DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.


FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to di-nccoe@nist.gov.

Public comment period: September 6, 2017 through November 6, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST Cybersecurity Practice Guides

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Businesses face a near-constant threat of destructive malware, ransomware, malicious insider activities, and even honest mistakes that can alter or destroy critical data. These data corruption events could cause a significant loss to a company’s reputation, business operations, and bottom line.

These types of adverse events, that ultimately impact data integrity, can compromise critical corporate information including emails, employee records, financial records, and customer data. It is imperative for organizations to recover quickly from a data integrity attack and trust the accuracy and precision of the recovered data.
The National Cybersecurity Center of Excellence (NCCoE) at NIST built a laboratory environment to explore methods to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also implemented auditing and reporting IT system use to support incident recovery and investigations.

This NIST Cybersecurity Practice Guide demonstrates how organizations can implement technologies to take immediate action following a data corruption event. The example solution outlined in this guide encourages effective monitoring and detection of data corruption in standard, enterprise components as well as custom applications and data composed of open-source and commercially available components.

**KEYWORDS**

*business continuity; data integrity; data recovery; malware; ransomware*

**ACKNOWLEDGMENTS**

We are grateful to the following individuals for their generous contributions of expertise and time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steve Petruzzo</td>
<td>GreenTec USA</td>
</tr>
<tr>
<td>Steve Roberts</td>
<td>Hewlett Packard Enterprise</td>
</tr>
<tr>
<td>Dave Larimer</td>
<td>IBM Corporation</td>
</tr>
<tr>
<td>John Unthank</td>
<td>IBM Corporation</td>
</tr>
<tr>
<td>Jim Wachhaus</td>
<td>Tripwire</td>
</tr>
<tr>
<td>Donna Koschalk</td>
<td>Veeam Software Corporation</td>
</tr>
<tr>
<td>Brian Abe</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Sarah Kinling</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Josh Klosterman</td>
<td>The MITRE Corporation</td>
</tr>
</tbody>
</table>
The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

<table>
<thead>
<tr>
<th>Technology Partner/Collaborator</th>
<th>Build Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>GreenTec USA</td>
<td>GreenTec WORMdisk, v151228</td>
</tr>
<tr>
<td>Hewlett Packard Enterprise</td>
<td>HPE ArcSight ESM, v6.9.1</td>
</tr>
<tr>
<td></td>
<td>HPE ArcSight Connector, v7.4.0</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>IBM Spectrum Protect, v8.1.0</td>
</tr>
<tr>
<td>Tripwire</td>
<td>Tripwire Enterprise, v8.5</td>
</tr>
<tr>
<td></td>
<td>Tripwire Log Center, v7.2.4.80</td>
</tr>
<tr>
<td>Veeam Software Corporation</td>
<td>Veeam Availability Suite, v9.5</td>
</tr>
</tbody>
</table>
Contents

1 Introduction .................................................................................................................. 1
  1.1 Practice Guide Structure ...................................................................................... 1
  1.2 Build Overview .................................................................................................... 2
  1.3 Typographical Conventions .................................................................................. 3

2 Product Installation Guides ......................................................................................... 3
  2.1 Active Directory and Domain Name System (DNS) Server .................................. 4
    2.1.1 Installing Features .................................................................................... 4
    2.1.2 Creating a Certificate Authority .............................................................. 17
    2.1.3 Configure Account to Add Computers to Domain ...................................... 30
    2.1.4 Adding Machines to the Correct Domain .................................................. 36
    2.1.5 Configuring Active Directory to Audit Account Activity ........................... 46
  2.2 Microsoft Exchange Server ................................................................................... 48
    2.2.1 Install Microsoft Exchange ....................................................................... 48
  2.3 SharePoint Server ................................................................................................. 60
    2.3.1 Install Roles and Features ......................................................................... 60
    2.3.2 Install SharePoint ..................................................................................... 67
    2.3.3 SharePoint Products Configuration Wizard ............................................. 73
    2.3.4 Configure SharePoint .............................................................................. 74
  2.4 Windows Server Hyper-V Role ........................................................................... 75
    2.4.1 Production Installation ............................................................................. 75
  2.5 MS SQL Server ..................................................................................................... 81
    2.5.1 Install and Configure MS SQL ................................................................. 81
    2.5.2 Open Port on Firewall ............................................................................. 90
    2.5.3 Add a New Login to the Database ....................................................... 95
  2.6 HPE ArcSight Enterprise Security Manager (ESM) ............................................... 97
    2.6.1 Install Individual ArcSight Windows Connectors .................................... 97
    2.6.2 Install a Connector Server for ESM on Windows 2012 R2 ....................... 116
    2.6.3 Install Syslog Connector for Ubuntu ..................................................... 131
2.13.5 Create a Policy to Backup to GreenTec disks ................................................................. 327
2.13.6 Create a Schedule That Uses the New Policy ............................................................ 332
2.13.7 Installing Open File Support on the Client ................................................................. 335
2.13.8 Temporarily Add Client to GreenTec IBM Server ...................................................... 340

2.14 Integration: Backing Up and Restoring System State with GreenTec ......................... 345
2.14.1 Installing Windows Server Essentials for System State Backup Capability ................. 346
2.14.2 Configure Network Accessible GreenTec Disk ......................................................... 351
2.14.3 Backup the System State ......................................................................................... 353
2.14.4 Restoring the System State ....................................................................................... 354

2.15 Integration: Copying IBM Backup Data to GreenTec WORMdisks ............................ 355
2.15.1 Copying Backups for a Single Machine to a GreenTec WORMDisk ......................... 356

2.16 Integration: Tripwire and MS SQL Server ................................................................. 360
2.16.1 Create a New Account on MS SQL Server ............................................................... 360
2.16.2 Create a New Audit on MS SQL Server .................................................................... 364
2.16.3 Create a New Node for the MS SQL Server on Tripwire Enterprise ..................... 371
1 Introduction

The following guides show IT professionals and security engineers how we implemented this data integrity solution example. We cover all the products employed in this reference design. We do not recreate the product manufacturers’ documentation, which is presumed to be widely available. Rather, these guides show how we integrated the products into our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the data integrity solution. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:
- NIST SP 1800-11a: Executive Summary
- NIST SP 1800-11c: How-To Guides – instructions for building the example solution (you are here)

Depending on your role in your organization, you may use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the Executive Summary (NIST SP 1800-11a), which describes the:

- challenges enterprises face in protecting their data from loss or corruption
- example solution built at the National Cybersecurity Center of Excellence (NCCoE)
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-11b, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.1, Assessing Risk Posture, provides a description of the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security characteristics of the example solution to cybersecurity standards and best practices.

Consider sharing the Executive Summary (NIST SP 1800-11a) with your leadership team to help them understand the importance of adopting standards-based data integrity solutions.
IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide (NIST SP 1800-11c) to replicate all or parts of the build created in our lab. The guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers’ documentation, which is generally widely available. Rather, we show how we integrated the products in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the data integrity solution. Your organization’s security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices.

A NIST cybersecurity practice guide does not describe “the” solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to di-nccoe@nist.gov.

1.2 Build Overview

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also explored the issues of auditing and reporting that IT systems use to support incident recovery and investigations. The servers in the virtual environment were built to the hardware specifications of their specific software components.

The NCCoE worked with members of the Data Integrity Community of Interest to develop a diverse (but non-comprehensive) set of use case scenarios against which to test the reference implementation. These are detailed in Volume B, Section 5.1. For a detailed description of our architecture, see Volume B, Section 4.
1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

<table>
<thead>
<tr>
<th>Typeface/ Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>filenames and pathnames, references to documents that are not hyperlinks, new terms, and placeholders</td>
<td>For detailed definitions of terms, see the NCCoE Glossary.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>names of menus, options, command buttons and fields</td>
<td>Choose File &gt; Edit.</td>
</tr>
<tr>
<td>Monospace</td>
<td>command-line input, on-screen computer output, sample code examples, status codes</td>
<td>mkt</td>
</tr>
<tr>
<td>Monospace <strong>Bold</strong></td>
<td>command-line user input contrasted with computer output</td>
<td>service sshd start</td>
</tr>
<tr>
<td><em>blue text</em></td>
<td>link to other parts of the document, a web URL, or an email address</td>
<td>All publications from NIST’s National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a></td>
</tr>
</tbody>
</table>

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all the products used to build an instance of the example solution.

The products presented in this document have the potential to quickly change both interfaces and functionality. This document aims to highlight the core configurations an organization could use along with visual representations of those configurations.
2.1 Active Directory and Domain Name System (DNS) Server

As part of our enterprise emulation, we included an Active Directory server that doubles as a DNS server. This section covers the installation and configuration process used to set up Active Directory and DNS on a Windows Server 2012 R2 machine.

2.1.1 Installing Features

1. Open Server Manager.

2. Click the link Add Roles and Features.
3. Click **Next**.

4. Select **Role-based or feature-based installation**.

5. Click **Next**.
6. Select **ADDNS** (or the correct Windows Server name) from the list.

7. Click **Next**.
8. Check the box next to **Active Directory Domain Services**.

9. Click **Add Features**.

10. Click **Next**.

12. Select any additional features and click Add Features on the popup.

13. Click Next.
14. Click **Next**.
15. Click **Install**.

16. Wait for the installation to complete.
17. Select **Post-Deployment Configuration** or **Promote this server to a domain controller**.

