COMMVAULT

Security Best Practices

INCREASING THE SECURITY OF THE COMMSERVE

A Commvault Engineering White Paper

This paper will explain the ways our security features and administrative tools can enhance your own data security plan to ensure that your data is kept private and safe from unauthorized users. Specifically it will tell you how to increase the security of the CommServe database, where all configuration data, job records and access control reside.

Contents

AUDIENCE

This white paper is intended for the most technical level of Commvault Administrators who are concerned with security.

INTRODUCTION

Data protection is our highest priority. Security is built into every step of our data management services from an end user's computer all the way to backup storage. This paper will explain the ways our security features and administrative tools can enhance your own data security plan to ensure that your data is kept private and safe from unauthorized users.

INCREASE COMMVAULT SERVER SECURITY

All configuration data, job records, and access control to Commvault managed data is contained within the CommServe database. Regardless of what other security barriers in place, if the CommServe database is compromised, the data is vulnerable. The primary means to protect the CommServe database are – and will always be - the physical, application, and network security measures taken. However, there are additional security precautions as listed in this whitepaper.

Some of the security precautions recommended involve configuration of the Microsoft SQL Server instance or the Windows Server host used by the CommServe component. Configuration steps listed here may vary depending on the versions of software being used - Microsoft Windows or SQL Server version 2008 or 2012 – initial or R2 variant. Consult the latest Microsoft's documentation for version specific steps.

LIMIT ACCESS TO COMMVAULT INSTALLATION

To prevent ransomware from encrypting the Commvault install folders, lock down those folders to only the Commvault service account and prohibit System Administrators from using that account unless absolutely necessary.

CONFIGURE DISASTER RECOVERY

An essential part of a recovery is having adequate disaster recovery procedures.

- Run disaster recovery backups - use these backed up database dumps from the remote media and recover the CommServe database on the same or new host
- Build a standby CommServe Host by replication - Databases and logs on the active or production CommServe host are replicated to the standby host at regular intervals.

When the active CommServe host goes offline, immediately fail over the CommServe functionality and resume CommCell operations on the standby CommServe host.

- Build a standby CommServe Host for disaster recovery - Microsoft SQL Server Agent is used to back up the database and transaction logs from the production CommServe host and restore in standby mode to the standby CommServe host.
- Take the DR storage offline when we are not writing to it - a common strategy to not only reduce the risk of online delete (assuming an attacker gained a wide access to network and server root access) but also manage costs.

RELOCATE THE COMMCELL CONSOLE AND WEB CONSOLE

In most cases, the CommServe host will be located in a data center and accessed remotely. Limit the need for users to have interactive logon rights by not having the CommCell Console, Webserver, and Web Console components installed on the CommServe host.

The CommCell Console is selected for installation by default when the CommServe component is installed. The Web Server and Web Console components are automatically selected for installation only if IIS is installed. Deselect these components during the installation process. There is no real requirement for any of these components to be installed on the CommServe component host.

IIS is only required when web-based access is needed for the CommCell Console or the Web Server.

If the Web Server and Web Console components are installed on hosts other than the CommServe component host, the firewall and SQL (ODBC) communication need to be configured. Consult Commvault documentation on Post-Installation Configurations for Web Server and Web Console.

The CommCell Console component can run as a stand-alone application or as a remote web-based application. For information on installation and configuration, consult Commvault documentation on CommCell Console – Advanced.

Additionally, as both the CommCell Console and the Web Console have reciprocal links, those links can be configured by consulting Commvault documentation - Linking Between the CommCell Console and the Web Console.

CONFIGURE WEB-BASED COMMCELL CONSOLE TO USE SSL/HTTPS

The CommServe uses Microsoft's Internet Information Server (IIS) to provide for remote web access. By default, this is an unsecure (HTTP) web page. The website is automatically

configured if IIS is present when the CommCell Console component is installed. If web-based CommCell Console access should be disabled, don't install IIS or disable the site after installation. If web-based CommCell Console access must be allowed, configure IIS to use a secure (HTTPS) web page for the CommCell Console. The procedure listed below assumes that the site already has a certificate assigned to it or that a self-signing certificate will be created.

