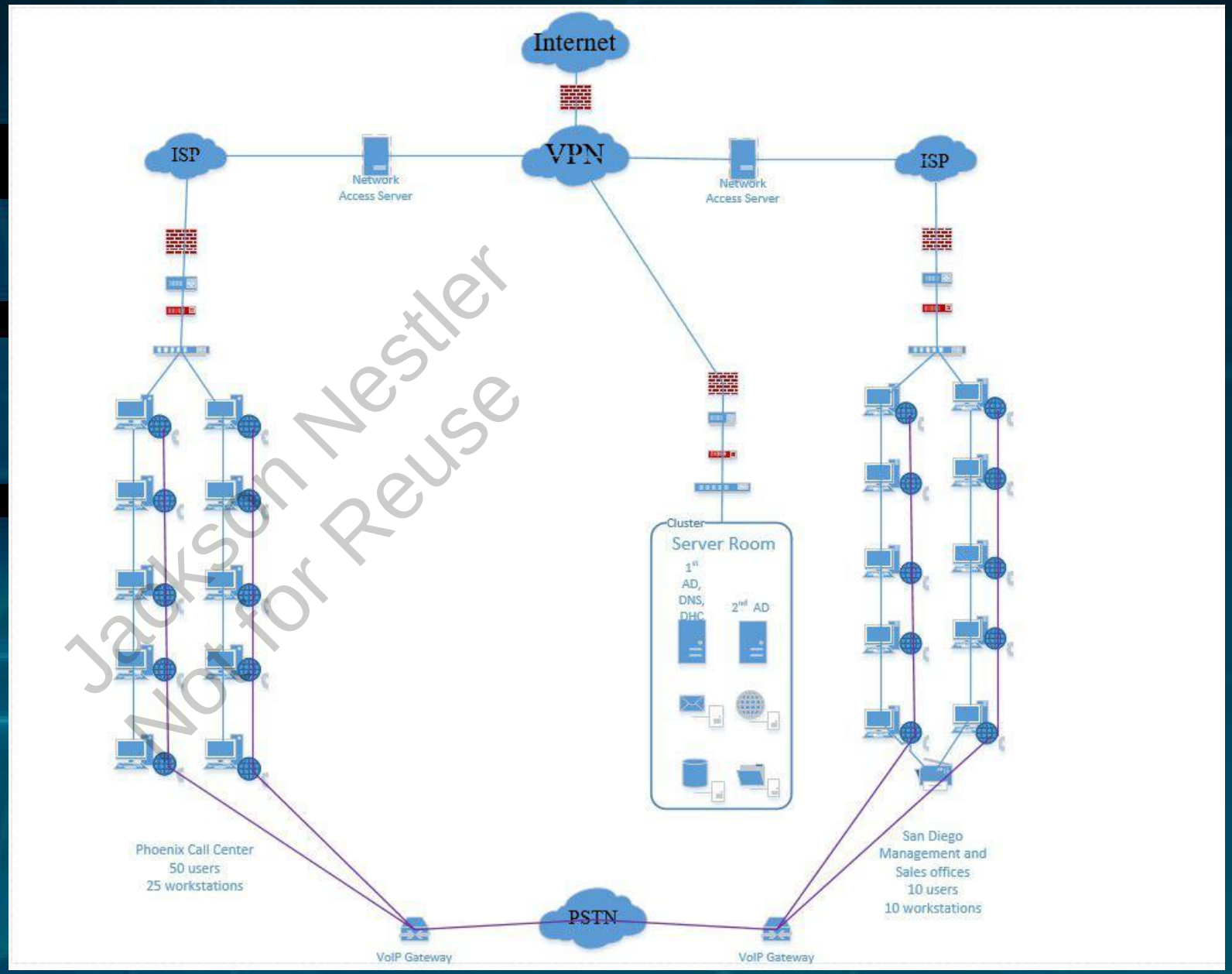
NTW216: Final Project

JACKSON NESTLER
[REDACTED]
[REDACTED]

Scenario

- 2x locations (San Diego, Phoenix)
- 50 users in call center, in Phoenix
- 10 users in management/sales, in San Diego.
- Include: VOIP, DNS, DHCP, Windows 2012/2016, Windows 10.

Visio


Internet
ISP
Network Access Server
VPN
Network Access Server
ISP
Cluster
Server Room
1st AD, DNS, DHC
2nd AD
Phoenix Call Center
50 users
25 workstations
PSTN
VoIP Gateway
VoIP Gateway
San Diego
Management and
Sales offices
10 users
10 workstations
Jackson Nestler
Not for Reuse

User Creation

- Ashley found a script that imports users from the contents of a csv into AD users & groups.
- Initially struggled to get the script to run; seemed code wasn't written properly.
- Due to time constraints, manually added users via the GUI.
- To-Do: Write a script that fills in information from a CSV or TXT.
  - Python imports the content of the CSV, using a "for x in NumUsers" loop create prepared PowerShell statements & saves prepared statements to a text file.
  - Admin copy and pastes the contents from the new text file into PowerShell.