18. Select **Add a new forest**.
19. Enter a **Root domain name**. Example: DI.TEST.

20. Click **Next**.

21. Select **Windows Server 2012 R2** for the **Forest Functional Level**.
22. Select **Windows Server 2012 R2** for the **Domain Functional Level**.

23. Check the box next to **DNS server** and **Global Catalog**.

24. Do not check the box next to **read-only domain controller**.

25. Specify a password for **DSRM** (D@T@Integrity#1).

26. Click **Next**.
27. Click Next.

28. Verify the NetBIOS name.

29. Click Next.
30. Click Next.

31. Click Next.
32. Click Install.

33. The server automatically reboots.
2.1.2 Creating a Certificate Authority

1. Open Server Manager.
2. Click the link **Add Roles and Features**.

3. Click **Next**.

4. Select **Role-based or feature-based installation**.

5. Click **Next**.
6. Select ADDNS (or the correct Windows Server name) from the list.
7. Click Next.
8. Check the box next to **Active Directory Certificate Services**
9. Click **Add Features**.

10. Click **Next**.
11. Click Next.

12. Click Next.
13. Select **Certification Authority** on the **Role Services** list.

14. Click **Next**.
15. Click Install.

16. Select **Configure Active Directory Certificate Services on the destination server**.

17. Click Next.
18. Select **Certification Authority**.

19. Click **Next**.

20. Select **Enterprise CA**.
21. Click Next.

22. Select Root CA.

23. Click Next.
24. Select **Create a new private key**.

25. Click **Next**.

26. Select **RSA#Microsoft Software Key Storage Provider**.

27. Enter **2048** in the box.
28. Select **SHA256** from the list.

29. Click **Next**.

30. Click **Next**.
31. Set the time to 5 years.

32. Click Next.

33. Click Next.
34. Click **Configure**.

![Configuration screenshot]

- **Certification Authority**
  - Enterprise Root
- **Cryptographic Providers**
  - RSA
- **Hash Algorithm**
  - SHA256
- **Key Length**
  - 2048
- **Certificate Validity Period**
  - 8/11/2022 10:52:00 AM
- **Distinguished Name**
  - CN=WIN-MR2BDTCRM01-CA,DC=DLDC=CTEST
- **Certificate Database Location**
  - C:\Windows\System32\CertLog
- **Certificate Database Log**
  - C:\Windows\System32\CertLog

**Results:**

- **Certification Authority**
  - **Configuration succeeded**

**More about CA Configuration**
2.1.3 Configure Account to Add Computers to Domain

1. Open the start menu.

2. Type dsa.msc and run the program.

3. Right click on Users in the left pane.
4. Click **Delegate Control**.

5. Click **Next**.
6. Click Add to add a user or group. Example: Domain Admins.

7. When finished adding users or groups, click OK.

8. Click Next.
9. Choose **Create a custom task to delegate**.

10. Click **Next**.

11. Choose **Only the following objects in the folder**.

12. Select the **Computer Objects** check box.
13. Check the box for **Create selected objects in this folder**.
14. Check the box for **Delete selected objects in this folder**.

15. Click **Next**.
16. In the Permissions List, choose Reset Password, Read and write Account Restrictions, Validated write to DNS host name, Validated write to service principal name.

17. Click Next.

18. Observe the successful installation and click Finish.
2.1.4 Adding Machines to the Correct Domain

1. Right click network icon in task bar.
2. Click **Open Network and Sharing center**.
3. Click the link for editing the network interface under **Connections**.

4. Click **Properties**.
5. Click **Internet Protocol Version 4**.
6. Click Properties.
7. Set the **DNS** field to the field of the AD/DNS server.

8. Click **OK**.

9. Exit out of the **Network and Sharing Center**

10. Push the **start menu** button.
11. Go to This PC.

12. Right click in the window and choose Properties.
13. Under **Name, domain, and workgroup settings**, click **Change settings**.

14. Click **Change**...
Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
WIN-MR2BO7CRM01

Full computer name:
WIN-MR2BO7CRM01

Member of

- Domain:
- Workgroup:
  WORKGROUP

[OK] [Cancel]
15. Select **Domain** and enter the domain specified on the AD/DNS server.

16. Click **OK**.
17. Enter the credentials of an account in AD which has the right permissions to add a group to the domain.

18. Click **OK** a few times and restart the server when prompted.
2.1.5 Configuring Active Directory to Audit Account Activity

1. Open Local Security Policy from the Start Menu.

2. Open Local Policies > Audit Policy.

3. Right click Audit account management.

4. Select Properties.
Audit account management Properties

Local Security Setting  Explain

Audit account management

Audit these attempts:

☐ Success
☐ Failure

Warning: This setting might not be enforced if the policy is configured to override category level audit policy.
For more information, see [Audit account management](Q321458).

OK  Cancel  Apply
5. Check the boxes next to Success and Failure.
6. Click OK.
7. Account management activities will now be reported to Windows Event Log – Security.

2.2 Microsoft Exchange Server

As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

2.2.1 Install Microsoft Exchange
1. Run Exchange2016-x64.exe.
2. Choose the directory for the extracted files and press **OK**.

3. Enter the directory and run **setup.exe**.
4. Select **Connect to the Internet and check for updates.**

![Microsoft Exchange Server 2016 Setup](image)

5. Wait for the check to finish.
6. Click **Next**.
7. Wait for the copying to finish.
8. Click **Next**.
9. Click **I accept the terms in the license agreement.**

![License Agreement](image)

10. Click **Next.**
11. Click **Use Recommended Settings**.
12. Click **Next**.
13. Check **Mailbox role**.
14. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.
15. Click **Next**.

16. Specify the installation path for MS Exchange.
17. Click **Next**.

18. Specify the name for the Exchange organization. Example: DI.
19. Decide whether to apply split permissions based on the needs of the enterprise.

20. Click **Next**.

21. Click **No**.
22. Click Next.

23. Install any prerequisites listed.
24. If necessary, restart the server and re-run `setup.exe`, following through steps 3-22 again.

25. Click **Install**.
26. Wait for setup to complete.

2.3 SharePoint Server

As part of our enterprise emulation, we include a Microsoft SharePoint server. This section covers the installation and configuration process used to set up SharePoint on a Windows Server 2012 R2 machine.

2.3.1 Install Roles and Features

1. Open Server Manager.
2. Click **Manage**.

3. Click **Add Roles and Features**.
4. Click Next.

5. Choose **Role-based or feature-based installation**.

6. Click Next.

7. Choose **Select a server from the server pool**.

8. Choose the SharePoint server from the list.
9. Click **Next**.

10. Check **Application Server Role**.

11. Click **Next**.

12. Check **IIS Hostable Web Core**.
13. Click **Next**.

14. Click **Next**.

15. Check all boxes under **Application Server Role Services**.
16. Click **Next**.

17. Choose **Create a self-signed certificate**.

18. Click **Next**.
19. Click **Next**.

20. Check all boxes under Web Server (IIS) Role Services.

21. Click **Next**.

22. Check Restart the destination server automatically if required.
23. Click **Install**.

24. The server may automatically restart.

25. Right click the **.ISO file** for **SharePoint Server**.

26. Choose **Mount**.

### 2.3.2 Install SharePoint

1. Navigate to the main directory of the ISO.

2. Double click **pre-requisite installer**.
3. Click **Next**.
4. Click **I accept the terms of the License agreement**.
5. Click **Next**.
6. Resolve any dependencies and repeat steps 2-5.

7. After the successful installation, click **Finish**.
8. The server may automatically restart.
9. Remount the **.ISO file** for **SharePoint Server**.
10. Navigate to the main directory of the **.ISO file**.
11. Double click the program called setup.

12. Click Install SharePoint Server.

13. Enter your product key when prompted.
14. Click **Continue**.

15. Check **I accept the terms of this agreement**.

16. Click **Continue**.

17. Choose which **Server Type** fits your organization's purposes.
18. Click **Install Now**.
19. Wait for the installation to finish.
20. Check **Run the SharePoint Products Configuration Wizard now**.
21. Click **Close**.
2.3.3 SharePoint Products Configuration Wizard

1. Click **Next**.

2. Click **Yes**.

3. Click **Next**.
4. Wait for the configuration to complete (it may take up to 30 minutes depending on your system).

5. Click Finish.

2.3.4 Configure SharePoint

1. Open a browser and navigate to http://sharepoint (replace sharepoint with the hostname or IP address of the SharePoint server).

2. Choose the type of SharePoint template that fits your business needs. Example: Enterprise > Document Center.
2.4 Windows Server Hyper-V Role

As part of our simulated enterprise, we include a Windows Hyper-V server. This section covers the instructions for installing Windows Server Hyper-V on a Windows Server 2012 R2 machine.

The instructions for enabling the Windows Server Hyper-V Role are retrieved from https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx and are replicated below for preservation and ease of use.

2.4.1 Production Installation

1. In Server Manager, on the Manage menu, click Add Roles and Features.
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.

3. Click **Next**.

4. On the **Select installation type** page, select **Role-based or feature-based installation**.
536 5. Click Next.

537 6. On the Select destination server page, select a server from the server pool.

538 7. Click Next.

540 8. On the Select server roles page, select Hyper-V.
9. To add the tools that you use to create and manage virtual machines, click **Add Features**.

