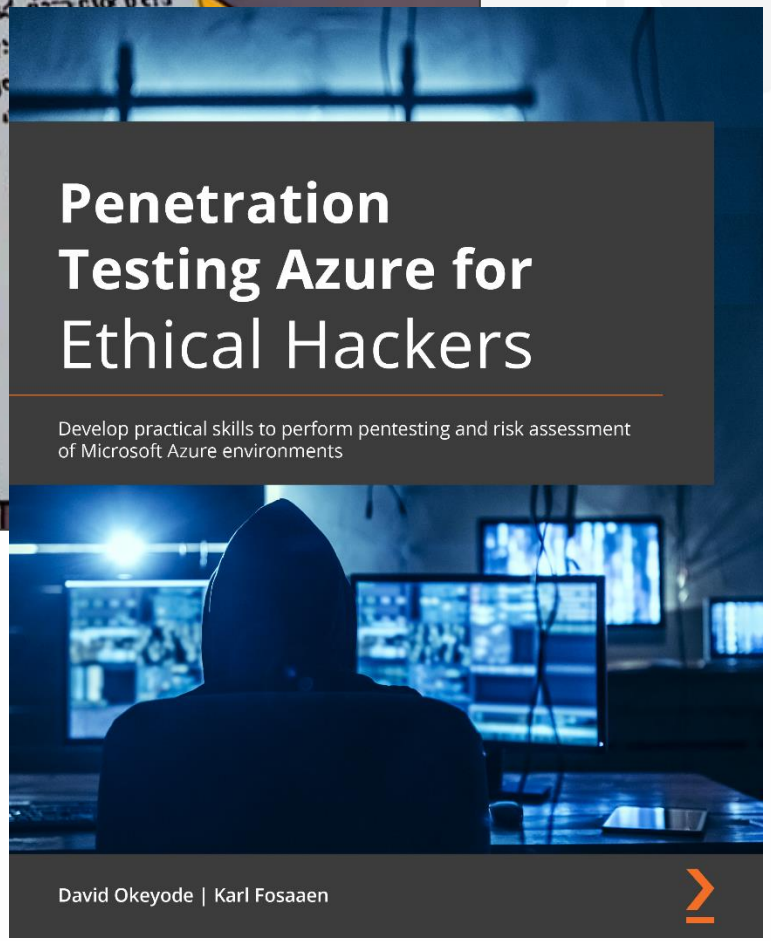
AUTOMATING INSECURITY IN AZURE

Karl Fosaaen

- Karl Fosaaen
  - Pen Tester
  - MicroBurst
  - Cloud Enthusiast
  - Private Pilot
  - Co-Author
  - Merch Goon

