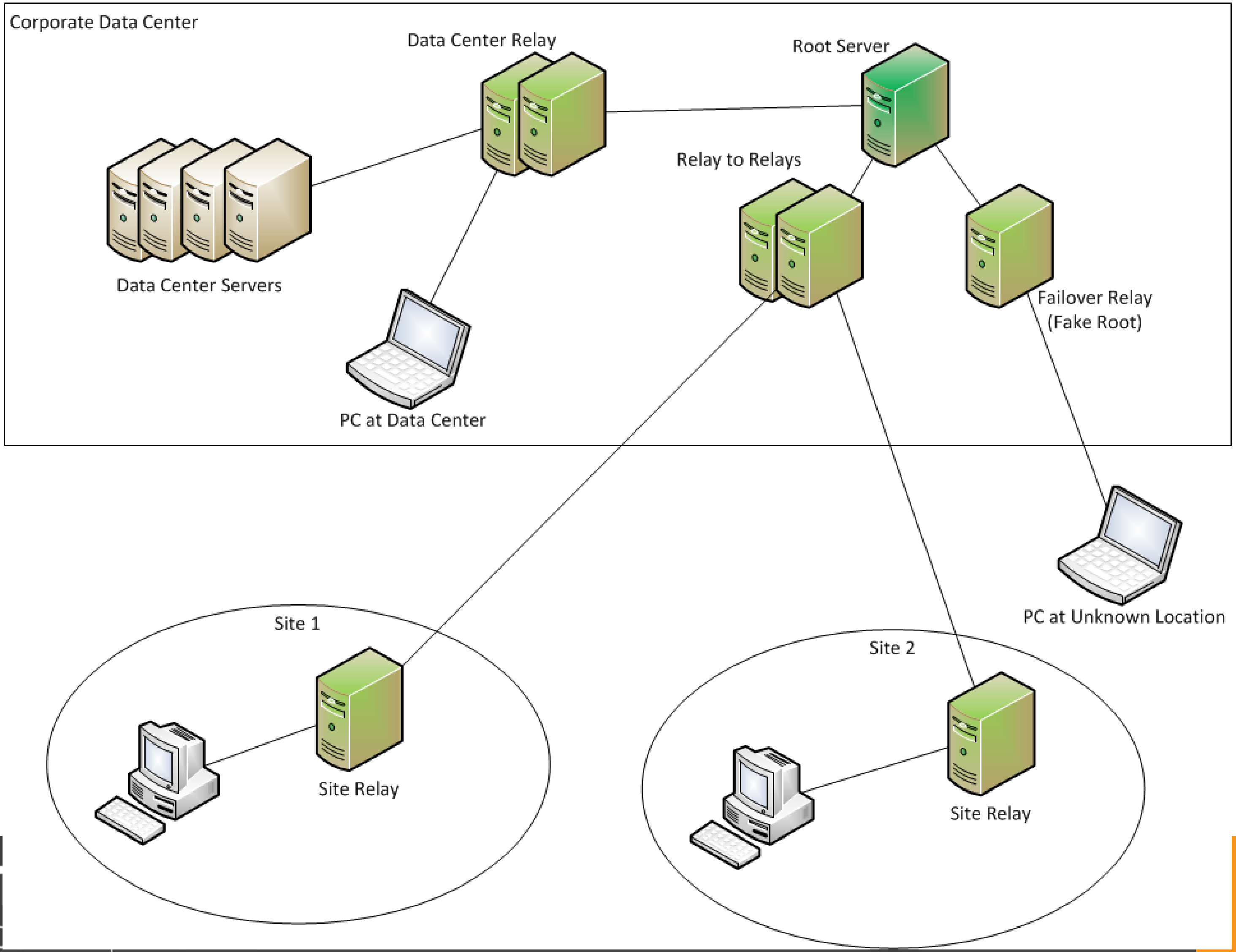
Client Relay Affiliation

Preventing Cross-Site Communication

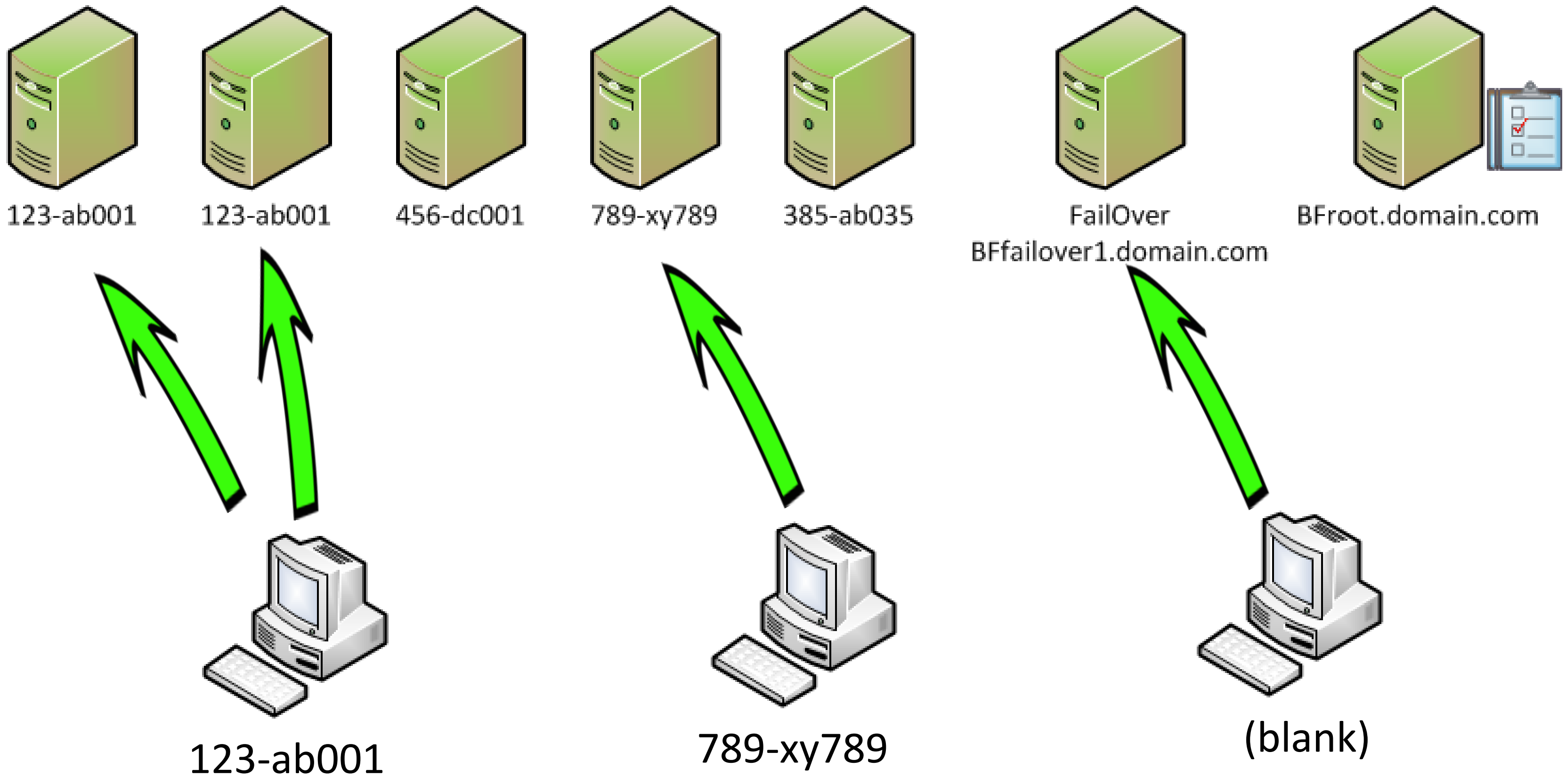
KROGER TECHNOLOGY

CUSTOMER | QUALITY | INNOVATION

Ideal Relay setup for Large/Medium BigFix Arch.



