Knightcraft Technology
Information Security Specialists

UL

A Knightcraft Technology and UL (QSA) White Paper

PCI DSS Compliance for HPE NonStop Servers

PCI DSS Version 3.2

Document Version 3.2.02 (A4 Format)

September 2017

This paper is downloadable from www.knightcraft.com

Knightcraft Technology	www.knightcraft.com
UL (QSA)	www.ul.com

TABLE OF CONTENTS

PCI DSS COMPLIANCE AND THE HPE NONSTOP SERVER 11
Introduction 11
What is PCI DSS compliance? 12
Card Payment Applications on HPE NonStop servers 12
Template for ROC 12
Cardholder Data Elements 13
Compensating Controls 15
The Assessment process – what to expect 16
The difference between compliant and secure systems 16
Preparation for a PCI DSS assessment 17
Privileged Userids 19
Security Audit Logs 20
Independent Software Vendors 20
Evaluating Security Software Products 21
Useful References 25
REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA 26
Requirement Introduction 26
Requirement Description 26
The Requirement - 1 28
REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS 31
Requirement Introduction 31
Requirement Description 31
Change Default Settings 31
Default System Console Settings 33
System Configuration Standards 33
Single Function Server 34
Services and Protocols 35
System Security Parameters 35
Session Encryption 37
The Requirement - 2 39
REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA 46
Requirement Introduction 46
Requirement Description 46
Protection of Cardholder Data 47

Compensating Controls and Requirement 3.4 47
Locating Cardholder Data 48
Protecting Backup Data 48
Disk Encryption 49
Encryption Key Custodians 49
Encryption Keys 50
The Requirement - 3 51
REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS 57
Requirement Introduction 57
Requirement Description 57
The Requirement - 4 58
REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS 59
Requirement Introduction 59
Requirement Description 59
Securing the System Console 59
The Requirement - 5 61
REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS 62
Requirement Introduction 62
Requirement Description 62
Security Updates to Software 62
Role Based Application Access Control 63
Separation of Test and Development from Production 63
Change Control 64
Gaining privileged access through security configuration gaps 64
The Requirement - 6 66
REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW 70
Requirement Introduction 70
Requirement Description 70
Roles and Responsibilities 71
Use of Privileged Userids 71
Safeguard Security-Groups 72
User Access Privileges 72
Access Control System 72
“Need to Know” Access 73
Role Based User Access 75
The Requirement - 7 76
REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS 79

Requirement Introduction 79
Requirement Description 79
Accountability of User Sessions 80
Two Step Authentication 80
Multi-Factor Authentication 81
Off Box Authentication 81
Password Encryption 82
Password Management 82
New Passwords for Users 82
Revoking of Userids 83
Password Expiry 83
Vendor or Third Party Userids 83
Service Provider Access to Systems 84
Session Capture 84
Password Length and Complexity 85
Authenticate Fail Freeze 85
User session inactivity timeout 86
Application Userids 87
The Requirement - 8 88
REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA 95
Requirement Introduction 95
Requirement Description 95
System Console Physical Security 95
Removable Media 96
Clearonpurge Parameter 96
The Requirement - 9 97
REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA 101
Requirement Introduction 101
Requirement Description 101
Access to System Components 101
Individual Access to Cardholder Data 102
Recording Privileged User Actions 103
Access to Audit Trails 103
Failed Logon Attempts 103
Userid Management Attempts 104
Security Management Events 104
System level Objects 104

OSS File Auditing 105
Synchronization of System Time 105
Access to audit logs 105
Storage of Audit Logs 106
Audit Log Retention 106
Security Reports 107
The Requirement - 10 108
REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES 119
Requirement Introduction 119
Requirement Description 119
File Integrity Monitoring 119
Review of Security Configuration 119
The Requirement - 11 121
REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL 124
Requirement Introduction 124
Requirement Description 124
The Requirement - 12 125
REQUIREMENT A1: ADDITIONAL PCI DSS REQUIREMENTS FOR SHARED HOSTING PROVIDERS 128
Requirement Introduction 128
Requirement Description 128
Segregation of Environments 128
Resource Allocation 128
The Requirement – A1 129
REQUIREMENT A2: ADDITIONAL PCI DSS REQUIREMENTS FOR ENTITIES USING SSL/EARLY TLS 131
Requirement Introduction 131
Requirement Description 131
SSL/TLS Encryption In the HPE NONSTOP SERVER ENVIRONMENT 131
The Requirement – A2 132
REQUIREMENT A3: DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION (DESV) 133
Requirement Introduction 133
Requirement Description 133
The Requirement – A3 134
INDEPENDENT SOFTWARE VENDOR PRODUCTS 135
GLOSSARY 139
RESOURCES 141
ACKNOWLEDGEMENTS 142

TRADEMARK ACKNOWLEDGEMENTS

The following are trademarks or service marks of Hewlett-Packard Company:

NonStop Kernel
Enscribe
FUP
NonStop SQL
Event Management Service (EMS)
Distributed System Management (DSM)
PATHCOM
SAFECOM
SCF
Arcsight
NonStop
PATHWAY
TACL
Guardian
SAFEGUARD
NETBATCH

The following are trademarks or service marks of 4tech Software Ltd:

PANfinder
Integrity Detective

The following are trademarks or service marks of XYPRO Technology Corporation:

XYGATE Password Quality (XPQ)
XYGATE Safeguard Manager (XSM)
XYGATE Compliance PRO (XSW)
XYGATE File Encryption (XFE)
XYGATE Host Encryption (XHE)
XYGATE CMON (XCM)
XYGATE User Authentication (XUA)
XYGATE Encryption Library (XEL)
XYGATE Safeguard Reports (XSR)
XYGATE Merged Audit (XMA)
XYGATE Process Control (XPC)
XYGATE Object Security (XOS)
XYGATE Access Control (XAC)
XYGATE Key Manager (XKM)
XYGATE Report Manager (XRM)
XYGATE Data Protection (XDP)
XYPRO
XYGATE

The following are trademarks or service marks of comForte 21 GmbH:

SecurCS
SecurData
SecurSH
SecurTape
SecurOS
SecurFTP
SecurLib
SecurSSO
SecurPrint
SecurTN

The following are trademarks or service marks Computer Security Products Inc:

ProtectXP
CSP Passport
CSP Client Shield
CSP File Integrity Checker
CRM
OSS Explorer
CSP FTP Shield

The following are trademarks or service marks of Greenhouse Software & Consulting:

BaReLib
INSET
CURIOUS
LISTLIB
DiskWipe
MPWD
FTPSERV-E
Object Integrity (OBI)
REPRIEVE
SECOM
MyLogin
PRCOSEEP

The following are trademarks or service marks of Oracle Corporation:

GoldenGate

The following are trademarks or service marks of ETI-NET:

BackBox

The following are trademarks or service marks of Network Technologies International, Inc.:

DRNet

The following are trademarks or service marks of Gravic, Inc.:

Shadowbase

The following are trademarks or service marks of EMC Corporation:

RSA
enVision
ACE/Server
SecurId

BASE24 and BASE24-eps are trademarks or service marks of ACI Worldwide:

CONNEX is a trademark of Fidelity National Information Services, Inc: (FIS™)

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

PCI Security Standards Council, LLC (the Council) is the owner of the copyright of the material known as PCI Data Security Standards (PCI DSS). PCI DSS is the exclusive property of the Council.

COPYRIGHT

DISCLAIMER

This paper reflects the opinions and recommendations of the authors only and does not in any way represent the views or endorsements of Hewlett Packard Enterprise, comForte 21 GmbH, Greenhouse Software, Computer Security Products Inc, 4tech Software, XYPRO Technology Corporation, TANDsoft, Integrated Research, ACI Worldwide, FIS, PCI Security Standards Council or any other organization.