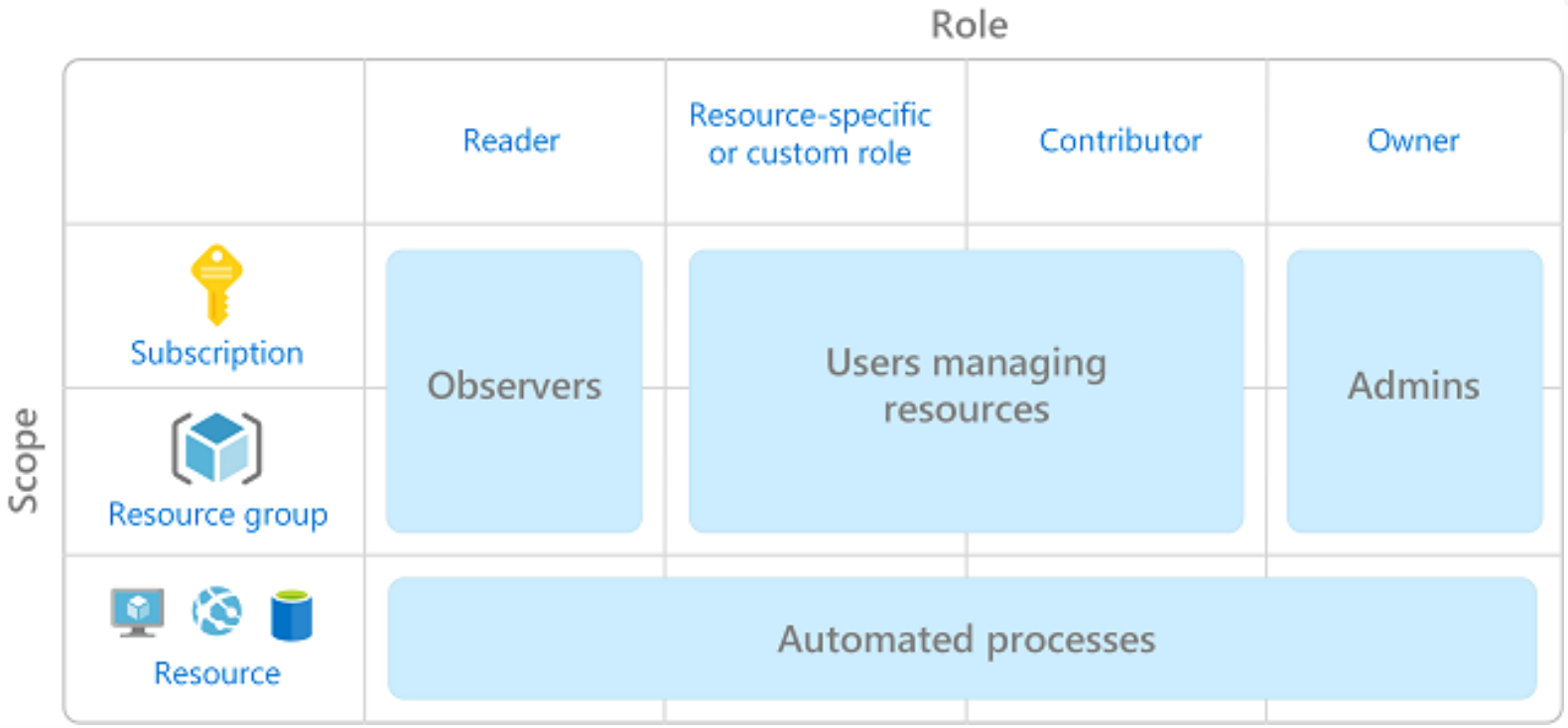


- https://github.com/netspi
- https://blog.netspi.com/
- Twitter - @kfosaaen

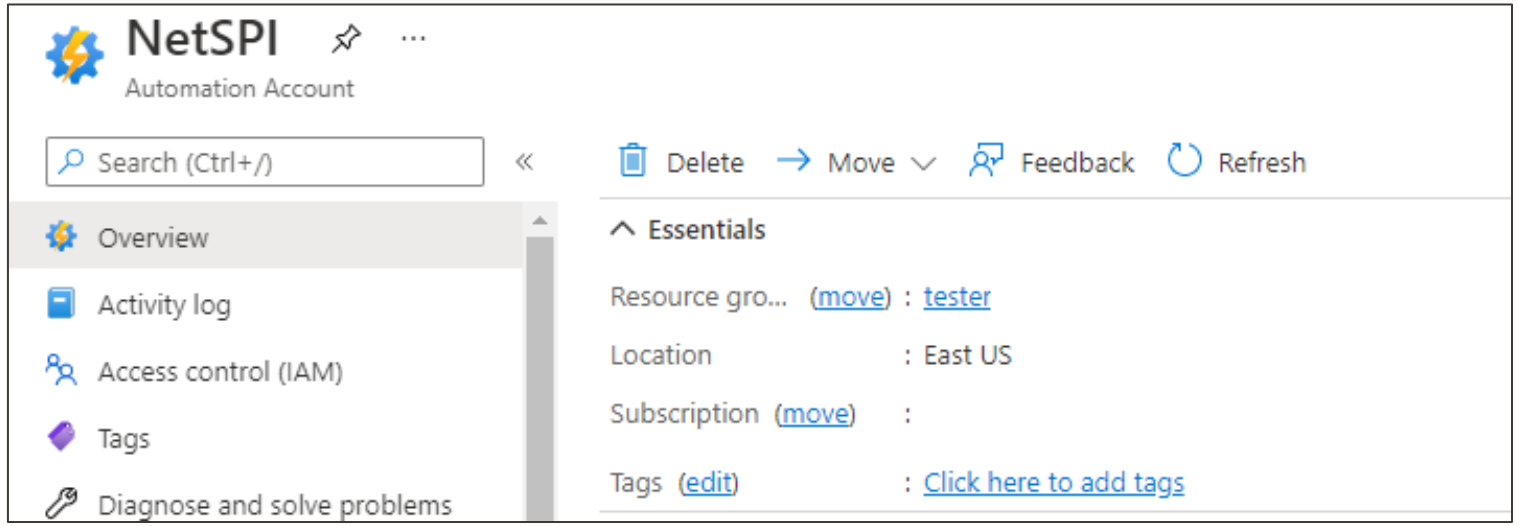
MicroBurst
TOOLS.NETSPI.COM

- Azure AD Tenant
  - The core of Identity (RBAC / IAM) in Azure
  - Security Principals
    - Users / Guest Users
      - AD Synced versus Azure Managed
    - Managed Identities
      - System Assigned
      - User Assigned
    - Service Principals
      - Application Accounts
  - Security Principals are assigned Roles

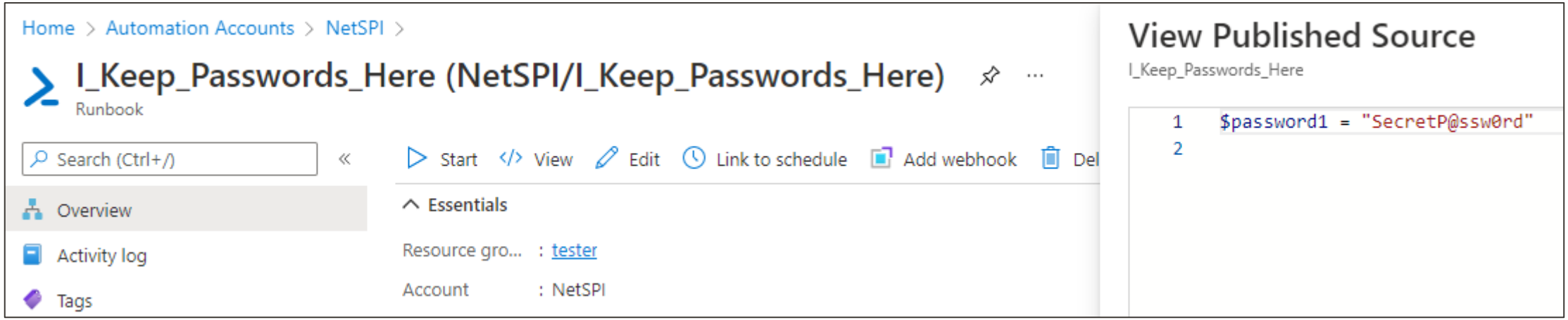
- Subscription Level
  - Owner
  - Contributor
  - Reader
- Special/Custom Roles
  - Multi-Level
  - Service Specific
  - Application Specific
- Application of Roles
  - Management Group / Child Management Group / Subscription / Resource Group / Resource



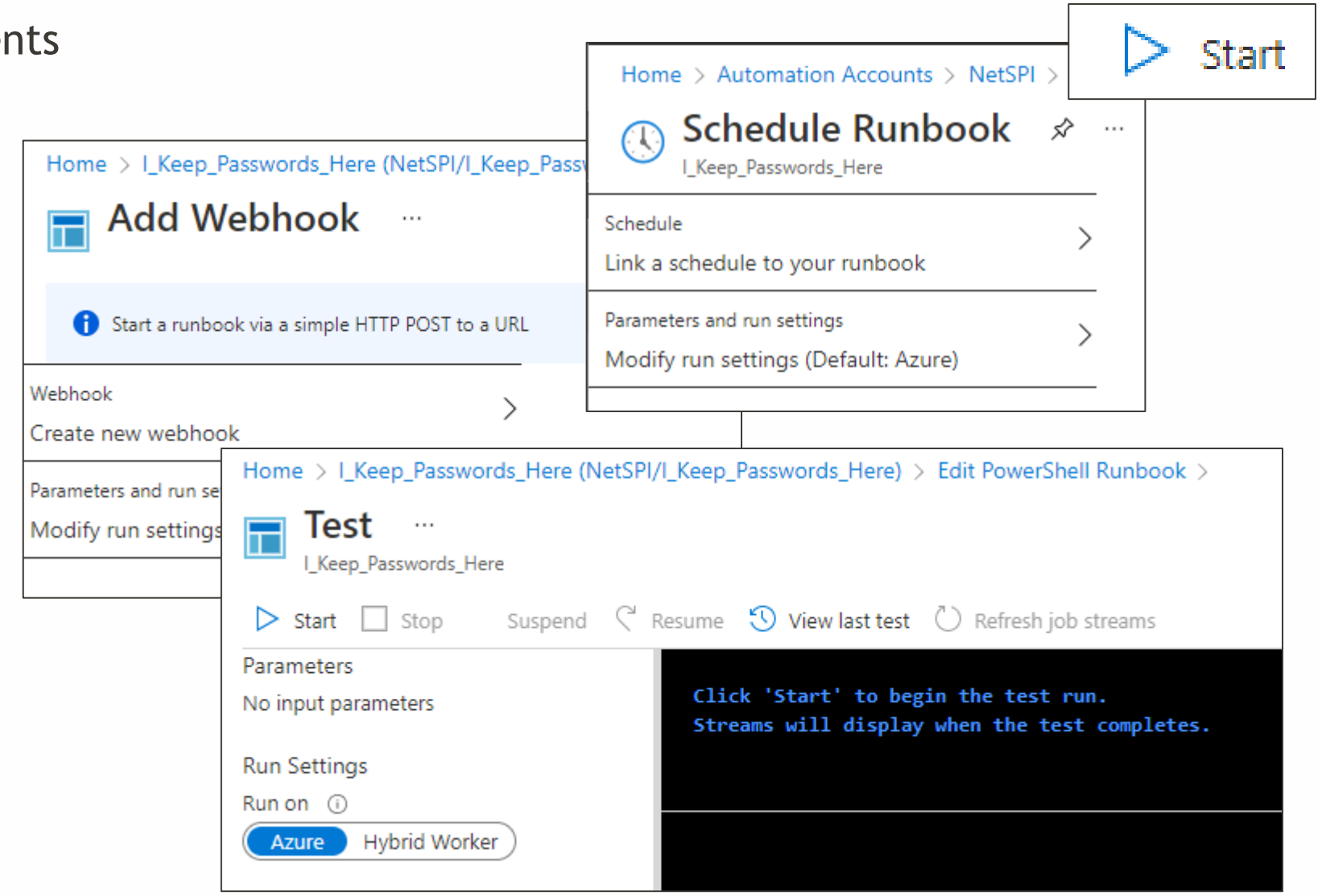
- What are Automation Accounts?
  - Service for automating actions in Azure subscriptions
    - Resource Management
    - Applying Updates
    - Rotating Credentials
    - Ensuring Configurations
  - A great target during a pen test
    - Credential Access
    - Privilege Escalation
    - Lateral Movement
    - Persistence