How Named Affiliation Works

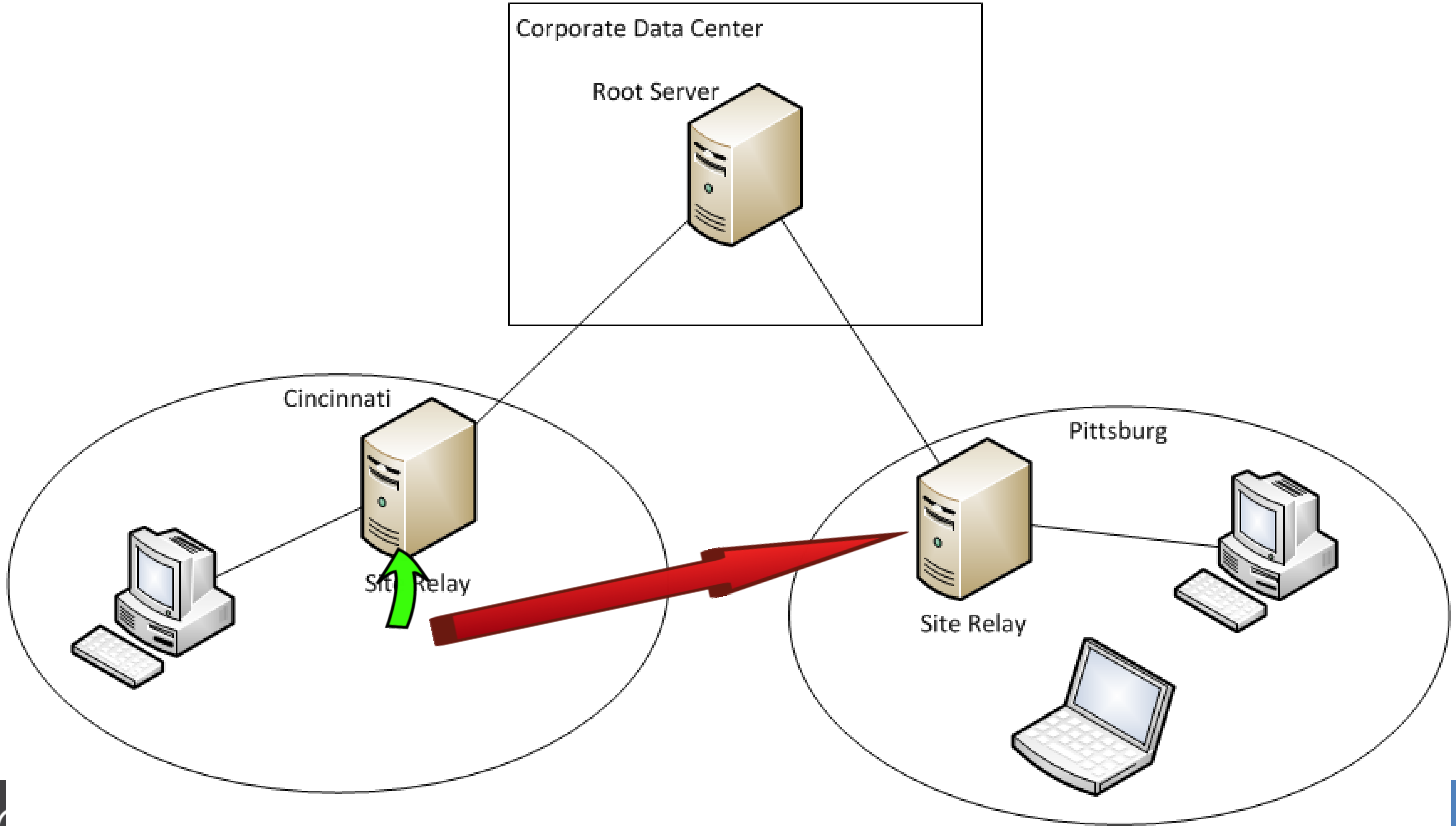


How do we map relays

- AD Site
- IP address range
- DHCP Domain
- Web Service
- Any consistent/unique string across your environment

