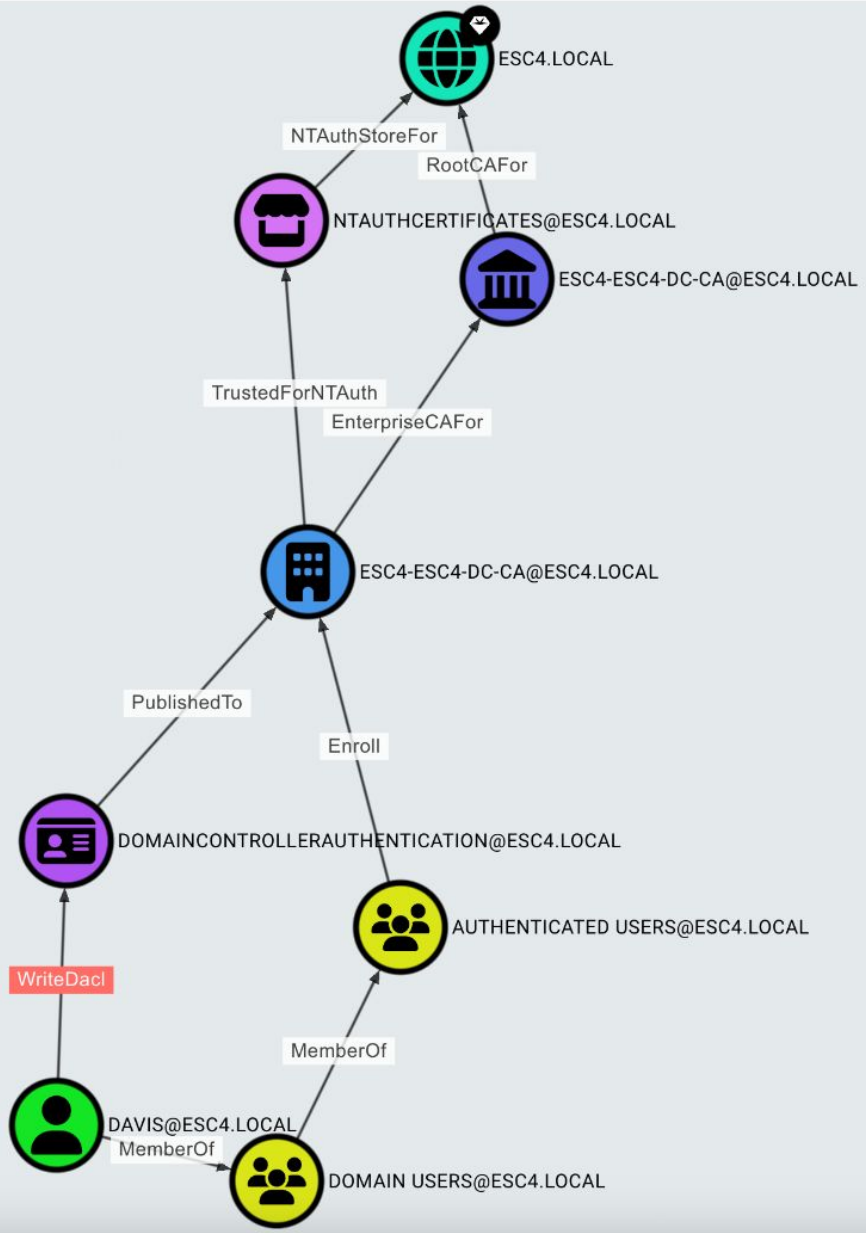
PKI hierarchy

Public Key Services container

Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

Enrollment rights on published enrollment agent certificate templates



Layout | Export | Search Current Results

WriteDacl

Relationship Information

Source Node:	DAVIS@ESC4.LOCAL
Target Node:	DOMAINCONTROLLERAUTHENTICATION@ESC4.LOCAL
Is ACL:	TRUE
Is Inherited:	FALSE
Last Collected by BloodHound:	2024-06-07 16:47 GMT+2 (GMT+0200)

General

The user DAVIS@ESC4.LOCAL has permissions to modify the DACL (Discretionary Access Control List) on the certificate template DOMAINCONTROLLERAUTHENTICATION@ESC4.LOCAL

With write access to the target object's DACL, you can grant yourself any permission you want on the object.