This document is a guide to assist you in your compliance efforts and should be treated as a guide only. It does not guarantee that you will necessarily be compliant by following the recommendations herein. You should seek professional advice to determine your organization’s specific situation and exactly what needs to be done for your organization to achieve compliance. Your status in regards to PCI DSS compliance will ultimately be determined by your QSA.

UL is an independent PCI QSA Company and as such does not endorse any specific commercial product. Furthermore, UL does not receive material gain from any product that their clients choose to implement to assist with PCI DSS compliance or system security in general.

FEEDBACK

While best efforts have been made by the authors to ensure technical accuracy, the software industry is renowned for the speed at which new and innovative ways for achieving goals emerge and are implemented. Industries change and products change accordingly.

We will be endeavoring to keep this document as up to date as possible, taking in any changes to the PCI DSS specification and changes in regards to HPE NonStop platform software.

We welcome your feedback. If you have any comments, corrections or suggestions for inclusion in the next version of the document, please submit feedback at http://www.knightcraft.com.

INTENDED AUDIENCE

The intended audience for this document is as follows:

- Technical or security personnel responsible for ensuring that the applicable HPE NonStop server environments within an organization satisfy PCI DSS compliance.
- QSAs responsible for performing PCI DSS compliance assessments on organizations that use HPE NonStop servers for processing, storing or transmitting payment card data.
- Auditors of HPE NonStop servers looking for technical information on security of HPE NonStop servers.
- Technical or security personnel looking to improve security and auditability of their HPE NonStop servers, even if they operate in an environment that is not subject to PCI DSS.

HOW TO USE THIS DOCUMENT

The *PCI DSS (Requirements and Security Assessment Procedures)*[1] i.e. the actual standard document, and the *Template for Report On Compliance (ROC) for use with PCI DSS v3.2*[2] should be used in conjunction with this white paper to assist in achieving compliance on the HPE NonStop Server. The Template for ROC indicates, in a platform neutral manner, what a QSA needs to look for as part of their PCI DSS assessment. This white paper provides more specific details on what the PCI DSS requirements actually mean specific to the HPE NonStop Server environment and how this relates to what a QSA will typically look for on the NonStop. For requirements that do not relate specifically or are not relevant to the HPE NonStop Server, the reader is pointed to the Template for ROC for details on what a QSA will require during a PCI DSS assessment.

Where a requirement cannot be readily achieved using standard HPE NonStop OS tools, this paper suggests Independent Software Vendor (ISV) software that may be able to help. See the section on Independent Software Vendor Products for information on which ISV products may assist with compliance. See also the section on Evaluating Security Software Products for some questions to ask ISVs that may help you determine which software product is most suitable for your needs.

PCI DSS VERSION

This document applies to PCI DSS version 3.2, April 2016. The full specification can be obtained from the PCI SSC website at https://www.pcisecuritystandards.org/document_library.

[1] *PCI DSS (Requirements and Security Assessment Procedures) https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf*

[2] *PCI DSS Template for ROC https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-ROC-Reporting-Template.pdf*

The PCI SSC website contains a number of other documents that may be helpful in interpreting the PCI DSS specification. These supporting documents can also be accessed from this document library link.

THE AUTHORS

Greg Swedosh is a Senior Security Consultant and the owner of **Knightcraft Technology**, which specializes in providing security and PCI DSS compliance consultancy services for the HPE NonStop (Tandem) Server platform. Greg is a co-author of the book *Securing HP NonStop Servers in an Open Systems World* and has presented in a number of countries on security for the HPE NonStop server platform. [Website: www.knightcraft.com].

in http://au.linkedin.com/in/gregswedosh

Dr. Sajal Islam is Audit Manager with **UL (PCI Service Stream)**, and a leading independent consultant in information security with specialist expertise in the payments sector. UL is accredited by PCI as a QSA, PA QSA and P2PE QSA company, and owns three of only eight laboratories around the world that are accredited to evaluate devices against the PCI PIN Transaction Security (PCI PTS) standard. [Website: http://industries.ul.com/transaction-security].

in http://au.linkedin.com/in/sajal-islam-qsa

ABOUT KNIGHTCRAFT TECHNOLOGY

With more than two decades in the international HPE NonStop (Tandem) world, a working partnership with QSA UL, and extensive "hands on" experience with all things NonStop, including Safeguard, XYGATE and comForte software, Knightcraft is the expert on PCI DSS and platform security for the HPE NonStop server. Knightcraft has a proven track record of assisting customers in the USA, Europe, Asia and Australia/New Zealand to achieve their security and compliance requirements.

Knightcraft's range of services includes the following:

- Security Review Service (full analysis of all security related configuration and recommendations on remediating any gaps – Safeguard, Guardian, OSS, XYGATE, comForte, Pathway, Netbatch, TACL environment, communications subsystems etc.).
- PCI DSS Consultancy Service (assisting organizations in their PCI compliance efforts with configuration, documentation and approach) that ensure security as well as compliance.
- HPE NonStop Security Implementation (Safeguard, XYGATE, comForte and all NonStop related subsystems).
- Education and Training (customized security training, security forensics, customized XYGATE training).
- PAN Data Discovery (using the PANfinder tool from 4tech Software).

Knightcraft services can be procured through HPE, comForte or directly. Go to http://www.knightcraft.com to see how Knightcraft can help your organization achieve PCI DSS Compliance and ensure a fully secure HPE NonStop environment. Alternately, contact your HPE or comForte account team.

PCI DSS COMPLIANCE AND THE HPE NONSTOP SERVER

INTRODUCTION

HPE NonStop™ servers run applications that process more than half of the world's electronic transactions. As the HPE NonStop server is THE core processing platform for these card payment systems, the security configuration, monitoring, documentation and procedures around it will be subject to the Payment Card Industry (PCI) Data Security Standard (DSS). Typically in these application environments, the HPE NonStop needs to store cardholder data on disk for extended periods of time. As such it is unlikely to be de-scoped from PCI DSS and so the data, application and system environment needs to meet the requirements of the standard. A typical organization using the HPE NonStop for processing electronic transactions may process thousands of transactions per second, resulting potentially in millions of new log record entries containing the PAN, cardholder name and potentially expiration date – every single day.

The PCI DSS sets forth twelve categories of requirements related to, but not limited to, system and network security, protection of payment card data and auditing of user access and actions. It details not only requirements that must be achieved through configuration, but also specifies documentation and procedural requirements that must be adhered to in order to be compliant with the standard.

This document provides guidance for addressing PCI DSS compliance in relation to an HPE NonStop server. A summary of the standard is provided for each section along with recommendations that address the various requirements. A matrix is provided for each section, giving an indication of what a PCI Qualified Security Assessor (QSA) will likely require during a PCI DSS assessment for the individual sub requirements, specific to HPE NonStop servers. This paper should be used in conjunction with the PCI DSS and the PCI DSS Template for ROC which describes more generically what a QSA will require during an assessment.

In cases where compliance cannot be easily or readily achieved using standard HPE NonStop tools, this document illustrates how compliance can be assisted by using software from Independent Software Vendors (ISV) and optional software from HPE. Organizations should consider implementing one of the suggested solutions or a similar solution where requirements cannot be achieved using standard HPE NonStop tools.

This document includes recommendations only as they relate to the HPE NonStop server. Sections that do not typically relate to the NonStop are included for completeness, but are marked as Not Applicable. Sections that are not specific to the HPE NonStop server but are more generic in nature refer to the Template for ROC for details on what a QSA will require. To achieve PCI DSS compliance, an organization must address all of the requirements. Once compliance is achieved, the organization must then maintain compliance.