10. Click **Next**.

11. Click **Next**.
12. Click **Next**.

13. On the **Create Virtual Switches** page, select the appropriate options.

14. Click **Next**.

15. On the **Virtual Machine Migration** page, select the appropriate options.
16. Click Next.

17. On the Default Stores page, select the appropriate options.

18. Click Next.
19. On the Confirm installation selections page, select Restart the destination server automatically if required.

20. Click Install.

21. When installation is finished, verify that Hyper-V installed correctly. Open the All Servers page in Server Manager, select a server on which you installed Hyper-V. Check the Roles and Features tile on the page for the selected server.

2.5 MS SQL Server

As part of both our enterprise emulation and data integrity solution, we include a Microsoft SQL Server. This section covers the installation and configuration process used to set up Microsoft SQL Server on a Windows Server 2012 R2 machine.

2.5.1 Install and Configure MS SQL

2. Locate the installation media in the machine and click on SQL2014_x64_ENU to launch SQL Server Installation Center.
3. On the left menu, select **Installation**.
4. Select New SQL Server stand-alone installation or add features to an existing installation. This will launch the SQL Server 2014 setup.

5. In the Product Key section, enter your product key.

6. Click Next.
7. In the **License Terms** section, read and click **I accept the license terms**.

8. Click **Next**.

9. In the **Install Rules** section, note and resolve any further conflicts.
10. Click **Next**.

11. In the **Setup Role** section, select **SQL Server Feature Installation**.
12. Click Next.

13. In the Feature Selection section, select the following:
   a. Database Engine Services
   b. Client Tools Connectivity
   c. Client Tools Backwards Compatibility
   d. Client Tools SDK
   e. Management Tools – Basic
   f. Management Tools – Complete
   g. SQL Client Connectivity SDK
   h. Any other desired features

14. Click Next.

15. In the Instance Configuration section, select Default instance.
16. Click **Next**.

17. In the **Server Configuration** section, click **Next**.
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.

19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User**.
   
a. For Domain accounts, simply type in `$DOMAINNAME\$USERNAME` into **Enter the object names to select** textbox.

   b. Click **OK**.

   c. For local computer accounts, click on **locations** and select the computers name.

   d. Click **OK**.

   e. Type the username into the **Enter the object names to select** textbox.

   f. Once you are finished adding users, click **Next**.

20. In the **Ready to install** section, verify the installation and click **Install**.
21. Wait for the install to finish.
2.5.2 Open Port on Firewall


2. Click Inbound Rules and then New Rule.
3. Select **Port**.

4. Click **Next**.

5. Select **TCP** and **Specific local ports**.

6. Type **1433** into the text field.
7. Click **Next**.

8. Select **Allow the connection**.
9. Click **Next**.

10. Select all applicable locations.
11. Click **Next**.
12. Name the rule **Allow SQL Access**.
13. Click Finish.

2.5.3 Add a New Login to the Database

1. Open SQL Server Management Studio.
2. Hit **Connect** to connect to the database.

3. In the **Object Explorer** window, expand the **Security** folder.

4. Right click on the **Logins** folder and click **New Login**.

5. Input the desired user.

6. Click **OK**.
2.6 HPE ArcSight Enterprise Security Manager (ESM)

HPE ArcSight Enterprise Security Manager is primarily a log collection/analysis tool with features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs generated by various systems, applications, and security solutions.

This installation guide assumes a pre-configured CentOS 7 Virtual Machine with ESM already installed and licensed. This section covers the installation and configuration process used to set up ArcSight agents on various machines.

2.6.1 Install Individual ArcSight Windows Connectors

1. Log in to your DNS server.

2. Add the host name of the ESM server *vm-esm691c* to the DNS list and associate it with the IP address of the ESM server.

3. Run the installation file *ArcSight-7.4.0.7963.0-Connector-Win64*. 
4. Wait for the initial setup to finish.

5. Click Next.
6. Choose a destination folder. Note: It is recommended to change the default destination folder to `<default>\Windows`. This is to avoid conflicts if you wish to install more than one connector.

7. Click Next.
8. Click **Next**.

9. Click **Install**.

10. Wait for the installation to finish.
11. Select **Add a Connector**.
12. Click **Next**.
13. Choose **Microsoft Windows Event Log - Native** from the list.
14. Click Next.

15. Check **Security log**, **System log**, and **Application Log**.
16. Click Next.
17. Click **Next**.

18. Choose **ArcSight Manager (encrypted)**.
19. Click Next.
20. For Manager Hostname, put vm-esm691c, or the hostname of your ESM server.
21. For Manager Port, put 8443 (or the port that ESM is running on) on the ESM server.
22. Enter the username and password used for logging into ArcSight Command Center. Default: (admin/password)
23. Click Next.

24. Set identifying details about the system to help identify the connector (include a value for Name; the rest is optional).
25. Click **Next**.

26. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the Virtual Machine.
27. Click **Next**.
28. Click **Next**.

29. Choose **Install as a service**.
30. Click **Next**.
31. Click **Next**.
32. Click **Next**.

33. Choose **Exit**.
34. Click **Next**.
35. Click **Done**.
36. Open **Task Manager**.
37. Click **More Details**.

38. Go to the **Services** tab.
39. Find the service just created for ArcSight and right click it.
40. Choose **Start**.
41. The machine will now report its logs to ArcSight ESM.

2.6.2 Install a Connector Server for ESM on Windows 2012 R2

1. Run the installation file ArcSight-7.4.0.7963.0-Connector-Win64.
2. Wait for the initial setup to finish.

3. Click **Next**.

4. Choose a destination folder. Note: It is recommended to change the default destination folder to `<default>\Windows`. This is to avoid conflicts if you wish to install more than one connector.
5. Click Next.

6. Click Next.
7. Click **Install**.
8. Wait for the installation to finish.
9. Select **Add a Connector**.
10. Click **Next**.
11. Choose **Microsoft Windows Event Log - Native** from the list.
12. Click **Next**.
13. Check **Security log, System log, Application Log**.
14. Check **Use Active Directory**.
15. Click **Next**.

16. Fill out the form with the appropriate information for your Active Directory server. It is recommended to create an account on Active Directory specifically for ArcSight.

17. Select **Replace Hosts** for Use Active Directory host results for.
18. Click Next.

19. Select all the event types you would like forwarded from each machine.

20. Click Next.
21. Click **Next**.
22. Choose **ArcSight Manager (encrypted)**.
23. Click **Next**.
24. For **Manager Hostname**, use **vm-esm691c** or the hostname of your ESM server.
25. For **Manager Port**, use **8443** (or the port that ESM is running on) on the ESM server.
26. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)
27. Click **Next**.

28. Set identifying details about the system to help identify the connector (include **Name**; the rest is optional).

29. Click **Next**.

30. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the VM.
31. Click **Next**.

32. Click **Next**.

33. Choose **Install as a service**.
34. Click **Next**.
35. Click **Next**.

36. Choose **Exit**.
37. Click **Next**.

38. Click **Done**.
39. Open **Task Manager**.
40. Click **More Details**.

41. Go to the **Services** tab.
42. Find the service just created for ArcSight and right click it.
43. Choose **Start**.
The machine will now report all collected Windows logs to ArcSight ESM.

### 2.6.3 Install Syslog Connector for Ubuntu

1. Run `./ArcSight-7.4.0.7963.0-Connector-Linux64.bin`. 

---

**NIST SP 1800-11C: Data Integrity** 131
2. Click Next.

3. Choose a folder to install the connector in.

4. Click Next.
5. Click **Next**.

6. Click **Install**.

7. Choose **Add a Connector**.
8. Click **Next**.
9. Choose **Syslog File**.
10. Click Next.

11. For File Absolute Path Name, select a log file from which to forward events to ESM. Example: /var/log/syslog

12. Select realtime to have events be streamed or batch to have events sent over in sets.

13. For Action upon Reaching EOF, select None.
14. Click Next.

15. Select ArcSight Manager (encrypted).
16. Click Next.

17. For **Manager Hostname**, put `vm-esm691c` or the hostname of your ESM server. (You may need to add `dns-search.di.test` to `/etc/network/interfaces` if the hostname does not resolve on its own. For example, `vm-esm691c.di.test` may resolve but `vm-esm691c` may not.)

18. For **Manager Port**, put **8443** (or the port that ESM is running on) on the ESM server.

19. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)
20. Click Next.

21. Set identifying details about the system to help identify the connector (include Name; the rest is optional).
22. Click **Next**.

23. Choose **Import the certificate to connector from destination**.
24. Click Next.
25. Click **Next**.
26. Click **Next**.

27. Choose **Exit**.
28. Click **Next**.
29. Click Done.

2.7 IBM Spectrum Protect

IBM Spectrum Protect is a backup/restore solution that makes use of cloud-based object storage. It allows for administrative management of backups across an enterprise, providing users with mechanisms to restore their data on a file level. This section covers the installation and configuration process used to set up IBM Spectrum Protect on a Windows Server 2012 R2 machine, as well as the installation and configuration processes required for installing the backup/archive client on various machines.

2.7.1 Install IBM Spectrum Protect Server

1. You may need to disable Run all administrators in Admin Approval Mode. To do this go to Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options. Double click the User Account Control: Run all administrators in Admin Approval Mode section. Select Disable and click OK. Restart the computer.
User Account Control: Run all administrators in Admin Approval Mode

- Enabled
- Disabled

[OK] [Cancel] [Apply]
2. Run **WIN_SER_STG_ML** in its own folder to extract the contents.

