```
# MZ2POL-04: Policies and Boundaries

> **Series:** MZ2POL | **Notebook:** 5 of 8 | **Created:** December 2025

## Overview

This notebook provides a comprehensive guide to **IAM Policies** and **Policy
Boundaries** - the two components that together replace Management Zone
access control. Policies define **WHAT** users can do, while boundaries
define **WHERE** those permissions apply.

## Prerequisites

- Completed MZ2POL-01 through MZ2POL-03
- Access to Dynatrace Account Management
- Policy Management permissions

## Learning Objectives

By the end of this notebook, you will:
1. Understand policy statement syntax and structure
2. Know the default policies and when to use them
3. Understand boundary syntax and how boundaries restrict policies
4. Be able to map MZ access patterns to policy + boundary combinations
5. Know the recommended group-policy-boundary structure for SAML/AD
integration

---

## 1. Understanding the Relationship

### Policies vs Boundaries

![Policy Boundary Relationship]
```

(data:image/svg+xml;base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdm
ciIHZpZXdCb3g9IjAgMCA4MDAgMzQwIj4KICA8ZGVmcz4KICAgIDxsaW5lYXJHcmFkaWVudCBpZD0
icG9saWN5T25seUdyYWQiIHgxPSIwJSIgeTE9IjAlIiB4Mj0iMTAwJSIgeTI9IjAlIj4KICAgICAg
PHN0b3Agb2Zmc2V0PSIwJSIgc3R5bGU9InN0b3AtY29sb3I6IzNiODJmNjtzdG9wLW9wYWNpdHk6M
SIgLz4KICAgICAgPHN0b3Agb2Zmc2V0PSIxMDAlIiBzdHlsZT0ic3RvcC1jb2xvcjojMjU2M2ViO3
N0b3Atb3BhY2l0eToxIiAvPgogICAgPC9saW5lYXJHcmFkaWVudD4KICAgIDxsaW5lYXJHcmFkaWV
udCBpZD0iYm91bmRlZEdyYWQiIHgxPSIwJSIgeTE9IjAlIiB4Mj0iMTAwJSIgeTI9IjAlIj4KICAg
ICAgPHN0b3Agb2Zmc2V0PSIwJSIgc3R5bGU9InN0b3AtY29sb3I6I2VjNDg5OTtzdG9wLW9wYWNpd
Hk6MSIgLz4KICAgICAgPHN0b3Agb2Zmc2V0PSIxMDAlIiBzdHlsZT0ic3RvcC1jb2xvcjojZGIyNz
c3O3N0b3Atb3BhY2l0eToxIiAvPgogICAgPC9saW5lYXJHcmFkaWVudD4KICAgIDxmaWx0ZXIgaWQ
9InBiU2hhZG93Ij4KICAgICAgPGZlRHJvcFNoYWRvdyBkeD0iMSIgZHk9IjEiIHN0ZERldmlhdGlv
bj0iMiIgZmxvb2Qtb3BhY2l0eT0iMC4xNSIvPgogICAgPC9maWx0ZXI+CiAgPC9kZWZzPgoKICA8I
S0tIEJhY2tncm91bmQgLS0+CiAgPHJlY3Qgd2lkdGg9IjgwMCIgaGVpZ2h0PSIzNDAiIGZpbGw9Ii

```
NmOGY5ZmEiIHJ4PSIxMCIvPgoKICA8IS0tIFRpdGxlIC0tPgogIDx0ZXh0IHg9IjQwMCIgeT0iMjg
iIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxOCIgZm9udC13ZWln
aHQ9ImJvbGQiIGZpbGw9IiMzMzMiIHRleHQtYW5jaG9yPSJtaWRkbGUiPlBvbGljeSArIEJvdW5kY
XJ5IFJlbGF0aW9uc2hpcDwvdGV4dD4KICA8dGV4dCB4PSI0MDAiIHk9IjQ4IiBmb250LWZhbWlseT
0iQXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTIiIGZpbGw9IiM2NjYiIHRleHQtYW5jaG9
yPSJtaWRkbGUiPlBvbGljaWVzIGRlZmluZSBXSEFULCBCb3VuZGFyaWVzIHJlc3RyaWN0IFdIRVJF
PC90ZXh0PgoKICA8IS0tIFdpdGhvdXQgQm91bmRhcnkgU2VjdGlvbiAtLT4KICA8cmVjdCB4PSIzM
CIgeT0iNzAiIHdpZHRoPSIzNTUiIGhlaWdodD0iMTMwIiByeD0iOCIgZmlsbD0iI2ZmZiIgc3Ryb2
tlPSIjM2I4MmY2IiBzdHJva2Utd2lkdGg9IjIiIGZpbHRlcj0idXJsKCNwYlNoYWRvdykiLz4KICA
8cmVjdCB4PSIzMCIgeT0iNzAiIHdpZHRoPSIzNTUiIGhlaWdodD0iMzAiIHJ4PSI4IiBmaWxsPSJ1
cmwoI3BvbGljeU9ubHlHcmFkKSIvPgogIDx0ZXh0IHg9IjIwNyIgeT0iOTAiIGZvbnQtZmFtaWx5P
SJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMiIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbG
w9IndoaXRlIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5XaXRob3V0IEJvdW5kYXJ5PC90ZXh0PgoKICA
8cmVjdCB4PSI1MCIgeT0iMTE1IiB3aWR0aD0iMzE1IiBoZWlnaHQ9IjM1IiByeD0iNCIgZmlsbD0i
I2RiZWFmZSIvPgogIDx0ZXh0IHg9IjIwNyIgeT0iMTM4IiBmb250LWZhbWlseT0ibW9ub3NwYWNlI
iBmb250LXNpemU9IjExIiBmaWxsPSIjMWU0MGFmIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5Qb2xpY3
k6IEFMTE9XIHN0b3JhZ2U6bG9nczpyZWFkPC90ZXh0PgoKICA8dGV4dCB4PSIyMDciIHk9IjE3NSI
gZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjExIiBmaWxsPSIjMzMz
IiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5SZXN1bHQ6IEFjY2VzcyB0byBBTEwgbG9ncyBpbiBlbnZpc
m9ubWVudDwvdGV4dD4KICA8cmVjdCB4PSI4MCIgeT0iMTgyIiB3aWR0aD0iMjU0IiBoZWlnaHQ9Ij
giIHJ4PSI0IiBmaWxsPSIjM2I4MmY2Ii8+CgogIDwhLS0gV2l0aCBCb3VuZGFyeSBTZWN0aW9uIC0
tPgogIDxyZWN0IHg9IjQxNSIgeT0iNzAiIHdpZHRoPSIzNTUiIGhlaWdodD0iMTMwIiByeD0iOCIg
ZmlsbD0iI2ZmZiIgc3Ryb2tlPSIjZWM0ODk5IiBzdHJva2Utd2lkdGg9IjIiIGZpbHRlcj0idXJsK
CNwYlNoYWRvdykiLz4KICA8cmVjdCB4PSI0MTUiIHk9IjcwIiB3aWR0aD0iMzU1IiBoZWlnaHQ9Ij
MwIiByeD0iOCIgZmlsbD0idXJsKCNib3VuZGVkR3JhZCkiLz4KICA8dGV4dCB4PSI1OTIiIHk9Ijk
wIiBmb250LWZhbWlseT0iQXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTIiIGZvbnQtd2Vp
Z2h0PSJib2xkIiBmaWxsPSJ3aGl0ZSIgdGV4dC1hbmNob3I9Im1pZGRsZSI+V2l0aCBCb3VuZGFye
TwvdGV4dD4KCiAgPHJlY3QgeD0iNDM1IiB5PSIxMTAiIHdpZHRoPSIzMTUiIGhlaWdodD0iMjUiIH