1. Log on to the Web server computer as an administrator.
2. Click **Start**, point to **Settings**, and then click **Control Panel**.
3. Double-click **Administrative Tools**, and then double click **Internet Services Manager**.
4. Select the Web site from the list of different served sites in the left pane.
5. Right-click the Web site, folder, or file to configure SSL communication, and then click **Properties**.
6. Click the **Directory Security tab**.
7. Click **Edit**.
8. Click **Require secure-channel (SSL)** if the Web site, folder, or file requires SSL communications.
9. Click **Require 128-bit encryption** to configure 128-bit (instead of 40-bit) encryption support.
10. To allow users to connect without supplying their own certificate, click **Ignore client certificates**. Alternatively, to allow a user to supply their own certificate, use **Accept client certificates**.
11. To configure client mapping, click **Enable client certificate mapping**, and then click **Edit** to map client certificates to users. If this functionality is configured, map the client certificates to individual users in Active Directory. Use this functionality to automatically identify a user according to the certificate they supplied when they access the Web site. Map users to certificates on a one-to-one basis (one certificate identifies one user) or map many certificates to one user (a list of certificates is matched against a specific user according to specific rules. The first valid match becomes the mapping).
12. Click **OK**.

CREATE A CERTIFICATE FOR AN SSL (HTTPS) CONNECTION

If a certificate for SSL is not assigned, create one using the following steps:

1. On the IIS host, click **Start | All Programs | Administrative Tools | Internet Information Services (IIS) Manager**. The IIS Manager dialog box should open.
2. In the **IIS Manager** dialog box's **Connection**s, click to select <host>.
3. In the <host> **Home Features View**, scroll down to **IIS** section and double-click to open **Server Certificates**.
4. In Action Panel on right, click on **Create Self-Signed Certificate**..
5. In **Create Self-Signed Certificate** dialog box, enter a friendly name for the certificate. (Example: Secure CommCell Access)
6. Click **OK** to create the certificate.

SET UP AN HTTPS (SSL) CONNECTION FOR A COMMCELL CONSOLE

1. On the IIS host, click **Start | All Programs | Administrative Tools | Internet Information Services (IIS) Manager**. The IIS Manager dialog box should open.
2. In IIS Manager dialog box's **Connections,** expand **<host> | Sites** and click to select **Default Web Site**.
3. In **Action Panel** on right, click on **Bindings**.
4. In **Site Bindings** dialog box's list of bindings, click on **https** then click **Remove**. Close the Site Bindings dialog box.
5. In IIS Manager dialog box's **Connections**, expand **<host> | Sites** and click to select **Consoles**.
6. In **Action Panel** on right, click on **Bindings**.
7. In **Site Bindings** dialog box's list of bindings, click **Add**.
8. In the **Add Site Binding** dialog box
    a. For **Type**: Select **https**
    b. For **IP Address**: Select **All Unassigned**
    c. For **Port**: Enter **443**
    d. For **Host name**: Enter the fully qualified domain name (**FQDN**) for the IIS host.
9. Click **OK** to save
10. Close the **Site Bindings** dialog box.
11. In the **<host> Home Features View**, scroll down to **IIS section** and double-click to open **Server SSL Settings.**
12. In the **SSL Settings** window, select **Require SSL** then in the **Actions panel** on right, click **Apply.**
13. In **IIS Manager** dialog box's **Connections**, click to select **<host>.**
14. In **Action Panel** on right, click **restart.**
15. Close **Internet Information Services (IIS) Manager.**

Note: Port 443 is the default port used by SSL. A different port number is possible by specifying that port number in the URL (example: https:\\commserve.commcell.com:9315). Using a non-default port number can provide additional security.

LIMIT DATABASE ACCESS

Your primary means to protect the CommServe database are – and will always be - the physical, application, and network security measures you take. However, there are additional security precautions you can take as listed in this whitepaper. Recommendations are listed in order from basic security to more advanced steps.

Some of the security precautions recommended involve configuration of the Microsoft SQL Server instance or the Windows Server host used by the CommServe component. Configuration steps listed here may vary depending on whether you are using Microsoft Windows or SQL Server version 2008 or 2012 – initial or R2 variant. Consult the latest Microsoft's documentation for version specific steps.