WHAT IS PCI DSS COMPLIANCE?

If an organization stores, processes or transmits cardholder data, or can impact the security of a cardholder data environment, then it is subject to the requirements of PCI DSS.

For an organization to be considered compliant with the PCI DSS, the organization must be compliant with **ALL** applicable requirements specified in the standard or have approved compensating controls in place.

Once an organization has achieved PCI DSS compliance, they must ensure that they continue to meet the requirements of the standard. Assistance with assuring this may be found in the PCI DSS section on *Best Practices for Implementing PCI DSS into Business-as-Usual Processes*.

Full and detailed information on PCI DSS can be obtained from the PCI SSC web site www.pcisecuritystandards.org.

CARD PAYMENT APPLICATIONS ON HPE NONSTOP SERVERS

The HPE NonStop server has been the de facto standard for payment applications for more than 40 years due to the high availability, performance and scalability associated with its architecture. The most widely used electronic transaction application on the HPE NonStop server is BASE24 from ACI Worldwide. There are two general flavors of this – BASE24 "Classic" and BASE24-eps, both of which have components for processing POS and ATM transactions. Other applications used on the HPE NonStop for processing card payments include CONNEX (FIS), ElectraCard (ECS), Tango (Lusis Payments), OmniPayments (Opsol Integrators), SmartVista (BPC).

While some of these applications may contain the capabilities to encrypt or tokenize cardholder data as a part of application functionality, do not assume that this is so. Even if the application is PA-DSS (Payment Application Data Security Standard) validated, it may not protect data itself in accordance with requirement 3.4 and may require the user to take some action to protect the data. Make sure that you have all applicable information in regards to this from your payment application vendor. The onus is on you, not the vendor, to determine whether or not your cardholder data is adequately protected in accordance with PCI DSS.

TEMPLATE FOR ROC

Prior to September 2011, QSAs would use a document called the ROC Scoring Matrix to assess whether or not an organization satisfied the PCI DSS requirements. This document was not publicly available, being provided only to QSAs. A document called the *Template for ROC (Report On Compliance)* is now used by QSAs as a basis for assessing compliance. This document is available as a public document and can be downloaded from https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-ROC-Reporting-Template.pdf.

It is recommended that organizations download and use the Template for ROC document in conjunction with this white paper to assist in their PCI DSS compliance efforts. In certain places where requirements are not specific to the HPE NonStop and are more likely to fall under a wider scope within the organization, or are likely to be the responsibility of a non-HPE NonStop specific department, this paper references to the Template for ROC.

CARDHOLDER DATA ELEMENTS

The following table[3] identifies the various data elements or items of sensitive cardholder information. The table indicates whether it is permissible under PCI DSS for each data element to be stored on the system, if protection is required and if it needs to be rendered unreadable as per PCI DSS Requirement 3.4.

	Data Element	**Storage Permitted**	**Render Stored Account Data Unreadable per Requirement 3.4**
Cardholder Data	Primary Account Number (PAN)	Yes	**Yes**
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data[2*]	Full Track Data [3*]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID[4*]	No	Cannot store per Requirement 3.2
	PIN/PIN Block[5*]	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

Sensitive Authentication Data (SAD) must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment. Organizations should contact their acquirer or the individual payment brands directly to understand whether SAD is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.

2 - Sensitive authentication data must not be stored after authorization (even if encrypted).*

3 - Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere*

4 - The three- or four-digit value printed on the front or back of a payment card*

5 - Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message*

Note that the “Service Code” is also known as the “Service Restriction Code”. See ISO 8583 Financial transaction card originated messages — Interchange message specifications (*http://en.wikipedia.org/wiki/ISO_8583#Data_elements*) for a detailed list of cardholder data elements.

[3] *PCI DSS Applicability Information*, from PCI Data Security Standard v3.2

Depending on the nature and design of the application being used, there are a number of places on an HPE NonStop server where cardholder data may be located. All of these locations should be protected in accordance with PCI DSS. Typical locations where cardholder data may be stored are:

- Cardholder database - Often the PAN (cardholder number) is used as a primary key
- Transaction logfiles
- TMF auditdumps and audittrails
- Backup media
- Data replication transaction queues (for example those associated with GoldenGate®, DRNet®, Shadowbase® etc.)
- Application trace files
- Communication line/process trace files (e.g. SCF traces)
- Swap files
- Saveabend (or other memory dump) files

While "off the shelf" financial applications such as BASE24™ and CONNEX™ are user customizable, with organizations receiving source code for the software, customization tends to normally be in regards to different message formats and interfaces. The storage locations of cardholder data will often still be found in the standard locations. There may however be non-standard locations where cardholder data is also stored, depending on specific organizational requirements and industry practices. There should be no assumptions made that all cardholder data on the system and in the network is protected, on the basis that a new version of a card processing application is "encryption enabled" or that the application is PA-DSS validated. A full analysis needs to be conducted of all possible locations where cardholder data may exist and a determination made as to whether all data elements are protected as required by PCI DSS. The onus is on you to ensure that all locations of cardholder data have been correctly identified.

As well as data at rest, cardholder data in transit must be protected. It is typical for an acquirer's financial switching application to accept transactions into the application from merchants in an external message format, convert the transaction to an internal message format for processing, and then reconvert to another external message format for sending on to the relevant financial organization or issuer. Depending on the mechanisms used, this may provide a number of potential areas that need consideration in determining if cardholder data is suitably protected. For example, if processes involved in the handling of cardholder data were to abend for some reason, are any saveabend files produced and if so, are they suitably protected? Are the processes themselves protected so that they can't be put into debug by an unauthorized user?

The internal format of the message is often used as the "official" record of the transaction and may be used for reporting to financial institutions. In certain instances, it may be necessary for an organization to store this data to satisfy legal or regulatory requirements. If such reporting procedures are in place, this may indicate an extra location or locations where cardholder data is stored or transmitted.

Another area to consider is at the point where card transactions enter or exit the application. Often there will be a trace facility (either application level or at the communications level via SCF) that will enable the reading of the raw transaction, including cardholder data, by certain personnel. This may be in place for application troubleshooting and support purposes, and may be enabled either permanently or only when troubleshooting. If traces that will be capturing cardholder data are likely to be run at some stage, procedures should be put in place to ensure that the trace data is dealt with in accordance with PCI DSS. All of the requirements around protection of cardholder data (such as requirement 3.4) apply. The procedures should be documented and known to support staff so that they can be put into effect whenever such a trace is required.

Consideration must also be given to unauthorized locations containing cardholder data, such as cardholder data files or records copied from the production database to the test system for testing purposes, or copies of communications line trace files used for troubleshooting problems. The use of production data on a test or development system is specifically forbidden by PCI DSS, but such data is not so easy to find without an appropriate automated tool.

Independent Software Vendor Products exist that can locate where unprotected PAN data or unauthorized copies of cardholder data are stored on the system. PANfinder automatically searches files to determine if they contain PANs or Sensitive Authentication Data, such as full track or card expiry dates, and produces PCI compliant reports based on its findings.

COMPENSATING CONTROLS

Compensating controls[4] may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be “above and beyond” other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

[4] *Appendix B – Compensating Controls*, from PCI Data Security Standard 3.2

For further details on compensating controls including procedures for applying for compensating controls, see the PCI Data Security Standard v3.2 Appendices B and C.

Until recently, many HPE NonStop organizations have used compensating controls to satisfy requirement 3.4. This was largely due to the complexity and cost involved in adding encryption to their application. With the advent of HPE NonStop based tools that provide data tokenization using intercept libraries, with minimal application and database changes required, organizations should be looking to satisfy requirement 3.4 fully rather than using compensating controls. See the section on Compensating Controls and Requirement 3.4 for further details.