J4PSI0IiBmaWxsPSIjZGJlYWZlIi8+CiAgPHRleHQgeD0iNTkyIiB5PSIxMjgiIGZvbnQtZmFtaWx
5PSJtb25vc3BhY2UiIGZvbnQtc2l6ZT0iMTAiIGZpbGw9IiMxZTQwYWYiIHRleHQtYW5jaG9yPSJt
aWRkbGUiPlBvbGljeTogQUxMT1cgc3RvcmFnZTpsb2dzOnJlYWQ8L3RleHQ+CgogIDxyZWN0IHg9I
jQzNSIgeT0iMTQwIiB3aWR0aD0iMzE1IiBoZWlnaHQ9IjI1IiByeD0iNCIgZmlsbD0iI2ZjZTdmMy
IvPgogIDx0ZXh0IHg9IjU5MiIgeT0iMTU4IiBmb250LWZhbWlseT0ibW9ub3NwYWNlIiBmb250LXN
pemU9IjEwIiBmaWxsPSIjOWQxNzRkIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5Cb3VuZGFyeTogc2Vj
dXJpdHlfY29udGV4dCA9ICJ0ZWFtLWEiPC90ZXh0PgoKICA8dGV4dCB4PSI1OTIiIHk9IjE4NSIgZ
m9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjExIiBmaWxsPSIjMzMzIi
B0ZXh0LWFuY2hvcj0ibWlkZGxlIj5SZXN1bHQ6IEFjY2VzcyB0byB0ZWFtLWEgbG9ncyBPTkxZPC9
0ZXh0PgogIDxyZWN0IHg9IjUyMCIgeT0iMTkwIiB3aWR0aD0iMTQ0IiBoZWlnaHQ9IjgiIHJ4PSI0
IiBmaWxsPSIjZWM0ODk5Ii8+CgogIDwhLS0gVGhyZWUgRG9tYWlucyBTZWN0aW9uIC0tPgogIDxyZ
WN0IHg9IjMwIiB5PSIyMTUiIHdpZHRoPSI3NDAiIGhlaWdodD0iMTEwIiByeD0iOCIgZmlsbD0iI2
ZmZiIgc3Ryb2tlPSIjZTJlOGYwIiBzdHJva2Utd2lkdGg9IjIiLz4KICA8dGV4dCB4PSI0MDAiIHk
9IjIzOCIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjEyIiBmb250
LXdlaWdodD0iYm9sZCIgZmlsbD0iIzMzMyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+Q29tcGxldGUgT
VogUmVwbGFjZW1lbnQ6IFVzZSBBbGwgVGhyZWUgRG9tYWlucyBpbiBCb3VuZGFyeTwvdGV4dD4KCi
AgPCEtLSBEb21haW4gYm94ZXMgLS0+CiAgPHJlY3QgeD0iNTUiIHk9IjI1NSIgd2lkdGg9IjIyMCI
gaGVpZ2h0PSI1NSIgcng9IjYiIGZpbGw9IiNmZWYzYzciIHN0cm9rZT0iI2Y1OWUwYiIgc3Ryb2tl
LXdpZHRoPSIxIi8+CiAgPHRleHQgeD0iMTY1IiB5PSIyNzUiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc
2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMCIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IiM5MjQwMG
```

```
UiIHRleHQtYW5jaG9yPSJtaWRkbGUiPmVudmlyb25tZW50Om1hbmFnZW1lbnQtem9uZTwvdGV4dD4
KICA8dGV4dCB4PSIxNjUiIHk9IjI5NSIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBm
b250LXNpemU9IjEwIiBmaWxsPSIjOTI0MDBlIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5DbGFzc2ljI
GVudGl0eSBhY2Nlc3M8L3RleHQ+CgogIDxyZWN0IHg9IjI5MCIgeT0iMjU1IiB3aWR0aD0iMjIwIi
BoZWlnaHQ9IjU1IiByeD0iNiIgZmlsbD0iI2RiZWFmZSIgc3Ryb2tlPSIjM2I4MmY2IiBzdHJva2U
td2lkdGg9IjEiLz4KICA8dGV4dCB4PSI0MDAiIHk9IjI3NSIgZm9udC1mYW1pbHk9IkFyaWFsLCBz
YW5zLXNlcmlmIiBmb250LXNpemU9IjEwIiBmb250LXdlaWdodD0iYm9sZCIgZmlsbD0iIzFlNDBhZ
iIgdGV4dC1hbmNob3I9Im1pZGRsZSI+c3RvcmFnZTpkdC5zZWN1cml0eV9jb250ZXh0PC90ZXh0Pg
ogIDx0ZXh0IHg9IjQwMCIgeT0iMjk1IiBmb250LWZhbWlseT0iQXJpYWwsIHNhbnMtc2VyaWYiIGZ
vbnQtc2l6ZT0iMTAiIGZpbGw9IiMxZTQwYWYiIHRleHQtYW5jaG9yPSJtaWRkbGUiPkdyYWlsIGRh
dGEgKGxvZ3MsIHNwYW5zLCBtZXRyaWNzKTwvdGV4dD4KCiAgPHJlY3QgeD0iNTI1IiB5PSIyNTUiI
HdpZHRoPSIyMjAiIGhlaWdodD0iNTUiIHJ4PSI2IiBmaWxsPSIjZmNlN2YzIiBzdHJva2U9IiNlYz
Q4OTkiIHN0cm9rZS13aWR0aD0iMSIvPgogIDx0ZXh0IHg9IjYzNSIgeT0iMjc1IiBmb250LWZhbWl
seT0iQXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTAiIGZvbnQtd2VpZ2h0PSJib2xkIiBm
aWxsPSIjOWQxNzRkIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5zZXR0aW5nczpkdC5zZWN1cml0eV9jb
250ZXh0PC90ZXh0PgogIDx0ZXh0IHg9IjYzNSIgeT0iMjk1IiBmb250LWZhbWlseT0iQXJpYWwsIH
NhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTAiIGZpbGw9IiM5ZDE3NGQiIHRleHQtYW5jaG9yPSJtaWR
kbGUiPlNldHRpbmdzIG9iamVjdHM8L3RleHQ+Cjwvc3ZnPgo=)
```

```
| Component | Purpose | Analogy |
|-----------|---------|--------|
| **Policy** | Defines WHAT actions are allowed | "You can read logs" |
| **Boundary** | Defines WHERE policies apply | "...but only for team-
frontend" |

### How They Work Together

![Policy vs Boundary]
```

```
(data:image/svg+xml;base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdm
ciIHZpZXdCb3g9IjAgMCA3MDAgMzQwIj4KICA8ZGVmcz4KICAgIDxsaW5lYXJHcmFkaWVudCBpZD0
icHZiSGVhZGVyR3JhZCIgeDE9IjAlIiB5MT0iMCUiIHgyPSIxMDAlIiB5Mj0iMCUiPgogICAgICA8
c3RvcCBvZmZzZXQ9IjAlIiBzdHlsZT0ic3RvcC1jb2xvcjojM2I4MmY2O3N0b3Atb3BhY2l0eToxI
iAvPgogICAgICA8c3RvcCBvZmZzZXQ9IjEwMCUiIHN0eWxlPSJzdG9wLWNvbG9yOiMxZDRlZDg7c3
RvcC1vcGFjaXR5OjEiIC8+CiAgICA8L2xpbmVhckdyYWRpZW50PgogICAgPGxpbmVhckdyYWRpZW5
0IGlkPSJwdmJXYXJuR3JhZCIgeDE9IjAlIiB5MT0iMCUiIHgyPSIxMDAlIiB5Mj0iMTAwJSI+CiAg
ICAgIDxzdG9wIG9mZnNldD0iMCUiIHN0eWxlPSJzdG9wLWNvbG9yOiNmNTllMGI7c3RvcC1vcGFja
XR5OjEiIC8+CiAgICAgIDxzdG9wIG9mZnNldD0iMTAwJSIgc3R5bGU9InN0b3AtY29sb3I6I2Q5Nz
cwNjtzdG9wLW9wYWNpdHk6MSIgLz4KICAgIDwvbGluZWFyR3JhZGllbnQ+CiAgICA8bGluZWFyR3J
hZGllbnQgaWQ9InB2Ykdvb2RHcmFkIiB4MT0iMCUiIHkxPSIwJSIgeDI9IjEwMCUiIHkyPSIxMDAl
Ij4KICAgICAgPHN0b3Agb2Zmc2V0PSIwJSIgc3R5bGU9InN0b3AtY29sb3I6IzEwYjk4MTtzdG9wL