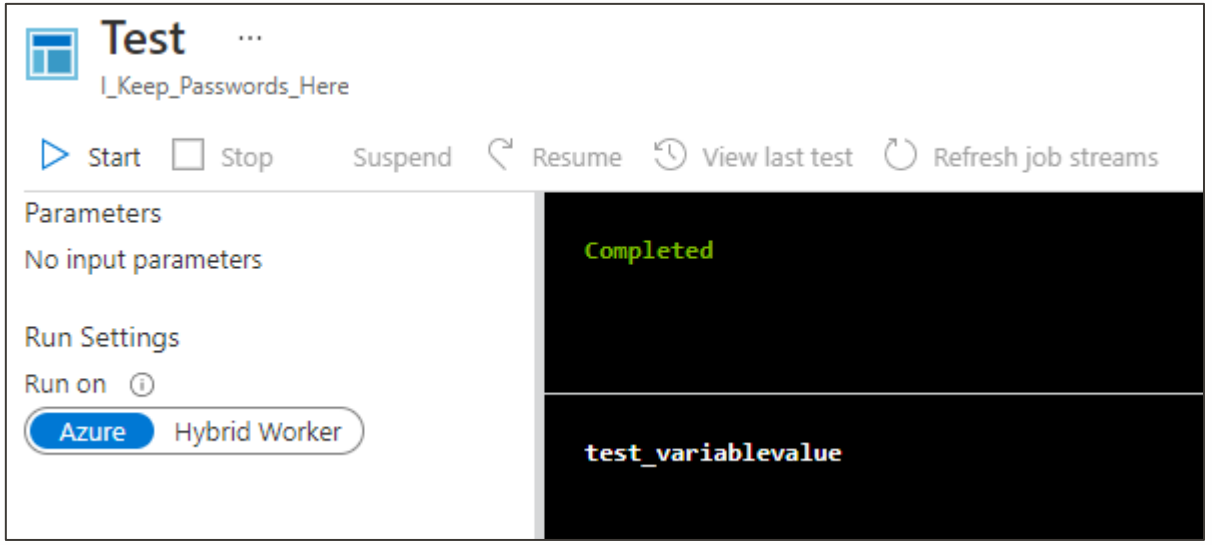
- Automation Account Components
  - Runbooks
    - PowerShell or Python Scripts
      - Can use custom modules or packages
    - Code available to the Reader role
      - Hardcoded credentials in code
    - Normally executes within a Microsoft managed container

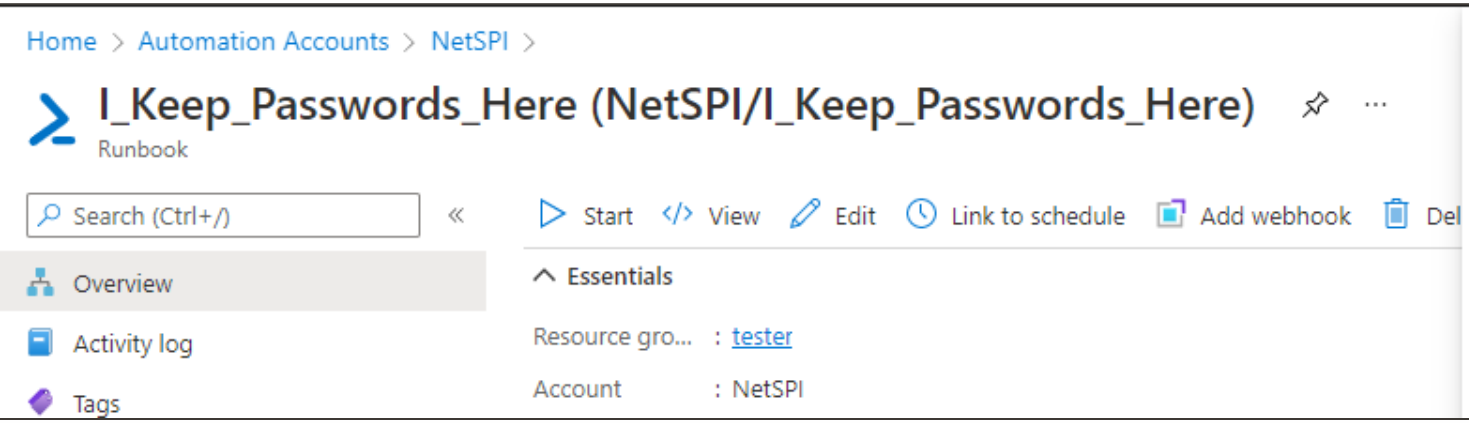


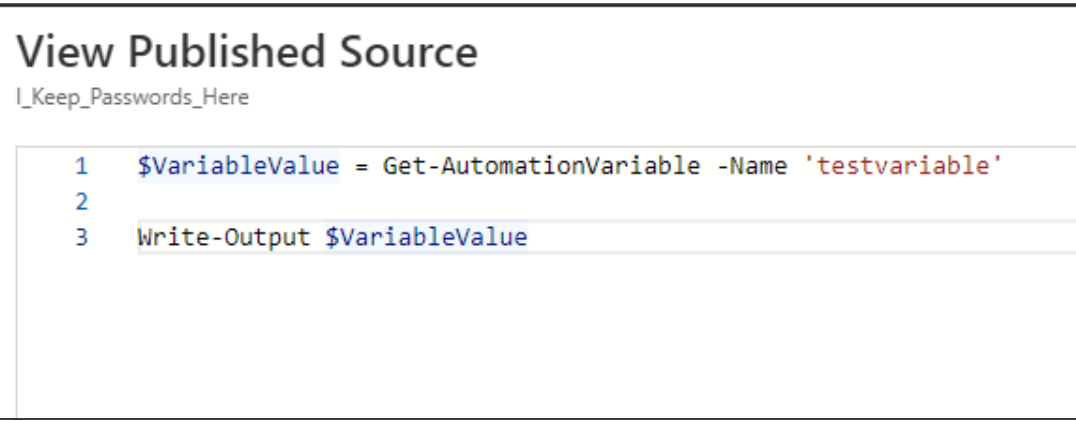
- Automation Account Components
  - Runbook Execution
    - Run as a Job
      - Very visible in logs
    - Schedule to Run
      - Persistence option
    - Trigger with Webhook
      - Persistence option
      - Can accept parameters
      - Command Injection Potential
    - Run in Test Pane
      - Less noise in the logs