THE ASSESSMENT PROCESS – WHAT TO EXPECT

For each requirement of the PCI DSS specification, different items of information (artifacts) may be required by the QSA performing the assessment. This could be any combination of the following:

- Proof of system settings or configuration
- Review of documentation
- Interview by a QSA
- Witnessing of current state or actions performed

During a PCI DSS assessment a QSA will examine each requirement as specified in the standard and will assess whether the requirement is "In Place", "In Place with a Compensating Control Worksheet", "Not Applicable", "Not Tested" or "Not In Place" in accordance with the Template for ROC.

Note that some requirements differ for merchants, acquirers and issuers. PCI assessments will vary accordingly.

THE DIFFERENCE BETWEEN COMPLIANT AND SECURE SYSTEMS

Being PCI DSS compliant provides no guarantees that an organization will not experience credit card fraud. It provides a minimum standard for security and audit settings that must be in place to help reduce the risk of fraud. It can be seen from recent high profile data breaches that just because an organization has been passed as compliant at a point in time by their QSA and firmly believe that they are compliant, this is not necessarily the situation. In the case of HPE NonStop servers, QSAs often have limited experience or expertise with the platform so may not be in a position to assess accurately whether all appropriate subsystems are secured fully and appropriately. A QSA of limited HPE NonStop expertise may not know of the many different ways that it is possible for a non-privileged user to assume privileged userid capabilities on the system if the system is not appropriately secured. It is highly recommended that organizations ensure that they are not only PCI DSS compliant as per their QSA, but that they also regularly review their security. This review should be performed by personnel with the appropriate level of expertise but should not be performed by those personnel responsible for implementing the security so as to ensure full separation of duties. If the appropriate expertise is not available in-house, then external advice should be sought. See www.knightcraft.com to find out how Knightcraft can assist in this regard.

For more information on areas of the system that need to be addressed to ensure security as well as compliance, see You May Be PCI DSS Compliant, But Are You Really Secure? (http://www.knightcraft.com/2014-hp-nonstop-advanced-technical-boot-camp)

PREPARATION FOR A PCI DSS ASSESSMENT

In preparation for tackling PCI DSS compliance, there are preliminary steps that will help achieve the goal. Much of this information may be required by a QSA and it will also assist in determining what areas need to be addressed for the various sections of the standard.

- All the PCI DSS requirements have a documentation component, including all of Requirement 12 (with its 40+ sub-requirements). Take an inventory of all existing documentation related to:
    - Roles and responsibilities
    - Data access and associated auditing controls around access
    - System description, configuration, management
    - User management and associated policies and procedures
    - Security description, configuration, management, incident handling
    - Application design, development, implementation, configuration
    - Operational policies and procedures
    - Media handling
    - Change management
    - Any other documentation that may possibly relate to the HPE NonStop server environment within your organization. You'll probably need it!

  Beginning the PCI DSS readiness process with Requirement 12: Maintain a Policy that Addresses Information Security for is a good way to become familiar with what is involved with PCI DSS. Satisfying this requirement alone is potentially a very large task and having an understanding right up front will assist with the other requirements of the standard, as all of them have a large focus on documentation.
- Work out exactly where your cardholder data is stored. The PCI DSS states in the section titled "*Scope of Assessment for Compliance with PCI DSS Requirements*" as follows:

  "The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- *The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).*
- *Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).*
- *The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data.*
- *The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity."*

In essence this means that prior to starting your PCI DSS assessment, you must show a QSA documentation as to where all of your cardholder data exists and describe the process that you used to determine that these are the only locations where cardholder data does exist.

To help determine locations of cardholder data, the following should be done:

- Prepare a network diagram of the HPE NonStop server(s) identifying all access points in and out of the system(s).
- Prepare a high level diagram of applications that process card payments indicating the flow of transactions and where data is stored. This will assist in identifying all locations where cardholder data is stored, processed or transmitted.
- Identify and document the critical components and details of the environment where cardholder information is stored, processed or transmitted, such as:
  - The HPE NonStop servers that process card payments or store or transmit cardholder data.
  - The operating system versions of each of the HPE NonStop servers.
  - The core functions provided by each of the HPE NonStop servers.
  - Each file/table on the relevant systems containing cardholder data. See the Cardholder Data Elements section for details of which fields are regarded as sensitive cardholder data and how they need to be treated to comply with PCI DSS.
  - For each cardholder data element, determine if it is secured (for example through encryption or tokenization) and if there is an audit trail captured of any attempts to access the data element.

  See Section 4 of the Template for ROC for details about the reviewed environment that need to be provided to the QSA.

The QSA will also expect you to demonstrate how it was ascertained that the identified locations comprise the complete list of cardholder data locations on the system.

Independent Software Vendor Products exist that can assist by scanning the system and identifying all locations where unencrypted/non-tokenized cardholder data or sensitive authentication data is located. [Consider PANfinder]

A QSA may not analyze all systems when performing an assessment but may take a representative sample of the organization's nodes on which to analyze configuration, documentation and procedures. The sample will be defined at the commencement of the assessment.

The QSA will, however, want to see ALL of your documentation!

PRIVILEGED USERIDS

PCI DSS refers in a number of requirements to "Privileged Userids". The userid on an HPE NonStop server that invariably comes to mind is that of the all-powerful SUPER.SUPER. There are however other userids or aliases on an HPE NonStop server that should also be considered as privileged userids. These potentially include:

- SUPER.SUPER
- All SUPER group userids
- Security administrator userid (typically the owner of SUPER.SUPER and Safeguard user and protection records)
- Members of privileged Safeguard Security-Groups
- Operator userids used for backup and restore
- Userids associated with any HPE or third party security software
- Application/Data owner userids
- Application builder userids (i.e. userids for implementing new application object code)
- Data replication owner ID
- Netbatch supervisor and job owner userids
- Userids with any ability to modify system/subsystem startup or configuration files
- Userids with the ability to modify application objects or manipulate the application in any way
- Userids with the ability to read files in any location that may contain cardholder data
- Any userid or alias with the ability to gain the privileges of any of the above userids through use of utilities such as XYGATE Access Control (XAC), SECOM, CSP Passport etc.
- All aliases of the above Userids

Further to the above, any application specific userids (that is, userids for logging in to the application such as BASE24 or CONNEX) that have elevated privileged access within the application, should also be dealt with as "privileged userids". Actions that privileged application userids may be able to perform include addition or modification of other application userids, configuration of screen and function access to users and access to functions enabling the viewing of cardholder data (for example transaction trace functionality).

See the section on Gaining privileged access through security configuration gaps, Use of Privileged Userids, Role Based User Access and Recording Privileged User Actions for relevant topics around privileged Userids.

SECURITY AUDIT LOGS

When considering security audit logs in the context of PCI DSS requirements, audit logs from the following subsystems/programs/applications should be taken into account:

- Safeguard
- ISV software security logs (e.g. XYGATE, comForte, CSP, Greenhouse software etc.)
- Application security logs, for example BASE24 OMF logs
- EMS logs
- System console audit logs
- CLIM authentication logs
- In some instances, compliance to PCI DSS might result in having to modify existing applications to add and/or extend audit logging capabilities

INDEPENDENT SOFTWARE VENDORS

There are a number of Independent Software Vendors (ISVs) who produce security, auditing and compliance related software for the HPE NonStop server platform. Often their software provides functionality that does not exist in the standard toolset provided with the HPE NonStop server Operating System, or it provides added or enhanced functionality. In cases where standard software that comes as part of the HPE NonStop OS cannot fulfill PCI DSS requirements, software tools from ISVs are suggested for consideration. The various vendors are as follows:

• 4tech Software	(www.4techsoftware.com)
• ACI	(www.aci.com)
• Bowden	(www.bsi2.com)
• CAIL	(www.cail.com)
• comForte 21 GmbH	(www.comforte.com)
• Crystal Point	(www.crystalpoint.com)
• CSP Security	(www.cspsecurity.com)
• Crossroads	(www.crossroads.com)
• ETI-NET	(www.etinet.com)
• GreenHouse Software	(www.greenhouse.de)

IdentityForge	(www.identityforge.com)
Opsol Integrators	(www.opsol.com)
TANDsoft	(www.tandsoft.com)
TSI	(www.tributary.com)
XYPRO Technology Corporation	(www.xypro.com)

A list of software products from ISVs is defined in the Independent Software Vendor Products section of this document. Please note that the list is not exhaustive, so readers should check out the websites of the vendors above for the latest product offerings.