W9wYWNpdHk6MSIgLz4KICAgICAgPHN0b3Agb2Zmc2V0PSIxMDAlIiBzdHlsZT0ic3RvcC1jb2xvcj
ojMDU5NjY5O3N0b3Atb3BhY2l0eToxIiAvPgogICAgPC9saW5lYXJHcmFkaWVudD4KICAgIDxmaWx
0ZXIgaWQ9InB2YlNoYWRvdyI+CiAgICAgIDxmZURyb3BTaGFkb3cgZHg9IjIiIGR5PSIyIiBzdGRE
ZXZpYXRpb249IjMiIGZsb29kLW9wYWNpdHk9IjAuMTUiLz4KICAgIDwvZmlsdGVyPgogICAgPG1hc
mtlciBpZD0icHZiQXJyb3ciIG1hcmtlcldpZHRoPSIxMCIgbWFya2VySGVpZ2h0PSI3IiByZWZYPS
I5IiByZWZZPSIzLjUiIG9yaWVudD0iYXV0byI+CiAgICAgIDxwb2x5Z29uIHBvaW50cz0iMCAwLCA
```

```
xMCAzLjUsIDAgNyIgZmlsbD0iIzY0NzQ4YiIvPgogICAgPC9tYXJrZXI+CiAgPC9kZWZzPgoKICA8
IS0tIEJhY2tncm91bmQgLS0+CiAgPHJlY3Qgd2lkdGg9IjcwMCIgaGVpZ2h0PSIzNDAiIGZpbGw9I
iNmOGY5ZmEiIHJ4PSIxMCIvPgoKICA8IS0tIFRpdGxlIC0tPgogIDx0ZXh0IHg9IjM1MCIgeT0iMz
IiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIC1hcHBsZS1zeXN0ZW0sIHNhbnMtc2VyaWYiIGZvbnQ
tc2l6ZT0iMTgiIGZvbnQtd2VpZ2h0PSJib2xkIiBmaWxsPSIjMWUyOTNiIiB0ZXh0LWFuY2hvcj0i
bWlkZGxlIj5Qb2xpY3kgdnMuIFBvbGljeSArIEJvdW5kYXJ5PC90ZXh0PgogIDx0ZXh0IHg9IjM1M
CIgeT0iNTIiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIC1hcHBsZS1zeXN0ZW0sIHNhbnMtc2VyaW
YiIGZvbnQtc2l6ZT0iMTIiIGZpbGw9IiM2NDc0OGIiIHRleHQtYW5jaG9yPSJtaWRkbGUiPlVuZGV
yc3RhbmRpbmcgaG93IGJvdW5kYXJpZXMgcmVzdHJpY3QgcG9saWN5IHNjb3BlPC90ZXh0PgoKICA8
IS0tIExlZnQgQm94OiBXaXRob3V0IEJvdW5kYXJ5IChXYXJuaW5nKSAtLT4KICA8cmVjdCB4PSI0M
CIgeT0iNzUiIHdpZHRoPSIyOTAiIGhlaWdodD0iMjMwIiByeD0iMTAiIGZpbGw9IiNmZmYyIiIHN0cm
9rZT0iI2Y1OWUwYiIgc3Ryb2tlLXdpZHRoPSIyIiBmaWx0ZXI9InVybCgjcHZiU2hhZG93KSIvPgo
KICA8IS0tIExlZnQgSGVhZGVyIC0tPgogIDxyZWN0IHg9IjQwIiB5PSI3NSIgd2lkdGg9IjI5MCIg
aGVpZ2h0PSI0NSIgcng9IjEwIiBmaWxsPSJ1cmwoI3B2Yldhcm5HcmFkKSIvPgogIDxyZWN0IHg9I
jQwIiB5PSIxMDUiIHdpZHRoPSIyOTAiIGhlaWdodD0iMTUiIGZpbGw9InVybCgjcHZiV2FybkdyYW
QpIi8+CiAgPHRleHQgeD0iNjAiIHk9IjEwMyIgZm9udC1mYW1pbHk9InN5c3RlbS11aSwgc2Fucy1
zZXJpZiIgZm9udC1zaXplPSIxNCIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IiNmZmYiPldpdGhv
dXQgQm91bmRhcnk8L3RleHQ+CiAgPHRleHQgeD0iMzAwIiB5PSIxMDMiIGZvbnQtZmFtaWx5PSJze
XN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTYiIGZpbGw9IiNmZmYiIHRleHQtYW5jaG
9yPSJlbmQiPuKaoO+4jzwvdGV4dD4KCiAgPCEtLSBMZWZ0IENvbnRlbnQgLS0+CiAgPHRleHQgeD0
iNjAiIHk9IjE1MCIgZm9udC1mYW1pbHk9InN5c3RlbS11aSwgc2Fucy1zZXJpZiIgZm9udC1zaXpl
PSIxMyIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IiMxZTI5M2IiPlBvbGljeTo8L3RleHQ+CiAgP
HJlY3QgeD0iNjAiIHk9IjE2MCIgd2lkdGg9IjI1MCIgaGVpZ2h0PSIzNSIgcng9IjYiIGZpbGw9Ii
NmZWYzYzciLz4KICA8dGV4dCB4PSI3NSIgeT0iMTgzIiBmb250LWZhbWlseT0ibW9ub3NwYWNlIiB
mb250LXNpemU9IjEyIiBmaWxsPSIjOTI0MDBlIj5BTExPVyBsb2dzOnJlYWQ8L3RleHQ+CgogIDx0
ZXh0IHg9IjYwIiB5PSIyMjAiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvb
nQtc2l6ZT0iMTMiIGZvbnQtd2VpZ2h0PSJib2xkIiBmaWxsPSIjMWUyOTNiIj5SZXN1bHQ6PC90ZX
h0PgogIDxyZWN0IHg9IjYwIiB5PSIyMzAiIHdpZHRoPSIyNTAiIGhlaWdodD0iNTUiIHJ4PSI2IiB
maWxsPSIjZmVmOWMzIiBzdHJva2U9IiNmZGUwNDciIHN0cm9rZS13aWR0aD0iMSIvPgogIDx0ZXh0
IHg9Ijc1IiB5PSIyNTUiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQtc
2l6ZT0iMTIiIGZpbGw9IiM4NTRkMGUiPkFjY2VzcyB0byBBTEwgbG9ncyBpbiBlbnZpcm9ubWVudD
wvdGV4dD4KICA8dGV4dCB4PSI3NSIgeT0iMjc1IiBmb250LWZhbWlseT0ic3lzdGVtLXVpLCBzYW5
zLXNlcmlmIiBmb250LXNpemU9IjExIiBmaWxsPSIjYTE2MjA3Ij5ObyByZXN0cmljdGlvbnMgb24g
d2hpY2ggbG9ncyBjYW4gYmUgcmVhZDwvdGV4dD4KCiAgPCEtLSBSaWdodCBCb3g6IFdpdGggQm91b
mRhcnkgKEdvb2QpIC0tPgogIDxyZWN0IHg9IjM3MCIgeT0iNzUiIHdpZHRoPSIyOTAiIGhlaWdodD
0iMjMwIiByeD0iMTAiIGZpbGw9IiNmZmYiIHN0cm9rZT0iIzEwYjk4MSIgc3Ryb2tlLXdpZHRoPSI
yIiBmaWx0ZXI9InVybCgjcHZiU2hhZG93KSIvPgoKICA8IS0tIFJpZ2h0IEhlYWRlciAtLT4KICA8
cmVjdCB4PSIzNzAiIHk9Ijc1IiB3aWR0aD0iMjkwIiBoZWlnaHQ9IjQ1IiByeD0iMTAiIGZpbGw9I
nVybCgjcHZiR29vZEdyYWQpIi8+CiAgPHJlY3QgeD0iMzcwIiB5PSIxMDUiIHdpZHRoPSIyOTAiIG
hlaWdodD0iMTUiIGZpbGw9InVybCgjcHZiR29vZEdyYWQpIi8+CiAgPHRleHQgeD0iMzkwIiB5PSI
xMDMiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTQiIGZv
bnQtd2VpZ2h0PSJib2xkIiBmaWxsPSIjZmZmIj5XaXRoIEJvdW5kYXJ5PC90ZXh0PgogIDx0ZXh0I
Hg9IjYzMCIgeT0iMTAzIiBmb250LWZhbWlseT0ic3lzdGVtLXVpLCBzYW5zLXNlcmlmIiBmb250LX
NpemU9IjE2IiBmaWxsPSIjZmZmIiB0ZXh0LWFuY2hvcj0iZW5kIj7inJM8L3RleHQ+CgogIDwhLS0
gUmlnaHQgQ29udGVudCAtLT4KICA8dGV4dCB4PSIzOTAiIHk9IjE1MCIgZm9udC1mYW1pbHk9InN5
c3RlbS11aSwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMyIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpb
Gw9IiMxZTI5M2IiPlBvbGljeTo8L3RleHQ+CiAgPHJlY3QgeD0iMzkwIiB5PSIxNjAiIHdpZHRoPS
IyNTAiIGhlaWdodD0iMzUiIHJ4PSI2IiBmaWxsPSIjZGNmY2U3Ii8+CiAgPHRleHQgeD0iNDA1IiB
```