3. Run the install script.

4. Make sure all the boxes are checked.

5. Click Next.
6. Read and select **I accept the terms in the license agreement.**

7. Click **Next.**
8. Select the location for files to be installed to.

![IBM Installation Manager](image1.png)

9. Click **Next**.

![IBM Installation Manager](image2.png)
10. Click **Next**.

11. Make sure all the packages are checked.

12. Click **Next**.
13. Select **IBM Spectrum Protect**.

14. Click **Next**.
15. Read and select **I accept the terms in the license agreement.**

16. Click **Next.**
17. Read and select **I accept the terms in the license agreement.**

18. Click **Next**.
19. Specify **11090** for the port.

20. Click **Next**.
21. Select **Strict** for the **SP800-131a Compliance**.

22. Click **Next**.

23. Create a password.
24. Click Next.
25. Click Install.

26. Wait for the install to finish.

27. Click Finish.
2.7.2 Install IBM Spectrum Protect Client Management Services

1. Run `WIN64_CMS_ML` in its own folder to extract the contents.

2. Run the install script.
3. Click **Install**.

4. Check the box next to **IBM Spectrum Protect Client Management Services**.
5. Click **Next**.

6. Select **Use the existing package group**.

7. Click **Next**.
8. Make sure all the boxes next to the package Client Management Services are checked.

9. Click **Next**.
10. Set the port to **9028**.

11. Click **Next**.
12. Click **Strict** for **SP800-131a compliance**.

13. Click **Next**.
14. Click **Install**.

15. Observe the successful installation and click **Finish**.
2.7.3 Configure IBM Spectrum Protect

1. Go to Start > IBM Spectrum Protect Configuration Wizard.

2. Click OK.
3. Click **Next**.

4. Specify a name and an account for the IBM server to use. Example: (name: BACKSRVR, User ID: DI\spadmin).
5. Click **Next**.
6. Choose a directory.
7. Click **Next**.
8. Click **Yes** if prompted to create the directory.
9. Choose **The database directories are listed below**.
10. Create a directory to contain the database. Example: `C:\BACKSRVR\IBMBackupServer`.
11. Enter the directory in the space provided.

12. Click **Next**.
13. Create directories for **logs** and **archive logs**. Example: `C:\BACKSRVR\IBMBackupServerLogs`, `C:\BACKSRVR\IBMBackupServerArchiveLogs`.
14. Enter the directories in their respective fields.

15. Click Next.
16. Specify the **server name**.

17. Click **Next**.
18. Specify an **Administrator account**.

19. Click **Next**.

20. Select a **port**. Example: 1500.
21. Check the box next to **Enable SSL Communication** and enter a **port**. Example: 23444.

22. Click **Next**.
23. Click **Next**.

24. Wait for the installation to finish.

25. Click **Next**.

26. Click **Done**.

27. Log in to **Operations Center** by going to localhost:11090/oc/. If issues occur, check firewall permissions for ports 1500 and 23444 (or whichever ports were designated in steps 20 and 21).

28. Log in using the credentials provided in the **Configuration Wizard**.
29. Enter the password for a new account to be created on the system.

30. Click **Next**.

31. Select the time interval for data collection.
32. Click **Next**.

33. Select time intervals that suit your organization's needs.

34. Click **Configure**.
2.7.4 Adding Clients to IBM Spectrum Protect

1. Log in to Operations Center.

2. Add clients by clicking the Clients tab.
3. Click +Client

4. Select the server running the IBM backup capabilities.

5. Check the box next to Always use for SSL.
6. Click **Next**.

7. Enter the name of a client machine that you want to be able to backup data from and a password.

8. Decide whether to use **Client-side deduplication** (it reduces the required storage space for backups).

9. Click **Next**. Note the information on the next page as it is required to connect the server to the client.
10. Click Next.

11. Click Next.
12. Click Next.

13. Click Next.

15. Click Add Client.

16. Make sure to allow the ports for SSL and TCP traffic through the firewall (23444, 1500).
17. Run the following command to set cert256.arm as the default certificate on the IBM Backup server. Execute this command from the root server directory. Example: C:\Program Files\Tivoli\TSM\BACKSRVR

`gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"`

Note: By default, gsk8capicmd_64 is located at C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin.
2.7.5 Install the Spectrum Protect Client on Windows

1. Extract SP_CLIENT_8.1_WIN_ML

2. Run the `spinstall` script (install any prerequisites required).

3. Click Next.
4. Specify an installation path.

5. Click Next.

6. Select Custom Install.
7. Click **Next**. Make sure that all packages are selected for installation.

8. Click **Next**.

9. Click **Install**.
10. Click Finish.

11. Run Backup-Archive GUI from the Start menu. This should open the IBM Spectrum Protect Client Configuration Wizard.

12. Click Next.
13. Select **Create a new options file**.
14. Click **Next**.
15. Enter the **Node Name** that you created in the **Operations Center**.
16. Click **Next**.
17. If prompted, allow the program through the firewall.
18. Select **TCP/IP** for the communication method.

19. Click **Next**.

20. Specify the **IP address** of the server running the IBM backup server.

21. Specify the **port** that the server is accepting connections on (Example: 23444).

22. Click **Next**.
23. Click Select All or choose specific items from the recommended list of inclusions/exclusions.

24. Click Next.

25. Select certain file types to exclude from backup, if any.

26. Click Next.

27. Check the box next to Backup all local file systems.
28. Select **Incremental** for the **Backup Type**.

29. Click **Next**.

30. Click **Apply**.

31. Click **Finish**.

32. In the **Backup-Archive GUI** (you may have to log in using the credentials specified on the server or you may have to choose to ignore a warning that you couldn't connect), go to **Edit > Client Preferences**.
33. Click **Communication**.
34. Ensure that the **server address** is correct and that the **ports** point to your SSL port (23444).
35. Check the boxes next to **Send transaction to the server immediately**, **Use Secure Sockets Layer (SSL)**, and **Require TLS 1.2 or above**.
36. Select Yes for SSL is Required.

37. Click OK.

38. Retrieve cert256.arm from the server.

39. On the client machine, create a new key database by running the following commands:

```bash
> set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin;C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
> gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```
40. Import **cert256.arm** by running the command:

```bash
> gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server BACKSRVR self-signed key" -file <path-to-cert256.arm> -format ascii
```
41. Copy the resulting `dsmcert.kdb` and `dsmcert.sth` to `C:\Program Files\Tivoli\TSM\baclient`.

2.7.6 Install the Spectrum Protect Client on Ubuntu

1. Extract `SP_CLIENT_8.1_LIN86_ML.tar.gz`.

```
root@screenshotsubuntu-virtual-machine:~/screenshotsubuntu# tar xf SP_CLIENT_8.1_LIN86_ML.tar.gz
```


2. Navigate to TSMCLI_LNX/tsmcli/linux86_DEB.

3. Install all the .deb files in this directory, except tivsm-jbb.amd64.deb, by running the following command (they must be dpkg'd individually since they have interdependencies):

   a. dpkg -i [name of package].deb

4. Issue the following commands to setup the options files:

   a. cd /opt/tivoli/tsm/client/ba/bin
   b. mv dsm.sys.smp dsm.sys
   c. mv dsm.opt.smp dsm.opt
5. Install Java with:
   a. `sudo apt-get install default-jre`
6. Run `dsmj` to start the Java BAClient.

7. After about 5 minutes, it will be unable to connect and will ask if you wish to start the client anyway. Click Yes.
8. Open Edit > Client Preferences. Enter the node name as the name of the client you added to the Spectrum Protect server.

9. Click the Communication tab.

10. Enter the IP Address for the server.

11. Enter the Server port and Admin port (23444).

12. Check the boxes next to Send transaction to the server immediately, Use Secure Sockets Layer (SSL), and Require TLS 1.2 or above.
13. **Select Yes for SSL is Required.**

14. Click **OK**.

15. Retrieve **cert256.arm** from the server.

16. On the client machine create a new key database by running the following commands:

```bash
> gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```
17. Import `cert256.arm` by running the command:

    > gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "TSM server BACKSRVR self-signed key" -file <path-to-cert256.arm> -format ascii
18. Copy the resulting "dsmcert.kdb" and "dsmcert.sth" to /opt/tivoli/tsm/client/ba/bin.

19. You may be asked to reconfigure the dsm.opt file when setting up the scheduler but the options should be filled out already.

20. To start the scheduler as a background process, run the following command:

   > nohup dsmc schedule 2>/dev/null &

21. You can add this command to the startup programs in Ubuntu to make it start automatically.

2.8 GreenTec WORMdisks

See the Installation of GreenTec Command Line Utilities document, that should accompany the installation disk, for a detailed guide on how to install the GreenTec command line utilities.
Furthermore, refer to the *GT_WinStatus User Guide*, that should also accompany the installation disk, for instructions on how to effectively use GreenTec disks to preserve data. Read these instructions carefully, as locking GreenTec WORMdisks can result in making some or all of the disk or the entire disk unusable. Having portions of the disk, or the entire disk, permanently locked is sometimes desirable but it is dependent on the needs of your organization. For example, if you want to store backup information or logs securely.

The *GT_WinStatus User Guide* provides instructions for locking and temporarily locking disk sectors. In this practice guide, we will not include instructions on when or how to lock GreenTec disks. However, in some cases, we will provide instructions detailing how to save data to these disks and leave locking them to the implementing parties.