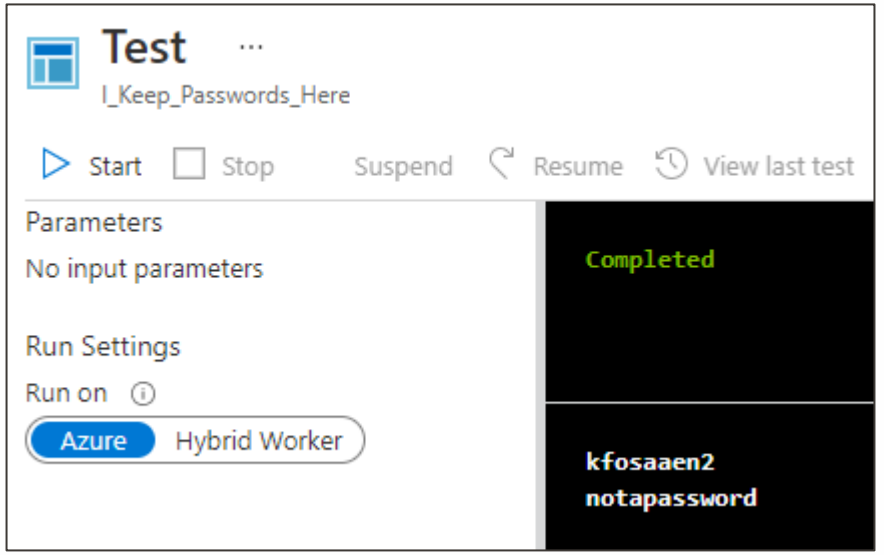
- Automation Account Components
  - Variables
    - Stores commonly used variable values
    - Often contains credentials or keys
    - Easy to cast to outputs for extraction
    - Available to the Reader role
      - *Unless they're encrypted

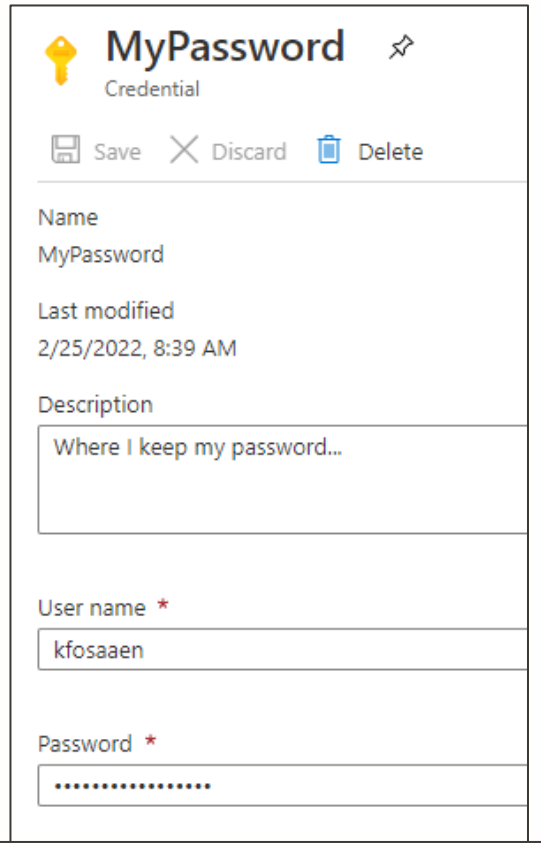


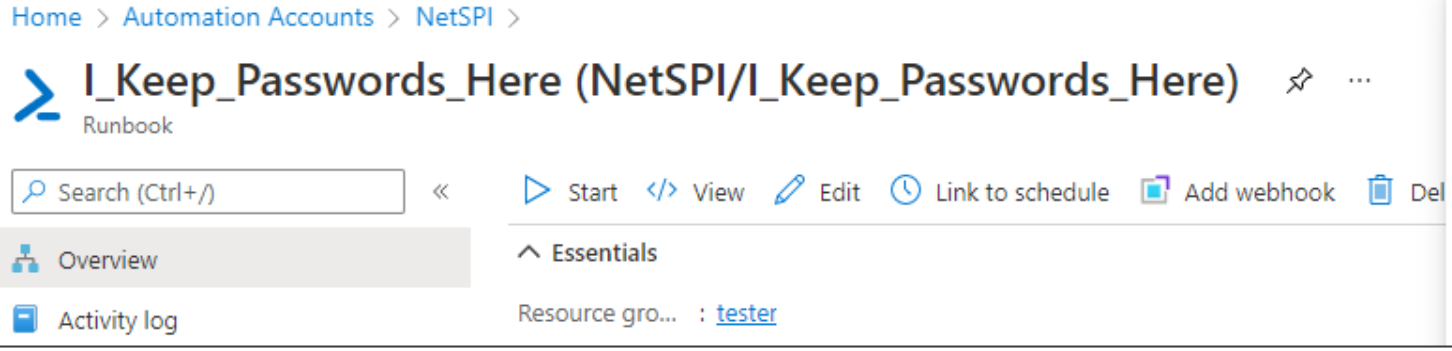


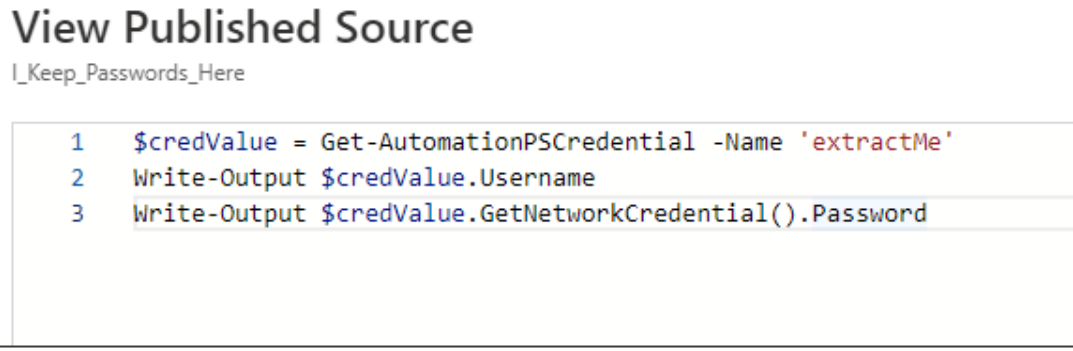


- Automation Account Components
  - Platform Credential Options
    - "Credentials"
      - Username and Password combination
        - AAD credentials
        - Domain or Local credentials for VMs
      - Easy to cast to outputs for extraction
      - Key Vaults are the safer option