+ Windows Abuse

+ Linux Abuse

+ OPSEC

+ References

BLOODHOUND COMMUNITY EDITION

EXPLORE | GROUP MANAGEMENT

SEARCH | PATHFINDING | CYPHER

```
1 MATCH p = (n)-[r]->(m)
2 WHERE TYPE(r) CONTAINS "ADCS"
3 RETURN p
```

SAVE QUERY | HELP | SEARCH

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Shortest Paths

Active Directory Certificate Services

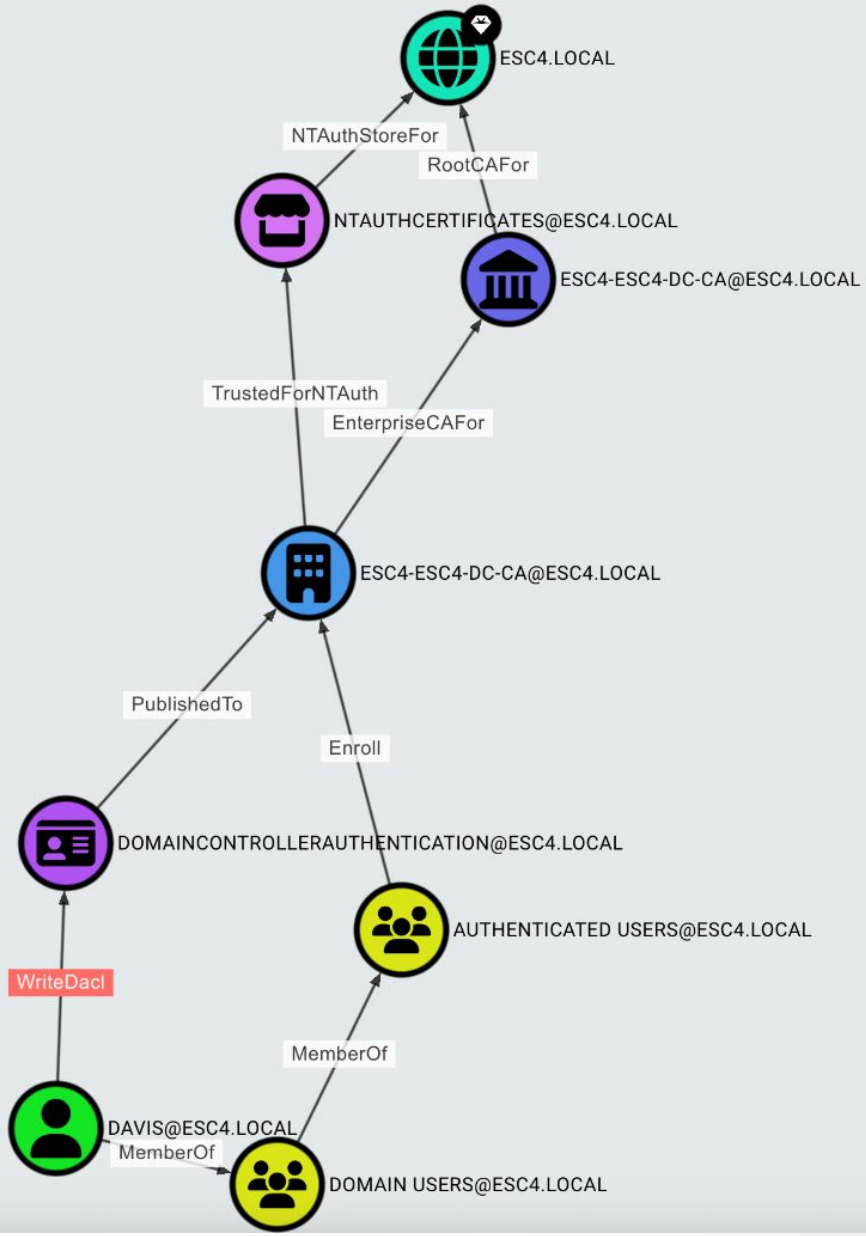
PKI hierarchy

Public Key Services container

Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

Enrollment rights on published enrollment agent certificate templates



Layout | Export | Search Current Results

WriteDacl

+ General

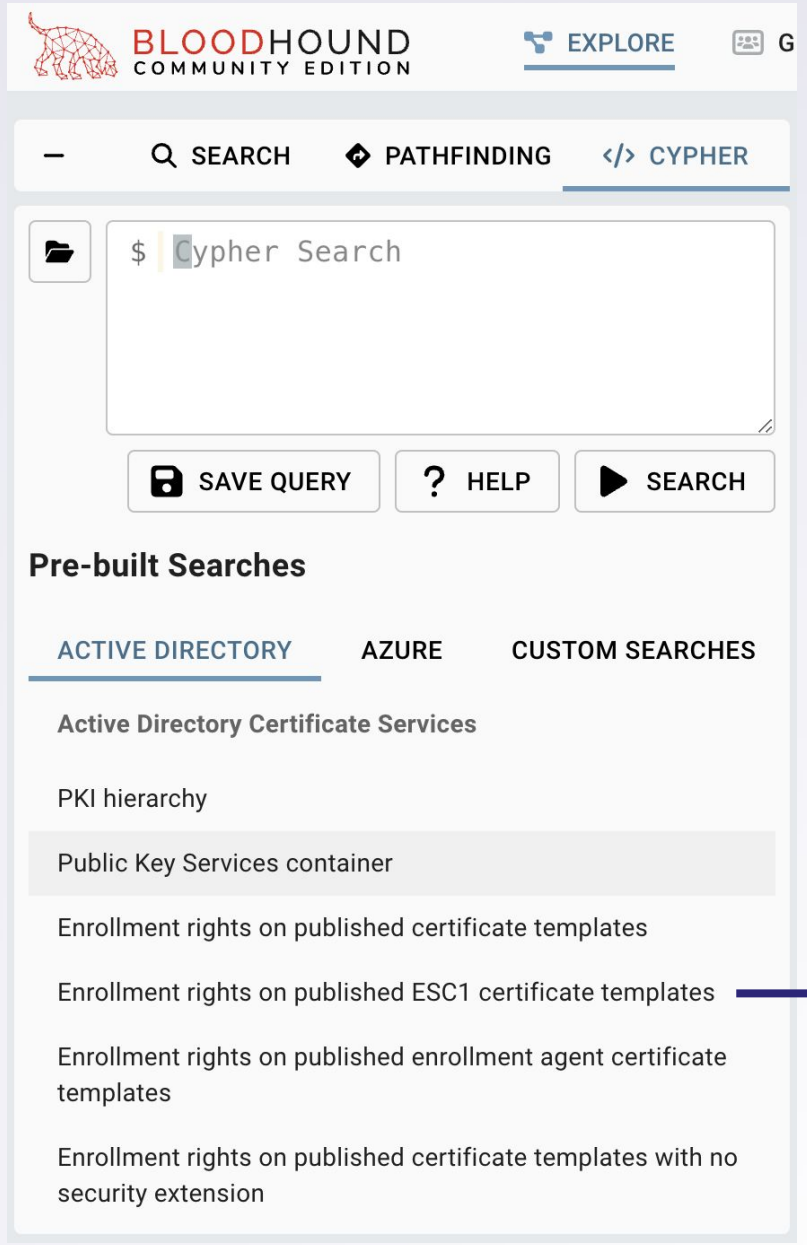
+ Windows Abuse

+ Linux Abuse

+ OPSEC

– References

https://github.com/PowerShellMafia/PowerSploit/blob/dev/Re
https://www.youtube.com/watch?v=z8thoG7gPd0
https://eladshamir.com/2019/01/28/Wagging-the-Dog.html
https://github.com/GhostPack/Rubeus#s4u
https://github.com/n00py/DCSync
https://gist.github.com/HarmJ0y/224dbfef83febdaf885a8451e
https://blog.harmj0y.net/redteaming/another-word-on-delegatic
https://github.com/PowerShellMafia/PowerSploit/blob/dev/Re
https://github.com/Kevin-Robertson/Powermad#new-machinea
https://docs.microsoft.com/en-us/dotnet/api/system.directory
https://github.com/Kevin-Robertson/Powermad#new-machinea
https://www.thehacker.recipes/ad/movement/dacl/addmembe
https://www.thehacker.recipes/ad/movement/dacl/targeted-ke
https://www.thehacker.recipes/ad/movement/group-policies
https://www.thehacker.recipes/ad/movement/dacl/forcechang
https://www.thehacker.recipes/ad/movement/kerberos/shadov
https://www.thehacker.recipes/ad/movement/credentials/dum
https://www.thehacker.recipes/ad/movement/kerberos/delega
https://www.thehacker.recipes/ad/movement/dacl/grant-rights
https://github.com/eladshamir/Whisker
https://posts.specterops.io/shadow-credentials-abusing-key-tru



Calculates for you which templates are susceptible to ESC1 based on their version and other properties. Displays the principals that have been granted enroll rights on each template.

BLOODHOUND COMMUNITY EDITION

EXPLORE | GROUP MANAGEMENT

SEARCH | PATHFINDING | CYPHER

```
1 MATCH p = ()-
  [:Enroll|GenericAll|AllExtendedRi
  ghts]->(ct:CertTemplate)-
  [:PublishedTo]->(:EnterpriseCA)
2 WHERE ct.enrolleesuppliessubject
  = True
3 AND ct.authenticationenabled =
  True
4 AND ct.requiresmanagerapproval =
  False
5 AND (ct.authorizedsignatures = 0
  OR ct.schemaversion = 1)
6 RETURN p
```

SAVE QUERY | HELP | SEARCH

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Active Directory Certificate Services