5PSIxODMiIGZvbnQtZmFtaWx5PSJtb25vc3BhY2UiIGZvbnQtc2l6ZT0iMTIiIGZpbGw9IiMxNjY1
MzQiPkFMTE9XIGxvZ3M6cmVhZDwvdGV4dD4KCiAgPHRleHQgeD0iMzkwIiB5PSIyMjAiIGZvbnQtZ
mFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTMiIGZvbnQtd2VpZ2h0PS
Jib2xkIiBmaWxsPSIjMWUyOTNiIj5Cb3VuZGFyeTo8L3RleHQ+CiAgPHJlY3QgeD0iMzkwIiB5PSI
yMzAiIHdpZHRoPSIyNTAiIGhlaWdodD0iMzAiIHJ4PSI2IiBmaWxsPSIjZDFmYWU1Ii8+CiAgPHRl
eHQgeD0iNDA1IiB5PSIyNTAiIGZvbnQtZmFtaWx5PSJtb25vc3BhY2UiIGZvbnQtc2l6ZT0iMTEiI
GZpbGw9IiMxNjY1MzQiPnNlY3VyaXR5X2NvbnRleHQgPSAidGVhbS1hIjwvdGV4dD4KCiAgPHRleH
QgeD0iMzkwIiB5PSIyODAiIGZvbnQtZmFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQ
tc2l6ZT0iMTMiIGZvbnQtd2VpZ2h0PSJib2xkIiBmaWxsPSIjMWUyOTNiIj5SZXN1bHQ6PC90ZXh0
PgogIDx0ZXh0IHg9IjM5MCIgeT0iMjk4IiBmb250LWZhbWlseT0ic3lzdGVtLXVpLCBzYW5zLXNlc
mlmIiBmb250LXNpemU9IjEyIiBmaWxsPSIjMTU4MDNkIj5BY2Nlc3MgdG8gdGVhbS1hIGxvZ3MgT0
5MWTwvdGV4dD4KCiAgPCEtLSBBcnJvdyBpbiBtaWRkbGUgLS0+CiAgPGxpbmUgeDE9IjM0MCIgeTE
9IjE5MCIgeDI9IjM2MCIgeTI9IjE5MCIgc3Ryb2tlPSIjNjQ3NDhiIiBzdHJva2Utd2lkdGg9IjIi
IG1hcmtlci1lbmQ9InVybCgjcHZiQXJyb3cpIi8+CiAgPHRleHQgeD0iMzUwIiB5PSIxNzUiIGZvb
nQtZmFtaWx5PSJzeXN0ZW0tdWksIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTAiIGZpbGw9IiM2ND
c0OGIiIHRleHQtYW5jaG9yPSJtaWRkbGUiPmFkZDwvdGV4dD4KCiAgPCEtLSBCb3R0b20gZXhwbGF
uYXRpb24gLS0+CiAgPHJlY3QgeD0iNDAiIHk9IjMxNSIgd2lkdGg9IjYyMCIgaGVpZ2h0PSIyMCIg
cng9IjQiIGZpbGw9IiNlMGYyZmUiLz4KICA8dGV4dCB4PSIzNTAiIHk9IjMzMCIgZm9udC1mYW1pb
Hk9InN5c3RlbS11aSwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMSIgZmlsbD0iIzAzNjlhMSIgdG
V4dC1hbmNob3I9Im1pZGRsZSI+Qm91bmRhcmllcyByZXN0cmljdCBXSEFUIGRhdGEgYSBwb2xpY3k
gYXBwbGllcyB0by4gUG9saWNpZXMgZGVmaW5lIFdIQVQgYWN0aW9ucyBhcmUgYWxsb3dlZC48L3Rl
eHQ+Cjwvc3ZnPgo=)