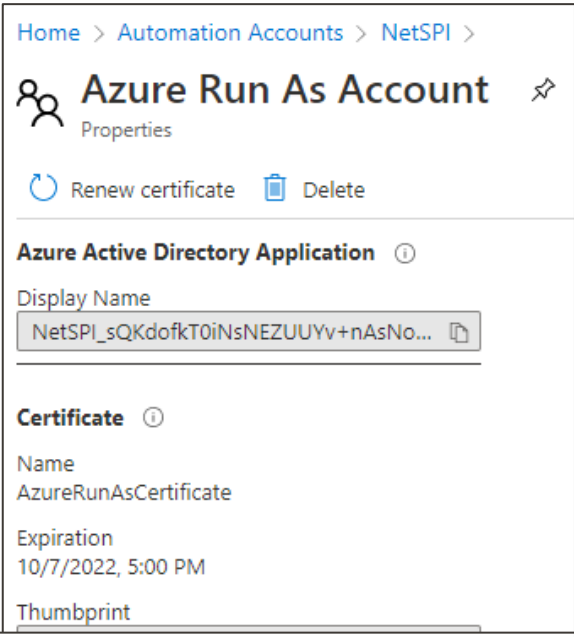








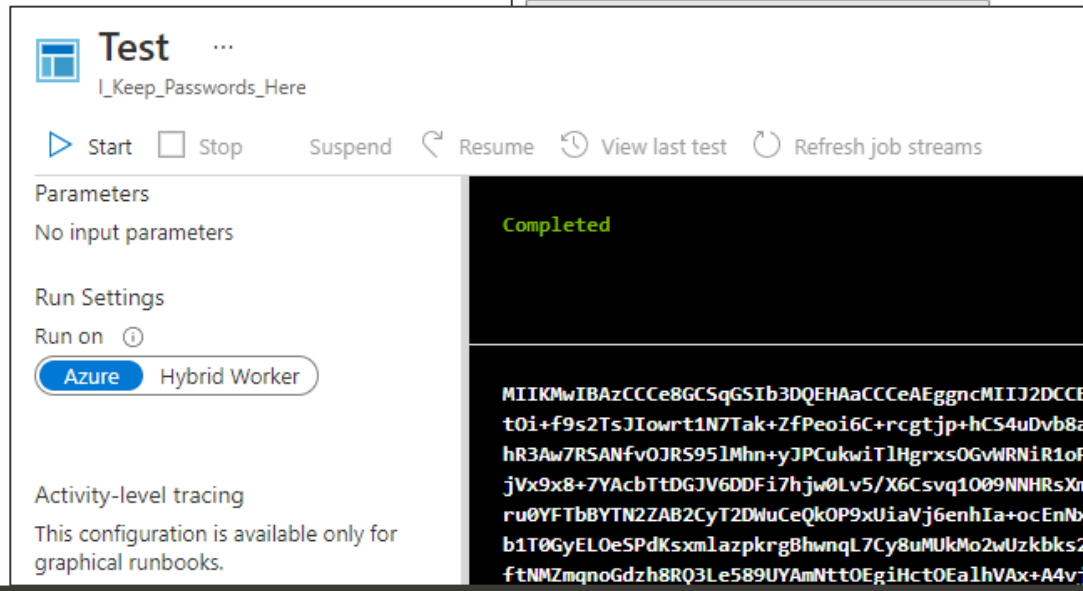
- Automation Account Components
  - Platform Credential Options
    - "Run as" Accounts / "Connections"
      - Older Method
      - Relies on App Registration
      - Uses Certificates for Authentication
      - Granted "Contributor" role on the subscription by default