PKI hierarchy

Public Key Services container

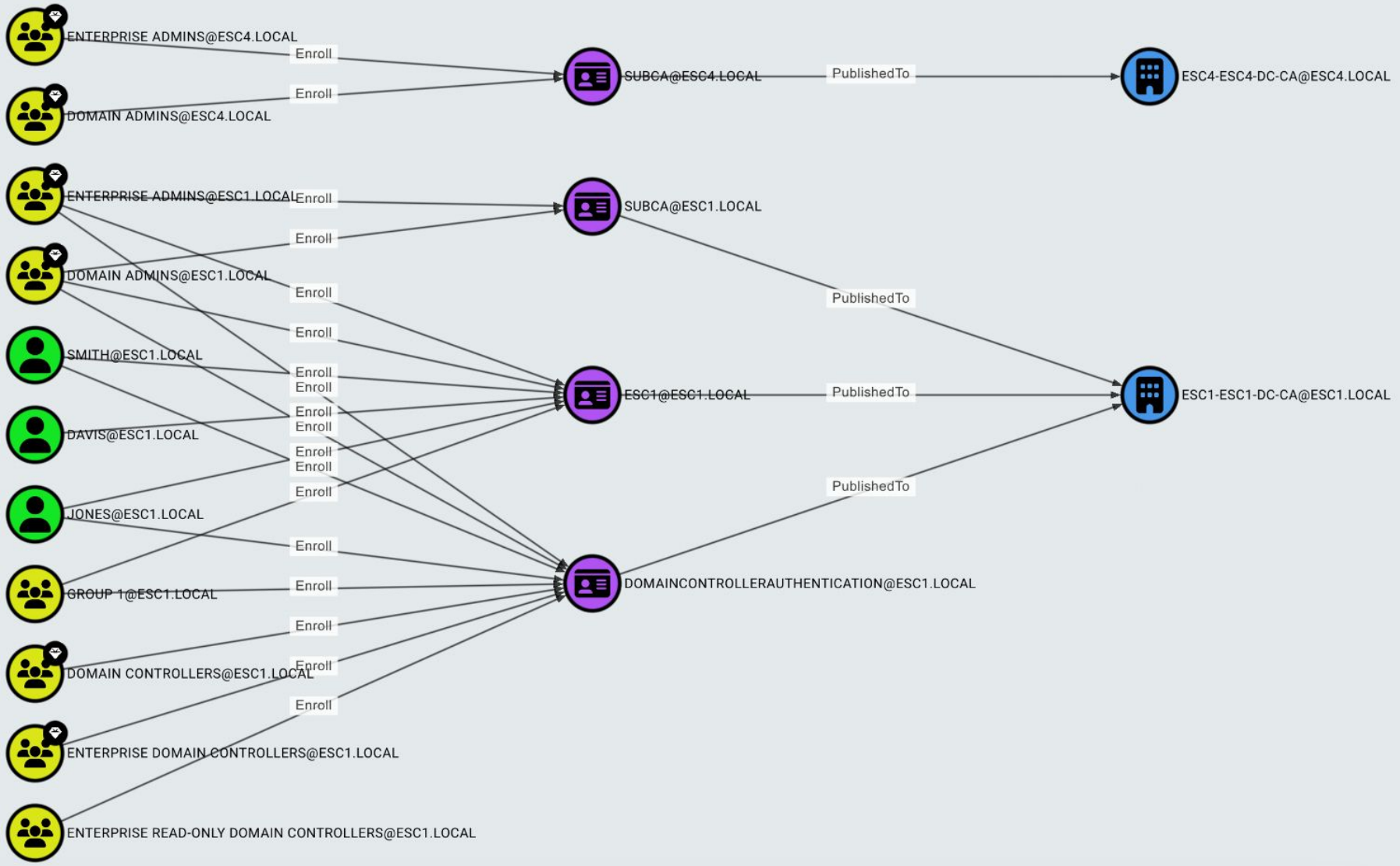
Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

Enrollment rights on published enrollment agent certificate templates

Enrollment rights on published certificate templates with no security extension

Layout | Export | Search Current Results



SEARCH | PATHFINDING | CYPHER

```
1 MATCH p=()-
  [:HostsCAService|IssuedSignedBy|EnterpriseCAFor|Roo
  tCAFor|TrustedForNTAuth|NTAuthStoreFor*..]->()
2 RETURN p
```

SAVE QUERY | HELP | RUN

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Active Directory Certificate Services

PKI hierarchy

Public Key Services container

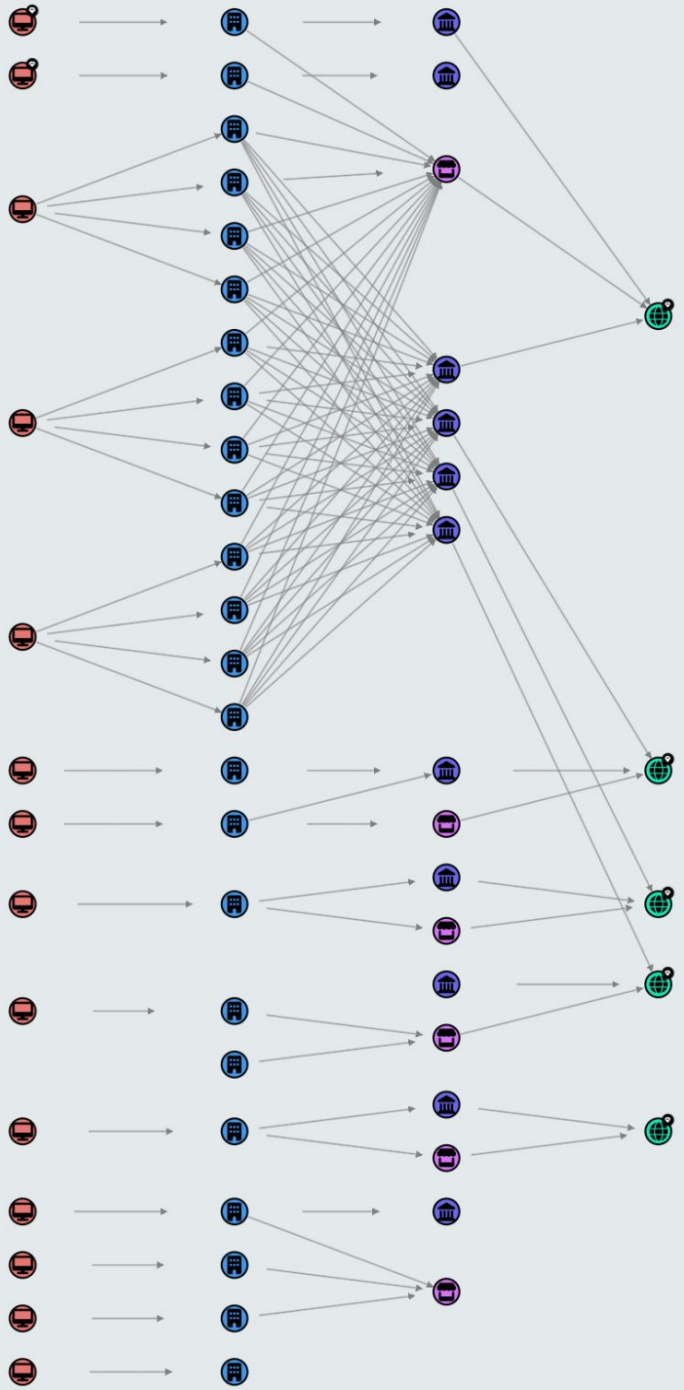
Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

Enrollment rights on published ESC2 certificate templates

Enrollment rights on published enrollment agent certificate templates

Enrollment rights on published certificate templates with no security extension



SEARCH | PATHFINDING | CYPHER

```
1 MATCH p = (c:Container)-[:Contains*..]->()
2 WHERE c.distinguishedname starts with "CN=PUBLIC
  KEY SERVICES,CN=SERVICES,CN=CONFIGURATION,DC="
3 RETURN p
```