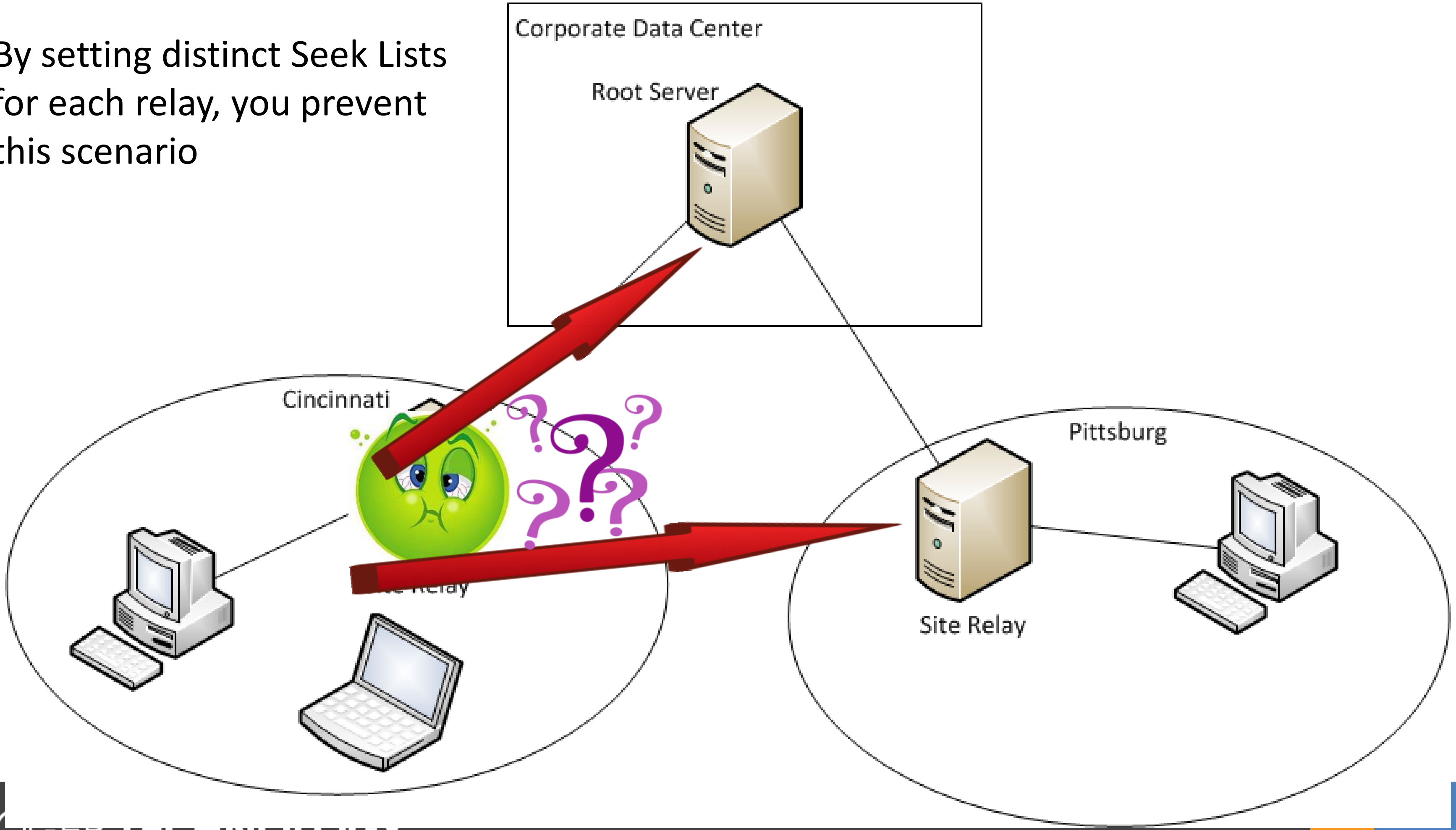
Set distinct names to specific networks/roles

Traveling PC Example



Failed Site Relay

By setting distinct Seek Lists for each relay, you prevent this scenario



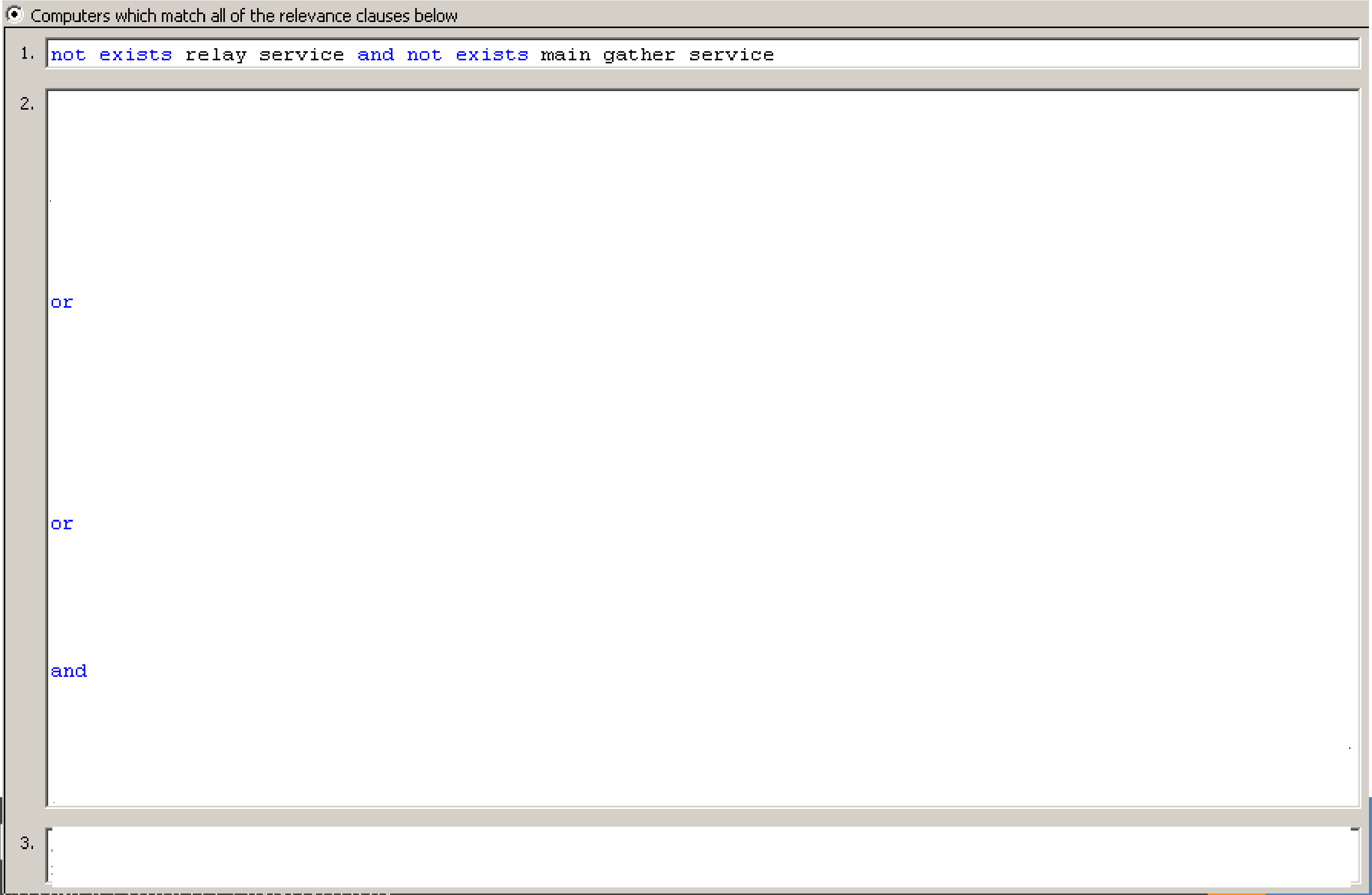
"_BESClient_Register_Affiliation_SeekList" Update Example (AD Site)