The section on Evaluating Security Software Products provides a list of questions that will be useful in helping you determine which optional HPE or ISV security products are most suitable for your organization in satisfying your individual security and compliance needs.

It should be noted that the software recommendations provided in this document may not be the only solutions available. Offerings from the various security software vendors change with time as new products are added, or new functionality is added to existing products, or new vendors come on the scene. It is recommended that organizations become familiar with the offerings of all vendors and evaluate software appropriately to ensure that it fits in with their specific requirements.

EVALUATING SECURITY SOFTWARE PRODUCTS

When choosing which security software products you will use to fill PCI DSS compliance requirements not catered for by standard HPE NonStop OS software, there are a number of significant factors that you should include in your decision making process. Depending on your specific environment and own internal requirements, the following questions may assist you in choosing the right product for your situation:

For all software types (where relevant)

- Does the software need to run as SUPER.SUPER or can any designated userid be used for running/managing the software?
- Is the software configured on the HPE NonStop host, via a client based GUI or via a web browser?
- How is the software configured? Have a look to see how complex the configuration files or configuration screens are.
- What authentication is required to manage the software configuration (if GUI or browser based)?
- Is it necessary to set up and maintain a separate dedicated database of userids or aliases and/or passwords specific to the software? Or does the software use standard Guardian userids/aliases for authentication? If the software does have a separate database, does it have adequate userid/password management to satisfy PCI requirements in those areas?
- How is the configuration protected from unauthorized access?
- Does the software have "NonStop" capabilities or can it be added as a kernel managed persistent process i.e. if it stops for some reason, is it automatically restarted?

- Does the software run as a SEEP (Security Event Exit Process) and if so, are there any management or configuration issues around this?
- Are there special procedures required as part of an operating system upgrade?
- Does the software produce audit logs that include all required PCI DSS information as per requirement 10.3?
- What performance impact is there in running the software?
- Is there a requirement for other infrastructure such as web services to make the product work?

See also the questions below related to Audit Logging/Reporting/Alerting.

For Session capture/logging software

- Does it operate fully in both Guardian and OSS (OSH) environments?
- What kind of sessions are captured (TACL, OSH, FTP… etc.)?
- Does it capture block mode sessions as well as conversational/command line sessions?
- Are passwords captured and displayed "in the clear" in the audit logs?
- Is it possible to "get around" the audit capabilities of the software by specifying a different IN and OUT runtime parameter for an object? i.e. can sessions be reconfigured or created that are non-audited sessions? E.g. SCF/IN <myterm>, OUT <myterm>/
- Can the software capture the commands within a TACL macro and/or OBEY file? See the section on Session Capture for further related info.
- Is the origination of the event (i.e. IP address) captured for user sessions?
- Does an auto logoff feature exist where sessions terminate after a configurable period of inactivity?
- What overhead exists in capturing user sessions using the software?
- What reporting tools can be used for viewing user sessions? Ask for sample reports to see how clear the presentation of user sessions is.

For role based access control software (i.e. software that allows users to perform authorized privileged commands from their own non-privileged userid)

- Does it operate fully in both Guardian and OSS environments? If not, what restrictions exist?
- Does the software support use of aliases or does it require use of standard Guardian userids?
- Can user roles be allocated by group membership or does each user need to be configured individually?
- Do userids/aliases/groups for the software correspond to the user's standard Guardian userid/alias/group or does the software require separate user administration or mapping? If the software does have a separate database, does it have adequate userid/password management to satisfy PCI requirements in those areas?
- Can the software restrict access of privileged aliases separate from the underlying ID?
- Does the tool allow definition of a "role" and allow mapping one or multiple users to that "role"?

- Are all commands (input and output) fully audited? See details on *Session Capture/Logging Software* above.

For ALL encryption based products (session encryption, data encryption/tokenization, encrypted backup etc.)

- Does it support strong protocols/encryption algorithms/cipher suites? For strong encryption definitions as regards PCI DSS, see Strong Cryptography.
- Are the protocols/encryption algorithms/cipher suites configurable, allowing you to disable one individually in case a serious vulnerability is discovered without waiting for a patch to become available?
- Do the encryption algorithms/cipher suites used meet industry standards and best practices? If so, do they have some kind of industry certification (e.g. FIPS validation)?
- How is the key management for encryption keys handled? Find out as much detail as possible on key management if relevant.
- Is key management software or hardware based?
- Does the encryption solution interface with your existing HSMs?
- Are encryption keys stored unencrypted anywhere on disk?
- Are there performance figures or test tools that can assist in determining the processing overhead that will be added by encrypting the data?
- For session encryption or encrypted backup: Does the implementation of the encryption add overhead beyond the cryptographic operations?

For data encryption/tokenization products

- What modifications, if any, are required to the data file/table structure to implement field/column level encryption?
- What modifications, if any, are required to the application to enable the writing and reading of encrypted data?
- Which programming languages are supported? Are both native and TNS mode supported, and if so is there a performance penalty for TNS mode?
- Are both the Guardian and OSS environments supported?
- Are there programming examples in your required programming language provided to assist in implementation of the encryption solution?
- Does the solution allow for integration with applications on other computing platforms?

For File Integrity Monitoring

- Does it use a fingerprinting technique such as SHA2 or MD5 to establish if a file has changed? Is the fingerprinting hash algorithm configurable?
- Can it detect changes to attributes of dynamic files such as owner, security and so on, without raising an exception because the last modification date or file fingerprint has changed (e.g. for logfiles which will be continually changing)?

- Does the software operate in real time or are collections run in batch (e.g. daily, weekly etc.)? For batch runs, how flexibly can you configure frequency?
- What mechanisms exist to ensure that the software does not adversely impact the performance of the core application and system?
- Is the software controlled at the NonStop host, from a Windows workstation or both? If from a Windows workstation only, are there any firewall issues within your organization that need to be addressed? Is communication between the Windows workstation and NonStop server appropriately secured?
- Is a full history kept of when the files have been checked for changes and the results?
- Does the software log every occurrence of a file being re-baselined after a change of the file has been detected?
- How much historic data (i.e. how far back in time) can be kept online/offline?
- What mechanism is used for retrieving historic collection data?
- Is there a suitable security framework in place that prevents unauthorized changes of configuration?
- How are changes to the configuration audited?
- How flexible and user-friendly are the configuration and reporting?

For Session Encryption Software

- Is the product an SSL/SSH proxy? If so, can the audit logs link the “real” IP Address to each user session?
- If your organization is requiring session IP address for auditing or control purposes, you should ensure the interoperability of the session encryption software with your other security related software, as SSL proxies typically return an IP address of 127.0.0.1 (the loopback IP address) when interrogated by other processes.