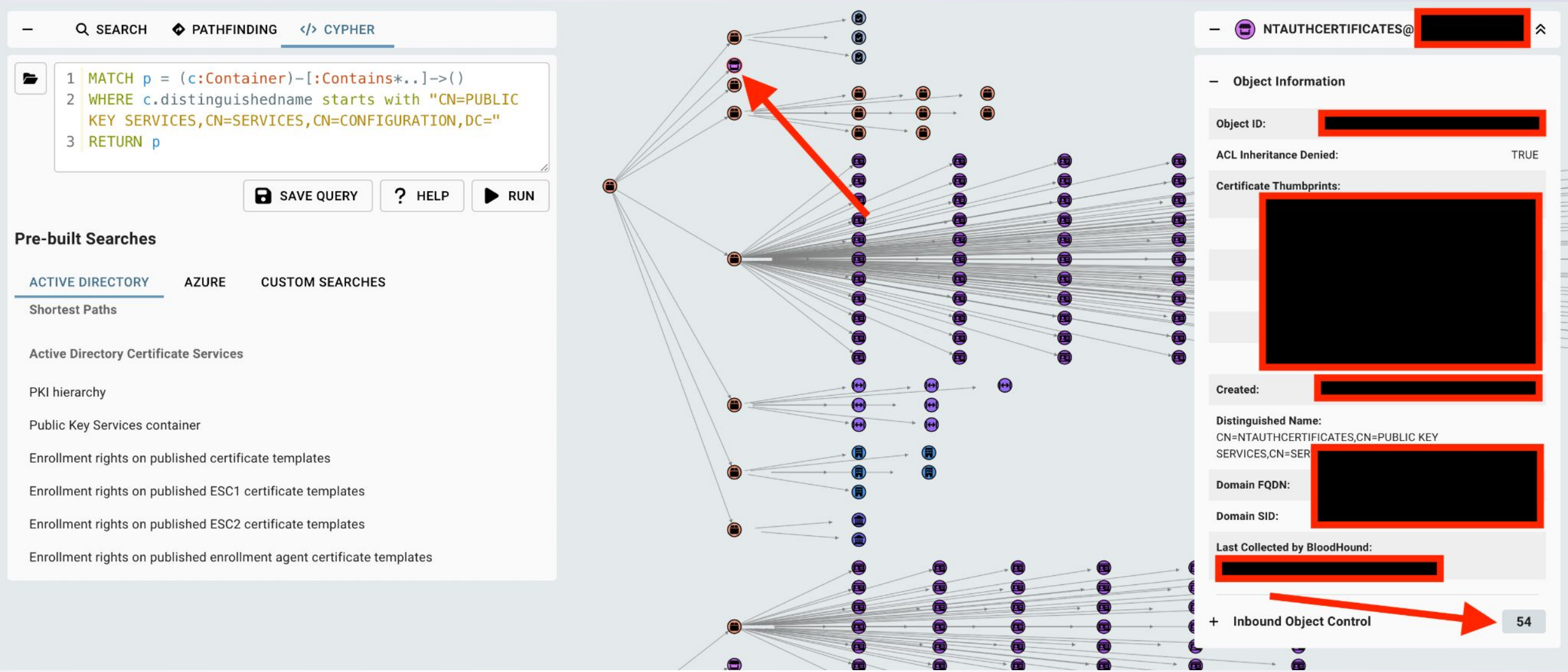
SAVE QUERY | HELP | RUN

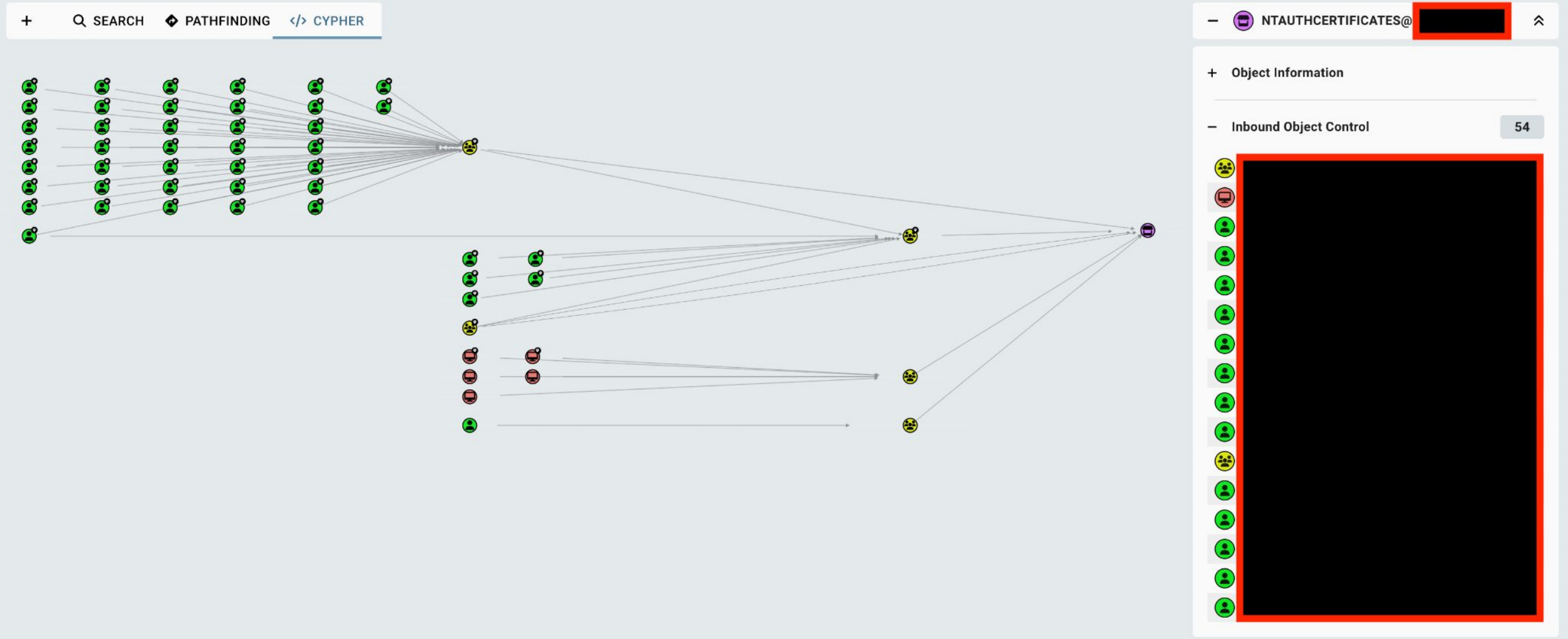
Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Active Directory Certificate Services

- Public Key Services container
- Enrollment rights on published certificate templates
- Enrollment rights on published ESC1 certificate templates
- Enrollment rights on published ESC2 certificate templates
- Enrollment rights on published enrollment agent certificate templates
- Enrollment rights on published certificate templates with no security extension
- Enrollment rights on certificate templates published to Enterprise CA with User Specified SAN enabled


SEARCH
PATHFINDING
CYPHER
1 MATCH p = (c:Container)-[:Contains*..]->()
2 WHERE c.distinguishedname starts with "CN=PUBLIC KEY SERVICES,CN=SERVICES,CN=CONFIGURATION,DC="
3 RETURN p
SAVE QUERY
HELP
RUN
Pre-built Searches
ACTIVE DIRECTORY
AZURE
CUSTOM SEARCHES
Shortest Paths
Active Directory Certificate Services
PKI hierarchy
Public Key Services container
Enrollment rights on published certificate templates
Enrollment rights on published ESC1 certificate templates
Enrollment rights on published ESC2 certificate templates
Enrollment rights on published enrollment agent certificate templates
NTAUTHCERTIFICATES@
Object Information
Object ID:
ACL Inheritance Denied:
TRUE
Certificate Thumbprints:
Created:
Distinguished Name:
CN=NTAUTHCERTIFICATES,CN=PUBLIC KEY
SERVICES,CN=SER
Domain FQDN:
Domain SID:
Last Collected by BloodHound:
Inbound Object Control
54


SEARCH
PATHFINDING
CYPHER
NTAUTHCERTIFICATES@
Object Information
Inbound Object Control
54

SEARCH PATHFINDING CYPHER

```
1 MATCH p = ()-
  [:Enroll|GenericAll|AllExtendedRights]->
  (ct:CertTemplate)-[:PublishedTo]->(:EnterpriseCA)
2 RETURN p
```

