Implement JIT and JEA Administration in Windows Server 2019

DEPLOYING JUST ENOUGH ADMINISTRATION FOR SECURE MANAGEMENT

Robert McMillen
MICROSOFT CERTIFIED TRAINER AND SOLUTIONS EXPERT

Techpublishing.com

Registering your JEA Endpoint

Created Role Capability File

Session Configuration File

Register your Endpoint

Single Machine Configurations

Register using PowerShell

Register-PSSessionConfiguration

Test files

Test Role Configuration and Session files after created

Single Machine Configurations

Login as a standard user

Request admin access as needed

Create a JEA endpoint name

Each endpoint needs an identification

Multiple Machine Registration

JEA with Desired State Configuration

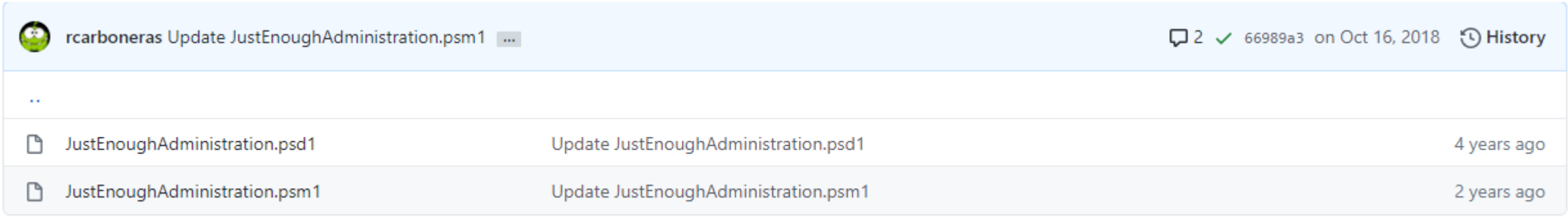
Role capabilities file has been created

Session configuration determined

Download the JEA DSC resource

JEA DSC Resource

https://github.com/powershell/JEA/tree/master/DSC%20Resource



Local Configuration Manager

- The engine of the DSC
- Determining refresh mode (push or pull)
- Specifying how often a node pulls and enacts configurations
- Associating the node with pull service
- Specifying partial configurations

Virtual Accounts

Run-As Account

Specified in the session config file

Virtual Account

Recommended over local accounts for higher security

Credentials are Hidden

The user doesn't know the creds so a hacker won't either

Virtual Accounts

Local administrator's group

Full local rights but no default server rights

Domain controller have different rules

Auditing account access

`WinRM Virtual Users\WinRM_VA_1_company_Joshua`

JEA Usage

Group Managed Service Accounts

Privileged Access Management (PAM)

Builds on Just in Time Administration

Administrative tasks are limited

Uses expiring permissions

Prepare

Protect

Operate

Monitor

Setting up PAM

How Does PAM Work?

New capabilities in Active Directory

Adds new objects to AD

Separation of duties

Be concise and keep the text to four lines or fewer

New Utilizations

Utilizes Bastion Forests and Microsoft Identity Manager

Why Should We Use PAM?

Isolation/scoping of privileges

Step-up and proof-up

Additional logging

Customizable workflow

JIT Access

Animation built in

Room for a bit more text

Use this layout for

- Longer sentence fragments
- List of things
- Procedure list
- Talking points

What Does JIT Solve?

Unauthorized system wide changes

Potential malware introduction

Possible stolen credentials

Change Control Needed

Process changes through policy

Prevents unplanned changes to AD

Allows only authorized users to make changes for limited times

How Can Privilege be Managed?

- Active Directory Delegation
- Third-party products
- Just Enough Administration (JEA)
- Privileged Access Management (PIM)

What Does JIT Need to Work?

Shadow Security Principals

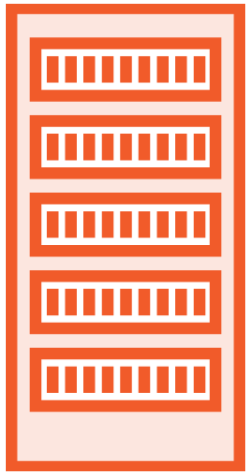
Time limits to administration

Bastion forest with cross-forest trust

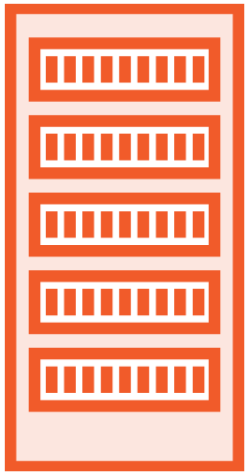
MIM for workflow

A Bastion Forest and Company Forest

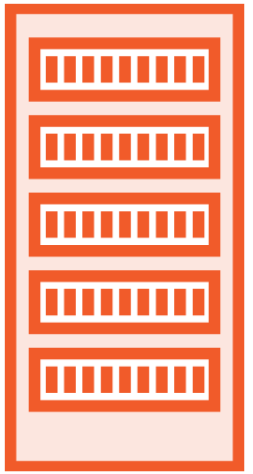
Company Forest trusts Bastion Forest



Company Forest Active Directory
DC1.Company.PRI



Bastion Forest Active Directory
DC1.Bastion.PRI



Microsoft Identity Management Server
MIM.Bastion.PRI

Monitoring JIT

- Audits
- Alerts
- Event Viewer
- Reporting

How is Access Requested?

MIM Web Portal

REST endpoint

PowerShell: New-PAMRequest