DNS/DHCP

- DNS is configured the same way it ships with AD…Any changes to it felt unwarranted.
- DHCP is enabled & configured but it's recommended that the machines receive a static address and fall back to DHCP when an image needs to be made.

Group Policy

- The previous work-order that requested Group Policy had a few less-than-ideal choices. As security contractors we've made changes.
- DoD Secure Baseline: https://github.com/iadgov/Secure-Host-Baseline
  - Auto-magically configured Group Policy for common software (BitLocker, Chrome, EMET, Internet Explorer, Windows & Windows Firewall)
  - Left out some configuration (ie Adobe Reader) as it's proprietary and hasn't shown up in a work-order.
  - Enforced on the Domain Controller and Clients.

Lab

- Small sample set of actual users

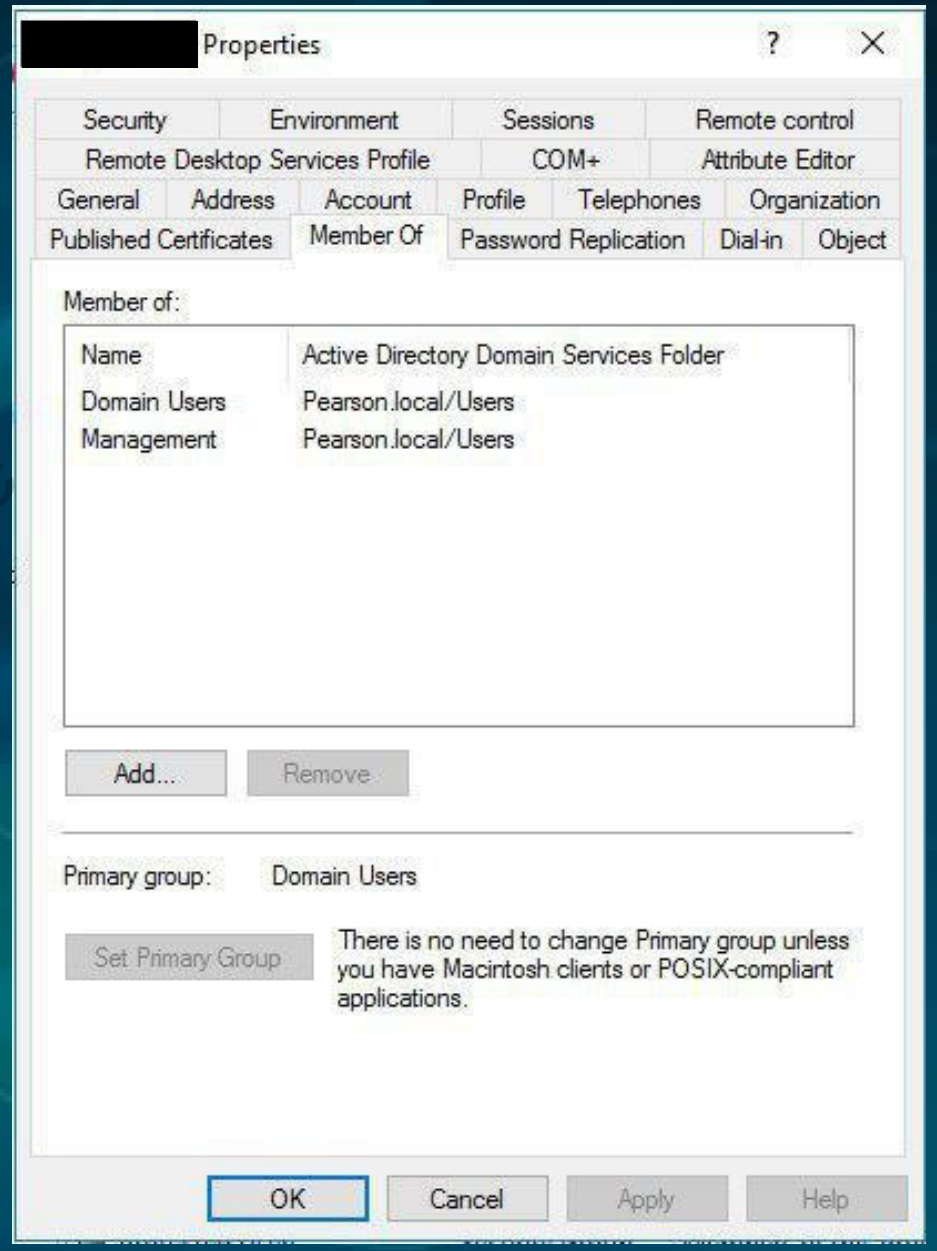
Administrator	User	Built-in account for ad...	
Alice Cooper	User		Alice Cooper
[redacted]	User		
	User		[redacted]
Bob Thorn	User		Bob Thorn
DefaultAccount	User	A user account manage...	
Guest	User	Built-in account for gue...	
[redacted]	User		[redacted]
Jackson Nestler	User		Jackson Nestler
Jane Doe	User		Jane Doe
John Doe	User		John Doe
krbtgt	User	Key Distribution Center ...	
[redacted]	User		[redacted]
SharePoint Farm Account	User		SharePoint Farm Account
SharePoint Install Account	User		SharePoint Install Account
SharePoint Profile Account	User		SharePoint Profile Account
SharePoint Search Conten...	User		SharePoint Search Content Crawl
SharePoint Service App A...	User		SharePoint Service App Account
SharePoint Web App Acc...	User		SharePoint Web App Account
SQL Install Account	User		SQL Install Account
SQL Service Account	User		SQL Service Account
Todd Bowman	User		Todd Bowman
Wayne Kibbe	User		Wayne Kibbe
Janet Jackson	User		Janet Jackson