SAVE QUERY HELP RUN

Pre-built Searches

ACTIVE DIRECTORY AZURE CUSTOM SEARCHES

Active Directory Certificate Services

Enrollment rights on published certificate templates

Enrollment rights on published ESC1 certificate templates

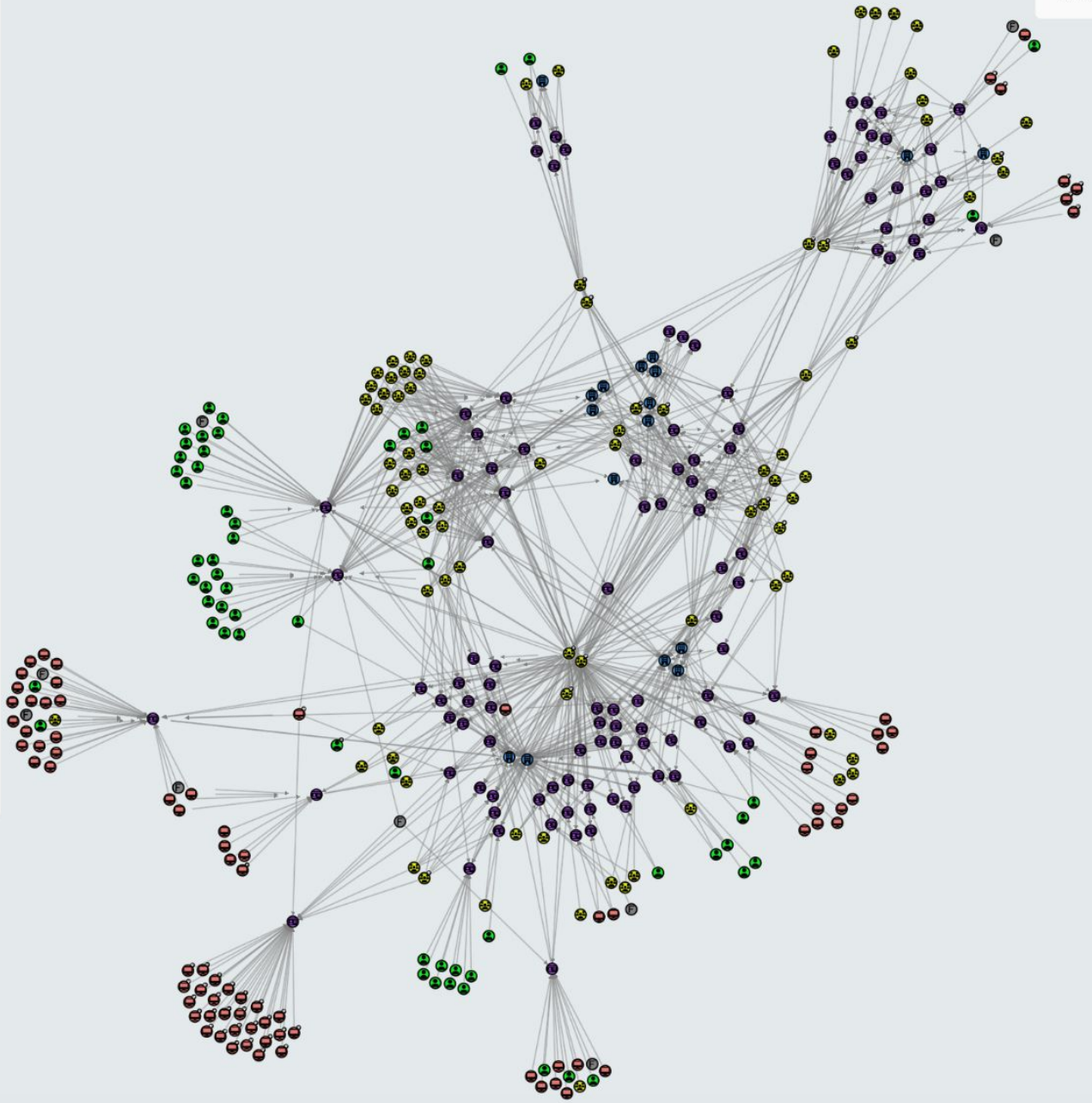
Enrollment rights on published ESC2 certificate templates

Enrollment rights on published enrollment agent certificate templates

Enrollment rights on published certificate templates with no security extension

Enrollment rights on certificate templates published to Enterprise CA with User Specified SAN enabled

CA administrators and CA managers



Layout Export Search Current Results

SEARCH | PATHFINDING | </> CYPHER

```
1 MATCH p = ()-
  [:Enroll|GenericAll|AllExtendedRights]->
  (ct:CertTemplate)-[:PublishedTo]->(:EnterpriseCA)
2 WHERE ct.enrolleesuppliessubject = True
3 AND ct.authenticationenabled = True
4 AND ct.requiresmanagerapproval = False
5 AND (ct.authorizedsignatures = 0 OR
  ct.schemaversion = 1)
6 RETURN p
```

