Capturing Matches with Subexpressions

Josh Duffney
DEVOPS ENGINEER

@joshduffney http://duffney.io/

Subexpressions and Capture Groups

\\server\share\file.txt

($share -split '\\')[2,3]

\\server\share\file.txt

$share –match
'\\\\(\w+)\\(\w+)'

```
'202-555-0148' -match '(202)-555-0148‘

‘202-555-0148’ –replace ‘\d+-(\d+-\d+)’,’$1’

‘\\server\share\file.txt’ –match ‘\\\\(\w+)\\(\w+)(?:.*)’
```

Subexpressions…

Are used to capture specific sections of an expression by using parentheses. The section of the expression inside the parentheses is referred to as a subexpression or capture group.

Demo

Subexpressions

- Capturing subexpressions
- Capture groups
- Multiple subexpressions
- Non-capturing subexpressions

Using subexpressions

- Capture a server name from a UNC path
- Extract a user name from a distinguished name
- Convert a distinguished name to a domain name
- Extract event source node names from a windows event forwarding subscription

Summary

Subexpressions

- Used to capture sections of an expression
- Created capture groups within $matches
- Stored in variables starting at $1
- Repeat subexpressions with quantifiers
- Non-capturing subexpressions

Used subexpressions

- Capture a server name from a UNC path
- Extract information from Active Directory
- Collect event sources for a Windows event forwarding subscription