### Key Characteristics

Policies:
- Define permissions (ALLOW statements)
- Can include conditions (WHERE clauses)
- Default policies cover most use cases

Boundaries:
- Separate from policies (decoupled)
- Reusable across multiple policies
- Can only narrow permissions, never expand
- Optional - policies work without them (full scope)

## 2. Policy Fundamentals

### Policy Statement Structure

```
 :: [WHERE ]
```

~~~
| Component | Description | Examples |
|-----------|-------------|----------|
| **Effect** | Permission type | `ALLOW` (only option currently) |
| **Service** | Dynatrace service | `storage`, `settings`, `app` |
| **Resource** | Resource type | `logs`, `buckets`, `objects` |
| **Action** | Operation | `read`, `write`, `delete` |
| **Condition** | Optional filter | `WHERE field = "value"` |

### Basic Policy Statements

```
// Grant read access to all logs
ALLOW storage:logs:read

// Grant read/write to buckets
ALLOW storage:buckets:read
ALLOW storage:buckets:write

// Grant all actions on a resource
ALLOW storage:logs:*
```

### Common Services and Resources

| Service | Resources | Common Actions |
|---------|-----------|----------------|
| `storage` | `logs`, `spans`, `events`, `metrics`, `buckets` | `read`, `write`, `delete` |
| `settings` | `objects`, `schemas` | `read`, `write`, `delete` |
| `app` | `apps`, `functions` | `run`, `install` |
| `automation` | `workflows` | `read`, `write`, `run` |
| `document` | `documents` | `read`, `write`, `delete`, `share` |

---

## 3. Default Policies

Dynatrace provides **default policies** that cover common access patterns. These are **read-only** but cover most use cases.

### Dynatrace Access Policies

| Policy | Use Case | Key Permissions |
|--------|----------|-----------------|
| **Dynatrace Viewer** | Read-only access | View dashboards, data, settings |
| **Dynatrace Operator** | Basic operations | Viewer + create dashboards, notebooks |
| **Dynatrace Standard User** | Regular users | Operator + modify some
~~~

~~~
settings |
| **Dynatrace Professional User** | Power users | Standard + advanced
features |
| **Dynatrace Admin User** | Administrators | Full platform access |

### Data Access Policies

| Policy | Use Case | Key Permissions |
|--------|----------|----------------|
| **Data Viewer** | Read monitored data | Query logs, metrics, traces |
| **Data Editor** | Modify data configs | Viewer + data configuration |

### Choosing the Right Default Policy

```
User Type              → Dynatrace Policy       + Data Policy
─────────────────────────────────────────────────────────────
Executives/Viewers     → Dynatrace Viewer       + Data Viewer
Developers             → Dynatrace Standard     + Data Viewer
SRE/Operations         → Dynatrace Professional + Data Editor
Platform Admins        → Dynatrace Admin        + Data Editor
```

---

## 4. Condition and Boundary Syntax

Policies and boundaries share the same condition syntax.

### Supported Operators

| Operator | Description | Example |
|----------|-------------|----------|
| `=` | Exact match | `field = "value"` |
| `!=` | Not equal | `field != "value"` |
| `startsWith` | Prefix match | `field startsWith "prefix"` |
| `in` | Value in list | `field in ("a", "b", "c")` |
| `IN` | Value in list (alternative) | `field IN ("a", "b")` |

### Supported Fields

| Field | Description | Used In |
|-------|-------------|----------|
| `environment` | Environment restrictions | Boundaries |
| `environment:name` | Environment by name | Boundaries |
| `environment:management-zone` | MZ-based (transitional) | Boundaries |
| `storage:dt.security_context` | Security context | Both |
| `storage:bucket` | Grail bucket | Both |
~~~

~~~
| `settings:schemaId` | Settings schema ID | Policies |
| `settings:dt.security_context` | Settings security context | Boundaries |

### Combining Conditions

**AND logic** (all conditions must match):
```
ALLOW storage:logs:read
  WHERE storage:dt.security_context = "team-a"
  AND storage:bucket = "production_logs"
```

**OR logic** (multiple statements or lines):
```
// In policies: Multiple statements
ALLOW storage:logs:read WHERE storage:dt.security_context = "team-a"
ALLOW storage:logs:read WHERE storage:dt.security_context = "team-b"

// In boundaries: Each line is OR-combined
storage:dt.security_context = "team-a"
storage:dt.security_context = "team-b"
```

---

## 5. Creating Boundaries

### Via UI

1. Navigate to **Account Management** → **Identity & Access Management**
2. Select **Policy Boundaries** → **Boundaries** tab
3. Click **Create boundary**
4. Enter:
   - **Boundary name**: Descriptive name
   - **Boundary query**: Restriction conditions
5. Click **Save**

### Boundary Examples

**Team-Based Boundary:**
```
Name: Frontend Team Scope
Query: storage:dt.security_context = "team-frontend"
```

**Environment Boundary:**
```
Name: Production Only
~~~

~~~
Query: storage:dt.security_context startsWith "prod-"
```

**Multi-Team Boundary (OR logic):**
```
Name: Platform Teams
Query:
storage:dt.security_context = "team-infra"
storage:dt.security_context = "team-sre"
storage:dt.security_context = "team-platform"
```

### Boundary Limitations

| Limitation | Description | Workaround |
|------------|-------------|------------|
| Max 10 lines | Only 10 conditions per boundary | Create multiple boundaries |
| No AND in lines | Each line is one condition | Use multiple boundaries for AND |
| No complex expressions | Limited to basic operators | Simplify conditions |

---

## 6. Best Practice: Complete Boundary for MZ Restriction

When restricting access to replicate a Management Zone, use **all three domains** in your boundary query:

```
environment:management-zone IN ("LOB5");
storage:dt.security_context IN ("LOB5");
settings:dt.security_context IN ("LOB5");
```

### Why All Three Domains?

| Domain | What It Restricts |
|--------|-------------------|
| `environment:management-zone` | Classic entity access (hosts, services, processes) |
| `storage:dt.security_context` | Grail data (logs, spans, metrics, events) |
| `settings:dt.security_context` | Settings objects |

Using only one domain leaves gaps in access control. For complete MZ replacement, include all three.

---
~~~

~~~~
## 7. Recommended Group–Policy–Boundary Structure

For organizations using SAML/SSO with Active Directory, this structure
provides clear separation of duties:

```
Group: "LOB5-Team" (SAML from Active Directory)
├── Policy: Dynatrace Viewer (standard read access)
└── Policy: Dynatrace Professional
    └── Boundary:
        environment:management-zone IN ("LOB5");
        storage:dt.security_context IN ("LOB5");
        settings:dt.security_context IN ("LOB5");
```

### Key Benefits

- **SAML Group**: Ties to existing AD group membership — no separate user
management
- **Standard User Policy**: Provides baseline access without boundary (if
needed)
- **Pro User + Boundary**: Advanced permissions restricted to team's scope

### Alternative: All Policies with Boundary

For stricter isolation, apply the boundary to all policies:

