Assignment 2:  
Server Monitoring, Auditing, Remote Access and IIS

*Kyle Walker*

*NETW2500*

*10/03/2024*

Table of Contents

[Task 1: Preparing Domain Management Environment 2](#_Toc178866628)

[Task 2: System Monitoring: 4](#_Toc178866629)

[Part 3: 4](#_Toc178866630)

[Task 4: IIS Service 7](#_Toc178866631)

[Part 1 – Understanding IIS Service 7](#_Toc178866632)

# Task 1: Preparing Domain Management Environment

*RSATReport.txt:*

Name InstallState

---- ------------

RSAT-RemoteAccess Available

RSAT-RemoteAccess-Mgmt Available

RSAT-NFS-Admin Available

RSAT-Print-Services Available

RSAT-System-Insights Available

RSAT-Storage-Replica Available

RSAT-RemoteAccess-PowerShell Available

RSAT-WINS Available

RSAT-Hyper-V-Tools Available

RSAT-Online-Responder Available

RSAT-ADCS-Mgmt Available

RSAT-Fax Available

RSAT-ADRMS Available

RSAT-DFS-Mgmt-Con Available

RSAT-FSRM-Mgmt Available

RSAT-ADCS Available

RSAT-File-Services Available

RSAT-Bits-Server Available

RSAT-Feature-Tools-BitLocker-BdeAducExt Available

RSAT-Clustering Available

RSAT-DataCenterBridging-LLDP-Tools Available

RSAT-Feature-Tools-BitLocker-RemoteAdminTool Available

RSAT-Feature-Tools Available

RSAT-VA-Tools Available

RSAT-Feature-Tools-BitLocker Available

RSAT-SMTP Available

RSAT-Clustering-Mgmt Available

RSAT-SMS Available

RSAT-Shielded-VM-Tools Available

RSAT-SNMP Available

RSAT-Clustering-CmdInterface Available

RSAT-Clustering-PowerShell Available

RSAT-NLB Available

RSAT-Clustering-AutomationServer Available

RSAT-NPAS Installed

RSAT Installed

RSAT-DNS-Server Installed

RSAT-ADDS Installed

RSAT-AD-AdminCenter Installed

RSAT-AD-PowerShell Installed

RSAT-Role-Tools Installed

RSAT-AD-Tools Installed

RSAT-ADDS-Tools Installed

RSAT-RDS-Licensing-Diagnosis-UI Installed

RSAT-DHCP Installed

RSAT-RDS-Gateway Installed

RSAT-ADLDS Installed

RSAT-RDS-Tools Installed

# Task 2: System Monitoring:

## Part 3:

*Scripts\_audit.txt:*

Log Name: Security

Source: Microsoft-Windows-Security-Auditing

Date: 10/3/2024 2:56:00 PM

Event ID: 4907

Task Category: Audit Policy Change

Level: Information

Keywords: Audit Success

User: N/A

Computer: MS01A1C22.kaw.netw2500.ca

Description:

Auditing settings on object were changed.

Subject:

Security ID: kaw\sysop.kaw

Account Name: sysop.kaw

Account Domain: kaw

Logon ID: 0x9C380

Object:

Object Server: Security

Object Type: File

Object Name: C:\Scripts

Handle ID: 0x5f8

Process Information:

Process ID: 0x1a04

Process Name: C:\Windows\System32\dllhost.exe

Auditing Settings:

Original Security Descriptor:

New Security Descriptor: S:ARAI(AU;OICISAFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)

Event Xml:

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">

<System>

<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />

<EventID>4907</EventID>

<Version>0</Version>

<Level>0</Level>

<Task>13568</Task>

<Opcode>0</Opcode>

<Keywords>0x8020000000000000</Keywords>

<TimeCreated SystemTime="2024-10-03T17:56:00.545041600Z" />

<EventRecordID>12363</EventRecordID>

<Correlation />

<Execution ProcessID="4" ThreadID="5920" />

<Channel>Security</Channel>

<Computer>MS01A1C22.kaw.netw2500.ca</Computer>

<Security />

</System>

<EventData>

<Data Name="SubjectUserSid">S-1-5-21-3862670836-4240091929-1018321389-1105</Data>

<Data Name="SubjectUserName">sysop.kaw</Data>

<Data Name="SubjectDomainName">kaw</Data>

<Data Name="SubjectLogonId">0x9c380</Data>

<Data Name="ObjectServer">Security</Data>

<Data Name="ObjectType">File</Data>

<Data Name="ObjectName">C:\Scripts</Data>

<Data Name="HandleId">0x5f8</Data>

<Data Name="OldSd">

</Data>

<Data Name="NewSd">S:ARAI(AU;OICISAFA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;AU)</Data>

<Data Name="ProcessId">0x1a04</Data>

<Data Name="ProcessName">C:\Windows\System32\dllhost.exe</Data>

</EventData>

</Event>

# Task 4: IIS Service

## Part 1 – Understanding IIS Service

**Question 1. What is a Web Farm? Name three advantages of a Web Farm.**

A web farm is a collection of servers all working together to host a website. This helps ensure redundancy, performance and scalability. So, if one server goes down the entire website won’t be offline and helping spread out traffic to keep the site running fast and efficiently. If a number of requests are coming from multiple servers, a web farm can also provide load balancing to help maintain performance. (scholarhat, n.d.)

**Question 2. What is a Web Garden? Name three advantages of a Web Garden.**

A Web Garden is similar to a Web Farm, although instead of multiple servers handling a website, it is a collection of processes running on one web server to handle the requests from the website. This helps break up a process to utilize server resources more efficiently, adds reliability similar to a web farm and helps isolate applications so any problems like memory leaks do not spread and effect other processes in the Web Garden. (scholarhat, n.d.)

**Question 3. What is an Application Pool?**

An Application Pool is a feature in IIS that enables you to host many web applications on one server. (Solar Winds, n.d.)

**Question 4. What is a Worker Process?**

Worker Processes are what makes up a Web Garden. Many Worker Processes working together handle requests for the web server to help spread out the load.

|  |  |
| --- | --- |
| **Authentication Name** | **Description of Authentication type** |
| Active Directory Client Certification Authentication | A security feature that allows users to access a network using certificates from AD. |
| Anonymous Authentication | A way for users to access a website without any credentials |
| ASP.NET Impersonation | Allows an ASP.NET application to work using the credentials of an authenticated user instead of an application pool identity |
| Basic Authentication | A simple method of logging into a website with just a username and password |
| Digest Authentication | A more secure version of basic authentication, encrypting passwords instead of sending them in plaintext |
| Forms Authentication | Forms authentication works with ASP.NET to create custom login forms and manage user sessions |
| Windows Authentication | Uses Kerberos and NT LAN Manager to authenticate based on Windows credentials[[1]](#footnote-1) |

# Documentation:

*Snapshots:*

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

*Gold Copies:*

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated(MS01)

1. (OpenAI, n.d.) [↑](#footnote-ref-1)