- Activate Directory Sites & Services is primarily used to map DC -to- network LANs, but we can use it for more

SeekList Client Update Triggers

- “Net Signature” client property
- AD Site Registry (client registry) -vs- stored AD Site Property
- Has a valid IP address

SeekList Update Triggers



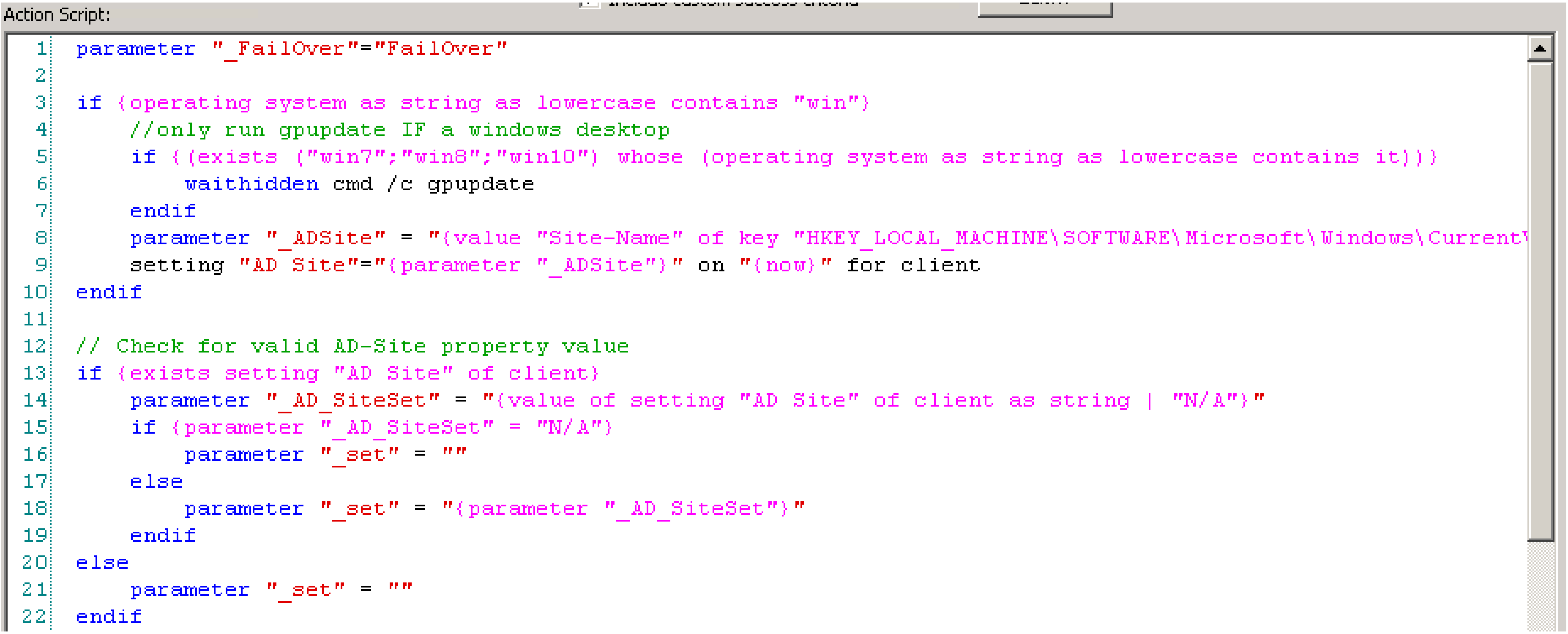
● Computers which match all of the relevance clauses below

1. `not exists relay service and not exists main gather service`

2.
```
or

or

and
```

3.