```
Group: "LOB5-Team" (SAML from AD)
├── Policy: Dynatrace Viewer
│   └── Boundary: LOB5-Scope
└── Policy: Dynatrace Professional
    └── Boundary: LOB5-Scope
```

### Binding via UI

1. Navigate to **Group Management**
2. Select or create a group
3. Go to **Permissions** tab
4. Click **Add permission**
5. Select:
   - **Policy**: Choose policy to bind
   - **Boundary** (optional): Select restriction
   - **Environment**: Select target environment
6. Click **Save**
~~~~

```
---

## 8. Mapping MZ Access to Policies + Boundaries

### Common MZ Permission Patterns

![MZ Pattern Mapping]
```

```
(data:image/svg+xml;base64,PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdm
ciIHZpZXdCb3g9IjAgMCA4MDAgMzYwIj4KICA8ZGVmcz4KICAgIDxsaW5lYXJHcmFkaWVudCBpZD0
ibXpHcmFkIiB4MT0iMCUiIHkxPSIwJSIgeDI9IjEwMCUiIHkyPSIwJSI+CiAgICAgIDxzdG9wIG9m
ZnNldD0iMCUiIHN0eWxlPSJzdG9wLWNvbG9yOiNmNTllMGI7c3RvcC1vcGFjaXR5OjEiIC8+CiAgI
CAgIDxzdG9wIG9mZnNldD0iMTAwJSIgc3R5bGU9InN0b3AtY29sb3I6I2Q5NzcwNjtzdG9wLW9wYW
NpdHk6MSIgLz4KICAgIDwvbGluZWFyR3JhZGllbnQ+CiAgICA8bGluZWFyR3JhZGllbnQgaWQ9Im5
ld01vZGVsR3JhZCIgeDE9IjAlIiB5MT0iMCUiIHgyPSIxMDAlIiB5Mj0iMCUiPgogICAgICA8c3Rv
cCBvZmZzZXQ9IjAlIiBzdHlsZT0ic3RvcC1jb2xvcjojMjJjNTVlO3N0b3Atb3BhY2l0eToxIiAvP
gogICAgICA8c3RvcCBvZmZzZXQ9IjEwMCUiIHN0eWxlPSJzdG9wLWNvbG9yOiMxNmEzNGE7c3RvcC
1vcGFjaXR5OjEiIC8+CiAgICA8L2xpbmVhckdyYWRpZW50PgogICAgPGZpbHRlciBpZD0ibWFwU2h
hZG93Ij4KICAgICAgPGZlRHJvcFNoYWRvdyBkeD0iMSIgZHk9IjEiIHN0ZERldmlhdGlvbj0iMiIg
Zmxvb2Qtb3BhY2l0eT0iMC4xNSIvPgogICAgPC9maWx0ZXI+CiAgICA8bWFya2VyIGlkPSJtYXBBc
nJvdyIgbWFya2VyV2lkdGg9IjEwIiBtYXJrZXJIZWlnaHQ9IjciIHJlZlg9IjkiIHJlZlk9IjMuNS
Igb3JpZW50PSJhdXRvIj4KICAgICAgPHBvbHlnb24gcG9pbnRzPSIwIDAsIDEwIDMuNSwgMCA3IiB
maWxsPSIjNjQ3NDhiIi8+CiAgICA8L21hcmtlcj4KICA8L2RlZnM+CgogIDwhLS0gQmFja2dyb3Vu
ZCAtLT4KICA8cmVjdCB3aWR0aD0iODAwIiBoZWlnaHQ9IjM2MCIgZmlsbD0iI2Y4ZjlmYSIgcng9I
jEwIi8+CgogIDwhLS0gVGl0bGUgLS0+CiAgPHRleHQgeD0iNDAwIiB5PSIyOCIgZm9udC1mYW1pbH
k9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjE4IiBmb250LXdlaWdodD0iYm9sZCIgZml
sbD0iIzMzMyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+TVogUGF0dGVybiB0byBOZXcgTW9kZWwgTWFw
cGluZzwvdGV4dD4KCiAgPCEtLSBIZWFkZXJzIC0tPgogIDxyZWN0IHg9IjMwIiB5PSI1MCIgd2lkd
Gg9IjMwMCIgaGVpZ2h0PSIzMCIgcng9IjYiIGZpbGw9InVybCgjbXpHcmFkKSIvPgogIDx0ZXh0IH
g9IjE4MCIgeT0iNzAiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSI
xMiIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IndoaXRlIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5N
YW5hZ2VtZW50IFpvbmUgUGF0dGVybjwvdGV4dD4KCiAgPHJlY3QgeD0iNDcwIiB5PSI1MCIgd2lkd
Gg9IjMwMCIgaGVpZ2h0PSIzMCIgcng9IjYiIGZpbGw9InVybCgjbmV3TW9kZWxHcmFkKSIvPgogID
x0ZXh0IHg9IjYyMCIgeT0iNzAiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1
zaXplPSIxMiIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IndoaXRlIiB0ZXh0LWFuY2hvcj0ibWlk
ZGxlIj5OZXcgTW9kZWwgU29sdXRpb248L3RleHQ+CgogIDwhLS0gUGF0dGVybiAxOiBUZWFtLUJhc
2VkIC0tPgogIDxyZWN0IHg9IjMwIiB5PSI5NSIgd2lkdGg9IjMwMCIgaGVpZ2h0PSI0NSIgcng9Ij
YiIGZpbGw9IiNmZWYzYzciIHN0cm9rZT0iI2Y1OWUwYiIgc3Ryb2tlLXdpZHRoPSIxIiBmaWx0ZXI
9InVybCgjbWFwU2hhZG93KSIvPgogIDx0ZXh0IHg9IjE4MCIgeT0iMTE1IiBmb250LWZhbWlseT0i
QXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTEiIGZvbnQtd2VpZ2h0PSJib2xkIiBmaWxsP
SIjOTI0MDBlIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5UZWFtLUJhc2VkIE1aczwvdGV4dD4KICA8dG
V4dCB4PSIxODAiIHk9IjEzMCIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXN
pemU9IjEwIiBmaWxsPSIjOTI0MDBlIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj4iVGVhbS1Gcm9udGVu
ZCIsICJUZWFtLUJhY2tlbmQiPC90ZXh0PgoKICA8cGF0aCBkPSJNMzMwLDExNyBMNDcwLDExNyIgc
3Ryb2tlPSIjNjQ3NDhiIiBzdHJva2Utd2lkdGg9IjIiIGZpbGw9Im5vbmUiIG1hcmtlci1lbmQ9In
VybCgjbWFwQXJyb3cpIi8+CgogIDxyZWN0IHg9IjQ3MCIgeT0iOTUiIHdpZHRoPSIzMDAiIGhlaWd
odD0iNDUiIHJ4PSI2IiBmaWxsPSIjZDFmYWU1IiBzdHJva2U9IiMyMmM1NWUiIHN0cm9rZS13aWR0
aD0iMSIgZmlsdGVyPSJ1cmwoI21hcFNoYWRvdykiLz4KICA8dGV4dCB4PSI2MjAiIHk9IjExNSIgZ
m9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjExIiBmb250LXdlaWdodD
```

```
0iYm9sZCIgZmlsbD0iIzA0Nzg1NyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+U2VjdXJpdHkgQ29udGV
4dCArIFBvbGljaWVzICsgQm91bmRhcmllczwvdGV4dD4KICA8dGV4dCB4PSI2MjAiIHk9IjEzMCIg
Zm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjEwIiBmaWxsPSIjMDQ3O
DU3IiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5kdC5zZWN1cml0eV9jb250ZXh0ID0gInRlYW0tZnJvbn
RlbmQiPC90ZXh0PgoKICA8IS0tIFBhdHRlcm4gMjogRW52aXJvbm1lbnQgLS0+CiAgPHJlY3QgeD0
iMzAiIHk9IjE1NSIgd2lkdGg9IjMwMCIgaGVpZ2h0PSI0NSIgcng9IjYiIGZpbGw9IiNmZWYzYzci
IHN0cm9rZT0iI2Y1OWUwYiIgc3Ryb2tlLXdpZHRoPSIxIiBmaWx0ZXI9InVybCgjbWFwU2hhZG93K
SIvPgogIDx0ZXh0IHg9IjE4MCIgeT0iMTc1IiBmb250LWZhbWlseT0iQXJpYWwsIHNhbnMtc2VyaW
YiIGZvbnQtc2l6ZT0iMTEiIGZvbnQtd2VpZ2h0PSJib2xkIiBmaWxsPSIjOTI0MDBlIiB0ZXh0LWF
uY2hvcj0ibWlkZGxlIj5FbnZpcm9ubWVudCBNWnM8L3RleHQ+CiAgPHRleHQgeD0iMTgwIiB5PSIx
OTAiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMCIgZmlsbD0iI
zkyNDAwZSIgdGV4dC1hbmNob3I9Im1pZGRsZSI+IlByb2R1Y3Rpb24iLCAiU3RhZ2luZyIsICJEZX
ZlbG9wbWVudCI8L3RleHQ+CgogIDxwYXRoIGQ9Ik0zMzAsMTc3IEw0NzAsMTc3IiBzdHJva2U9IiM
2NDc0OGIiIHN0cm9rZS13aWR0aD0iMiIgZmlsbD0ibm9uZSIgbWFya2VyLWVuZD0idXJsKCNtYXBB
cnJvdykiLz4KCiAgPHJlY3QgeD0iNDcwIiB5PSIxNTUiIHdpZHRoPSIzMDAiIGhlaWdodD0iNDUiI
HJ4PSI2IiBmaWxsPSIjZDFmYWU1IiBzdHJva2U9IiMyMmM1NWUiIHN0cm9rZS13aWR0aD0iMSIgZm
lsdGVyPSJ1cmwoI21hcFNoYWRvdykiLz4KICA8dGV4dCB4PSI2MjAiIHk9IjE3NSIgZm9udC1mYW1
pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjExIiBmb250LXdlaWdodD0iYm9sZCIg
ZmlsbD0iIzA0Nzg1NyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+Qm91bmRhcmllcyB3aXRoIEVudmlyb
25tZW50IENvbmRpdGlvbnM8L3RleHQ+CiAgPHRleHQgeD0iNjIwIiB5PSIxOTAiIGZvbnQtZmFtaW
x5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMCIgZmlsbD0iIzA0Nzg1NyIgdGV4dC1
hbmNob3I9Im1pZGRsZSI+c2VjdXJpdHlfY29udGV4dCBzdGFydHNXaXRoICJwcm9kLSI8L3RleHQ+
CgogIDwhLS0gUGF0dGVybiAzOiBSZWdpb25hbCAtLT4KICA8cmVjdCB4PSIzMCIgeT0iMjE1IiB3a
WR0aD0iMzAwIiBoZWlnaHQ9IjQ1IiByeD0iNiIgZmlsbD0iI2ZlZjNjNyIgc3Ryb2tlPSIjZjU5ZT
BiIiBzdHJva2Utd2lkdGg9IjEiIGZpbHRlcj0idXJsKCNtYXBTaGFkb3cpIi8+CiAgPHRleHQgeD0
iMTgwIiB5PSIyMzUiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIx
MSIgZm9udC13ZWlnaHQ9ImJvbGQiIGZpbGw9IiM5MjQwMGUiIHRleHQtYW5jaG9yPSJtaWRkbGUiP
lJlZ2lvbmFsL0dlb2dyYXBoaWMgTVpzPC90ZXh0PgogIDx0ZXh0IHg9IjE4MCIgeT0iMjUwIiBmb2
50LWZhbWlseT0iQXJpYWwsIHNhbnMtc2VyaWYiIGZvbnQtc2l6ZT0iMTAiIGZpbGw9IiM5MjQwMGU
iIHRleHQtYW5jaG9yPSJtaWRkbGUiPiJOQS1FYXN0IiwgIkVVLVdlc3QiLCAiQVBBQyI8L3RleHQ+
CgogIDxwYXRoIGQ9Ik0zMzAsMjM3IEw0NzAsMjM3IiBzdHJva2U9IiM2NDc0OGIiIHN0cm9rZS13a
WR0aD0iMiIgZmlsbD0ibm9uZSIgbWFya2VyLWVuZD0idXJsKCNtYXBBcnJvdykiLz4KCiAgPHJlY3
QgeD0iNDcwIiB5PSIyMTUiIHdpZHRoPSIzMDAiIGhlaWdodD0iNDUiIHJ4PSI2IiBmaWxsPSIjZDF
mYWU1IiBzdHJva2U9IiMyMmM1NWUiIHN0cm9rZS13aWR0aD0iMSIgZmlsdGVyPSJ1cmwoI21hcFNo
YWRvdykiLz4KICA8dGV4dCB4PSI2MjAiIHk9IjIzNSIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zL
XNlcmlmIiBmb250LXNpemU9IjExIiBmb250LXdlaWdodD0iYm9sZCIgZmlsbD0iIzA0Nzg1NyIgdG
V4dC1hbmNob3I9Im1pZGRsZSI+U2VnbWVudHMgd2l0aCBSZWdpb24gRmlsdGVyczwvdGV4dD4KICA
8dGV4dCB4PSI2MjAiIHk9IjI1MCIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250
LXNpemU9IjEwIiBmaWxsPSIjMDQ3ODU3IiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5tYXRjaGVzVmFsd
WUodGFncywgInJlZ2lvbjp1cy1lYXN0LTEiKTwvdGV4dD4KCiAgPCEtLSBQYXR0ZXJuIDQ6IEFwcG
xpY2F0aW9uIC0tPgogIDxyZWN0IHg9IjMwIiB5PSIyNzUiIHdpZHRoPSIzMDAiIGhlaWdodD0iNDU
iIHJ4PSI2IiBmaWxsPSIjZmVmM2M3IiBzdHJva2U9IiNmNTllMGIiIHN0cm9rZS13aWR0aD0iMSIg
ZmlsdGVyPSJ1cmwoI21hcFNoYWRvdykiLz4KICA8dGV4dCB4PSIxODAiIHk9IjI5NSIgZm9udC1mY
W1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjExIiBmb250LXdlaWdodD0iYm9sZC
IgZmlsbD0iIzkyNDAwZSIgdGV4dC1hbmNob3I9Im1pZGRsZSI+QXBwbGljYXRpb24tQmFzZWQgTVp
zPC90ZXh0PgogIDx0ZXh0IHg9IjE4MCIgeT0iMzEwIiBmb250LWZhbWlseT0iQXJpYWwsIHNhbnMt
c2VyaWYiIGZvbnQtc2l6ZT0iMTAiIGZpbGw9IiM5MjQwMGUiIHRleHQtYW5jaG9yPSJtaWRkbGUiP
iJQYXltZW50LVN5c3RlbSIsICJVc2VyLVBvcnRhbCI8L3RleHQ+CgogIDxwYXRoIGQ9Ik0zMzAsMj
```

```
k3IEw0NzAsMjk3IiBzdHJva2U9IiM2NDc0OGIiIHN0cm9rZS13aWR0aD0iMiIgZmlsbD0ibm9uZSI
gbWFya2VyLWVuZD0idXJsKCNtYXBBcnJvdykiLz4KCiAgPHJlY3QgeD0iNDcwIiB5PSIyNzUiIHdp
ZHRoPSIzMDAiIGhlaWdodD0iNDUiIHJ4PSI2IiBmaWxsPSIjZDFmYWU1IiBzdHJva2U9IiMyMmM1N
WUiIHN0cm9rZS13aWR0aD0iMSIgZmlsdGVyPSJ1cmwoI21hcFNoYWRvdykiLz4KICA8dGV4dCB4PS
I2MjAiIHk9IjI5NSIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LXNpemU9IjE
xIiBmb250LXdlaWdodD0iYm9sZCIgZmlsbD0iIzA0Nzg1NyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+
U2VnbWVudHMgd2l0aCBTZXJ2aWNlIEZpbHRlcnM8L3RleHQ+CiAgPHRleHQgeD0iNjIwIiB5PSIzM
TAiIGZvbnQtZmFtaWx5PSJBcmlhbCwgc2Fucy1zZXJpZiIgZm9udC1zaXplPSIxMCIgZmlsbD0iIz
A0Nzg1NyIgdGV4dC1hbmNob3I9Im1pZGRsZSI+bWF0Y2hlc1BocmFzZShzZXJ2aWNlLm5hbWUsICJ
wYXltZW50Iik8L3RleHQ+CgogIDwhLS0gS2V5IGluc2lnaHQgLS0+CiAgPHJlY3QgeD0iMzAiIHk9
IjMzMCIgd2lkdGg9Ijc0MCIgaGVpZ2h0PSIyMiIgcng9IjQiIGZpbGw9IiNlMGYyZmUiLz4KICA8d
GV4dCB4PSI0MDAiIHk9IjM0NSIgZm9udC1mYW1pbHk9IkFyaWFsLCBzYW5zLXNlcmlmIiBmb250LX
NpemU9IjEwIiBmaWxsPSIjMDM2OWExIiB0ZXh0LWFuY2hvcj0ibWlkZGxlIj5LZXk6IFRlYW0vRW5
2aXJvbm1lbnQg4oaSIEJvdW5kYXJpZXMgZm9yIGFjY2VzcyBjb250cm9sIHwgUmVnaW9uL0FwcGxp
Y2F0aW9uIOKGkiBTZWdtZW50cyBmb3IgZGF0YSBmaWx0ZXJpbmc8L3RleHQ+Cjwvc3ZnPgo=)
```

```
| MZ Permission | Equivalent Policy + Boundary |
|---------------|-----------------------------|
| View only | `Dynatrace Viewer` + Boundary |
| View + Edit | `Dynatrace Standard User` + Boundary |
| Full access to MZ | `Dynatrace Professional User` + Boundary |
| Admin in MZ | Custom policy + Boundary |

### Migration Example: Team-Based MZ

**Before (MZ-based):**
- Management Zone: "Frontend-Team"
- Rules: Services with tag `team:frontend`
- Users assigned via RBAC

**After (Policy + Boundary):**
```
1. Set security context on entities:
   - Services get dt.security_context = "team-frontend"