### 2.9 Veeam Backup & Replication

Veeam’s Backup & Replication tool provides backup and restore capabilities. In the data integrity solution, Veeam is used to backup and restore virtual machines residing within Windows Server Hyper-V. In this section is the installation and configuration process for Veeam Backup & Replication on a Windows Server 2012 R2 machine. Additional installation and configuration instructions can be found at [https://helpcenter.veeam.com/docs/backup/hyperv/install_vbr.html?ver=95](https://helpcenter.veeam.com/docs/backup/hyperv/install_vbr.html?ver=95).

#### 2.9.1 Production Installation

1. Start the *Veeam Setup Wizard* and click to begin the installation process for *Veeam Backup & Replication* with the appropriate version number.
2. Read and accept the license agreement.

3. Click Next.

4. Browse to the location of the license file.
5. Click Next.
6. Select installation components required by your organization.
7. Click Next.
8. Specify account credentials for Service account.
9. Click Next.
10. Specify details of the SQL Server Instance.

11. Click Next.
12. Specify port numbers for Veeam Backup & Replication services.
13. Click Next.

14. Specify data storage locations.

15. Click Next.

16. Review installation and configuration details and click Install.
17. Observe the successful installation and click Finish.
2.10 Tripwire Enterprise and Tripwire Log Center (TLC)

Tripwire Enterprise is a data integrity solution that monitors file activity and associated information across an enterprise. In this solution, we use it to monitor both a MS SQL database and file changes in certain folders. Tripwire Log Center allows for the collection and standardization of logs produced by Tripwire Enterprise.

Please see the Tripwire Enterprise Install and Maintenance Guide, accessible at http://download.tripwire.com/te_en/docs852/te_install_and_maint_guide.pdf?VymLyYUTw_9Yx-EB3c3uK07JcgvoIghm3YK_zuCfJtyYm5c9NPiogn8hIakZL3NLlqa, for a detailed, illustrated guide to the installation. The only addition to this documentation is that the MS SQL Server should be in “Mixed Mode” for authentication purposes. This section covers the installation and configuration process we used to set up Tripwire Agents on various machines as well as the installation and integration of Tripwire Log Center with Tripwire Enterprise. The result of this integration is the generation and forwarding of events from Tripwire Enterprise to Tripwire Log Center.

2.10.1 Install Tripwire Agent on Windows

1. Run te_agent.msi on the client machine.

2. Click Next.

3. Accept the license agreement.
4. Click **Next**.

5. Specify the installation path.
6. Click **Next**.

7. Enter the **IP address** of the Tripwire server.
8. Click Next.
9. Leave the proxy settings blank.
10. Click **Next**.

11. Enter the **services password** specified in the server upon installation twice.
12. Click **Next**.
13. Click **Install**.
14. Start **Tripwire Agent** from the start menu (on some systems it may start automatically - check `services.msc` to verify that it is running).

### 2.10.2 Install Tripwire Agent on Ubuntu

1. Execute the following commands as root.
2. Run **te_agent.bin** by issuing the command:
   a. `./te_agent.bin`
3. Press **Enter** repeatedly to read through the EULA.
4. Enter **Y** to accept the EULA.
5. Press Enter.
6. Enter the IP address of the Tripwire server.
7. Press Enter.
8. Enter Y if the address was entered correctly.

10. Press Enter.

11. Enter Y to use the default port number.
12. Press Enter.

13. Enter N to disable the use of the Federal Information Processing Standard (FIPS), unless your system requires the use of FIPS.

14. Press Enter.

15. Enter the services password twice, pressing Enter after each time. Note that no text will appear while typing the password.
16. Press Enter to skip using a proxy.

17. Press Y.
18. Press Enter.

19. Press Y to install Real Time Monitoring.

20. Press Enter.
21. Press Enter to accept the default port.

22. Press Y.

23. Press Enter.

24. The agent should install.
25. Run the following commands as root:

b. `cd "/usr/local/tripwire/te/agent/bin"

c. `./twdaemon start`
26. You may need to change /etc/hosts in Debian systems if there is a line which looks like this:

```
127.0.1.1   <hostname>
```

Change this to:

```
<IP of machine>   <hostname>
```

Otherwise, Tripwire Enterprise may consider multiple Debian machines as the same machine in the assets view of Tripwire Enterprise.
2.10.3 Install Tripwire Log Center
See the *Tripwire Log Center 7.2.4 Installation Guide* that should accompany the installation media for instructions on how to install TLC. Use the Tripwire Log Center Manager installer.

Notes:

a. It is recommended that you install Tripwire Log Center on a separate system from Tripwire Enterprise.

b. You will need to install JRE8 and the Crypto library. Instructions are also in the *Tripwire Log Center Installation Guide*.

c. You may need to unblock port 9898 on your firewall for the Tripwire enterprise agents.

d. Do not install PostgreSQL if you wish to use a database on another system.

e. When it finishes installing there should be a configuration wizard.

2.10.4 Configure Tripwire Log Center

1. Click **Start**.

2. Click **New Install**.
3. Click **Authorize**.
4. An error may appear asking you to install **.NET 3.5**.
5. To do this, open **Server Manager**.
6. Click **Manage**.
7. Click **Add Roles and Features**.
8. Click **Next**.
9. Select **Role-based or feature-based installation**.
10. Click **Next**.
11. Select the current server from the list.
12. Click **Next**.
13. Click **Next**.
14. Check the box next to **.NET Framework 3.5 Features**.
15. Click **Install**.
16. Wait for the installation to finish.
17. If prompted, enter **Name**, **Organization**, **Serial Number**, and **email address** in the fields. Click **Register**. This step will not appear if the software has already been registered.
18. Click Close.  
19. Continue with the **configuration wizard**.  
20. Enter appropriate details for your **Database Software**.
21. Select **Use Windows Authentication**.

22. Click **Next**.

23. Select a directory to store log messages in. Example: `C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT`
24. Click Next.
25. Create an Administrator password and enter it twice.
26. Enter your email address.
27. Click Next.
28. Select authenticate with the local windows system user account.
29. Click Next.

31. Click **Next**.
32. Click **Start**.
33. Click **Next** when the configuration finishes.
34. Observe the successful installation and click Finish.

2.10.5 Install Tripwire Log Center Console
See chapter 4 of Tripwire Log Center 7.2.4 installation guide for instructions on how to install Tripwire Log Center Console. Use the Tripwire Log Center Console installer. This can be done on any system, even the system running.

2.10.6 Integrate Tripwire Log Center with Tripwire Enterprise
1. Create a user account in Tripwire Log Center by logging into Tripwire Log Center Console.
2. Click the **Administration Manager** button.

3. On the side bar, click **User Accounts**.
4. Click the **Add** button.

5. Enter the details of the user.

6. Double click the user account.

7. Select the **Permissions** tab.
8. Click **Change User Permissions**.

9. Select **Databases** and check the box.
10. Select API and check the box.

11. Click OK.

12. Click OK.

13. Click OK.

15. Log in to the Tripwire Enterprise Console.

16. Click Settings.
17. Go to System > Log Management.
18. Check the box next to Forward TE log messages to syslog.
19. Enter the IP address and port of the Tripwire Log Center server. The default port is 1468.
20. Check the box next to Allow TE to use information from Tripwire Log Center.
21. Enter the service address like this: https://192.168.50.44:8091/tlc, replacing the IP address with the IP address of the Tripwire Log Center server.
22. Enter the account information for the account created with the Databases and API permissions.
23. Click Apply.
24. Click OK.
25. Go back to the Tripwire Log Center Console.
26. Click **Configuration Manager**.

27. Click **Resources > Tripwire Enterprise Servers**.
28. Click Add.

29. Enter a name for the Tripwire Enterprise server.

30. Enter the IP address and port for the Tripwire Enterprise server. By default, Tripwire Log Center and Tripwire Enterprise will communicate on port 443. ([https://192.168.50.43](https://192.168.50.43))

31. Enter the name of a user account on the Tripwire Enterprise server. The account must have the following permissions: create, delete, link, load, update, view.

32. Click Save.
2.11 Integration: Tripwire Log Center (TLC) and HPE ArcSight ESM

In this section is a process for integrating Tripwire Log Center and HPE ArcSight ESM. This integration assumes the correct implementation of Tripwire and ArcSight as described in earlier sections. The result of this integration is the forwarding of logs generated by Tripwire Enterprise to ArcSight ESM as well as a method for filtering specifically for file change events in ArcSight ESM.

2.11.1 Integrating TLC and ESM

1. Run ArcSight-7.4.0.7963.0-Connector-Win64 on any Windows server (except for the server running the Tripwire Log Center).
2. Click **Next**.

3. Specify a folder to install the connector.

4. Click **Next**.
5. Click **Next**.
6. Click **Install**.
7. Select **Add a Connector**.
8. Click **Next**.

9. Select **Syslog daemon**.
10. Click **Next**.
11. Select a **port** for the daemon to run on.
12. Leave **IP address** as *(ALL)*.
13. Select **Raw TCP** for **Protocol**.
14. Select **False** for **Forwarder**.
15. Click **Next**.

16. Choose **ArcSight Manager (encrypted)**.
17. Click **Next**.

18. For **Manager Hostname**, put `vm-esm691c` or the hostname of your ESM server.

19. For **Manager Port**, put **8443** (or the port that ESM is running on).

20. Enter the username and password used for logging into **ArcSight Command Center**. Default: (admin/password)
21. Click **Next**.