For Audit Logging/Reporting/Alerting (which may be a feature of any software product)

For software that includes audit logging (e.g. logging of sessions or activity within the utility):

- Do the audit logs contain all PCI required information (as per Requirement 10.3)?
    - User identification
    - Type of event
    - Date and time of event
    - Success or failure indication
    - Origination of the event (e.g. IP address. Note that NAT or use of SSL proxy may be an issue in the use of IP address to determine the origin of the event. See Session Encryption)
    - Identity or name of affected data, system component, or resource.
- What kind of event is generated when the software is shutdown or started?
- What kind of event is generated when the audit logs fill up or roll over?
- Can it be proven that the audit logs have not been tampered with (e.g. by use of audit record checksums such as MD5 or SHA2)?

- Can audit records be sent "off box" to a centralized audit logging solution (e.g. to a SIEM device such as RSA envision or HPE ArcSight)?
- Does the software allow configuration of alerting on selected events?
- How does the software function if audit records cannot be logged for some reason (e.g. if audit logging disk is full)? Does the software continue to function or does it stop all processing if audit cannot be captured? Is this configurable?
- Do audit logs automatically rollover when they are full?
- Do "old" audit logs get overwritten by new logs i.e. similar to Safeguard's "Recycle Files"? If so, what mechanism is in place to ensure that required files are not overwritten? Audit logs must be kept online for a minimum of 3 months to comply with PCI DSS.
- If "old" log files are not recycled or overwritten, is there an archive or cleanup mechanism to prevent disks from filling up with audit logs?
- Can reports be scheduled? If so, does the product have an inbuilt scheduler or does it use host based batch utilities such as NetBatch, Multibatch etc. or a workstation based utility such as Windows Scheduler?
- Are reports host based or PC based?
- Can reports be sent automatically to centralized locations e.g. network file server?
- How flexible/user-friendly/configurable are reporting and alerting? [probably more that could be added for these parts]

See Independent Software Vendor Products for a list of ISV software that may assist in helping achieve PCI DSS compliance.

If you need further assistance with evaluating security or compliance software for your organization, please email info@knightcraft.com with any questions.

USEFUL REFERENCES

- HPE NonStop Technical Library (www.hpe.com/info/nonstop-**j**docs, http://www.hpe.com/info/nonstop-**l**docs)
- HPE NonStop Security Hardening Guide [In the HPE NonStop Technical Library]
- HPE NonStop Server Security- A Practical Handbook, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)
  [Note that this text is now quite old and some recommended settings may no longer be valid]
- Securing HPE NonStop Servers in an Open Systems World, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)
  [Note that this text is now quite old and some recommended settings may no longer be valid]

For a full list of useful resources, please see the Resources section at the end of this document.

REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 1 of PCI DSS states:

> *Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.*
>
> *A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.*
>
> *All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.*
>
> *Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.*

REQUIREMENT DESCRIPTION

Much of Requirement 1 of PCI DSS deals with areas typically outside of the HPE NonStop server, predominantly in regards to firewalls and network security. Typically responsibility for the configuration and management of these aspects of the organization are dealt with by a network or infrastructure department. These departments should certainly ensure that appropriate firewall protection is configured. To verify appropriate firewall configuration, the following test could be performed:

Run a port scan from three type of workstations as follows:

1. From a workstation that should be able to access the HPE NonStop server.
2. From a workstation that should not be able to access the HPE NonStop server, but should be able to access other midrange or mainframe systems within the same server room.
3. From a workstation that should not be able to access any machine within the server room that houses the HPE NonStop server.

The results of the port scan should be consistent with the type of access that is required through the firewall.

When considering the requirements relating to workstations or laptops, the system console and any system monitoring consoles (for example a Prognosis console) must be taken into account, as well as user workstations and laptops used for accessing the HPE NonStop server.

All PCI DSS requirements for this section of this document are listed here for the sake of completeness. Requirements where there may be specific relevance to the HPE NonStop server environment have been annotated accordingly.

THE REQUIREMENT - 1

PCI DSS Requirement	Testing Procedure	Remark
1.1	1.1	
1.1.1	1.1.1.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	1.1.1.b	
	1.1.1.c	
1.1.2	1.1.2.a	
	1.1.2.b	
1.1.3	1.1.3	This requirement is not specific to the HPE NonStop server although there will be locations on the HPE NonStop server that must be documented as per this requirement. See Template for ROC for details on what a QSA will require for this requirement. See the section on Cardholder Data Elements for assistance in determining where on the system cardholder data may reside. A tool such as PANfinder may assist in determining where on the system any unprotected or unauthorized cardholder data is located.
1.1.4	1.1.4.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	1.1.4.b	
	1.1.4.c	
1.1.5	1.1.5.a	
	1.1.5.b	
1.1.6	1.1.6.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. Use of services, protocols and ports on the HPE NonStop server is dealt with in Requirement 2.2.2 .
	1.1.6.b	
	1.1.6.c	

PCI DSS Requirement	**Testing Procedure**	**Remark**
1.1.7	1.1.7.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	1.1.7.b	
1.2	1.2	
1.2.1	1.2.1.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	1.2.1.b	
	1.2.1.c	
1.2.2	1.2.2.a	
	1.2.2.b	
1.2.3	1.2.3 .a	
	1.2.3 .b	
1.3	1.3	
1.3.1	1.3.1	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
1.3.2	1.3.2	
1.3.3	1.3.3	
1.3.4	1.3.4	
1.3.5	1.3.5	
1.3.6	1.3.6	
1.3.7	1.3.7	
1.3.8	1.3.8.a	
	1.3.8.b	
1.4	1.4.a	This requirement is not specifically applicable to the HPE NonStop server itself. However, most access to an HPE NonStop server is via workstations or laptops which would be subject to this requirement. This requirement also includes the system console, operations monitoring consoles and so on, if they are connected to the internet.
	1.4.b	

PCI DSS Requirement	Testing Procedure	Remark
1.5	1.5	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

REQUIREMENT INTRODUCTION

The introduction for requirement 2 of PCI DSS states:

> *Malicious individuals (external and internal to a company) often use vendor-default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.*

REQUIREMENT DESCRIPTION

Requirement 2 deals with the need to ensure that unauthorized access to the system cannot be obtained by exploiting known vendor defaults. On an HPE NonStop server, this may be in terms of userids, passwords or default configurations of the various subsystems.

The requirement goes further to specify that it is necessary to “configure system security parameters to prevent misuse” (req. 2.2.4). This small sentence effectively means that you must have all subsystems (Safeguard, Pathway, Netbatch, Spooler etc.) secured correctly and in accordance with best practices to ensure that only authorized users have access to the system and its components. This will include ownership of the various entities as well as their security or access settings.

It is also a part of the requirement for all configuration items to be fully documented in a System Configuration Standards document that addresses “all known security vulnerabilities and are consistent with industry-accepted system hardening standards”. This is a large task and should be allocated appropriate resource and time.

CHANGE DEFAULT SETTINGS

When an HPE NonStop server is shipped, the userids NULL.NULL and SUPER.SUPER are provided as the owner of a logged off TACL process and as the owner of the operating system respectively.

In Guardian check that:

- NULL.NULL userid has been disabled (frozen) or deleted.
- SUPER.SUPER password has been changed from that set by the HPE engineer during the initial system build.

The default password settings that ship with an HPE NonStop server are very basic to non-existent. It is imperative that these are changed to a more robust configuration.

The following default passwords should also be changed and stored securely so that they can be retrieved when required and can be communicated to HPE engineers and support personnel for HPE maintenance activities:

- The system console administrator Windows user account (see below section on Default System Console Settings).
- CLIM root and user userids (using the CLIMCMD utility).
- iLO passwords for the Admin user account on each blade (OSM Service Connection).
- iLO passwords for the Admin user account for each CLIM (OSM Low Level Link).
- Onboard Administrator (OA) password for Administrator userid for each NonStop Blade and CLIM (OSM Service Connection).
- Internal InfiniBand switch Admin user.
- External InfiniBand switch Admin user.