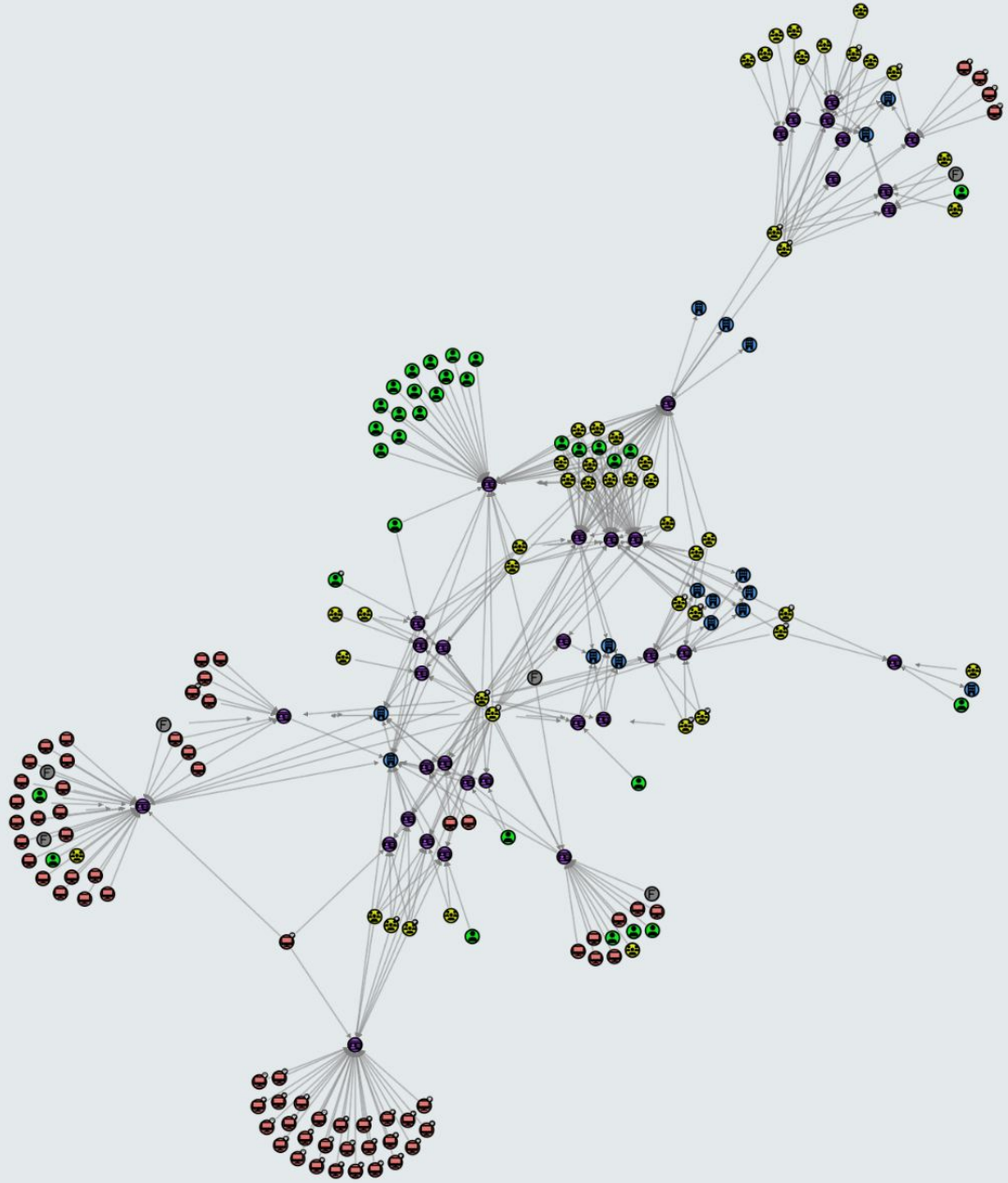
SAVE QUERY | HELP | RUN

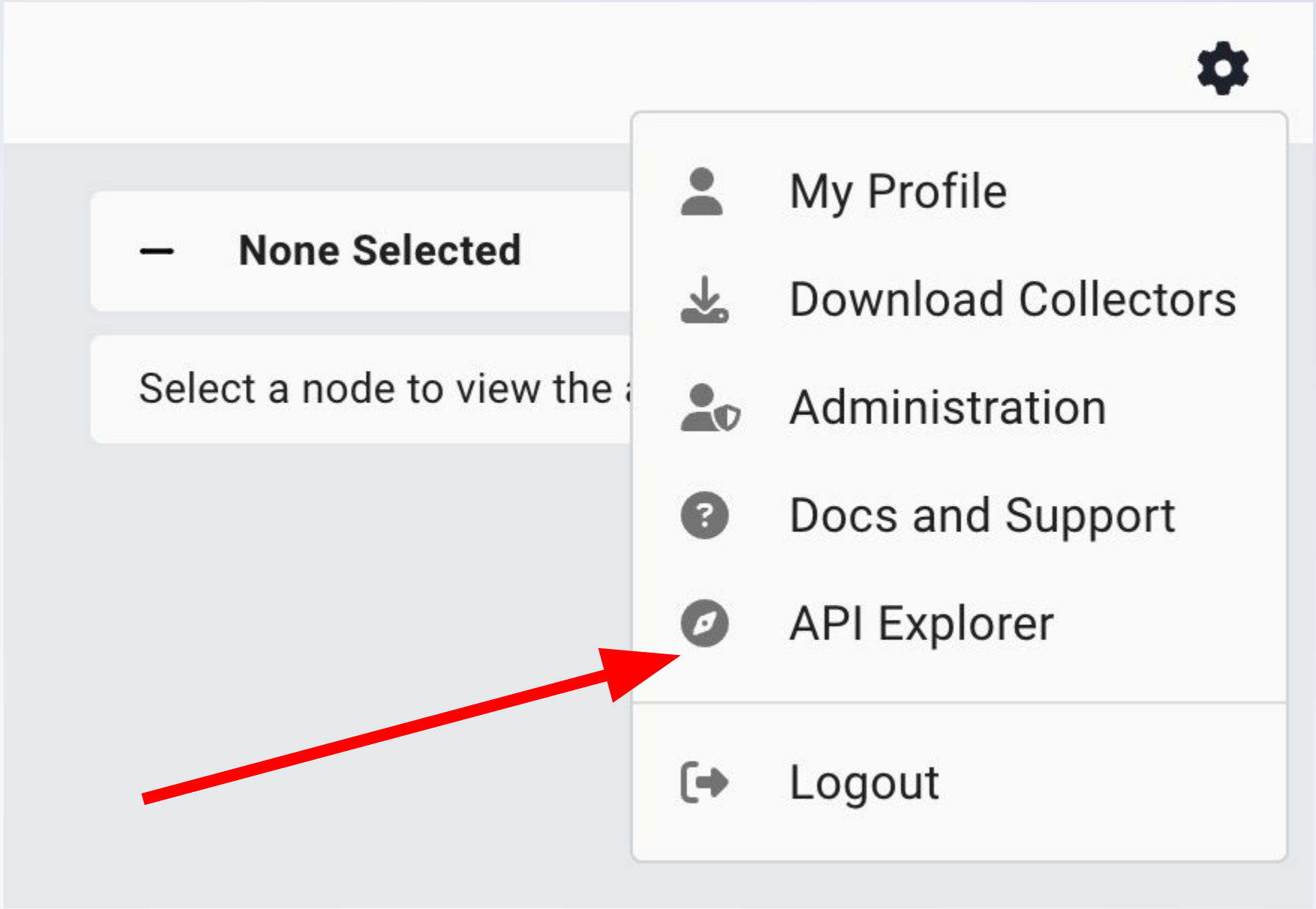
Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Active Directory Certificate Services

- Enrollment rights on published ESC1 certificate templates
- Enrollment rights on published ESC2 certificate templates
- Enrollment rights on published enrollment agent certificate templates
- Enrollment rights on published certificate templates with no security extension
- Enrollment rights on certificate templates published to Enterprise CA with User Specified SAN enabled
- CA administrators and CA managers




None Selected
Select a node to view the
My Profile
Download Collectors
Administration
Docs and Support
API Explorer
Logout

API Explorer

ca

AIACA Entity API

GET /api/v2/aiacas/{object_id} Get aiaca entity info

GET /api/v2/aiacas/{object_id}/controllers List aiaca controllers

EnterpriseCA Entity API

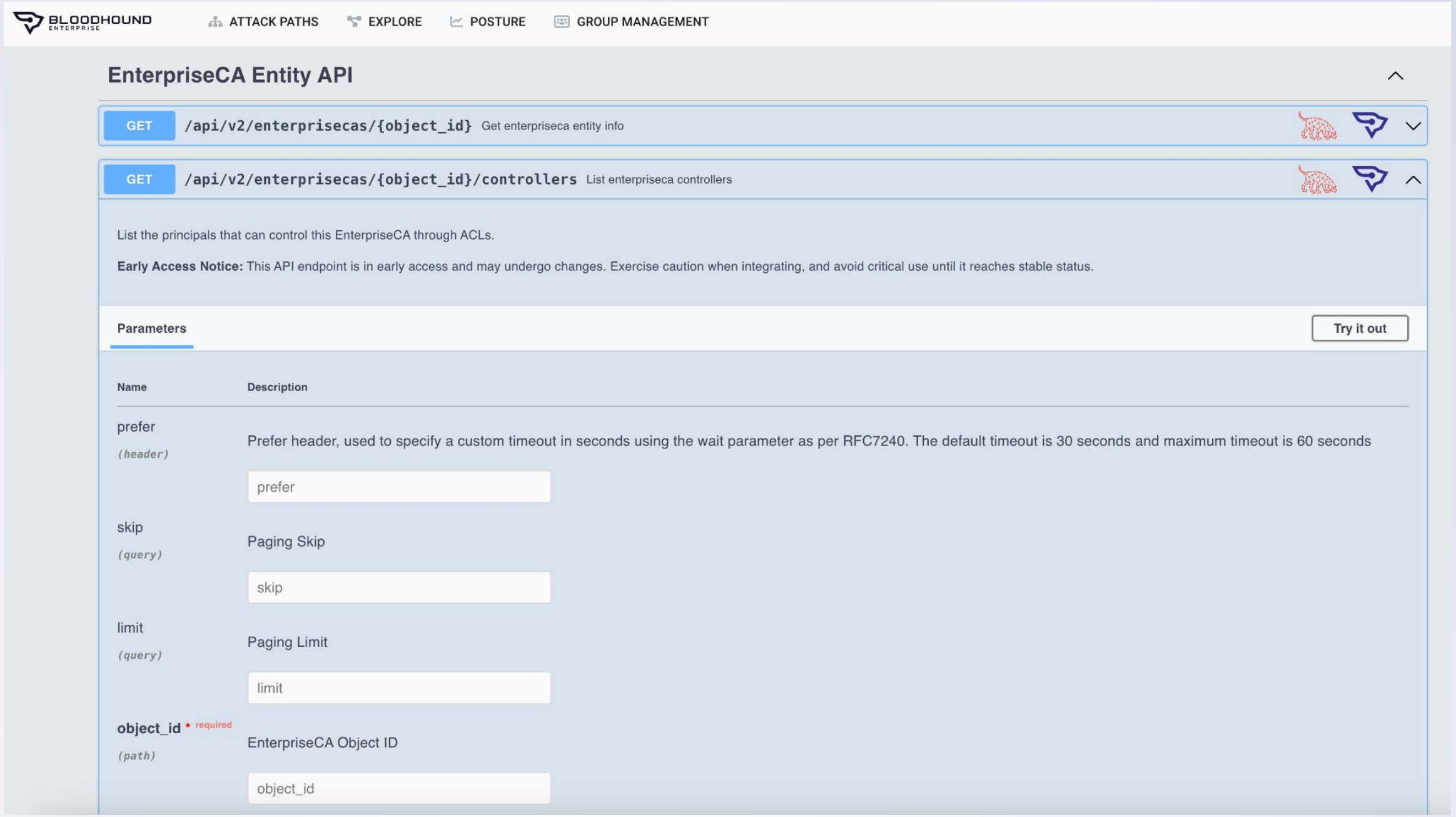
GET /api/v2/enterprisecas/{object_id} Get enterpriseca entity info