SeekList Update Action Script

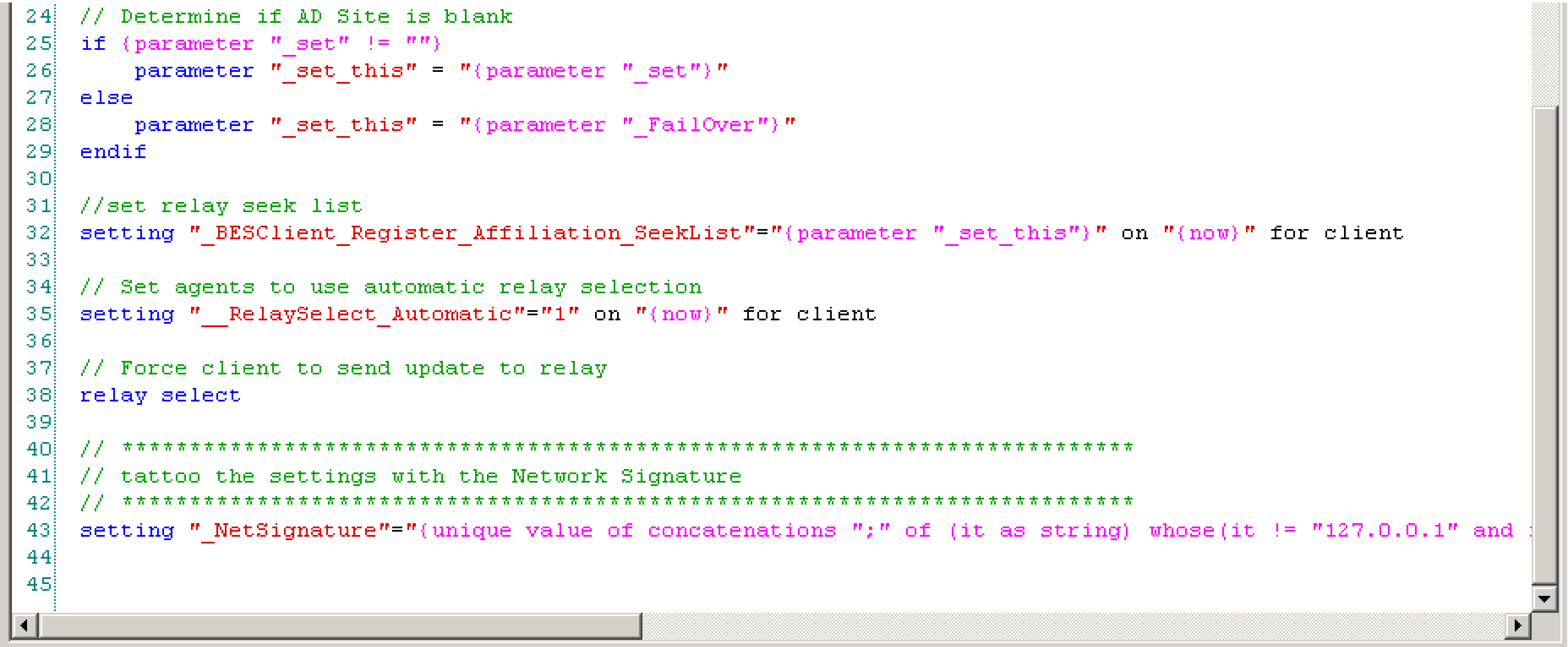


Action Script:

```
parameter "_FailOver"="FailOver"

if {operating system as string as lowercase contains "win"}
    //only run gpupdate IF a windows desktop
    if {(exists ("win7";"win8";"win10") whose (operating system as string as lowercase contains it))}
        waithidden cmd /c gpupdate
    endif
    parameter "_ADSite" = "{value "Site-Name" of key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\
    setting "AD Site"="{parameter "_ADSite"}" on "{now}" for client
endif

// Check for valid AD-Site property value
if {exists setting "AD Site" of client}
    parameter "_AD_SiteSet" = "{value of setting "AD Site" of client as string | "N/A"}"
    if {parameter "_AD_SiteSet" = "N/A"}
        parameter "_set" = ""
    else
        parameter "_set" = "{parameter "_AD_SiteSet"}"
    endif
else
    parameter "_set" = ""
endif
```

KROGER TECHNOLOGY
CUSTOMER | QUALITY | INNOVATION

SeekList Update Action Script

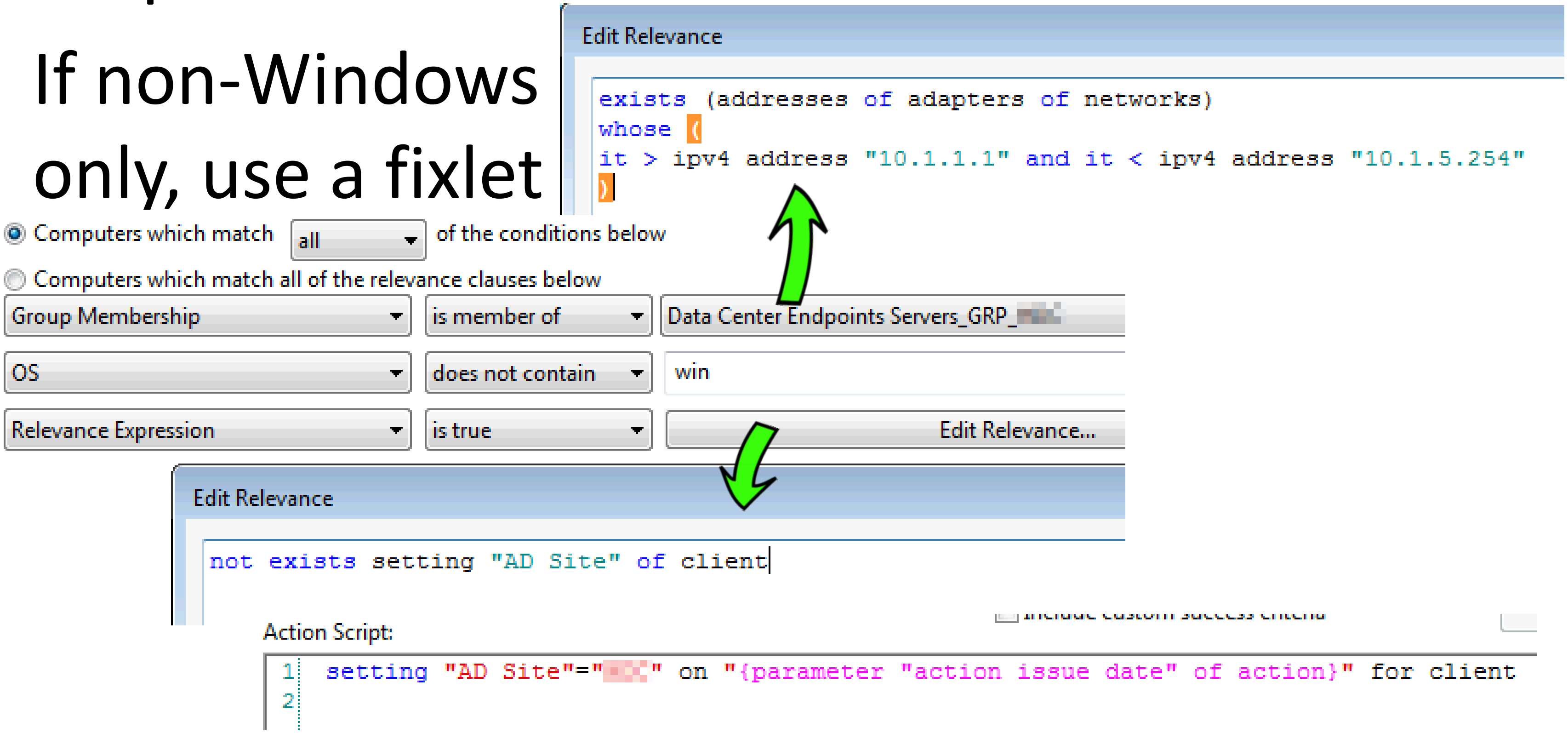


```
// Determine if AD Site is blank
if {parameter "_set" != ""}
    parameter "_set_this" = "{parameter "_set"}"
else
    parameter "_set_this" = "{parameter "_FailOver"}"
endif

//set relay seek list
setting "_BESClient_Register_Affiliation_SeekList"="{parameter "_set_this"}" on "{now}" for client

// Set agents to use automatic relay selection
setting "__RelaySelect_Automatic"="1" on "{now}" for client

// Force client to send update to relay
relay select

// ***************************************************************************
// tattoo the settings with the Network Signature
// ***************************************************************************
setting "_NetSignature"="{unique value of concatenations ";" of (it as string) whose(it != "127.0.0.1" and
```