The software uses an ODBC connection to communicate with the commserv database. Only the CommServe component accesses the database. The commserv database is in a DBO-only state allowing access only to

- System Administrator (SA)
- Windows account used to install the SQL Instance (used in ODBC)
- Application use-only accounts created by the installation process which cannot be used for direct log on.

Limiting database access would include these steps at a minimum:

- Maintain good physical security denying local/console access.
- Limit users with interactive logon rights.
- Use strong passwords and change them often.
- Implement a firewall to prevent remote network exploitation.

Additionally you can:

- Disable NETBIOS.
- Use the Local Security Policy tool to remove the right of the **Everyone** group to access the computer from the network. This tool is located in the Administrative Tools group on the computer.

- Disable null sessions to prevent anonymous, or unauthenticated, sessions. To accomplish this, set the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\RestrictAnonymous** registry value data to 1.

RENAME THE SQL SERVER ADMINISTRATOR 'SA' ACCOUNT

The CommServe database instance is installed with mixed-mode authentication. This means the default System Administrator 'sa' account is automatically created and enabled. Commvault uses the 'sa' account for initial database installation. It does not use the 'sa' account for normal operations.

Microsoft and other security experts recommend renaming the 'sa' account. If it ever becomes necessary the account name can be changed back to 'sa'. Alternately, the 'sa' account login during normal operations can be disabled. If at any time the 'sa' account is needed the account can be re-enabled.

Run these commands in the SQL Management Studio:

To disable the 'sa' login:

```
ALTER LOGIN sa DISABLE
```

To re-enable the 'sa' login when needed:

```
ALTER LOGIN sa ENABLE
```

Enable and disable the "sa" login using SQL Server Management Studio:

1. In the Object Explorer, expand the Security branch of the tree view and then expand Logins.

2. Right-click the "sa" login and choose "Properties" from the context-sensitive menu.

3. Change the enabled status of the account in the Status section of the dialog box.

CHANGE SQL SERVER DEFAULT PORTS

Another step to harden access to the SQL database on the CommServe server is to change the default service ports. A default installation of SQL Server 2012 use TCP port 1433 for client requests and communications. These ports are well known and are common targets for hackers.

To change the default ports:

1. From the **Start** menu, choose **All Programs | Microsoft SQL Server 2012 | Configuration Tools | SQL Server Configuration Manager**.
2. Expand the **SQL Server 2012 Network Configuration** node and select Protocols for the SQL Server instance to be configured.
3. In the right pane, right-click the protocol name **TCP/IP** and choose **Properties**.
4. In the TCP/IP Properties dialog box, select the **IP Addresses** tab.
   Note: There is a corresponding entry for every IP address assigned to the server.
5. Except for the IP addresses under IPAll, clear the values for both the **TCP Dynamic Ports** and **TCP** Port for each IP address.
6. In the **IPAll** section for each instance, type in a new port for SQL Server 2012 requests and communications. Port number should be in the dynamic range 49152-65535 to avoid conflict with Well-Known and Registered ports.
7. Click **Apply**.
8. Restart the SQL Server Services.

Note: If a Web Server component has been installed on a host other than the CommServe, update the ODBC connection information with the new SQL port number. Consult Commvault documentation on Post-Installation Configurations for Web Server and Web Console.

CHANGE AND HIDE SQL SERVER INSTANCE NAME

The default SQL Instance name used by Commvault software is COMMVAULT. Everyone familiar with Commvault software probably knows this so hiding the SQL Instance with the COMMVAULT name does little. That means you need to change the name before hiding the Instance. However, per Microsoft, modifying an existing named instance is not recommended without uninstall/reinstall. So two questions come to mind –

First question - Can you install the CommServe using a different SQL Instance Name? The answer is yes. It requires you to add a registry key and value prior to installing the CommServe.

Second question – Will reinstalling the CommServe with a different SQL Instance Name have any impact on past or future Commvault software operations? The answer is No. Commvault software server components that are installed on the CommServe host work through an ODBC connection. Remote server components or clients works through installed services on their respective hosts and do not communicate directly with the CommCell databases. As such, the SQL instance name is not relevant to any Commvault software operation.