Lab

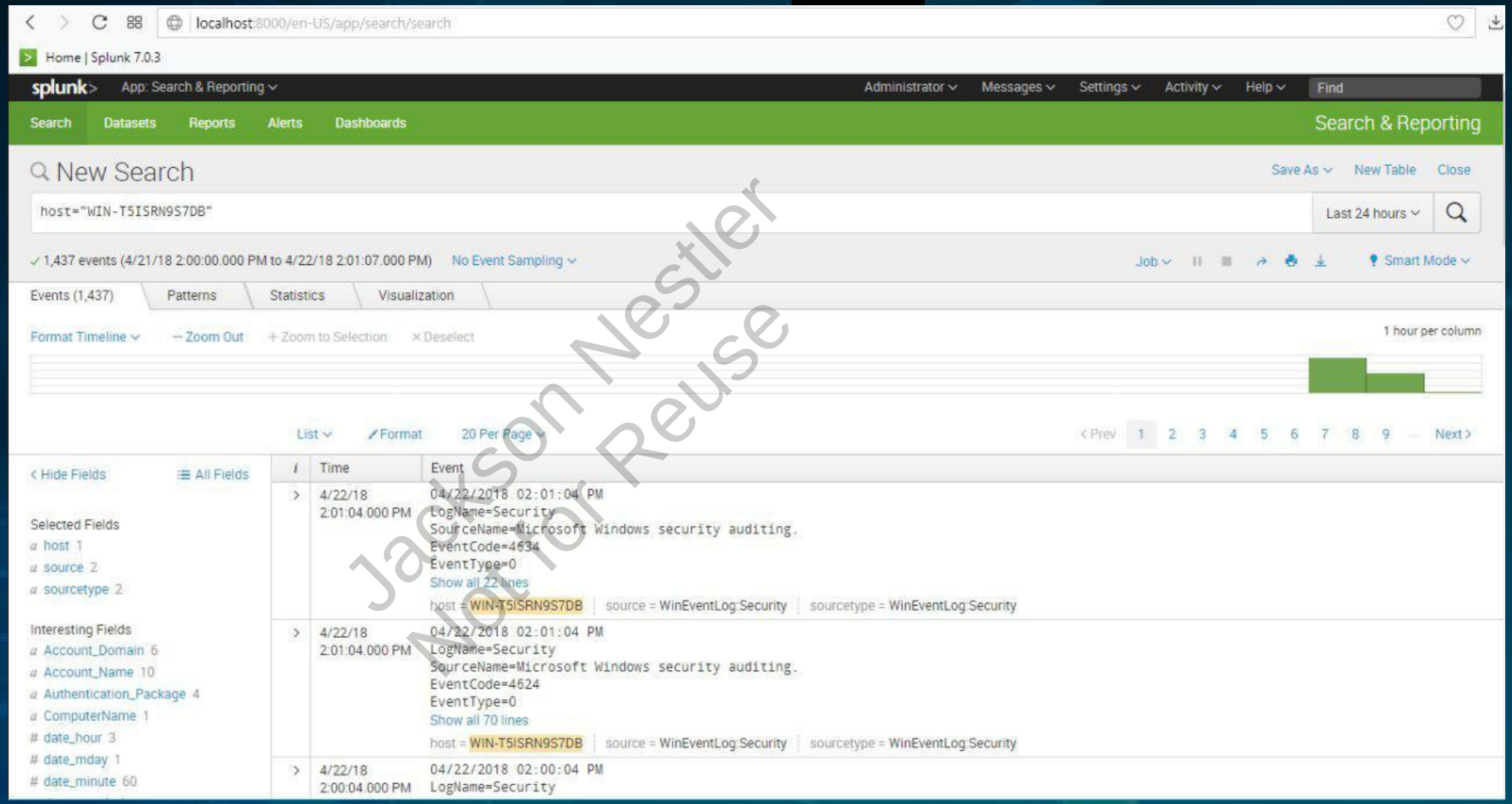
[redacted]