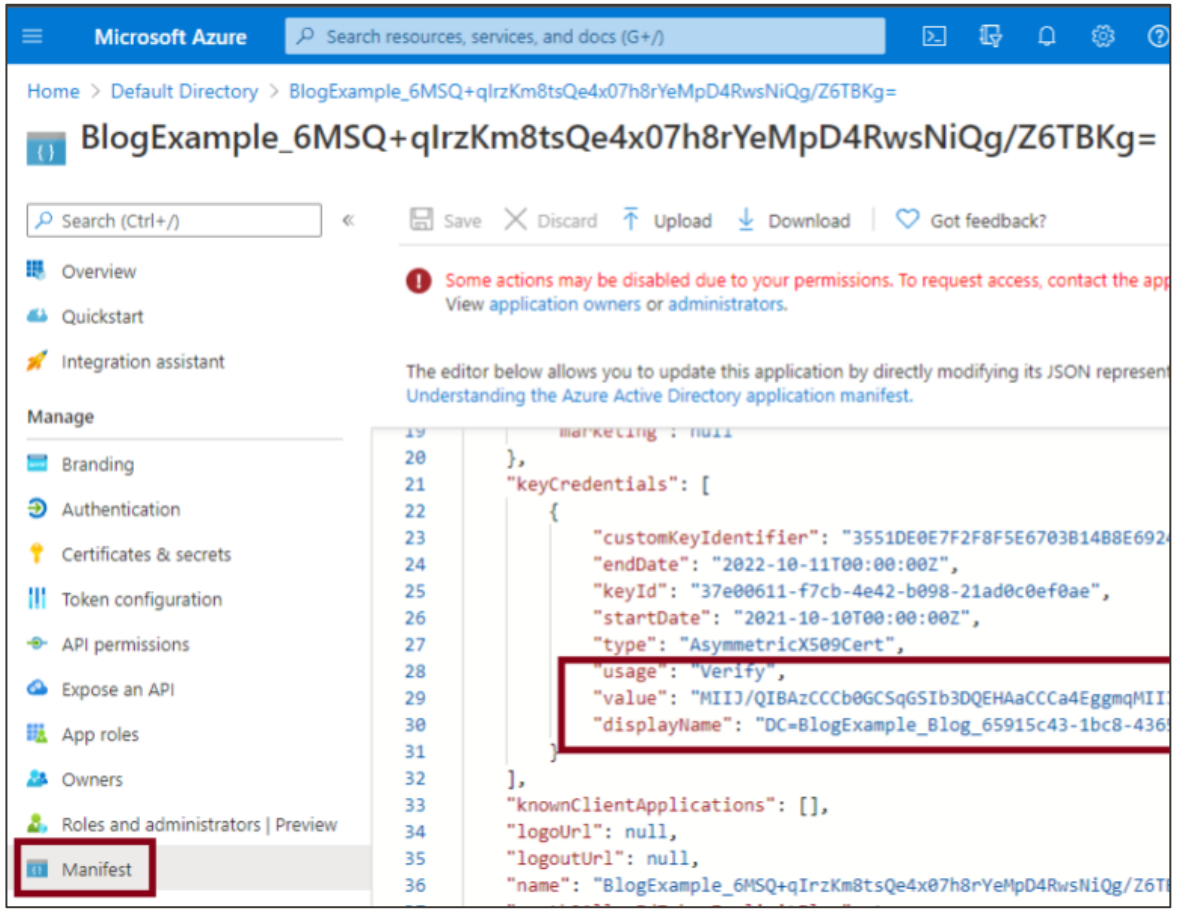
View Published Source

I_Keep_Passwords_Here

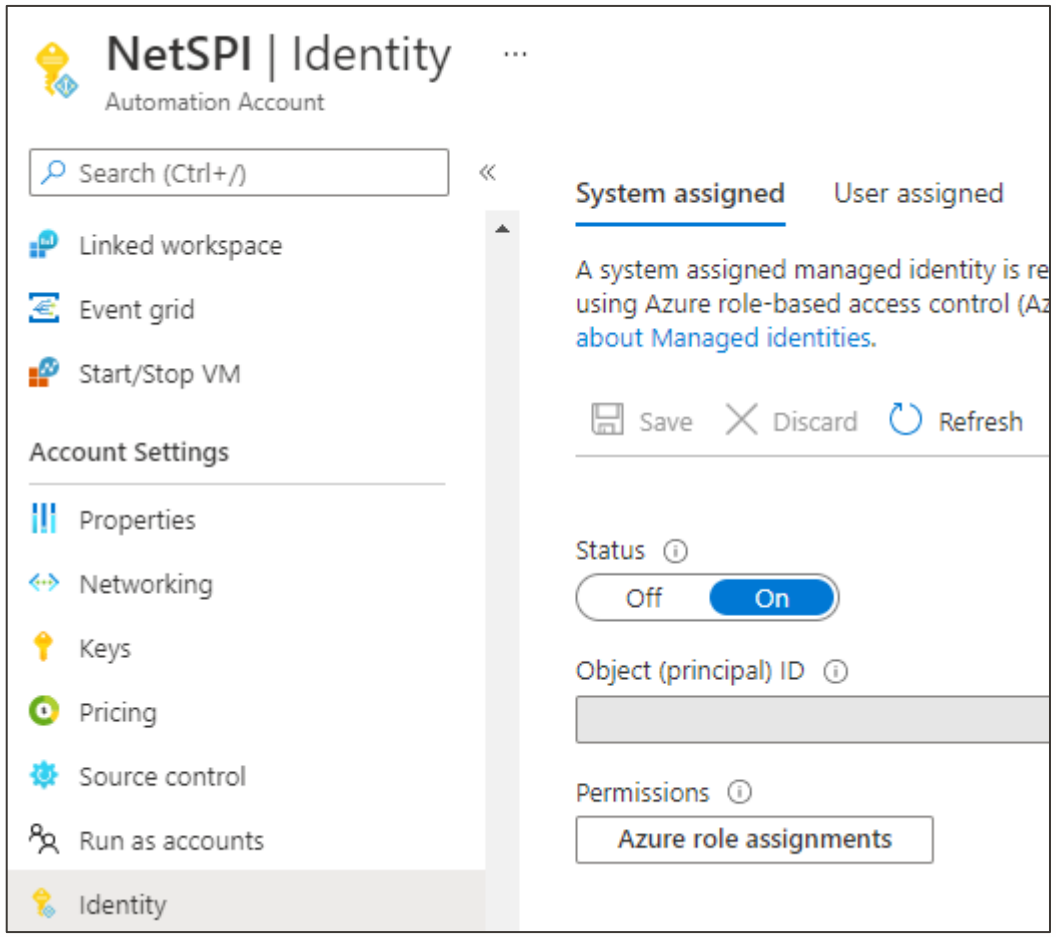
```
1  $RunAsCert = Get-AutomationCertificate -Name 'AzureRunAsCertificate'
2  $certPath = Join-Path $env:temp AzureRunAsCertificate.pfx
3  $Cert = $RunAsCert.Export('pfx','Password4theCert')
4  Set-Content -Value $Cert -Path $certPath -Force -Encoding Byte
5  $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($certPath))
6  Write-Output $base64string
```



- Automation Account Components
  - Platform Credential Options
    - “Run as” Account Credential Exposure
      - “CredManifest” (CVE-2021-42306) Vulnerability
      - Exposed PFX files in the App Registration Manifest files
      - Affected Services:
        - Automation Accounts
        - Azure Migrate
        - Azure Site Recovery
      - Applies to AAD users with ability to read App Registrations
        - Most cases, all users could read this data
        - Domain user -> Subscription Contributor
          - At a minimum…



- Automation Account Components
  - Platform Credential Options
    - Managed Identities
      - System assigned vs. User assigned
      - Generates tokens for temporary access
        - Uses localhost Managed Service Identity (MSI) endpoint
      - Safer alternative to “Run as” accounts
    - Extracting Tokens
      - Make a request to the MSI endpoint
      - Write to Job Output
      - Exfiltrate via POST request