INSTALL THE COMMSERVER COMPONENT USING A DIFFERENT SQL INSTANCE NAME

If the data/configuration information of an existing CommServe component should be retained, these steps should be done first:

- Back up the all user databases on the CommServe host
- Uninstall all Commvault software products
- Uninstall the existing SQL instance.

Use native SQL backup tools to create several backup copies of each user database and keep at least one copy in a secure place. Prior to installing the new SQL Server instance, create a registry value containing the new SQL Instance name. Use the following steps to configure the *szUserSQLInstanceName* registry key:

1. Log on to the computer as an Administrator or as a member of the Administrator group.
2. Click the Windows **Start** button and then click **Run**.
3. Type **regedit** and then click **OK** to open the **Registry Editor** window.
4. Navigate to HKEY_LOCAL_MACHINE > SOFTWARE > *GalaxyInstallerFlags*. If the key does not exist, create it.
5. Right click the GalaxyInstallerFlags key and select **New > String Value**.
6. Specify the Value name as **szUserSQLInstanceName**.
7. Double click **szUserSQLInstanceName** and in the Value data box, type the name of the SQL instance to use. Click **OK**.
8. Close the **Registry Editor** window.

INSTALL A NEW SQL SERVER INSTANCE

Once the new SQL Instance name is set, pre-install the SQL instance before installing the CommServe component. Use the following steps to install the SQL Instance using the software installation package provided by Commvault.

1. Log on to the client computer as an **Administrator** or as a member of the Administrator group on that computer.
2. Install .NET Framework 3.5.
3. From the CommServe installation package that was created using the Download Manager, run the following program:

WinX64\MSSQL\SQL_Enterprise_Edition\Setup.exe

The SQL Server Installation Center wizard is displayed.

4. In the left-hand navigation area, click **Installation** and then click **New SQL Server** stand-alone installation or add features to an existing installation.
5. On the **Setup Support Rules** page, click **OK** to start the setup of support rules.
6. On the **Product Key** page, click **Next**. Because the SQL installation software is provided by Commvault, the product key is already provided.
7. On the **License Terms** page, select **I accept the license terms** check box and then click **Next.**
8. On the **Product Updates** page, click **Next** to include the latest SQL Server updates.

   The Install Setup Files page is displayed, where the setup files are copied and then the installation automatically starts.

9. On the **Setup Support Rules** page, check that the verification process returns successful results. If the setup returns a few warnings or failures, make sure to fix them before proceeding with the installation, then click **Next**.
10. On the **Setup Role** page, click **Next** to proceed with the SQL Server Feature Installation.
11. On the **Feature Selection** page - for the features to install, select **Database Engine Services** and **Management Tools - Complete** and then click **Next.**
12. On the **Installation Rules** page, click **Next** after the setup completes running the rules.
13. On the **Instance Configuration page**, select **Named Instance** and type **the SQL Instance name assigned in the *szUserSQLInstancename* registry value**, then click **Next**.
14. On the **Disk Space Requirements** page, review the disk space summary and click Next.
15. On the **Server Configuration** page, complete the following steps:
    a. In the **Services Accounts** tab, click the **Account Name** cell that corresponds to the SQL Server Database Engine service, and from the list click **More** to specify the local system account. The account name for the service should display **NT AUTHORITY\SYSTEM.**
    b. Keep the default account names for the SQL Server Agent and SQL Server Browser services.
    c. Click the **Collation tab**, and make sure the collation of the **TEMPDB** is set to **SQL_Latin1_General_CP1_CI_AS** then click **Next**.
16. On the **Database Engine Configuration** page, complete the following steps in the Server Configuration tab:

a. Click **Mixed Mode (SQL Server authentication and Windows authentication)**.
b. Enter and confirm the password for 'sa' SQL user in the **Enter Password** and **Confirm password** boxes.
c. Click the **Add Current User** button.

17. In the Data Directories and FILESTREAM tabs, accept the default values and then click **Next**.
18. On **the Error Reporting** page, click **Next**.
19. On the **Installation Configuration Rules** page, check if the rules ran successfully and then click **Next**.
20. On the **Ready to Install** page, verify the features to be installed and then click **Install**. **The Installation Progress page** is displayed, showing the installation process.
21. On the **Complete** page, click **Close**. The SQL Server is successfully installed.