When you set up this policy action, be sure to set low retry intervals on failure

AD Site for non-Windows

- Quest’s QAS command: “vastool info site” outputs AD Site
- If non-Windows only, use a fixlet



Edit Relevance

```
exists (addresses of adapters of networks)
whose (
it > ipv4 address "10.1.1.1" and it < ipv4 address "10.1.5.254"
)
```

● Computers which match all of the conditions below

○ Computers which match all of the relevance clauses below

Group Membership	is member of	Data Center Endpoints Servers_GRP_[redacted]
OS	does not contain	win
Relevance Expression	is true	Edit Relevance...

Edit Relevance

```
not exists setting "AD Site" of client
```

□ Include custom success criteria

Action Script:

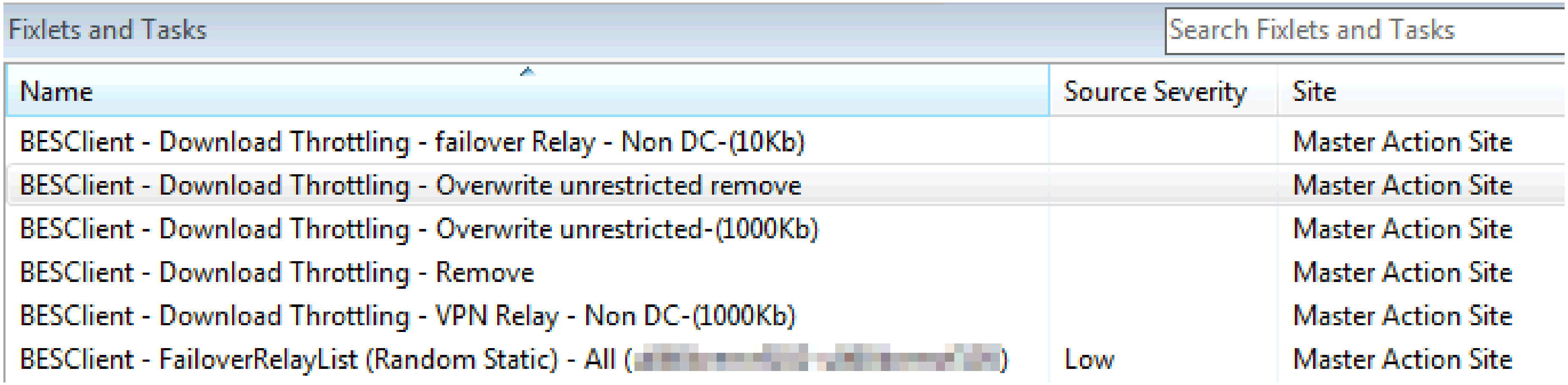
```
setting "AD Site"="[redacted]" on "{parameter "action issue date" of action}" for client
```

Addressing “Failover”

- Failover is when a client communicates with the core or failover relays
- You should have policy actions in place to check for and remediate (if possible)

Addressing “Failover”

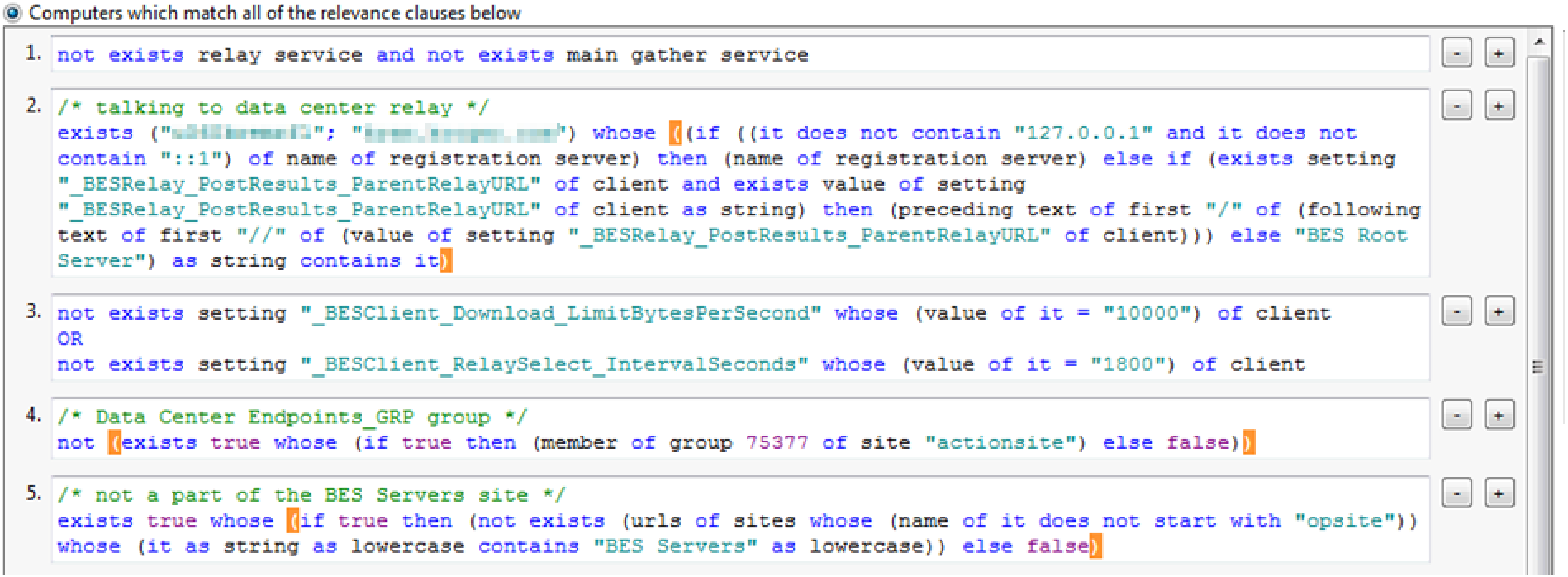
- Lower client download speeds if connected to the “Fail Over” servers