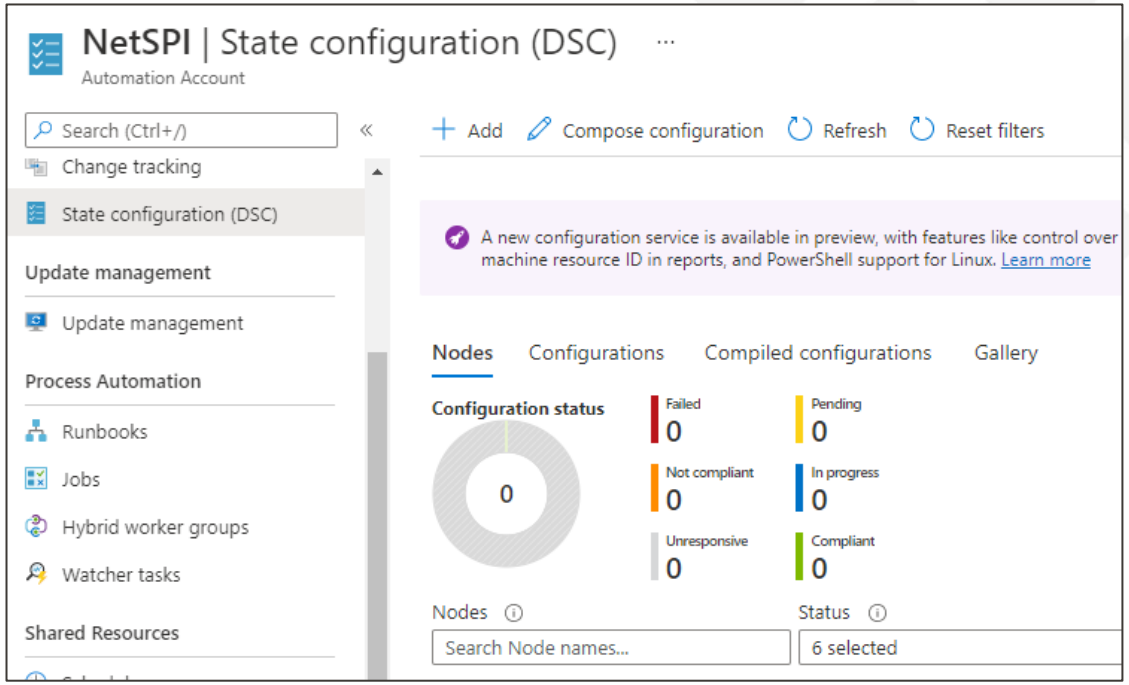


- Automation Account Components
  - Platform Credential Options
    - Managed Identities
      - “AutoWarp” Vulnerability
        - Cross-tenant isolation issue
        - MSI endpoint listening on high number port (40,000+)
        - Shared container space / lack of container isolation
        - Generate tokens for managed identities in other tenants

  - Blog:

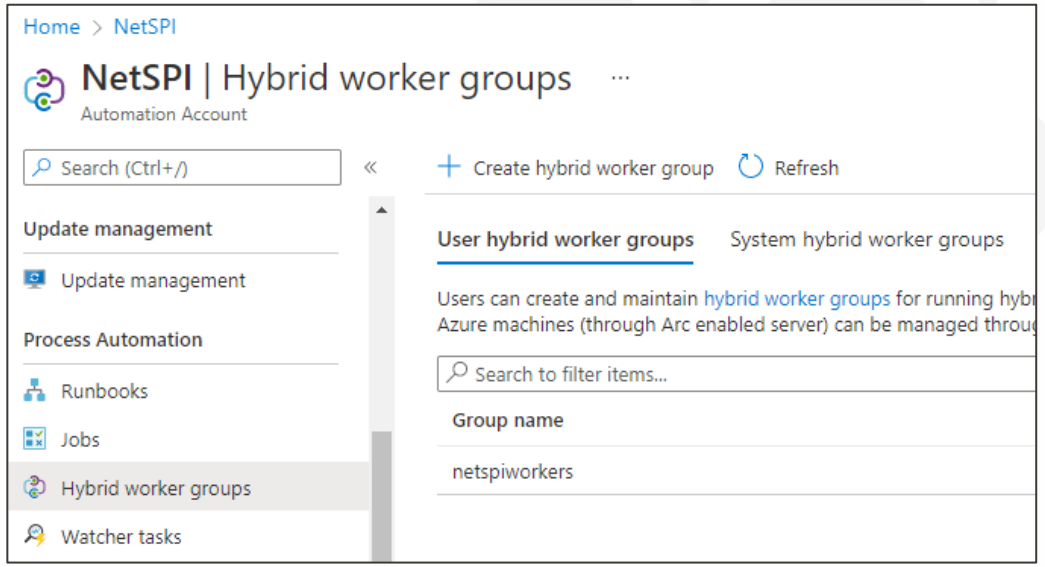
    https://orca.security/resources/blog/autowarp-microsoft-azure-automation-service-vulnerability/

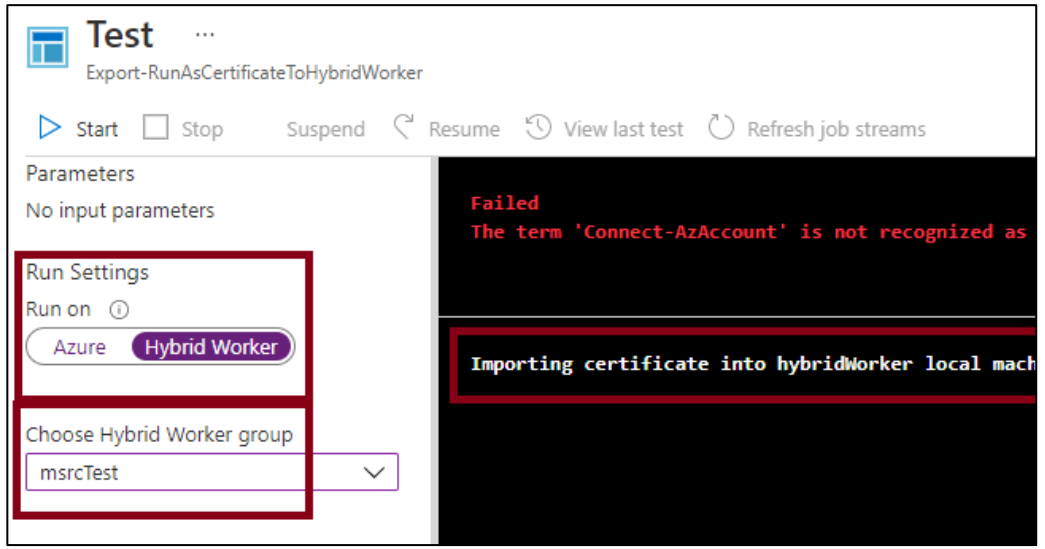
- Automation Account Components
  - Desired State Configurations
    - Used for managing system configurations
      - Domain joining
      - Running processes
      - Applying updates
    - Can be used for persistence / command execution
      - Ensure X process is running
      - If not, download exe and run it
    - Pivot to on-prem (ARC) systems
    - Can be a sneaky way to execute a Runbook
      - Configuration compilation happens in your Automation Account container



https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-persistence-with-desired-state-configurations/

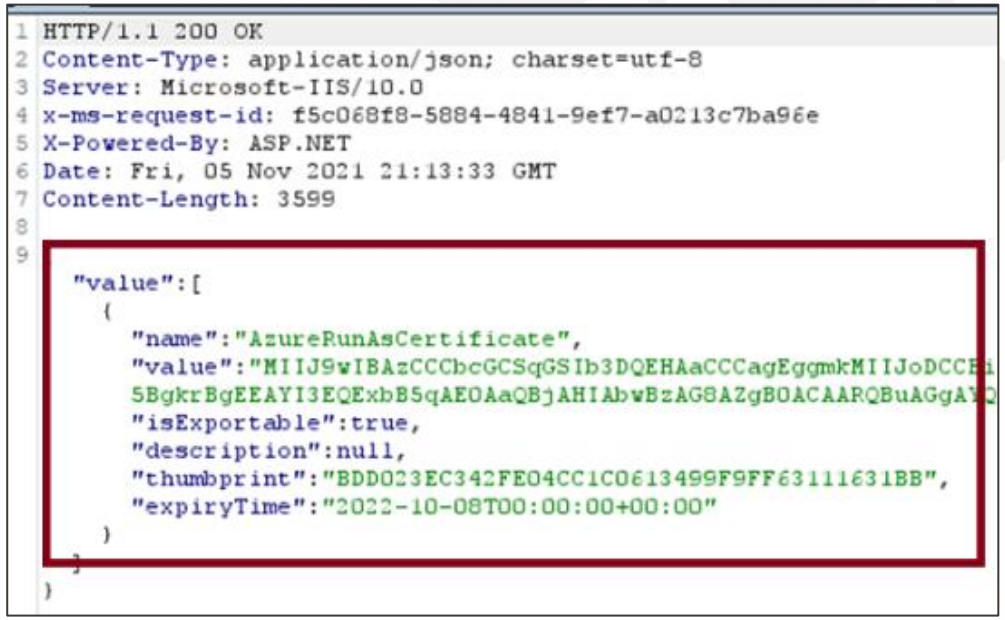
- Automation Account Components
  - Hybrid Workers
    - External systems that can be used to run Automation Runbooks
      - Greater CPU/RAM/Disk capacity
    - Requires “Run as” certificate to be installed for Authentication
    - Any user with local admin can extract the certificate
    - Multiple Azure roles can execute commands (as system) on VMs
      - Virtual Machine Contributor
      - Virtual Machine Administrator Login
      - Virtual Machine User Login
      - Azure Connected Machine Onboarding
      - Azure Connected Machine Resource Administrator
      - Log Analytics Contributor





AZURE AUTOMATION ACCOUNTS

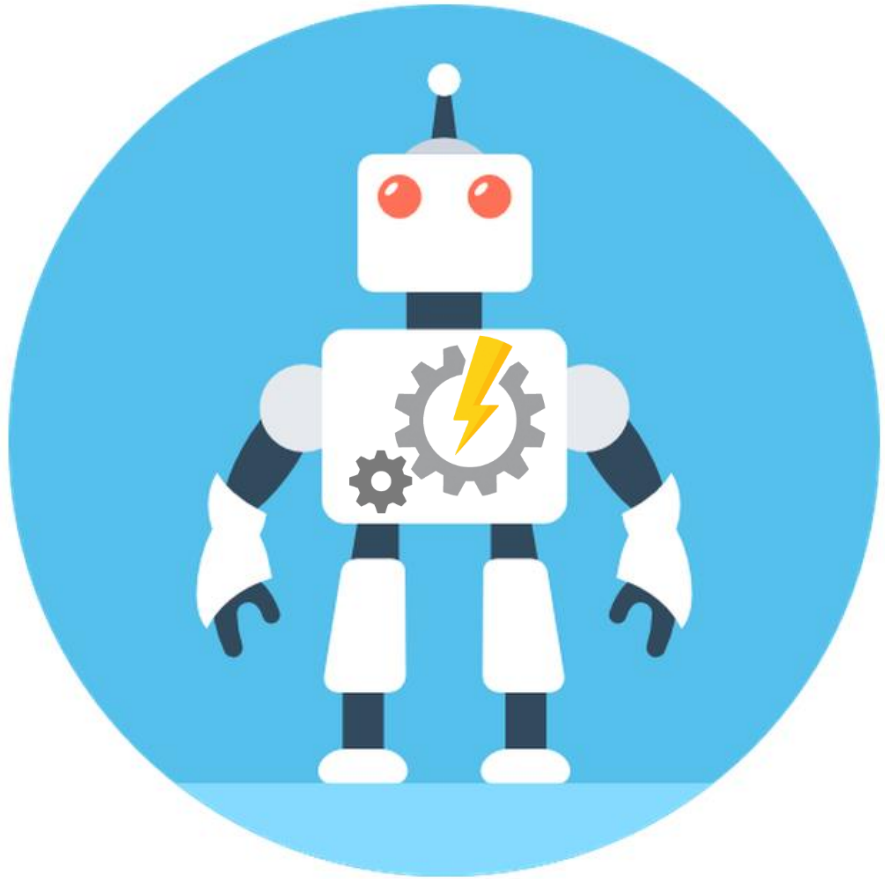
- Automation Account Components
  - Hybrid Workers
    - Undocumented APIs are used by the agent for tasking
      - Could be abused to access stored credentials and “Run as” certificates
    - Escalation from Reader to Contributor
      - Ability to read Automation Account enrollment key
      - Self enroll your own Hybrid Worker
      - Get token and request “Run as” certificate
      - Authenticate as the “Run as” account
    - Remediated by Microsoft
    - Subscription Reader can no longer read AA keys



- Remediated Privilege Escalation Path
  - Log Analytics Contributor Role
    - Initially allowed * permissions on Automation Accounts
    - Use Log Analytics Contributor role to export the “Run as” certificate
    - Use the exported certificate to login as a Contributor (slightly more privileges)

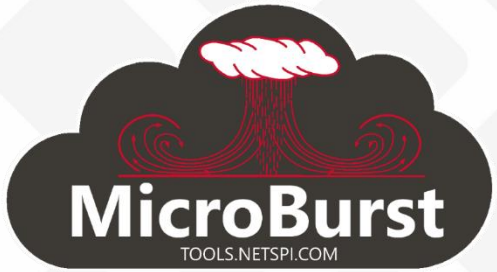
```
{
    "id": "/providers/Microsoft.Authorization/roleDefinitions/92aaf0da-9dab-42b6-94a3-d43ce8d16293",
    "properties": {
        "roleName": "Log Analytics Contributor",
        "description": "Log Analytics Contributor can read all monitoring data and edit monitoring settings.
        "assignableScopes": [
            "/"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read",
                    "Microsoft.Automation/automationAccounts/*",
                    "Microsoft.ClassicCompute/virtualMachines/extensions/*",
                    "Microsoft.ClassicStorage/storageAccounts/listKeys/action",
                    "Microsoft.Compute/virtualMachines/extensions/*",
```

- Automation Accounts Conclusions
  - Can be useful
    - Automates many of the tasks in an Azure environment
    - Security improvements are being made
  - Can be dangerous
    - Often misconfigured
    - Can expose credentials
    - Can allow for privilege escalation
  - Potential target during an Azure Pentest?
    - Absolutely



Questions?

ADDITIONAL INFO



- MicroBurst GitHub - https://github.com/NetSPI/MicroBurst
- NetSPI Blog - https://www.netspi.com/blog/technical/
- Automation Account Blogs:
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/encrypting-password-data-in-get-azpasswords/
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/maintaining-azure-persistence-via-automation-accounts/
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/exporting-azure-runas-certificates/
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-automation-accounts-key-stores/
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/escalating-azure-privileges-with-the-log-analystics-contributor-role/
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-cloud-vulnerability-credmanifest/
- Twitter - @kfosaaen

MINNEAPOLIS | NEW YORK | PORTLAND | DENVER | DALLAS

https://www.netspi.com


https://www.facebook.com/netspi


@NetSPI

https://www.slideshare.net/NetSPI