GET /api/v2/enterprisecas/{object_id}/controllers List enterpriseca controllers

RootCA Entity API

GET /api/v2/rootcas/{object_id} Get rootca entity info

GET /api/v2/rootcas/{object_id}/controllers List rootca controllers


BLOODHOUND ENTERPRISE
ATTACK PATHS
EXPLORE
POSTURE
GROUP MANAGEMENT
EnterpriseCA Entity API
GET /api/v2/enterprisecas/{object_id} Get enterpriseca entity info
GET /api/v2/enterprisecas/{object_id}/controllers List enterpriseca controllers
List the principals that can control this EnterpriseCA through ACLs.
Early Access Notice: This API endpoint is in early access and may undergo changes. Exercise caution when integrating, and avoid critical use until it reaches stable status.
Parameters
Try it out
Name
Description
prefer
(header)
Prefer header, used to specify a custom timeout in seconds using the wait parameter as per RFC7240. The default timeout is 30 seconds and maximum timeout is 60 seconds
prefer
skip
(query)
Paging Skip
skip
limit
(query)
Paging Limit
limit
object_id * required
(path)
EnterpriseCA Object ID
object_id

Responses

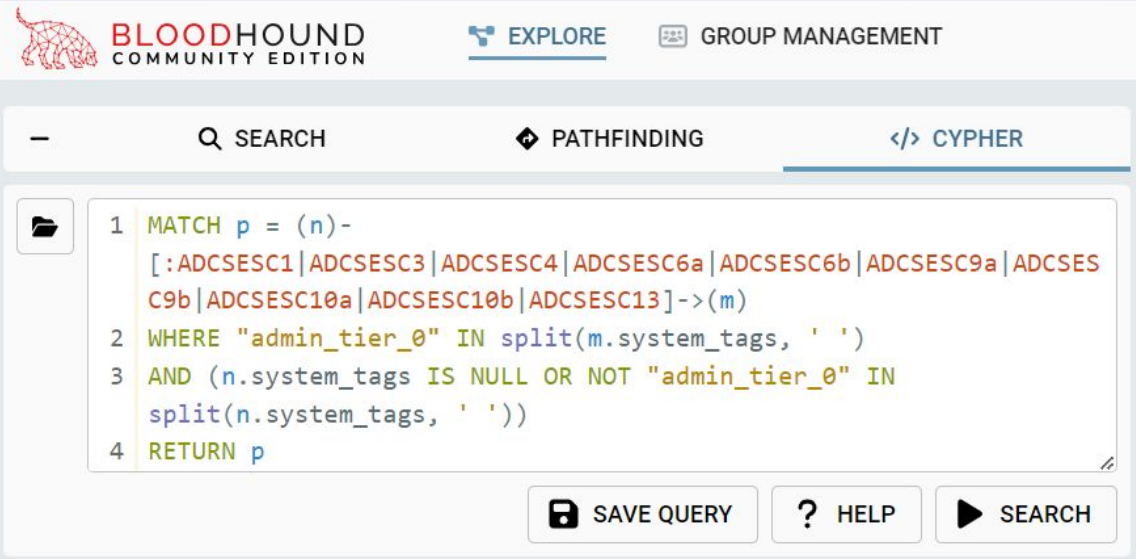
Code	Description	Links
200	OK Media type: application/json Controls Accept header. Example Value | Schema	*No links*
Error	Standard response for any errors that may occur. Media type: application/json Example Value | Schema	*No links*

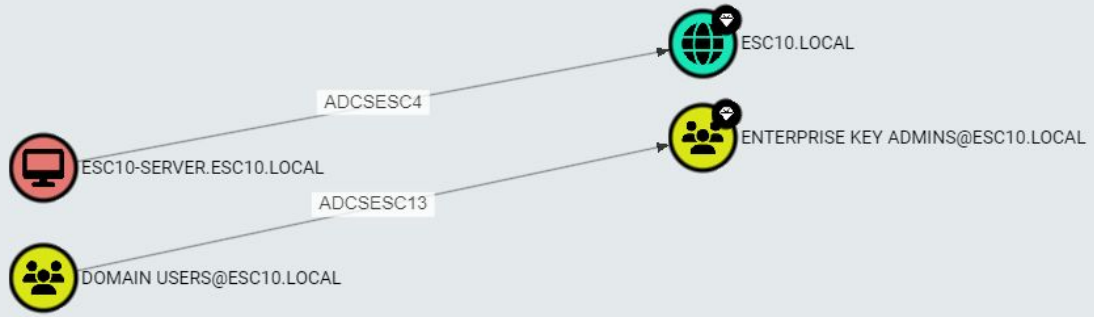
```
{
  "count": "string",
  "data": [
    {
      "label": "string",
      "name": "string",
      "objectID": "string"
    }
  ],
  "limit": "string",
  "skip": "string"
}
```

```
{
  "errors": [
    {
      "context": "string",
      "message": "string"
    }
```

Practical Remediation Strategies and Examples

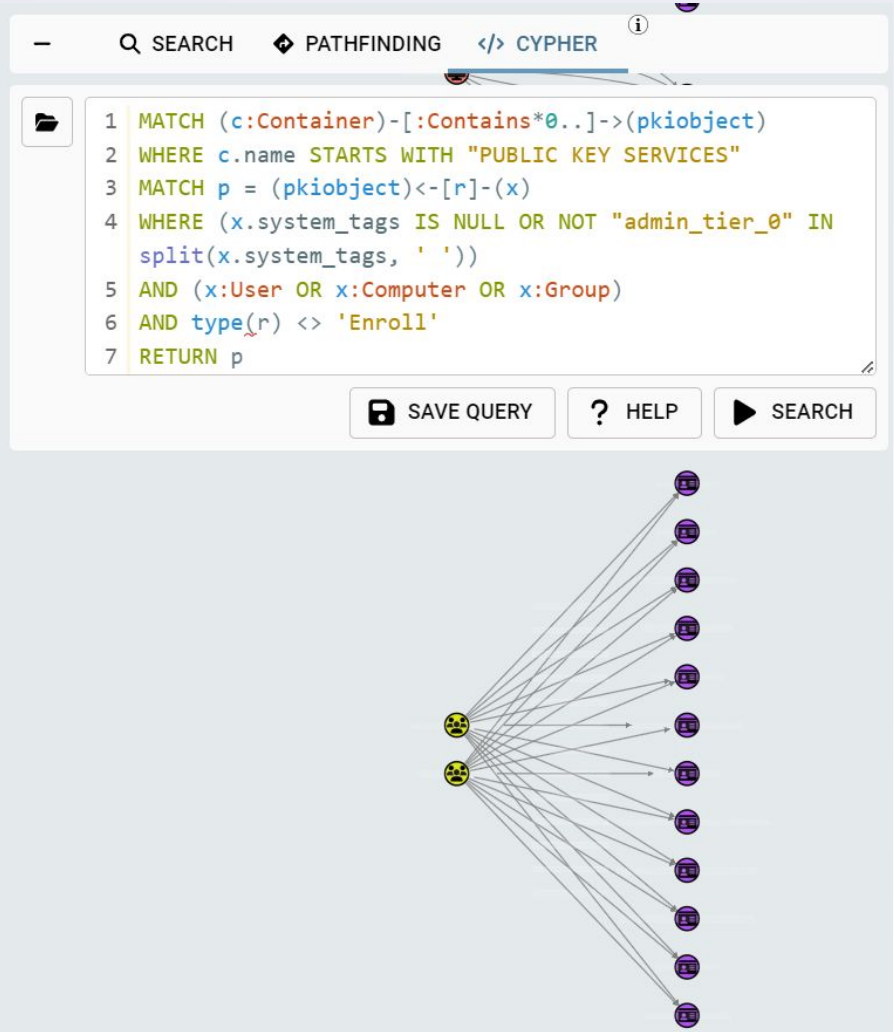
Find non-Tier Zero principals with ADCSESCx edges






```
MATCH p =
(n)-[:ADCSESC1|ADCSESC3|ADCSESC4|ADCSESC6a|ADCSESC6b|ADCSESC9a|ADCSESC9b|
ADCSESC10a|ADCSESC10b|ADCSESC13]->(m)
WHERE "admin_tier_0" IN split(m.system_tags, ' ')
AND (n.system_tags IS NULL OR NOT "admin_tier_0" IN split(n.system_tags,
' '))
RETURN p
```