After the above steps the CommServe installation will prompt for the SQL System Administrator (sa) password. Use the existing instance for the CommServe databases.

POST-INSTALL OPERATIONS

The maximum memory used by the SQL Server should be 50% of the physical memory available (both active and passive nodes). During normal CommServe installation, this tuning of memory is done automatically. When pre-installing the SQL instance, this step needs to be performed manually. Use the following steps to verify the SQL memory usage for the CommServe component.

1. On the CommServe, open the **Microsoft SQL Server Management Studio**.
2. Right-click the <**Server Instance**>, and then click **Properties**.
3. From the **Server Properties** dialog box, select the **Memory** page on the left pane.
4. In the **Maximum server memory (in MB)** box, specify 50% of the physical memory available in the computer.
5. Click **OK.**

HIDE THE SQL INSTANCE

If Web Console or Compliance Search is used, consult Support before hiding the SQL Instance. Otherwise, hide the SQL instance just created.

To hide SQL instances:

1. From the **Start** menu, choose **All Programs | Microsoft SQL Server 2012 | Configuration Tools | SQL Server Configuration Manager**.

2. Expand the **SQL Server 2012 Network Configuration** node and select Protocols for the SQL Server instance to be configured.
3. Right-click **Protocols for [Server\Instance Name]** and choose **Properties**.
4. In the **Hide Instance** box on the **Protocols for [Server\Instance Name] Properties** page select **Yes**.
5. Click **OK**.
6. Restart the SQL services for the change to take effect.

HAVE AN EFFECTIVE INFORMATION SECURITY PROGRAM

With the growing number of threats, coupled with the evolving sophistication of attacks, organizations need to invest in cybersecurity and employee education to mitigate the loss of access to critical data and the resulting impact on business operations.

Employee Best Practices

- Do not open attachments unless they are expected and come from a known and trusted source.
- Do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware.
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends.
- Employ safe social media conduct. Hot topics are prime bait for scams, not all links lead to real login pages.
- Encourage employees to raise the alarm if they see anything suspicious.

IT Best Practices

- Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches.
- Restrict software to corporate-approved applications, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites with secure certificates.
- Deploy two-step authentication on any website or app that offers it.

- Ensure employees have different passwords for every email account, applications and login—especially for work-related sites and services.

INCREASE COMMVAULT BACKUP DATA SECURITY

One of the key fundamentals is having external copies of the data (aka backup copies) beyond just snapshots or versions maintained on the source system. It is important to differentiate a backup copy from a 'version' which is on the same system, which is of course not protected. Snapshots are also not appropriate backups in this context because the data must be in persistent copies in other locations. In the same way any copy which is maintained as a replicated copy will also become corrupted. Versions of the data from prior recovery points that are preserved in protected locations are very important.

Ransomware can lead to a hacker gaining access to file servers – so far most tend to focus on office types which they encrypt and if they can find access paths to any online backup sets then they delete them. If they just penetrated a client server – then backup copies are separated back in the content store and the front end systems can be recovered. This is one case where local snaps may leave exposure as a hacker may find and delete them. This is why secondary copies are so important.

By using a Commvault driver component, ransomware is blocked in from encrypting or deleting backup data from the MediaAgent itself. If the disk is exposed to other systems and local admin rights are discovered, the attached backup pool can potentially be deleted. The risk is reduced through having copy separation, different MediaAgents, different sites and offline media. Using a cloud library is another possibility in that it is not visible to the OS local admin account off the MediaAgent, unless a deep analysis attack has exposed the cloud user account credentials as well.

Commvault places check files in special areas that our service will monitor for changes. If those check files are altered an alert and notification are launched to investigate, react and take systems off the network before additional exposure can occur. At that point managed data paths should be monitored and locked down if necessary. An admin can create an alert using rate of change criteria to detect an unusual rate of change. In addition, an event will occur when the backup software detects ransomware. This message will be created: "Detected a possible Ransomware attack. Please verify the data on the machine". It is also heavily recommended that UNC shares have a dedicated user name and password not used for any other purpose. In environments where the performance would be acceptable, files can be archived and then if the rate of recall exceeds a certain threshold a workflow can be constructed to shut down the recall mechanism.