Name	Source Severity	Site
BESClient - Download Throttling - failover Relay - Non DC-(10Kb)		Master Action Site
BESClient - Download Throttling - Overwrite unrestricted remove		Master Action Site
BESClient - Download Throttling - Overwrite unrestricted-(1000Kb)		Master Action Site
BESClient - Download Throttling - Remove		Master Action Site
BESClient - Download Throttling - VPN Relay - Non DC-(1000Kb)		Master Action Site
BESClient - FailoverRelayList (Random Static) - All ([redacted])	Low	Master Action Site

KROGER TECHNOLOGY
CUSTOMER | QUALITY | INNOVATION

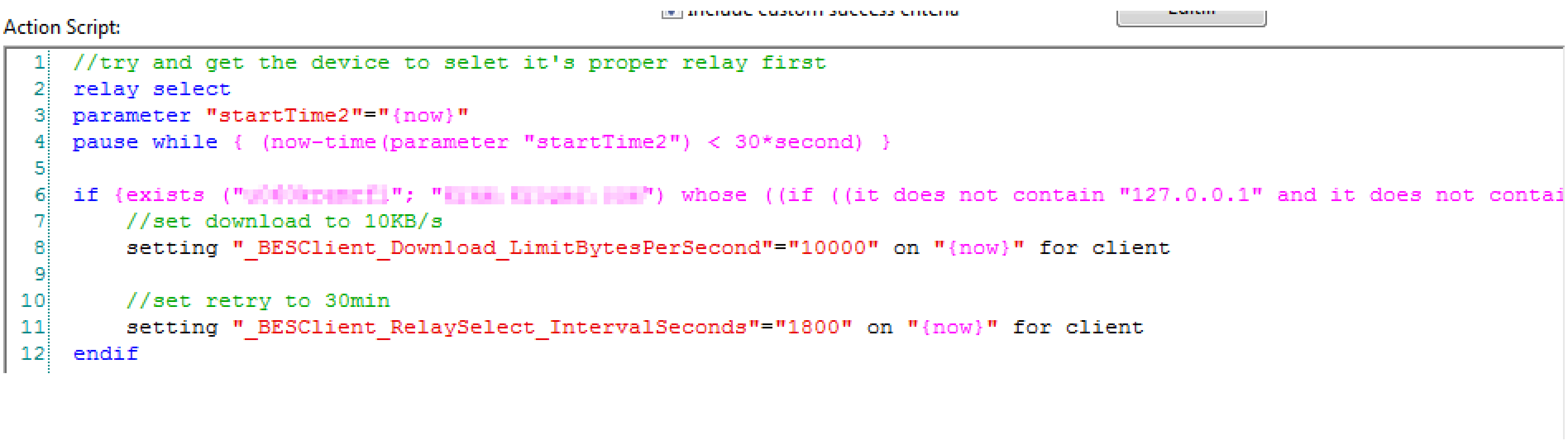
Failover Client Relay Relevance



● Computers which match all of the relevance clauses below

```
1. not exists relay service and not exists main gather service

2. /* talking to data center relay */
   exists ("[redacted]"; "[redacted]") whose ((if ((it does not contain "127.0.0.1" and it does not
   contain "::1") of name of registration server) then (name of registration server) else if (exists setting
   "_BESRelay_PostResults_ParentRelayURL" of client and exists value of setting
   "_BESRelay_PostResults_ParentRelayURL" of client as string) then (preceding text of first "/" of (following
   text of first "//" of (value of setting "_BESRelay_PostResults_ParentRelayURL" of client))) else "BES Root
   Server") as string contains it)

3. not exists setting "_BESClient_Download_LimitBytesPerSecond" whose (value of it = "10000") of client
   OR
   not exists setting "_BESClient_RelaySelect_IntervalSeconds" whose (value of it = "1800") of client

4. /* Data Center Endpoints_GRP group */
   not (exists true whose (if true then (member of group 75377 of site "actionsite") else false))

5. /* not a part of the BES Servers site */
   exists true whose (if true then (not exists (urls of sites whose (name of it does not start with "opsite"))
   whose (it as string as lowercase contains "BES Servers" as lowercase)) else false)
```

Failover Client Relay Action

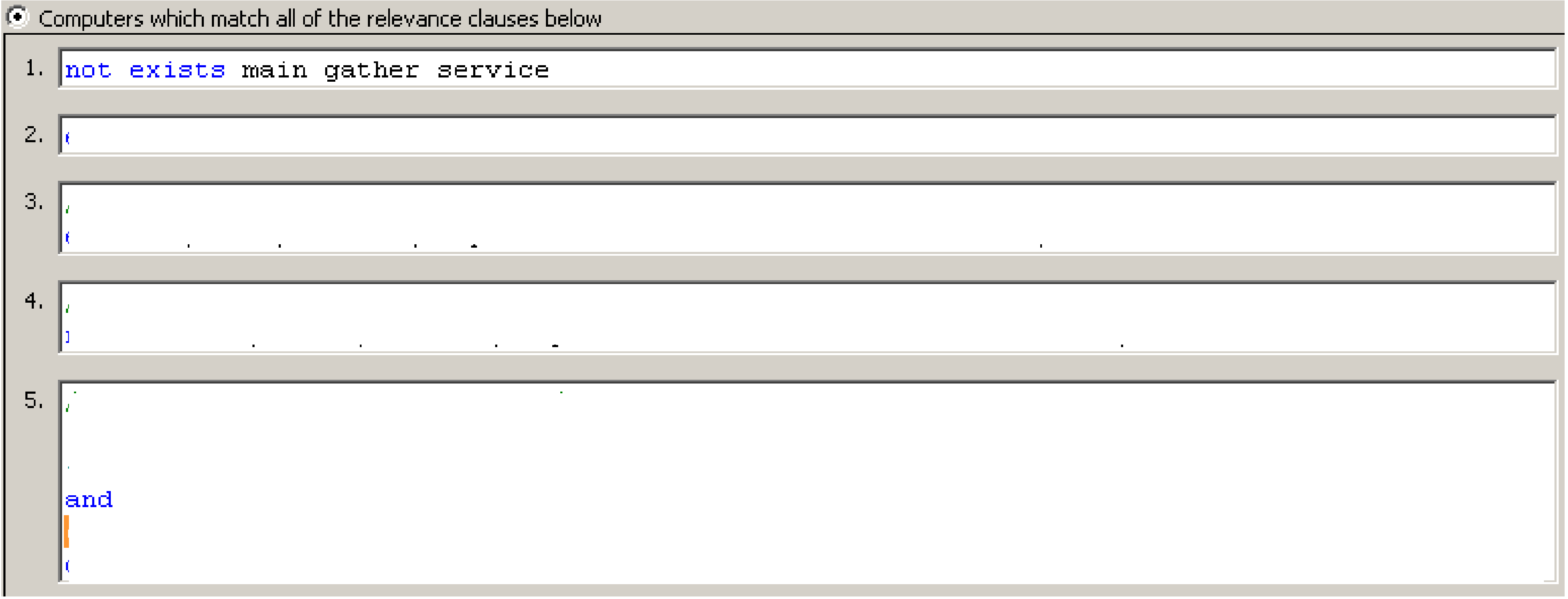


```
//try and get the device to selet it's proper relay first
relay select
parameter "startTime2"="{now}"
pause while { (now-time(parameter "startTime2") < 30*second) }

if {exists ("[redacted]"; "[redacted]") whose ((if ((it does not contain "127.0.0.1" and it does not contai
    //set download to 10KB/s
    setting "_BESClient_Download_LimitBytesPerSecond"="10000" on "{now}" for client

    //set retry to 30min
    setting "_BESClient_RelaySelect_IntervalSeconds"="1800" on "{now}" for client
endif
```

Automatic Relay Configuration

- New sites come on line and we don’t want to have to managed them one by one
- Use the same logic you use to configure the endpoints to configure your relays

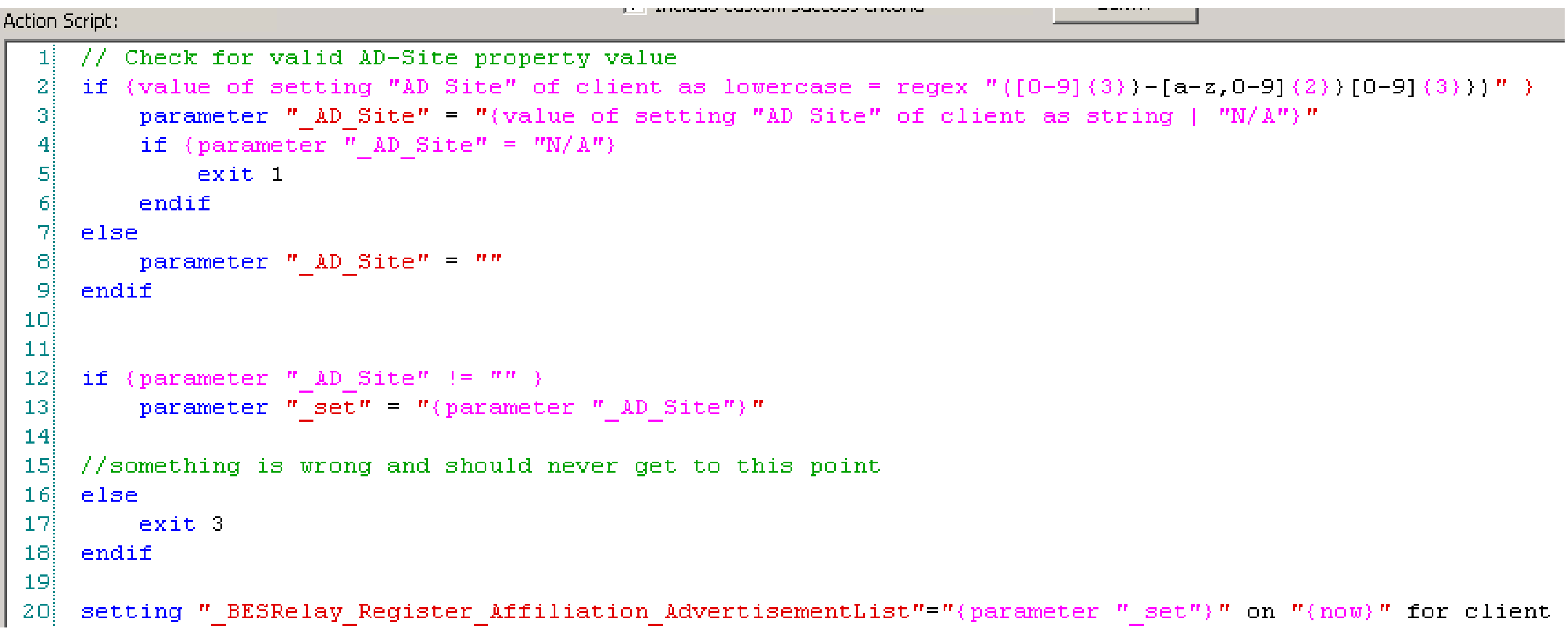
Affiliation_AdvertisementList Fixlet



● Computers which match all of the relevance clauses below

```
1. not exists main gather service
2.
3.
4.
5.
and
```

Affiliation_AdvertisementList Fixlet



Action Script:

```
// Check for valid AD-Site property value
if {value of setting "AD Site" of client as lowercase = regex "([0-9]{3})-[a-z,0-9]{2})[0-9]{3}))" }
    parameter "_AD_Site" = "{value of setting "AD Site" of client as string | "N/A"}"
    if {parameter "_AD_Site" = "N/A"}
        exit 1
    endif
else
    parameter "_AD_Site" = ""
endif


if {parameter "_AD_Site" != "" }
    parameter "_set" = "{parameter "_AD_Site"}"

//something is wrong and should never get to this point
else
    exit 3
endif

setting "_BESRelay_Register_Affiliation_AdvertisementList"="{parameter "_set"}" on "{now}" for client
```

Methods NOT to use

- Ggroup membership to trigger SeekList update
  - Groups don’t update quick enough
  - Faster to update if you build the logic in Relevance

Affiliation Obstacles

- Client loop times
  - Long Loop times prevent SeekList update
- Content delivery race conditions
  - Files being downloaded before SeekList/Relay update
- Action Prioritization
  - Guaranteed action evaluation times (every X minutes)
- Should be built into the core client functionality?

Published Fixlets

- https://bigfix.me/user/masonje
- Client Seek List
  - https://bigfix.me/fixlet/details/23802
- Set AD Site property
  - https://bigfix.me/fixlet/details/23805
- Contact: jon.mason@kroger.com

Questions