[redacted]

[redacted]



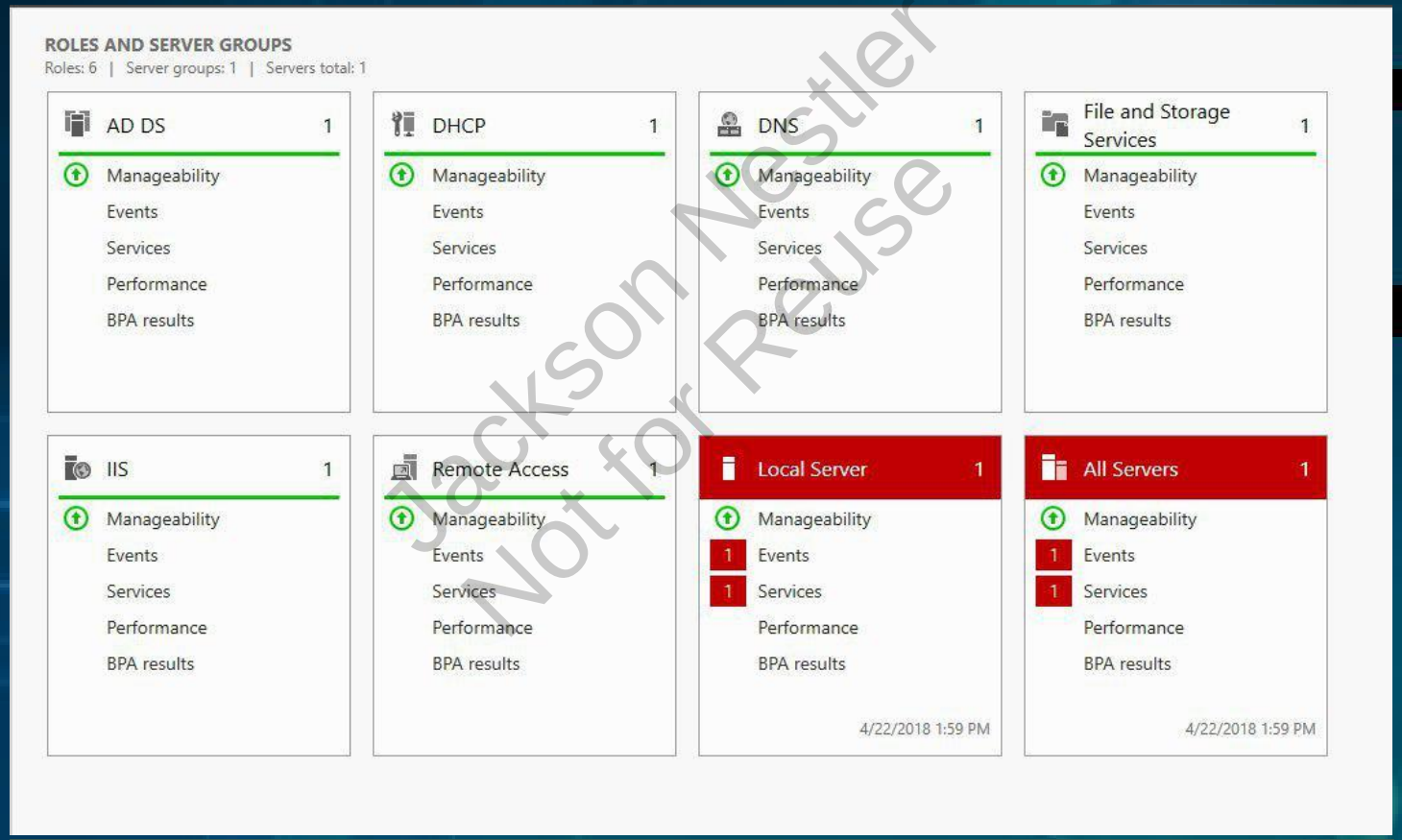
Splunk



Splunk

- Utilizing the free version of Splunk and IIS, we have a working logging platform running locally on the Domain Controller.
- In the screenshot, we're monitoring for events from a Windows client. We could refine these searches to include failed logins, attempts to enumerate ports, etc.

Services



* Local server & All Servers are denoted in red are due to Splunk.