Overall ransomware validates the need for persistent, secured copies in other locations.

CREATE OFFLINE BACKUP COPIES

Summary:

- Primary copy set is the MediaAgent with the deduplication store that lands all the backup copies – that is persistent and always on
- Set up two independent DASH Copy targets – different servers/storage systems for complete partitioning –all individually dedicated systems
- On even weeks write DASH copy to GOLD using selective copy; Blue is powered off.
- On odd weeks write DASH copy to BLUE using selective copy; Gold is powered off.
- Scheduling can be used to sequence the power up and down.
- Ensure aging and verification are not scheduled when the library is offline.

Ransomware works over time so this strategy stretches out over a week. Flipping a disk or MediaAgent store daily runs the risk the ransomware may learn that behavior and corrupt the system today and tomorrow. If the MA-primary is corrupted, then an immediate fallback is the SELECTIVE DASH COPY on that week. It should be at an RPO of the last replicated jobs. It is critical to pay attention to the DASH copy fall-behind and ensure enough bandwidth and performance to avoid latency or lag.

If the ransomware did traverse to the secondary site and it compromised the GOLD set (assume it is the active GOLD week) then the last line of defense is the BLUE offline collection. Realize the RPO is potentially a 7 day loss. This setup would offer independent dedupe stores on each of the three copies – for safety and minimizing the complete corruption loss.

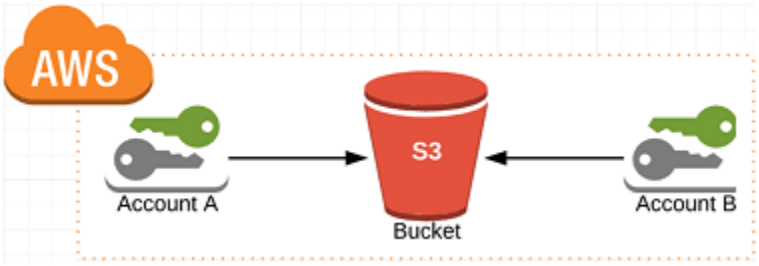
PROTECT AMAZON WEB SERVICES DATA

Even after adopting the best practices of moving the information to a separate resource like Amazon Web Services, it is still important to protect the credentials as the newer forms of ransomware also extract credential information.

Some recommendations to protect credentials and reduce the attack envelope:

- Lock away the AWS root keys
- Make extensive use of account segmentation
- Employ role based access controls within Commvault
- Always grant the least privileges
- Rotate credentials regularly
- Remove unnecessary credentials
- Monitor activity in both AWS and Commvault

AWS CLOUD STRATEGY – ANTICIPATE THE ATTACK TO HELP PREVENT IT



Account A Configuration

- Commvault server w/AD account
- Use S3 access/secret to access Account B's bucket

Account B Configuration

- Only accessible with a root account with FOB (Multi-Factor Authentication Device)
- Only one S3 user with no IAM or ACL access

To be hacked from account A

- Will need to compromise Active Directory
- Will need to logon to Commvault server
- Will need to manually delete jobs from Commvault

To be hacked from account B

- Will need to steal both root account credentials and MFA device

- Will need to steal S3 user credentials, then compromise account A, get into Commvault server, then access S3 endpoint of account A
- Except this user has no right or ACL or IAM so it cannot change its own rights

TAPE VERSUS DISK BASED BACKUPS

Disk-based backups offers a tremendous amount of benefits on operations – smaller windows (lower impact from backup), more frequency (more recovery points offers less risk of data loss), more consolidation (infrastructure reduction, simpler to manage and add capacity), better efficiency (deduplication reduction in resources, time, storage, etc.) and much faster recovery across the spectrum.

Disk-based backups have different implementation methods on copy management from persistent snapshots maintained on the source volumes, to secondary copy repositories managed in near-line (data is not directly mounted from the production host), secure areas, to far-line copy repositories managed on different sites and infrastructure formats (such as cloud storage services or different hardware combinations).

Ransomware may take longer to find than other types of malware. During that time it may compromise and corrupt files in production volumes. It can also delete any direct attached copy sets (such as snapshots or file copies).