In Safeguard check that:

- Password encryption has been set to HMAC256.
- Safeguard global password configuration items are appropriately set for minimum password length (minimum 7) and password history (minimum 4). Note that these are for PCI DSS compliance, but industry best practices would suggest that both of these values are significantly higher.
- Password complexity settings should be set.
- If there is no legacy reason specifically requiring it, PASSWORD-COMPATIBILITY-MODE should be set to OFF to allow passwords/passphrases of longer than 8 characters.
- PASSWORD-REQUIRED is set to ON to disable the ability of privileged Userids to log down to other Userids. If the organization security policy allows for logging down and this parameter is to be set to OFF, it should be noted as such in documentation. Permitting users to log down to other userids may make it more difficult to truly tie all actions on the system to a specific individual.
- Safeguard protection records have been added for all OBJECTTYPEs to ensure that only authorized users can add Safeguard records.
- All Safeguard globals have been appropriately set as per the organization's specific requirements. This includes the relevant audit settings. (SAFECOM INFO SAFEGUARD, DETAIL to check the current settings).
- If the organization plans on delegating the administration of Safeguard to one or more userids other than SUPER.SUPER, the appropriate userid(s) should be set up as part of the relevant security groups, such as the SECURITY-ADMINISTRATOR, SECURITY-OSS-ADMINISTRATOR and so on. See the section on Safeguard Security-Groups and the *Safeguard Administrators Guide* for further information.

DEFAULT SYSTEM CONSOLE SETTINGS

The system console typically ships with only one user configured and that user is configured with Administrator privileges. Potentially there is a generic or no password set. The system console is a powerful entry point to the HPE NonStop server and should be secured accordingly. If a user has administrator access to the console, they would have the required capability, for example, to install a keystroke logging program. It is quite likely that at some stage they would then be able to capture the SUPER.SUPER or other privileged userid logon credentials at that machine. This would give that person unauthorized privileged powers on the HPE NonStop server.

At a minimum, the following measures should be put in place:

- Individual non-administrator userids should be added for all users who have authorized access to the console.
- The default Administrator user account name should be changed and the password secured. Userids with administrator privileges should only be used under controlled situations as per PCI DSS requirements.
- The console should be viewed as a potentially vulnerable access point to the HPE NonStop server. Ensure that all PCI DSS requirements that may relate to Microsoft Windows machines are strictly adhered to.

For HPE's recommendations on how the system console should be secured, see the *HPE NonStop System Console Security Policy*[5] and *HPE NonStop Security – NSC Security Program* documents on HPE's website.

Change the password for the root userid for the Low-Level-Link application on the system console workstation also.

SYSTEM CONFIGURATION STANDARDS

It is necessary for the organization to have a System Configuration Standards document that contains at least the following:

- A list of all subvolumes and OSS directories present on the system required to "rebuild" the system and applications that process cardholder data.
- Description of all Guardian security, OSS file security, Safeguard or other security software configuration.
- Description of how to rebuild application(s) and recover/migrate application data.
- Description of all other required system build components.
- Details of what programs should be installed
- Details of what processes should be running
- Details of security audit events that are captured.

References that may help in the production of this documentation include the following:

[5] HPE NonStop System Console Security Policy (http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4aa2-0980enw&404m=secure-erc)

- *HPE NonStop Security Hardening Guide* (NonStop Technical Library)
- *Security Management Guide* (NonStop Technical Library).
- *HPE NonStop Server Security- A Practical Handbook*, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)
- *Securing HPE NonStop Servers in an Open Systems World*, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)

Note that the two XYPRO Technology books listed above were published some time ago (2004 and 2006 respectively), so some of the books' recommendations may no longer be valid and more recent subsystems and features may not be included. Nevertheless, there will still be sections of these books that may assist in helping with configuring security for HPE NonStop systems.

Independent Software Vendor Products are available that could be used to assist with creating the appropriate documentation. These products typically compare security related configuration on the system with a built-in set of recommended settings and allow for these settings to be tailored to an organization's individual needs. Note however that there will typically be some amount of set up time and expertise with the product to include all required aspects of the system. [Consider XYGATE Compliance PRO (XSW), CSP CRM]

Knightcraft Technology provides a PCI documentation service that can assist organizations prepare the required PCI DSS documents. Alternately Knightcraft has a System Configuration Standard document template which can provide the basis for this all-encompassing document, ensuring that you have taken all necessary requirements into account, and providing a framework to allow you to produce the document in a much quicker timeframe.

SINGLE FUNCTION SERVER

Requirement 2 specifies that each server (i.e. system) must perform only one function. This is often not the case on an HPE NonStop server. Systems are often used to run multiple applications, often with different functions with different security needs. In essence, for an HPE NonStop server, if multiple applications are running on the same system with different security needs, there must be a logical separation of application environments as follows:

- Different subvolumes and OSS directories for different applications.
- Each application environment should be owned by a unique userid.
- Application processes should run under an application specific userid.
- Application subvolumes should not exist on $SYSTEM or other system type volumes such as TMF or DSMSCM volumes.
- Safeguard protection of the different environments configured with ACLs that do not allow access from one environment to the other.
- Non-card payment processing applications running on the system should be secured to the same standard as those applications that are processing card payments and which are subject to PCI DSS.
- No cross access from one functional application to another.

- No write or create access to application data or objects from personal userids.

SERVICES AND PROTOCOLS

All required services and protocols must be documented as to what they do and why they are needed. Only required services/protocols should be allowed. For example, if ftp is not required for a particular TCP/IP stack, it should be disabled in the relevant portconf file (inetd configuration file in OSS). If a protocol such as ftp is required, it needs to be used in a secure manner (i.e. encrypted session) if sensitive data is transmitted over the link, or if a userid with access to cardholder data is used for transmission. Passwords for logon to TACL or OSS via telnet or ftp logons are inherently insecure. The passwords for these services are transmitted in the clear. If these services need to be used, some form of Session Encryption should be implemented to ensure that user credentials are appropriately protected.

If different services are required in different TCP/IP stacks, the relevant listener processes should be started using different portconf files. Likewise, application or non-standard listener processes must only have documented authorized services/protocols enabled. The output from the SCF LISTOPENS displays listening sockets for the relevant TCP/IP process.

Independent Software Vendor Products exist that can assist by providing details of which TCP/IP ports are open and which processes are running on the system. These can be analyzed and baselined. If any changes occur to the baseline from one data collection to the next, alerts can be raised. This provides a framework for continually tracking authorized processes across the HPE NonStop servers and minimizes the amount of time and effort required to reliably monitor these components. [Consider XYGATE Compliance PRO (XSW), CSP CRM]

SYSTEM SECURITY PARAMETERS

A part of requirement 2 is to configure system security parameters. This requirement effectively refers to the configuration of all security related settings across the system and would include the following:

- Safeguard globals
- Safeguard ACL protection for all critical files such as:
  - system files
  - files in global pmsearchlists
  - tacllocl
  - privileged userid/alias cstm files (taclcstm, scfcstm, fupcstm, ftpcstm etc.)
  - application files (object code, data, configuration, log files etc.)
- Safeguard ACL protection for critical processes
- User/alias configuration
- Privileged users/aliases configured on the system

- Other HPE optional or third party security software configuration
- Owners of files and Safeguard records
- Pathway/Application configuration and related files
- Batch configuration including privileged userid batch job infiles and attachment sets and NetBatch program files
- Spooler
- Licensed and Progid'ed files
- OSS security for relevant files/folders (application objects, profile files, inetd.conf etc.)
- SQL/MX access details
- Log files (application, system, security)

To assist in choosing which values should be selected for various system settings, it is recommended that the *HPE NonStop Security Hardening Guide*[6] is consulted. The Best Practice recommendations in the *HPE NonStop Server Security*[7] and *Securing HPE NonStop Servers in an Open Systems World*[8] may also provide useful recommendations in determining which configuration values to use, though as stated above, these books were published some time ago so should be treated as a checklist of items to be considered rather than necessarily accepting the recommended settings. This will help ensure that configuration items are not overlooked and that a conscious decision has been made for values rather than just accepting default values. It should be noted that more recently added Safeguard configuration parameters and some other subsystems (e.g. system DLLs) have been added subsequent to these books being published.