22. Set identifying details about the system to help identify the connector (include **Name**; the rest is optional).
23. Click **Next**.

24. Select **Import the certificate to connector from destination.** This will fail if the **Manager Hostname** does not match the hostname of the VM.
25. Click **Next**.
26. Click **Next**.

27. Choose **Install as a service**.
28. Click **Next**.
29. Click **Next**.
30. Choose **Exit**.
31. Click **Next**.

32. Click **Done**.
33. Open Task Manager.
34. Click More Details.
35. Go to the Services tab.
36. Find the service just created for ArcSight and right click it.

37. Choose Start.
38. Open the Tripwire Log Center Console.
39. Go to the Configuration Manager.

40. Select Resources > Managers.

41. Double click the Primary Manager listed.
42. Click the Advanced Settings tab.
43. Click the +Add button. This should add a row to the table.
44. In the Advanced Option box, select Log Message Forwarding - Destinations.
45. In the Value box next to it, type `<ip_address>:<port>:udp`, with the IP Address and port of the syslog daemon just created.

2.11.2 Configuring Tripwire Enterprise and HPE ArcSight ESM to Detect and Report File Integrity Events

2.11.2.1 Creating a Rule for Which Files to Monitor Across Your Enterprise

1. Log into Tripwire Enterprise by going to `https://tripwire` and entering the user name and password.
2. Click the Rules link.
3. Click New Rule.

5. Click **OK**.
6. Enter a **name** for the rule.

7. Click **Next**.

8. Click **New Start Point**. This will bring up a **New Start Point Wizard**.

9. Enter the **path** to a folder or file that will be monitored across all Windows Systems. For example, we chose to monitor *C:\Users*.

10. If you selected a directory and want the integrity check to recurse in all sub directories, make sure the box next to **Recurse directory** is checked.
11. Click **Next**.

12. Select **Windows Content and Permissions**.

13. Click **Next**.
14. Click Finish.

15. If you wish to exclude directories, click **New Stop Point**.

16. Enter the path name of directories you wish to exclude. For example, we chose to exclude `C:\Users\*\AppData` because that provided many false flags of routine application data modification.

17. Check the box next to **Stop Recursion**.
18. Click Finish.

19. The rule created defines a space for the tasks we will create to search through.

2.11.2.2 Creating a Baseline Task

1. Click the Tasks link.

2. Click New Task.

4. Click OK.
5. Enter a name for the baseline rule task.
6. Select a privileged user in Tripwire Enterprise to run the rule as.
7. Click Next.
8. Select All Baselines.
9. Click Next.
10. Expand Root Node Group > Smart Node Groups > System Tag Sets > Operating System.
11. You can select specific types of operating systems to run the task on or specific machines. We simply selected Operating System to have it run on all applicable Windows machines.
12. Once you have made your selection, click Next.
13. Select Selected nodes with rule or rule group.
14. Click the rule you created earlier.
15. Click **Next**.

16. Decide how often the baseline task should be run. We set it to **manually** but you can also set a very specific schedule by choosing **periodic**.

17. Click **Finish**.

18. This rule will create baselines of the specified objects. Baselines are essentially versions of the file that check rules will compare against. Baselines should be primarily taken when the integrity of files are known to be good.

2.11.2.3 **Creating a Syslog Action**

1. Click the **Actions** link.
2. Click **New Action**.

3. Select **Syslog Action**.

4. Click **OK**.
5. Enter a name for the Syslog Action.

6. Click Next.

7. Enter the IP address of the Tripwire Log Center server.

8. Enter the port that Tripwire Log Center receives TCP syslog messages on.

9. Enter a log name, a level, and a facility code per your needs. These will show up in logs, so you can use these to help separate or identify log sources.

10. Click Finish.

2.11.2.4 Creating a Check Task

1. Click the Tasks link.
2. Click **New Task**.

3. Select **Check Rule Task**.

4. Click **OK**.

5. Enter a **name** for the baseline rule task.

6. Select a privileged user in Tripwire Enterprise to run the rule as.
7. Click Next.

8. Expand Root Node Group > Smart Node Groups > System Tag Sets > Operating System.

9. Here, you can select specific types of operating systems to run the task on or specific machines. We simply selected Operating System to have it run on all applicable Windows machines.

10. Once you have made your selection, click Next.

11. Select Selected nodes with rule or rule group.

12. Click the rule you created earlier.
13. Click Next.

14. Decide how often the check task should be run. We set it to manually, but you can also set a very specific schedule by choosing periodic.

15. Click Next.
16. Click **Add**.

17. Select the **Syslog Action** created earlier.

18. Click **OK**.
19. Click Next.

20. Uncheck the box next to initialize baselines now if you do not wish to immediately take a baseline of all systems.

21. Click Finish.

22. This rule will check the current versions of the selected files against their baselines and log any changes to Tripwire Log Center.

2.11.2.5 Running the Baseline Task

1. Check the box next to the baseline task you created earlier.

2. Click Control > Run on the taskbar.
3. Wait for the run to finish. You can click the Log link to see the progress.
4. When it finishes, it will log a message such as “Task 'Baseline Rule Windows' was completed in 600 seconds.”

### 2.11.2.6 Make Changes to Monitored Objects

1. Open a machine being monitored by the rule you created.
2. Modify a file or files in the folder that you selected in the rule creation wizard (which are being monitored by Tripwire).

### 2.11.2.7 Running the Check Task

1. Check the box next to the check task you created earlier.
2. Click Control > Run on the taskbar.
3. Wait for the run to finish. You can click the Log link to see the progress.
4. If you made changes to a monitored object, the log message should appear at the time the changes were made even if the change was made prior to the scan.

### 2.11.2.8 Filtering for Tripwire Enterprise Integrity Events in HPE ArcSight ESM

1. Open the ArcSight ESM machine.
2. Log in by going to https://vm-esm691c:8443 and entering your username/password.
3. Click Events > Active Channels.
4. Click New.
5. Enter a name for the channel. Select a start time to show events, and leave $NOW as the end time.
6. Click **Configure Filter**.

7. Click the button that says **Configure a condition using field**.

8. Double click **Device Event Category**.

9. For **Operator**, choose **Contains**.

10. For **Value**, enter **Audit Event**.
11. Click **Apply Condition**.

12. Click **Update Filter Configuration** under the list of fields.

13. Click **Save Channel**.

14. Click the channel you just created. It should show all file changes in the time frame you specified forwarded from Tripwire Enterprise to Tripwire Log Center to ArcSight ESM.

### 2.12 Integration: HPE ArcSight ESM with Veeam and Hyper-V

This section covers the process for integrating HPE ArcSight ESM with Veeam and Hyper-V. This integration assumes the correct implementation of Veeam and ArcSight as described in earlier sections. The result is the forwarding of logs generated by Veeam and Hyper-V to ArcSight ESM, as well as custom parsers to supplement the information provided by this forwarding process.

#### 2.12.1 Install ArcSight Connector

1. Run the installation file **ArcSight-7.4.0.7963.0-Connector-Win64** on the Veeam Server.

2. Wait for the initial setup to finish.
3. Click Next.

4. Choose a destination folder. Note: It is recommended to change the default to <default>\HYPERV so that other installed connectors do not overwrite this one.

5. Click Next.
6. Click **Next**.

7. Click **Install**.

8. Wait for the installation to finish.

9. Select **Add a Connector**.
10. Click **Next**.

11. Choose **Microsoft Windows Event Log - Native** from the list.
12. Click Next.

14. Click Next.

15. Click on the box underneath Custom Event Logs.


17. You can add more application logs through the following process:
   a. Open Microsoft Event Viewer.
b. Find the log you wish to add.

c. Open the Details pane of a log and find the field Channel.
d. Note that this may differ from the Log Name in the General pane. (For example, one of the Hyper-V log’s Log Name is Microsoft-Windows-Hyper-V-VMMS/Admin but the channel name is Microsoft-Windows-Hyper-V-VMMS-Admin.)

e. Enter all these channel names separated by commas in the Custom Event Logs field.

18. Click Next.


20. Click Next.

21. For Manager Hostname, put \vm-esm691c, or the hostname of your ESM server.

22. For Manager Port, put 8443, or the port that ESM is running on, on the ESM server.

23. Enter the username and password used for logging into ArcSight Command Center (admin/password).
24. Click **Next**.

25. Set identifying details about the system to help identify the connector (include at least **Name**; the rest is optional).

26. Click **Next**.

27. Select **Import the certificate to connector from destination**. This will fail if the **Manager Hostname** does not match the hostname of the VM.
28. Click **Next**.
29. Wait for the process to complete.
30. Click **Next**.
31. Choose **Install as a service**.
32. Click **Next**.

33. Click **Next**.
34. Click **Next**.
35. Choose **Exit**.
36. Click Next.
37. Click **Done**.
38. Open **Task Manager**.
39. Click **More Details**.
40. Go to the **Services** tab.
41. Find the service just created **arc_winc** for ArcSight, and right click it.
42. Choose **Start**.
43. The machine will now report its logs to ArcSight ESM.

44. For more fine-grained reporting, such as including more information about the event, you may wish to include custom parsers that are described below.