Data copies stored on backup copy repositories can prevent rogue users from deleting the data, if the system is implemented in a hardened manner with strong security roles/access rights to minimize the risk of that system being compromised over the network.

It is important to be careful in configuring remote offices where the backup copy collections are implemented on the production host (to save on infrastructure costs). If the host is compromised at a root account then that copy set can be lost. Remote copy management strategies should use several "baskets" to store the data copies to avoid such risks and allow full system recovery if a production data set was lost.

Recently, the practice of creating external persistent backup copies has been stopped in preference to relying on local snapshots. However the snap collection can be deleted by OS root users. A tiered copy management strategy can minimize risk, while affording the right options and efficiencies to create data assurance and insurance on recovery and minimize infrastructure costs.

Tape is certainly a "safer" option in avoiding the risk of a root user deleting online collections… but most environments have outgrown the ability of tape to suffice in providing an active recovery tier to keep pace with the business. The better answer is creating the copy

repositories, ensuring the configuration is hardened, and managing at least two baskets to avoid the immediate risks.

REPLICATE USING A DASH COPY PROCESS

DASH copy is part of our embedded data copy management model. Data is replicated efficiently and securely between copy locations with embedded data verification, auditing and testing. This eliminates errors or other conditions that can occur if other third party tools move that data – while ensuring the transmission is secure/encrypted and efficient with deduplication to drive speed and minimize bandwidth and storage needs.

KEEP THE MEDIAAGENT FROM PROPAGATING MALWARE

We only copy data we manage. If malware got inserted into the storage area we use (such as shared folders) we do not blindly replicate all the contents. Rather we track and monitor what data copies and instances we have written to location 1 and only replicate those contents to the other managed copy in location 2.

This is more secure as compared to third party storage replication methods which will move all contents – since they do not have the indexing and intelligence. Our backup also maintains multiple versions to restore. An example could be a dedupe storage NAS device – if it is presenting shared folders and we wrote a collection of files to the folders and a malware also deposited some files on the folder – the NAS device will replicate all the contents and that will produce new instances of the malware on the destination; this is a downside of hardware driven replication.

Our process would alternatively only replicate the files we wrote to location 1 to location 2. We do not replicate the other foreign files in the same share.

ADHERE TO THE CSC 10.4 STANDARD BY MAINTAINING OFFLINE BACKUP COPIES

The CSC 10.4 standard is a collection of the Critical Security Controls recommendations by the Center for Internet Security related to data recovery. The CIS Critical Security Controls are based in the real-world knowledge of actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, policy-makers, auditors, etc.); and within many sectors (government, finance, academia, security) who have banded together to create, adopt, and support the controls. Specifically, section 10.4 of the CSC standard is: Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like

CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.

CONFIGURE THE NETWORK TO MITIGATE RANSOMWARE RISK

Create more selective network zones, provide backup recovery in partitioned/zones, and use firewall options. Use Commvault's extensive tools to test network connectivity and authentication, verify data, and test firewalls, performance and diagnostics (Network Tools).

RANSOMWARE IDENTIFICATION

Ransomware is a form of malware used by criminal organizations to encrypt data on infected systems, making the data inaccessible, typically requiring payment in return for a decryption key. Systems are typically infected by visiting a fraudulent website, or by opening unsafe email. Paying for the ransom does not guarantee that users will regain access to the infected system.

Any disruption in availability to data not only stops current operations but also negatively affects the perception of the company, affecting its future revenue. The decision to pay will be determined by various factors, including the scale of the attack, when it was detected, how quickly the business continuity plan kicked in, how widespread the ransomware encryption is, and when exactly the last back-up of uncorrupted data occurred.

Commvault identifies when a ransomware attack has taken place, alerts users and constantly protects backed up data by blocking rogue access. Commvault not only has had security built in since its inception, it employs special protections created to thwart ransomware attacks. Special files serve as known markers that can be monitored and agents block access to backed up data from the lowest level.

SUMMARY

Throughout its history, Commvault software has helped administrators achieve the highest level of security. Data protection is our highest priority. The procedures found in this white paper will make sure that Commvault software is configured in the most secure manner possible.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM