SECURE DATA SHARING

archTIS NC Protect with ONTAP

Information Protection for Unstructured data

Balbeer Bhurjhee
March 2023

Abstract

This is a field validated document where archTIS NC Protect with NetApp ONTAP software is used to provide advanced secure data protection and information sharing that helps organisations manage sensitive information and prevent data beaches. This solution applies to any system running ONTAP in hybrid multicloud.

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

The evolution of the current threat landscape presents every organisation with unique challenges for protecting its most valuable assets: data and information. The sophistication and dynamic nature of these attacks are ever increasing. For example, according to 2021 report by Verizon Data Breach Investigations report, 85% of the data breaches involved human element as social engineering, while only 15% involved technical vulnerabilities. And the average cost of Ransomware attack increased by 171% in 2020 according to a report by cybersecurity firm Coveware, and it also found the average downtime due to ransomware attack is 21days. Finally, when it comes to exposure of sensitive data, the Data Breach report by IBM in 2020, the average cost of data breach was $3.86millon, with healthcare and financial sectors experiencing the highest average cost per record breached. Couple these attacks with the increased effectiveness of the obfuscation and reconnaissance techniques on the part of potential intruders, today's system managers must proactively protect and secure the data and information that is core to the business and its reputational standing.

Although multiple solutions are available to protect your data, there is an ever-increasing desire to apply **dynamic access** to data based on a **data-centric**, Zero Trust Architecture. This is where the combined solution of NC Protect from archTIS and ONTAP from NetApp provides the next level insight and protection for Windows File Shares, Microsoft SharePoint data in the hybrid cloud. NC Protect will **discover, classify, and label unstructured data** found in files and email messages. Once the data is classified, NC Protect **dynamically adjusts access and protection applied to the files** based on a real-time comparison of user context and file content. It ensures files are accessed, used, and shared according to business and regulatory policies.

To be specific, NC Protect adds dynamic granular access and protection controls to business-critical content in Microsoft applications by applying **attribute-based access control (ABAC)** and data protection policies. While dynamic classification, access control and usage restrictions are NC Protect's first line of defense, when paired with Azure RMS or NC Encrypt, encryption can also be applied. For example, if a document that contains sensitive information is identified and **requires encryption** as per the organisation's governance policies, **it can encrypt the content immediately** – **limiting its audience to only correctly credentialed users**. This combination of NC Protect and ONTAP, protects customer information in Windows File Shares accessed through ONTAP using granular ABAC-powered zero trust policies applied at the file level to ensure secure collaboration.

Again, this document provides the detail system requirements should you need to test, deploy and run in production and highlights the key components on both NC Protect & ONTAP.

Use Cases

NC Protect with ONTAP helps address a myriad of use cases when it comes to the protection of information both in transit and at rest, leveraging dynamic access based on the user's attributes.

This document is limited to looking at the **Windows File Share** use case where it will be running on ONTAP system, whether it be on an on-premises NetApp appliance running ONTAP or a software-based system running ONTAP in any cloud, such as, Azure, Google or AWS. However, we will potentially look at evaluating other use cases in the future with NC Protect and ONTAP, such as the following:

- Exchange
- Office 365 – Microsoft Teams
- OneDrive
- SharePoint

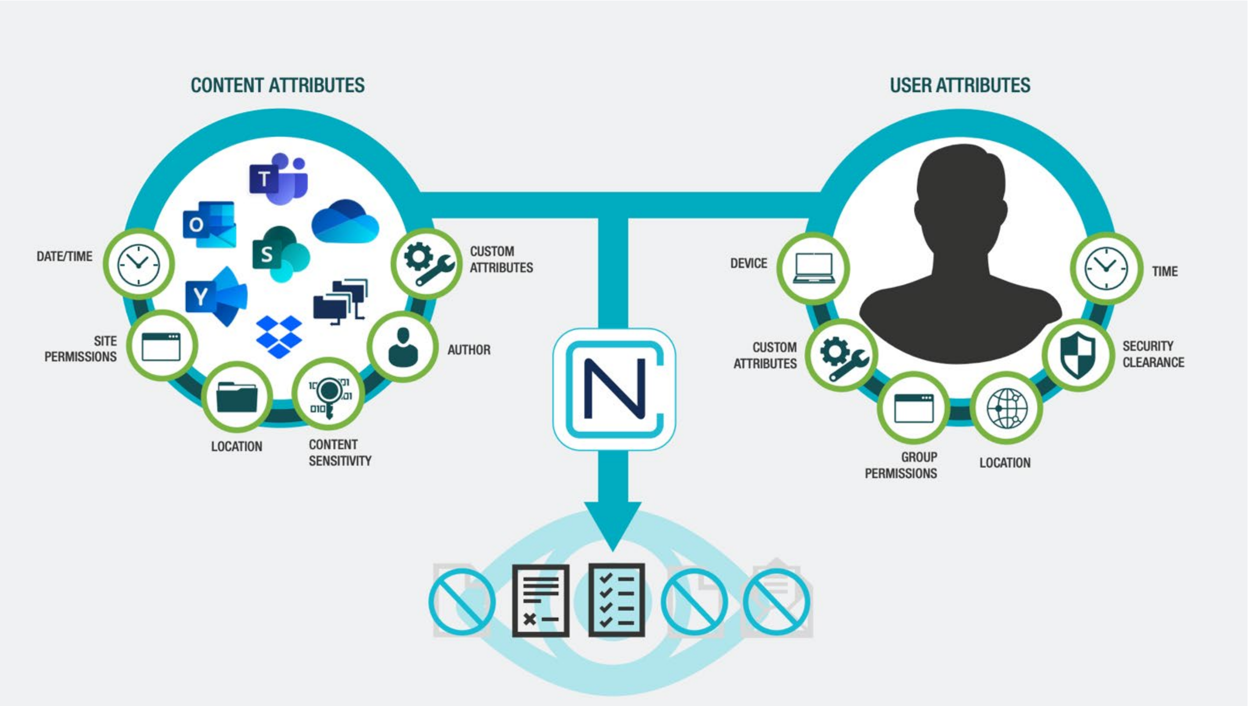
Solution

archTIS' NC Protect with NetApp ONTAP addresses the protection of information, dynamically at the data layer on-access. This is a 100% transparent layer to end-users when accessing their file data on Microsoft Windows shares running on ONTAP system, thus removes the complexity when compared to other solutions in the market. Specifically, NC Protect adds dynamic granular access and protection controls to the end user when reading or writing files with no impact to data storage like ONTAP.

In addition to the active directory user or group-based access controls, NC Protect provides customers' policy based, data-centric level protection based on a wide range of content-based attributes and user-based attributes. This is achieved with NC Protect, where it can apply transparent dynamic control or restrictions to the content layer, including encryption in transit and on-access, or at-rest, where the file(s) itself is encrypted on storage.

Furthermore, NC Protect provides data security capabilities as the user is viewing & opening files. This includes dynamic watermarking, secure viewing and redaction - all applied with no impact on ONTAP(i.e. no impact on storage capacity nor cost saving efficiencies such as, deduplication and compression). The only exception to this is when a policy within NC Protect applies encryption to files stored in ONTAP (the resulting file size being only slightly larger in some cases).

Figure 1) Dynamic Secure access of data using NC Protect with ONTAP



Solution Capabilities

The combined solution provides a multi-faceted 360degree layered approach to protecting customer's most important asset, data, that is accessed on Windows shares in ONTAP. Some of the key capabilities that are provided by combining ONTAP with NC Protect are as follows:

- **FPolicy**: is a file-access notification framework that you use to monitor and to manage file access over the NFS or SMB/CIFS protocol. This is built into ONTAP with the notion of Zero Trust Architecture, where an admin, regardless of super-administrator is also not trusted based on simple policies. The concept behind Zero Trust is to never trust and to always verify. This Zero Trust engine is valuable because you get extra security measures beyond permissions in access control lists (ACLs). FPolicy is also leveraged by 3rd party products, solutions that enables user-behavioral analytics, anti-virus scanning and much more.

- **External FPolicy:** FPolicy external mode in ONTAP uses UBA (sometimes referred to as User and Entity Behavior Analytics, or UEBA) as the key to stopping a zero-day ransomware attack. To understand how, you need a solid understanding of UBA.

  Human beings are creatures of habit. Our habits apply to many things, including how we access and work on data. Users and groups often access particular datasets to perform their jobs. UBA tracks these behaviors, identifies typical access patterns for a user, and can report when that user's behavior differs from the pattern. Going a step further, UBA can also deny access to file data if users are doing something outside their usual patterns. FPolicy external mode integrates with an external server that uses UBA to determine when users are doing things that they do not normally do.