2.12.2 Create a Parser for Veeam Logs

1. For a Veeam custom parser that handles event numbers 210, 251, and 290, create a configuration file with the following text:

   ```
   trigger.node.location=/EventData
   event.deviceVendor=__getVendor("Veeam")
   conditionalmap.count=1
   conditionalmap[0].field=event.externalId
   conditionalmap[0].mappings.count=3
   conditionalmap[0].mappings[0].values=210
   conditionalmap[0].mappings[0].event.name=__stringConstant("Restore session initiated.")
   ```
conditionalmap[0].mappings[1].values=251
conditionalmap[0].mappings[1].event.name=__stringConstant("Restore session has finished with success state.")
conditionalmap[0].mappings[2].values=290
conditionalmap[0].mappings[2].event.name=__stringConstant("Restore session has finished with success state.")

2. Save this file as C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\fcp\winc\veeam_backup\veeam_mp.sdkkeyvaluefilereader.properties

3. Copy this file to C:\Program Files\ArcSightSmartConnectors\<name of folder>\current\user\agent\winc\veeam_backup\veeam_mp.sdkkeyvaluefilereader.properties
2.12.3 Create a Parser for Hyper-V Logs

1. For a Hyper-V VMMS custom parser, create a configuration file with the following text:

   trigger.node.location=/EventData
   event.deviceVendor=__getVendor("Microsoft")
   token.count=1
   token[0].name=VmName
   token[0].location=VmlEventLog/VmName
   token[0].type=String
   conditionalmap.count=1
   conditionalmap[0].field=event.externalId
   conditionalmap[0].mappings.count=1
   conditionalmap[0].mappings[0].values=13003
   conditionalmap[0].mappings[0].event.name=__concatenate(__stringConstant("The virtual machine "), VmName, __stringConstant(" has been deleted.")))
2. Save this file as C:\Program Files\ArcSightSmartConnectors\name of folder\current\user\agent\fcp\winc\microsoft_windows_hyper_v_vmms_admin\microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties

3. Copy this file to C:\Program Files\ArcSightSmartConnectors\name of folder\current\user\agent\winc\microsoft_windows_hyper_v_vmms_admin\microsoft_windows_hyper_v_vmms.userdata.jsonparser.properties
These two parsers will allow for details of VM deletions and VM restores to be shown in ArcSight. Custom parsers are a functionality of ArcSight. For more information on the creation of custom parsers, please see the *ArcSight FlexConnector Developer's Guide*, as well as the *SmartConnector for Microsoft Windows Event Log - Native, Configuration Guide* (for information specific to Windows event logs).

### 2.13 Integration: GreenTec WORMdisks and IBM Spectrum Protect

This section covers the process for integrating IBM Spectrum Protect and GreenTec WORMdisks. The result is the capability to backup clients directly to WORMdisks in order to preserve data more securely. This integration process does not include instructions related to locking the WORMdisks — that process is found in the *GT_WinStatus User Guide*, that should accompany the installation disk. Scheduling the locking of these disks is left up to the discretion of the adapting organization.

#### 2.13.1 Install IBM Spectrum Protect Server on the GreenTec Server

1. You may need to disable *Run all administrators in Admin Approval Mode*. To do this go to **Control Panel > Administrative Tools > Local Security Policy > Local Policies > Security Options**. Double click the *User Account Control: Run all administrators in Admin Approval Mode* section. Select *Disable* and click *OK*. Restart the computer.
<table>
<thead>
<tr>
<th>Security Setting</th>
<th>Security Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Control: Run all administrators in Admin Approval Mode</td>
<td>User Account Control: Switch to the secure desktop when p...</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

2. Run **WIN_SER_STG_ML** in its own folder to extract the contents.
3. Run the install script.

4. Make sure all the boxes are checked.
5. Click **Next**.

6. Read and select **I accept the terms in the license agreement**.
7. Click **Next**.
8. Select the installation location for files.
9. Click **Next**.
10. Click Next.

11. Make sure all the packages are checked.
12. Click Next.
13. Select IBM Spectrum Protect.
14. Click Next.
15. Read and select I accept the terms in the license agreement.
16. Click Next.
17. Read and select I accept the terms in the license agreement.
18. Click **Next**.

19. Specify **11090** for the port.

20. Click **Next**.

21. Select **Strict** for the **SP800-131a Compliance**.
22. Click **Next**.

23. Create a password.
24. Click **Next**.

25. Click **Install**.

26. After the successful installation, click **Finish**.

2.13.2 **Configure IBM Spectrum Protect**

1. Go to **Start > IBM Spectrum Protect Configuration Wizard**.
2. Click OK.

3. Click Next.
4. Specify a name and an account for the IBM server to use. Example: (name: GRNBACK, User ID: D\sp_admin)
5. Click Next.
6. Choose a directory.
7. Click Next.
8. Click Yes if prompted to create the directory.
9. Choose The database directories are listed below.
10. Create a directory to contain the database. Example: C:\BACKSERV\IBMBackupServer.
11. Enter the directory in the space provided.
12. Click **Next**.

13. Create directories for **logs** and **archive logs**. Example: `C:\BACKSERV\IBMBackupServerLogs`, `C:\BACKSERV\IBMBackupServerArchiveLogs`.

14. Enter the directories in their respective fields.
15. Click **Next**.

16. Specify the **server name**.
17. Click **Next**.

18. Specify an **Administrator account**.
19. Click **Next**.
20. Select a **port** (example: 1500).
21. Check the box next to **Enable SSL Communication** and enter a **port** (example: 23444).

22. Click **Next**.
23. Click **Next**.
24. Wait for the installation to finish.
25. Click **Next**.

26. Click **Done**.

27. Log in to **Operations Center** by going to `localhost:11090/oc/`.

28. Log in using the credentials provided in the **Configuration Wizard**.

29. Enter the password for a new account to be created on the system.
30. Click **Next**.

31. Select the time interval for data collection.

32. Click **Next**.
33. Select time intervals that suit your organization's needs.

34. Click Configure.
2.13.3 Connect the GreenTec Server to the IBM Spectrum Protect Server

1. Go back to the primary IBM server.

2. Click Servers.

3. Click +Spoke.
4. Enter the **IP address** of the server with GreenTec disks attached.

5. Enter the **port** that the server is configured to listen for connections on (Example: 1500).
6. Click Next.
7. Enter the password for the new server twice.
8. Click Next.
9. Click **Connect Spoke**.

10. Click **Close**.

**2.13.4 Define a Volume on the GreenTec Server**

1. Issue the following command in the Operations Center (on the GreenTec server) command builder to create a device class for the backup disk (replace the name **golden**, max capacity value, and directory value as you see fit).
> define devclass golden devtype=file maxcapacity=350000M shared=yes mountlimit=1 directory="E:" library=backuplib
2. Go to Storage > Storage Pools.

3. Click +Storage Pool.

4. Enter a name.

5. Click Next.

6. Select Disk (primary).
7. Click **Next**.

8. Select the device class you just created.

9. Click **Next**.
10. Click **Next**.

11. Click **Add Storage Pool**.
12. Click **Close & View Policies**.

13. Issue the following command in the Operations Center command builder to create a volume on the backup disk.
14. The storage pool may indicate that there is no capacity, but once you backup something it should correctly show the capacity.

2.13.5 Create a Policy to Backup to GreenTec disks

1. Issue the following command in the Operations Center (on the GreenTec server) command builder to delete the standard policy domain:

   `delete domain standard`

2. Issue the following command to create a new domain.

   `define domain golden`

3. Issue the following command to create a new policy set in this domain.

   `define policyset goldenpolicy`

4. Issue the following command to create a management class in this domain.

   `define mgmtclass golden goldenpolicy goldenclass`
5. Click Services > Policy Sets.
6. Toggle the **Configure** button. This should allow you to edit the settings of the newly created management class.
7. Select *Default*.
8. For *Backup Destination*, select the storage pool you just created.
9. For *Backups*, select 1.
10. Select the rest of the settings per your organization's needs.
11. Click the **Activate** button.

12. Check the box next to **I understand that these updates can cause data deletion.**

13. Click **Activate.**
2.13.6 Create a Schedule That Uses the New Policy

1. On the primary IBM Spectrum Protect Server log in to the Operations Center.

2. Go to Clients > Schedules.

3. Click +Schedule.

4. Enter a name for the schedule.

5. For Server, select the GreenTec server.

6. For Domain, select the policy domain you just created.

7. For Type, select System.
8. Click **Next**.

9. Select **Daily incremental backup**.
10. Click **Next**.

11. Configure the schedule settings for your organization's needs. This can be changed later.
12. Click **Add Schedule**.

13. From the command builder, run the following command to update the schedule:

   ```
   update schedule golden golden starttime=now action=backup type=client
   objects="c:\*" startdate=06/10/2017 perunits=onetime
   ```

2.13.7 **Installing Open File Support on the Client**

1. Open the client machine (with the IBM Backup Archive Client installed) to make a golden disk.
2. Open the IBM BA Client.
3. Click Utilities > Setup Wizard.
4. Check the box next to Help me configure Open File Support.
5. Click Next.
6. Click Next.

7. Select **Volume Shadowcopy Services (VSS)**.

8. Click **Next**.
9. Click **Apply**.

10. Click **Finish**.

11. **Restart** the BA Client.
12. Click Edit > Client Preferences.