Find non-Tier Zero principals with ADCS permissions



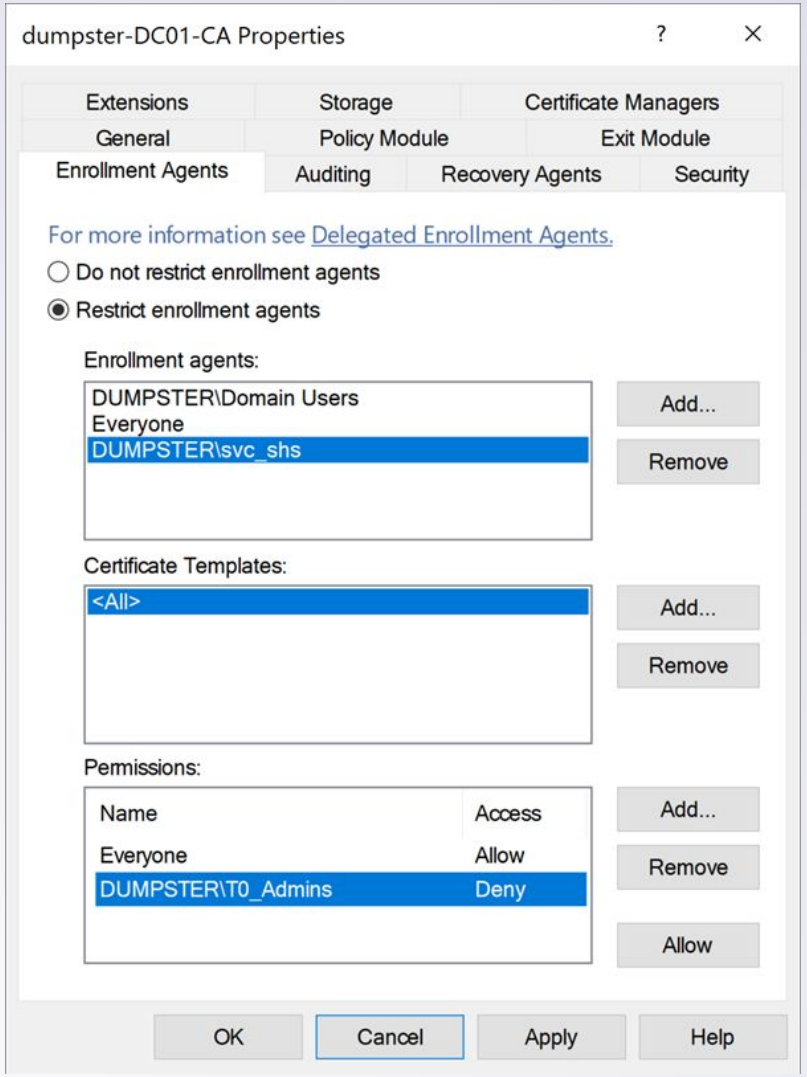

```
MATCH
(c:Container)-[:Contains*0..]->(pkiobject)
WHERE c.name STARTS WITH "PUBLIC KEY
SERVICES"
MATCH p = (pkiobject)<-[r]-(x)
WHERE (
x.system_tags IS NULL
OR NOT "admin_tier_0" IN
split(x.system_tags, ' ')
)
AND (x:User OR x:Computer OR x:Group)
AND type(r) <> 'Enroll'
RETURN p
```

ESC1 Remediation

- ESC1: Enrollee Supplies Subject
- If you can, then either:
  - Limit enrollment rights to Tier Zero principals
  - Remove EKUs that enable domain authentication

ESC1 Remediation

- Common scenario:
  Helpdesk (NOT Tier Zero) creates smart cards on behalf of others
- Solution: Enrollment agents - with restrictions
- Example:
  - Yubico - Setting up Smart Card Login for Enroll on Behalf of: https://support.yubico.com/hc/en-us/articles/360015669119-Setting-up-Smart-Card-Login-for-Enroll-on-Behalf-of



ESC1 Remediation

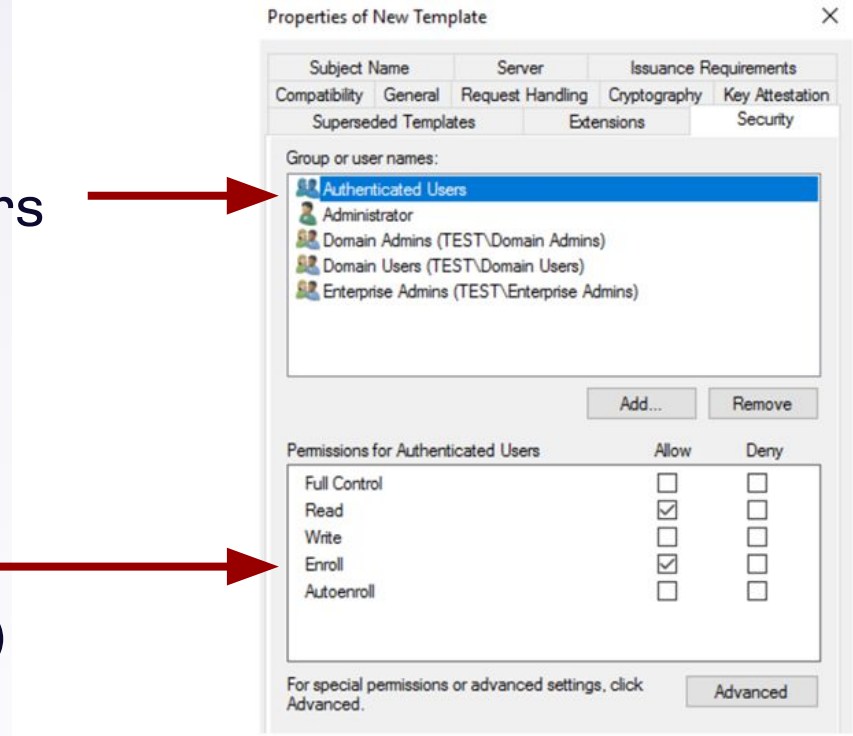
Be careful with vendor guides though

FIDO Security Keys — Home | Products | Guides | Compatible Service Catalog | FAQ

6. Under the **Security** tab, be sure the **Read** and **Enroll** ability is set for the user or group of users who will be setting up the smart cards for logon. The admin group is same as auto-enrollment settings.

Authenticated Users →

Enroll
(on agent template) →



SPECTEROPS

Thank you!

Get BloodHoundCE: https://ghst.ly/bh-github

Join the BloodHound Slack: https://ghst.ly/BHSlack

Jonas Bülow Knudsen | @Jonas_B_K

Andy Robbins | arobbins@specterops.com

TROOPERS