- **Autonomous Ransomware Protection (ARP):** ARP leverages built-in onbox ML that looks at volume workload activity plus data entropy to automatically detect ransomware. It also monitors for activity that is different from UBA so that it can detect attacks that UBA does not. This is also a unique capability that this combined solution with archTIS and NetApp provides to further protect, detect and help recover and provide secure access to the data, regardless of where it is stored.

- **Dynamic Security Watermarks:** NC Protect can dynamically add a custom security watermark containing user or file attributes to sensitive and confidential Word, PowerPoint, Excel and PDF for security and auditing purposes. NC Protect watermarks can incorporate attributes, such as, user's name or email and the time and date that the file was accessed.

  Dynamic Security Watermarks supplements user education and training relating to the safe handling of sensitive proprietary information providing users with a very impactful and personalised visual reminder of their responsibilities relating to the protection of data. Additionally, by having personalized security watermark in the body of the document, the user is deterred from taking a picture with their mobile device and sharing in an unauthorized manner or using it for malicious purposes, helping reduce data loss and misuse. Depending on the implementation, dynamic watermarks on-access has ZERO impact to storage capacity on ONTAP.

- **File View Augmentation:** An admin can define rules in NC Protect to completely hide and block the viewing of sensitive information or confidential documents to minimize the risk of data loss. This differs from other solutions that can encrypt and control access to files but leave them visible to all users regardless of their rights to fully open a view the content. For example, if a file is added to a site and a member does not have proper access rights to that category of document, then the file is different from the view of the unauthorized individual. Only authorized users will be able to see the document. This helps prevent data loss and minimize the creation of sites and channels to accommodate different access rights.

- **Secure Web Reader:** Users can be forced to view sensitive documents in NC Protect's secure web viewer for read only access. This prevents users from being able to download, copy or edit sensitive data. Combined with dynamic watermarks and redaction, it deters users from taking photos of content placing a digital thumbprint on the document for tracing and forensics purposes.

  Given the dynamic nature of this capability, i.e.: on-access for read, this has zero impact to storage capacity in ONTAP. This provides end-2-end efficient and superior solution with NC Protect and ONTAP.

Key Benefits

The combination of NC Protect and ONTAP provides the following benefits for protecting data for ONTAP Windows File Shares:

- Automatically discover, classify, and restrict access to or encrypt files, either on the fly or at rest, or both, based on the presence of sensitive data including PII, PHI, IP and other factors.
- Control who can access files and how they can use and share them with dynamic fine-grain policies.
- Adjust protection based on file and user attributes to control who can access information, and if and how it can be copied or shared.
- Dynamically obfuscate/Hide files from unauthorized users.
- Detect potential violations and initiate workflows and notifications in SIEM applications including Microsoft Sentinel and Splunk to mitigate risk.
- Encrypt individual files only when the situation requires it. Apply user specific encryption with DLP protection as the file is being opened, leaving the source file untouched.
- Enforce secure read-only viewing of sensitive/classified information with a built-in Secure Reader.
- File integrity checks prevent users from overwriting valid files with corrupted files and protect digital assets from being maliciously encrypted.
- Add dynamic security watermark(s) to Word, PowerPoint, Excel and PDF documents.
- Redact sensitive or confidential information, such as keywords or phrases, when viewed in Word, Excel, PowerPoint, and PDF files or in the NC Protect secure reader.
- Audit trails and logs track access to and actions taken with sensitive data to ensure transparency, accountability, and regulatory compliance.
- Seamless disaster recovery whilst retaining all the protected data in the protected site using SVM-DR, a capability in ONTAP.
- Encryption of data in transit and at rest when it comes to data storage infrastructure using replication techniques, such as SnapMirror.

- An ability to tier the data dynamically to low-cost object store, regardless of on-premises or in the cloud.

- File system analytics in ONTAP provides deep file, directory level data based on access patterns, historical data, hot and cold, that helps in decision making, such as, identifying a need-in-a-haystack when it comes to identifying performance bottlenecks, as well as to optimize costs.

- Using ONTAP capabilities, like FPolicy to detect, prevent and protect data as it is being read/written into a file share.

- The Anti-ransomware capability in ONTAP further helps in detecting abnormalities on the active data based on heuristics analytics to detect, prevent, and recover data in case of a ransomware attack.

In addition to the above benefits of the combined solution for file shares, automatic data classification, labelling based on sensitivity of the data can be applied to the discovered data using either archTIS NC Protect or NetApp Data Classification service available in BlueXP for compliance, governance, GDPR related use-cases. In addition, the NetApp Classification service in BlueXP provides out-of-box reports for the discovered data based on the applied policies. The reports available are for Privacy Risk Assessment, HIPAA Report and PCI DSS Report or a specified Data Subject which is related to Data Subject Access Request report.

System Validation

The archTIS NC Protect with NetApp ONTAP solution was validated i.e.: tested with both archTIS and NetApp to ensure

- the key solution capabilities work as expected and
- capture the overall system requirements from both NC Protect and ONTAP, its configuration and other observations.

Whilst NC Protect for File Share was installed and functionally tested using a virtual machine (VM) in Microsoft's Azure environment with NetApp Cloud Volume ONTAP (CVO = a software version of ONTAP in Azure) the working will be exactly the same if the solution were to be deployed on-premises systems or in any other public cloud, for example, AWS or Google cloud where both NC Protect & ONTAP will be needed to provide the best solution to protect & secure your data.

System Requirements

NC Protect Requirements for protecting Windows File Share Data

- **For on-premises installations:**
    - 64-bit version of Microsoft SQL® Server 2012 and later
    - Microsoft SQL Server 2012 Reporting Services or later (optional)
    - Microsoft .NET® Framework 4.7.1 and later
    - Microsoft Active Directory® RMS or Azure® for Encryption
    - Internet Information Server 8.5 and later for standalone Windows Server installations
    - Microsoft Windows Server 2012 and later

Windows File Share configured on ONTAP systems

- Microsoft® URL Rewrite Module 2.0 for IIS
- Windows PowerShell 5.1
- Microsoft Active Directory® RMS or Azure for Encryption

- **Hardware requirements for NC Protect:**
    - For on-premises installations
        - 64-bit, four or eight core CPU (depending on the deployment size)
        - At least 16GB RAM

- **Supported Capabilities of NC Protect:**
    - **Scanning, Classification & Encryption At-Rest:**
        - Detect and act on the presence of sensitive data within files,
        - Application of metadata classification labels on files and items utilized for access controls.

- Encrypt at-rest of any file type via Microsoft encryption technologies and I file types with the appropriate Microsoft client install and/or the optional NC Encrypt module.
- Third party Key Manager for encryption of data based on requirements

  - **Windows File Shares on ONTAP**
    - Scanning, classification, and encryption at-rest of file types as above with NC Protect for shares on ONTAP
    - ONTAP Storage Virtual Machine (SVM) is configured as a member server in the same AD domain as the server where NC Protect is installed or in a trusted domain.
  - **Conditional Access, Encryption in-transit and Usage Rights:**

    Attribute-based augmentation of access and enforcement of usage rights for file, emails. Encrypt in-transit, and the enforcement of read only content via the web-based NC Protect's Secure Reader, with the ability to apply dynamic watermarks and control user editing, copying, printing and download rights.

    - Conditional access, encryption in-transit and usage rights supported on NC Protect.

- **Other requirements:**
  - NC Protect for File Shares is managed via the Web UI that is published from the IIS proxy server that sits in front of the shares presented from ONTAP.
  - This requires an IIS server to be installed and configured as a WebDAV server

ONTAP System Requirements

- **For on-premises requirements:**
  - ONTAP 9.11.1 or later
  - ONTAP Select (Software Defined Storage) or ANY NetApp hardware-based appliance, AFF or FAS running the above version
- **For cloud requirements (need to evaluate):**
  - ONTAP 9.11.1 or later
  - Azure NetApp Files with integration into Azure Active Directory
  - AWS FSxN for ONTAP
  - CVO software in aws, azure or gcp
- **Supported capabilities or feature requirements.**
  - Minimum of CIFS license on the ONTAP Cluster
  - SMB 2.0 or later for File Share access
  - Storage Virtual Machine (SVM) must have CIFS protocol enabled and must join as a member server in the Active Directory Doman
  - SVM-DR for disaster recovery across two sites
  - FlexVol & FlexGroup support
  - File System Analytics

    - FPolicy
    - Anti-ransomware
    - Tiering (FabricPool)
    - Replication support with SnapMirror for DR (asynchronous and synchronous)
    - MetroCluster support for synchronous replication
    - OnBox Key Manager or third party Key Manager for data@rest encryption support
- **Other requirements**
    - IIS server (as in NC Protect section), needs to be installed and configured. See details on the following MS site: https://docs.microsoft.com/en-us/iis/install/installing-publishing-technologies/installing-and-configuring-webdav-on-iis
    - WebDAV Proxy requirement (see below section)

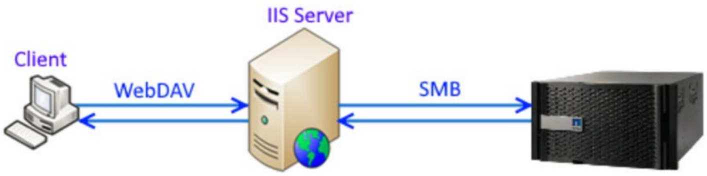
WebDAV Proxy requirement

NC Protect utilises the WebDAV service, which is an extension of HTTP/HTTPS protocols that allow clients to perform remote web content authoring operations collaboratively, to connect seamlessly with ONTAP. This WebDAV framework essentially enables a web server to act as a file server, by providing the ability for users to create, change and move documents on a server.

By utilising this WebDAV communication service and NC Protect's governance rules (policy engine), access to the content on the file server can be dynamically controlled based on the attributes of the end user (viewer) and content at the point in time of request. Depending on the sensitivity and/or user rights the content can be opened in a read-only secure reader. For further protection, this viewed content can also have a dynamically applied watermark as a deterrent or reminder to the end user to the sensitivity.

Figure 2) WebDAV Proxy requirement

Given NC Protect requires this WebDAV functionality implemented to provide the granular access controls, the joint solution will require an IIS server to act as an intermediary to sit between the end user and the ONTAP instance.

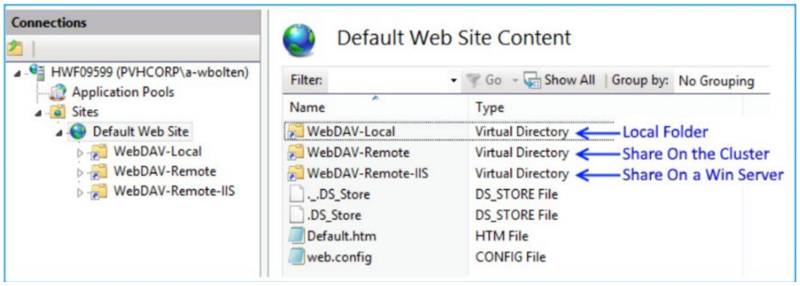


The high-level steps involved in configuring such a service are:

1. Install and configure an IIS server as a WebDAV server. For example, link for such a solution IIS_WebDAV.
2. Navigate in the IIS server virtual directory to the designated Storage Virtual Machine (SVM) on ONTAP CIFS share.

In this scenario, the user has opened WebDAV share from a client and unable to reach the data on the SVM share on ONTAP. However, if the user 'explore' the virtual directory configured from with-in the IIS website, it would open as expected.

A second virtual directory is added to the WebDAV website that is pointing to a share on a different Windows machine, this virtual directory worked as expected both from the 'explore' option and obviously from a WebDAV client.



Default Web Site Content

Name	Type	
WebDAV-Local	Virtual Directory	Local Folder
WebDAV-Remote	Virtual Directory	Share On the Cluster
WebDAV-Remote-IIS	Virtual Directory	Share On a Win Server
._.DS_Store	DS_STORE File	
.DS_Store	DS_STORE File	
Default.htm	HTM File	
web.config	CONFIG File	

ONTAP Feature Validation

Apart from some of the key feature validation especially from an impact, if any, on storage capacity with NC Protect capabilities, the implementation is very straight-forward. The high-level steps are as follows:

- Deploy ONTAP (physical appliance, CVO in any cloud, or Azure NetApp Files (ANF), and/or FSxN in AWS)
- Configure the ONTAP system so that it joins the Microsoft Active Directory Domain in your network.
- Create a File Share on ONTAP
- Once the above step is completed, use ArchTIS NC Protect via the IIS server and use the UNC path to the share that has been created on ONTAP.
- Apply the relevant security policies in NC Protect
- End-user maps the share as usual and accesses the data based on the policies applied.