2. Create boundary:
   Name: Frontend Team Scope
   Query:
   environment:management-zone IN ("Frontend-Team");
   storage:dt.security_context IN ("team-frontend");
   settings:dt.security_context IN ("team-frontend");

3. Bind to group:
   Group: Frontend Developers (SAML)
   Policy: Dynatrace Standard User
   Boundary: Frontend Team Scope
```
```

~~~
```

### Migration Example: Environment MZ

**Before (MZ-based):**
- Management Zone: "Production"
- Rules: Hosts with tag `env:production`
- Users get MZ-filtered view

**After (Policy + Boundary):**
```
1. Set security context on entities:
   - Hosts get dt.security_context = "prod-{region}"

2. Create boundary:
   Name: Production Environment
   Query:
   environment:management-zone IN ("Production");
   storage:dt.security_context startsWith "prod-";
   settings:dt.security_context startsWith "prod-";

3. Bind to group:
   Group: Production Operators (SAML)
   Policy: Dynatrace Professional User
   Boundary: Production Environment
```

---

## 9. Security Context Configuration

### What Is Security Context?

**Security Context** (`dt.security_context`) is an entity attribute used for
access control. It's the recommended way to scope boundaries for Grail data.

### Setting Security Context

Security context can be set via:
- **Auto-tagging rules**
- **OneAgent configuration**
- **API**
- **Settings UI**

### Security Context Naming Strategy

| Pattern | Example | Use Case |
|---------|---------|----------|
~~~

~~~~
| `team-{name}` | `team-frontend` | Team ownership |
| `env-{name}` | `env-production` | Environment separation |
| `region-{code}` | `region-us-east` | Geographic isolation |
| `app-{name}` | `app-checkout` | Application scoping |
| `{env}-{team}` | `prod-frontend` | Combined scoping |

### Query Entities by Security Context

```dql
// List services with their security context
// Identify services that need security context assignment
fetch dt.entity.service
| fields entity.name,
         dt.security_context,
         tags,
         managementZones
| sort dt.security_context asc
| limit 50
```

```dql
// Count entities by security context
// Helps verify security context distribution
fetch dt.entity.service
| summarize count = count(), by:{dt.security_context}
| sort count desc
```

---

## 10. Custom Policies

### When to Create Custom Policies

- Default policies are too broad or narrow
- Need specific permission combinations
- Require conditional access
- Compliance requirements

### Custom Policy Examples

**Log Viewer for Specific Team:**
```
// Policy Name: Frontend Team Log Access
// Description: Read-only access to frontend service logs

ALLOW storage:logs:read
  WHERE storage:dt.security_context = "team-frontend"
~~~~

~~~
ALLOW storage:spans:read
  WHERE storage:dt.security_context = "team-frontend"
```

**Environment-Restricted Admin:**
```
// Policy Name: Development Admin
// Description: Full access to development environment only

ALLOW storage:*:*
  WHERE storage:dt.security_context startsWith "dev-"

ALLOW settings:objects:*
  WHERE settings:scope startsWith "environment:dev"
```

**Dashboard and Notebook Creator:**
```
// Policy Name: Dashboard Creator
// Description: Create and manage dashboards and notebooks

ALLOW document:documents:read
ALLOW document:documents:write
ALLOW document:documents:delete
ALLOW document:documents:share

// Read data for dashboards
ALLOW storage:logs:read
ALLOW storage:metrics:read
ALLOW storage:spans:read
```

---

## 11. Best Practices

### Do's

- ✅ **Start with default policies** - customize only when needed
- ✅ **Use least privilege** - grant minimum required permissions
- ✅ **Document policies and boundaries** - clear names and descriptions
- ✅ **Test before production** - verify with test users
- ✅ **Use boundaries for scope** - keep policies reusable
- ✅ **Include all three domains** in boundaries for complete MZ replacement
- ✅ **Use SAML groups** tied to AD for team management

### Don'ts
~~~

~~~
- ❌ **Don't create policy per user** - use groups
- ❌ **Don't duplicate default policies** - extend instead
- ❌ **Don't use overly broad wildcards** - be specific
- ❌ **Don't embed conditions in policies** when boundaries are better
- ❌ **Don't forget the settings domain** in boundaries

### Naming Conventions

```
// Good names
"Frontend Team - Standard Access"     (policy)
"Production Environment"              (boundary)
"LOB5-Scope"                          (boundary)

// Bad names
"Policy 1"
"Test"
"John's boundary"
```

### Audit Checklist

- [ ] Each boundary has a clear purpose
- [ ] Boundary names follow naming convention
- [ ] All three domains included (environment, storage, settings)
- [ ] SAML groups aligned with AD structure
- [ ] Dependencies tracked (which policies use which boundaries)
- [ ] Regular review scheduled

---

## 12. Troubleshooting

### Common Issues

| Issue | Likely Cause | Solution |
|-------|-------------|----------|
| User can't access anything | No policy bound | Bind policy to user's group
|
| User sees too much | Boundary too broad or missing | Tighten boundary
conditions |
| User can't see expected data | Missing data policy | Add Data Viewer/Editor
|
| Permissions inconsistent | Multiple conflicting policies | Review all bound
policies |
| Works in classic, not Grail | Only environment domain used | Add storage
domain to boundary |
~~~

```
| Settings not restricted | Missing settings domain | Add
settings:dt.security_context |

### Debugging Steps

1. **Verify group membership**: Is user in correct group?
2. **Check policy bindings**: What policies are bound to group?
3. **Review boundaries**: Are all three domains included?
4. **Test with admin**: Does admin see the data?
5. **Check security context**: Is it set on the entities?

### Testing Boundaries

1. **Create test user** in target group
2. **Log in as test user**
3. **Verify access**:
   - Can access expected data?
   - Cannot access restricted data?
4. **Test edge cases**:
   - Entities at boundary edges
   - New entities without security context

---

## Summary

In this notebook, you learned:

1. **Policies define WHAT**, boundaries define **WHERE**
2. **Default policies** cover most use cases - customize only when needed
3. **Shared syntax** for conditions in both policies and boundaries
4. **Three domains** needed for complete MZ replacement (environment,
storage, settings)
5. **SAML + Policy + Boundary** structure for AD integration
6. **Migration patterns** for team-based and environment-based MZs

## Next Steps

Continue to **MZ2POL-05: Segments Implementation** to:
- Create DQL-based data filters
- Replace MZ data filtering with Segments
- Configure cross-app filtering

## Additional Resources

- [Working with Policies](https://docs.dynatrace.com/docs/manage/identity-
access-management/permission-management/manage-user-permissions-policies)
- [IAM Policy Reference](https://docs.dynatrace.com/docs/manage/identity-
access-management/permission-management/manage-user-permissions-
policies/advanced/iam-policystatements)
- [Policy Boundaries Documentation]
(https://docs.dynatrace.com/docs/manage/identity-access-
management/permission-management/manage-user-permissions-policies/iam-policy-
boundaries)
- [Grant Access with Security Context]
(https://docs.dynatrace.com/docs/manage/identity-access-management/use-
cases/access-security-context)
```