13. Click the Include-Exclude tab.
14. Click Add.
15. For Category, select Backup.
16. For Type, select Include.FS.
17. For Snapshot Provider Type, choose VSS.
18. For File or Pattern, enter *:*

![Image of preference editor]

19. Click OK.

2.13.8 Temporarily Add Client to GreenTec IBM Server

1. Assuming your GreenTec disks are on a separate IBM server, you will need to connect the client you wish to migrate in order to use the created schedule. On the GreenTec server, click Clients.

![Image of clients list]
2. Click +Client.

3. Select the GreenTec server.

4. Click Next.

5. Enter the information for the client you are migrating to this server.

6. Click Next.
7. Take note of the information presented here, namely the IP and port provided, as you will need it on the client machine to connect to the server.

8. Click Next.

9. Select the policy domain you created.

10. Click Next.
11. Select the schedule created earlier.

12. Click Next.

13. Click Next.

14. Select the at-risk options per your organization's needs.
15. Click Add Client.

16. Click Close.

17. On the client machine, open the BA client.

18. Click Edit > Client Preferences.
19. Click the Communication tab, and enter the new server address and port. Only leave Use SSL checked if you have set it up for this new server. Similarly, unselect SSL is required if you did not setup SSL on this second server.

![Communication Preferences](image)

20. Restart the BA client. The client should now connect to the new server.

21. You may be prompted for a password. Enter the password and press Enter.

22. To start the schedule, issue the following command in the Operations Center command builder:

   ```bash
   update schedule golden golden startdate=today starttime=now
   ```

2.14 Integration: Backing Up and Restoring System State with GreenTec

This section covers the process for backing up (and restoring) the Windows System State on a Windows Server with GreenTec as a backup medium. The backup of user information as well as other system state information to a networked GreenTec WORMdisk is intended for the recovery of damage to the Windows system state, such as account permission modification, account creation, account deletion, and various other applicable scenarios.
2.14.1 Installing Windows Server Essentials for System State Backup Capability

(NOTE: For older machines, IBM Spectrum Protect's option to backup SystemState may be sufficient. However, for newer, more complex versions of Windows, such as Windows Server 2012 and Windows 8+, you should use the following procedure.)

1. Open Server Manager.

2. Select Manage > Add Roles and Features.

3. Click Next.
4. Select **Role-based or feature-based installation**.

5. Click **Next**.

6. Select the server.

7. Click **Next**.

9. Click Next.

10. Click Next.
11. Click **Next**.

12. Click **Install**.

13. Click **Configure Windows Server Essentials Experience**.
14. Click **Configure**.

15. Click **Close**.
2.14.2 Configure Network Accessible GreenTec Disk

1. To configure a GreenTec disk to be network accessible, right click the disk on the GreenTec server.

2. Click **Share With > Advanced Sharing**.
3. Click Advanced Sharing.
4. Check the box next to Share this folder.
5. Click OK.
6. Click Close.

2.14.3 Backup the System State

1. Go to command prompt on the Active Directory server and enter the following command:

   `wbadmin start systemstatebackup -backuptarget:z:`
(Instead of z, put the location of a disk for the system state backup. You will get an error if you attempt to use the same location as the disc you are trying to backup. Examples of acceptable targets: C:, Z:, \backup-storage\g)

2.14.4 Restoring the System State

1. After determining the point in time of a malicious event, restart the Active Directory Server and press F2 > F8 to start the Advanced Boot menu.
2. Select Directory Services Repair Mode.
3. Log in as the machine administrator.
4. Open a command prompt.
5. Enter the following command to see the backup versions available:

   `wbadmin get versions`
6. Enter the following command to restore to a specific version (preferably before the malicious event occurred):
   
   ```
   wbadmin start systemstaterecovery -version:06/21/2017-15:33 -
   backupTarget:\192.168.52.12\g
   ```
   
   (Replace the `backupTarget` with the location of the backup, and the `version` with the version to restore to.)

7. The computer will restart when you finish the restore process.

2.15 Integration: Copying IBM Backup Data to GreenTec WORMdisks

This section covers the process for integrating IBM Spectrum Protect with GreenTec WORMDisks. This integration assumes the correct implementation of IBM Spectrum Protect, as well as the existence of
GreenTec WORMdisks as described in earlier sections. The result of this integration is the capability to store all backup data created by IBM Spectrum Protect for a single client on a secure WORMDisk.

### 2.15.1 Copying Backups for a Single Machine to a GreenTec WORMDisk

1. On the IBM Spectrum Protect server, log on to IBM Spectrum Protect Operations Center.
2. Create a new device class by running the following command in the Command Builder:

   ```
   define devclass backupset devtype=file maxcapacity=100000M shared=yes mountlimit=1 directory="C:\"
   ```

3. Go to Storage > Storage Pools.

4. Click +Storage Pool.

5. Enter a name.
6. Click **Next**.

7. Select **Disk (primary)**.

8. Click **Next**.
9. Click Next.

10. Click Add Storage Pool.
11. Create a backup set for the client whose data you wish to store securely. Run the following command on Command Builder:

```bash
generate backupset <name of client> <identifier> \<name of client>c$
devclass=file volumes=backupset1 nametype=unicode
```

For example:

```bash
generate backupset windowsvm1 windowsvm1_backupset \windowsvm1c$
devclass=file volumes=backupset1 nametype=Unicode
```
12. This will store all backup data for the client \texttt{WINDOWSVM1} in a file called \texttt{backupset1}. You can copy this file to a GreenTec disk and store for later use.

### 2.16 Integration: Tripwire and MS SQL Server

This section covers the process for integrating Tripwire Log Center and Microsoft SQL Server. This integration assumes the correct implementation of Tripwire as described in earlier sections. The result of this integration is the collection of database audit logs in Tripwire, allowing for detection and reporting of events such as specific types of queries, schema modification, and database modification.

#### 2.16.1 Create a New Account on MS SQL Server

1. Open \texttt{SQL Server Management Studio}.
2. Hit \texttt{Connect} to connect to the database.
3. In the \texttt{Object Explorer} window, expand the \texttt{Security} folder.
4. Right click on the Logins folder and click New Login....
5. Input the desired user.
6. Click **User Mapping**.
7. For each database that Tripwire should monitor, click the database and assign the role **db_datareader**.
8. Click **Securables**.

9. Under the **Grant** column, check the boxes next to **Alter trace** and **View any definition** (if this is not available, create the user, then edit properties for that user).
10. Click OK.

2.16.2 Create a New Audit on MS SQL Server

1. In the Object Explorer window, expand the Security folder.
2. Right click on the Audits folder.
3. Click New Audit...
4. Specify a filename or any other settings per your organization’s needs. Note: If you specify a filename, you will be able to view any queries you wish to monitor in this Audit log, but not in Tripwire. However, if you set the Audit Destination to Application Log, the messages will be forwarded to the Microsoft Application Log. This will result in less structured (but still detailed) messages and allows the capability to collect them easily using HPE ArcSight ESM. If your ArcSight Connector is configured to collect Application Logs from the MS SQL server, no further configuration of the connector is required.
5. Click **OK**.

6. Right click **Security > Server Audit Specifications**.

7. Click **New Server Audit Specification**.

8. For **Audit**: select the audit you just created.

9. Specify any **Audit Action Types** that Tripwire should be able to log.
10. Click **OK**.

11. Open a database that you wish to monitor specific objects in.

12. Right click **Databases** &gt; **<Database name>** &gt; **Security** &gt; **Database Audit Specifications**.
13. Click **New Database Audit Specification**.

14. Select an **Audit Action Type** to monitor.
15. Select **Object** for the **Object Class**.
16. In the **Object Name** field, use the **Browse** button to find objects that you wish to monitor for the specified **Audit Action Type**.
17. Create as many types as you wish Tripwire to monitor.
18. Click OK.
19. Find the audits you just created in the Object Explorer and right click.
20. Select Enable ___ Audit Specification for each one.

2.16.3 Create a New Node for the MS SQL Server on Tripwire Enterprise
1. Open the Tripwire Enterprise console.
2. Click Nodes.
3. Click Manage > New Node.

4. Click Types > Database Server > Microsoft SQL Server.

5. Click Ok.

6. Enter the hostname or IP of the MS SQL Server.

7. Enter the instance name of the database.
8. Click **Next**.

9. Enter the **port** the database listens on.

10. Click **Next**.

11. Enter the newly created **username** and **password** for the database.
12. Click Next.

13. Check the box next to **Collect audit-event information**.

14. Click Next.

15. Find the MSSQL Server on the list.
16. Click Next.

17. Test Login to ensure the information you entered was correct.

18. Click Finish.
# Appendix A  List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>BA</td>
<td>Client Backup-Archive Client</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>DI</td>
<td>Data Integrity</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>EOF</td>
<td>End of File</td>
</tr>
<tr>
<td>ESM</td>
<td>Enterprise Security Manager</td>
</tr>
<tr>
<td>HPE</td>
<td>Hewlett Packard Enterprise</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MS SQL</td>
<td>Microsoft Structured Query Language</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>MS</td>
<td>Microsoft</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>DSRM</td>
<td>Directory Services Restore Mode</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VSS</td>
<td>Volume Shadowcopy Services</td>
</tr>
<tr>
<td></td>
<td>Acronym</td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
</tr>
<tr>
<td>2266</td>
<td>VM</td>
</tr>
<tr>
<td>2267</td>
<td>VnE</td>
</tr>
<tr>
<td>2268</td>
<td>WORM</td>
</tr>
</tbody>
</table>