Storage Efficiencies: As the combined solution using archTIS NC Protect and NetApp ONTAP is dynamic from a point of view of user access, it was observed that there is no impact to data storage when on-demand access and security is applied using NC Protect. This is for the following scenarios:

- Dynamic Watermarking for content on-read: It was observed there was no impact to storage capacity utilisation when dynamic watermarking was applied using NC Protect in ONTAP
- Dynamic encryption in-transit for on-access of content: When this is enabled in NC Protect, there is no impact on storage capacity as the original content, if not encrypted already on storage, and upon read, there is no impact to storage capacity, regardless of the data is encrypted by NC Protect when presented to the end user and or when a file is closed.

Note: ***If file encryption at rest is enabled using NC protect. This implies, the file(s) are encrypted at rest on share in ONTAP, then, as you may expect, this will have impact to storage capacity. For example, potential impact to storage efficiencies for the volumes in concern and may also impact to old snapshots usage, esp the existing snapshots.***

Performance: Given NC Protect acts as a proxy or mediator via the WebDAV, there was no impact to performance from an ONTAP Storage systems standpoint. The exception to this is that, if upon enabling NC Protect to encrypt files at rest, then, depending on volume, for example100 millions or more, then there will be some impact. as expected. Hence, based on the use-case, consult your NetApp & archTIS counterpart.

Key Takeaways

- The joint solution of archTIS NC Protect and NetApp ONTAP provides a comprehensive data protection and security solution for Windows File Shares.
- NC Protect's policy engine dynamically controls access to content based on user attributes and content sensitivity, with the ability to apply dynamic watermarks and encryption in-transit.
- NetApp ONTAP's storage capabilities, including SVM-DR and SnapMirror, provide seamless disaster recovery and encryption of data in transit and at rest.
- The WebDAV service is utilized to connect NC Protect with ONTAP for granular access controls, with an IIS server required as an intermediary.
- The solution was validated through testing to ensure functionally it works as expected, and can be confidently deployed in production environments.
- There is no impact to data storage when on-demand access and security is applied using NC Protect, with no impact to performance from an ONTAP storage systems standpoint.
- The joint solution can be deployed on-premises or in any public cloud, with the ability to tier data dynamically to low-cost object stores.

Resources

- ArchTIS RBAC or ABAC (Attribute Based Access Control) https://info.archtis.com/role-based-access-control-rbac-or-attribute-based-access-control-abac/
- What is Attribute Based Access Control https://www.archtis.com/what-is-attribute-based-access-control-or-abac-video/
- ONTAP 9 Documentation Center http://docs.netapp.com/ontap-9/index.jsp
- ONTAP 9 Release Notes http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-rn%2Fhome.html
- ONTAP 9 Command Reference http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-cmpr930%2Fhome.html
- System Administration Reference http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-sag%2Fhome.html
- Administrator Authentication and RBAC Power Guide http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-adm-authrbac%2Fhome.html
- NetApp Encryption Power Guide http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html
- TR-4647: Multifactor Authentication in ONTAP 9.3 https://www.netapp.com/us/media/tr-4647.pdf
  36 Security hardening guide for NetApp ONTAP 9 © 2023 NetApp, Inc. All Rights Reserved.
- OPENSSL Ciphers https://www.openssl.org/docs/man1.0.2/man1/ciphers.html
- CryptoMod FIPS-140-2 Level 1 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3387
- Certificate-Based Authentication with the NetApp Manageability SDK for ONTAP https://netapp.io/2016/11/08/certificate-based-authentication-netapp-manageability-sdk-ontap/
- ONTAP 9 Network Management Guide https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-nmg/home.html
- ONTAP 9 Generating and Installing a CA-Signed Server Certificate https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-adm-auth-rbac/GUID-7D65DCFE-A3F7- 4898-BFA6-1E4DE6C60DE7.html
- Perfect Forwarding Secrecy Blog https://blog.netapp.com/protecting-your-data-perfect-forward-secrecy-pfs-with-netapp-ontap/

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

NetApp