Non-required features, processes, devices, printers, programs etc. should be disabled. For example:

- OSS subsystem if not running OSS
- iTP webserver if not required
- Compilers should be removed from production environments.
- Non-required programs such as adduser, deluser, OSS equivalents, rpasswrd, diver, tandump, inspect, einspect programs should be removed or disabled, unless there is a specific documented and justifiable reason why these programs should exist on a production or DR system.
- Old $system.sys*nn* subvolumes should be either purged or secured via Safeguard so that users cannot run old versions of operating system programs.

For more information on recommended security configuration, see Requirement 7: Restrict access to cardholder data by business need to know.

[6] HPE NonStop Security Hardening Guide is available in the HPE NonStop Manual Library.

[7] HP NonStop Server Security- A Practical Handbook, by XYPRO Technology Corporation (ISBN: 1-55558-314-8)

[8] Securing HP NonStop Servers in an Open Systems World, by XYPRO Technology Corporation (ISBN: 1-55558-344-X)

SESSION ENCRYPTION

Userid and password information is transmitted in the clear (unencrypted) by default for a number of subsystems, such as TACL and OSS via Telnet, and FTP. To satisfy requirement 2.3, session encryption must be used. All access by a privileged userid/alias - for example, access by super user group, security administrator, other security software owner userid or application owner - must be via an encrypted session.

Session types requiring encryption include telnet (TACL, osh), ftp, ixf, rsc sessions or any other type of session for a privileged userid/alias.

HPE Integrity NonStop Systems running H-series or J-series software now ship with SSL and SSH session encryption software from comForte included as standard. SFTP (SSH FTP) or FTPS (FTP over TLS) should be used for transferring files rather than FTP, IXF, PCFILE or any other non-encrypted file transfer method.

Other Independent Software Vendor Products are also available that provide session encryption.

When choosing session encryption products and configuration, it is imperative to ensure that only cipher suites satisfying PCI DSS are enabled for user sessions. These must come under the category of “Strong Cryptography” as defined by PCI DSS.

Note that if using SSL or early version TLS for any session encryption, plans should be made to upgrade to a secure version. Both SSL 3.0 and TLS 1.0 are susceptible to the POODLE exploit and are now considered insecure. At the time of publishing, TLS 1.2 is the latest version with TLS 1.3 in draft. A new PCI DSS requirement has been added regarding the use of SSL and early version TLS. See Requirement A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for details.

Whichever session encryption products are used, vendor documentation should be consulted to ensure that best practice settings are used to ensure strong encryption. If unsure about the configuration options to use or this information is not documented, consult your vendor for their recommendations. A QSA will typically want to see this information as part of requirement 2.3, so any information requested from a vendor should be sought in writing.

For organizations where IP address controls and tracking are required, it should be verified that whichever solution is used, the “real” session IP address is returned rather than the loopback IP address of the proxy i.e. 127.0.0.1.

If the standard HPE SSH product is used for session encryption, the SSH audit logs contain details of every session including the authenticating userid/alias and a record of the real connecting IP address.

Note that the use of Network Address Translation (NAT) within the organization network may reduce the effectiveness of IP address in determining the real origination of a security event.

Independent Software Vendor Products are available that provide a link between the user session and the corresponding Windows User name and Windows host name.
[Consider comForte SecurTN with comForte terminal emulation]

Consideration should be given to all types of sessions, such as FTP, HTTP, TELNET, RSC, ODBC/JDBC etc. If services such as FTP are enabled at the console, physical access to the console should be strictly controlled.

Any use of insecure network protocols such as Telnet or FTP will require completion of a Compensating Control Worksheet, fully documenting the purpose for the protocol being enabled and what is in place to mitigate the risk of it being enabled (e.g. Telnet connections only enabled via SSH or TLS).

THE REQUIREMENT - 2

PCI DSS Requirement	Testing Procedure	Remark
2.1	2.1.a	For this requirement, a QSA will typically: • Ask to witness a session by a user logging on to SUPER.SUPER without entering a password, or perform some similar test to demonstrate that a password has been set. The logon attempt should fail if no password has been entered. • Ask for verification that NULL.NULL userid is disabled (frozen) or deleted. • Ask for verification that CLIM, Blade, NSC and switch default passwords have been changed. • Ask for verification that the SNMP community name has been changed or disabled (if not required). For information on defaults that should be changed, see Change Default Settings and Default System Console Settings.
	2.1.b	
	2.1.c	
2.1.1	2.1.1	This is not applicable to the HPE NonStop server.
	2.1.1.a	
	2.1.1.b	
	2.1.1.c	
	2.1.1.d	
	2.1.1.e	
2.2	2.2.a	For this requirement, a QSA will typically: • Need to verify that a System Configuration Standards document exists and that there is content in the document. • Identify which system security hardening standard has been used as a basis for the document. The HPE NonStop Security Hardening Guide[9] could be used for this purpose. For details of contents to include in this document, see System Configuration Standards.

[9] See the Resources section of this document for details.

PCI DSS Requirement	Testing Procedure	Remark
	2.2.b	For this requirement, a QSA will typically: • Identify that an auditable process exists for assessing security vulnerabilities and that appropriate action has been taken. There should be documented evidence of the process such as a log of security vulnerabilities and the action taken in terms of updating system configuration and also the Security Hardening Standard. • The relevant person responsible for implementing this will be interviewed by the QSA. • This role should be documented.
	2.2.c	For this requirement, a QSA will typically: • Identify a document or documents that contain all of the required configuration settings and instructions for configuring a new system • For a new system, want to see that the system was built as per the System Configuration Standard document. Examples of such evidence could be: - A signed off document indicating that the build has been completed as specified. - Safeguard or other subsystem audit records or logs that show when and how system configuration settings have been applied. The dates found in the logs should correspond with when the system was delivered, built and went "live".
	2.2.d	For this requirement, a QSA will typically: • Review the documentation to ensure that the required content is included. See the subsections of Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters for extra information.
2.2.1	2.2.1.a	For this requirement, a QSA will typically ask for the following evidence from the sample node(s): • A list of all running processes to be able to define exactly what application functions are running on the system. If, for example, a web service is running (e.g. iTP Web Server), a QSA may ask for justification as to why this is the case if the primary function of the system is not specifically as a web server. • A list of all application-related subvolumes and OSS directories • Safeguard configuration that applies to all application objects • Security vectors or ACLs for OSS related objects • Details of relevant userids with access to each application environment As it is a requirement that only one primary function is implemented per server, if this is not the case and even if the application environments are suitably segregated, the QSA may ask the organization to apply for a compensating control. See the section on Compensating Controls for information on what may be required. See Single Function Server for more information on this requirement.
	2.2.1.b	This is not applicable to an HPE NonStop server environment.

PCI DSS Requirement	Testing Procedure	Remark
2.2.2	2.2.2.a	For this requirement, a QSA will typically: • Examine all open ports for all TCP/IP processes using SCF (state of LISTEN or ESTAB) • Examine PORTCONF and SERVICES files in the Guardian environment and the inetd.conf file in the OSS environment. In earlier versions of NonStop OS, the default PORTCONF file included entries for FTP, FINGER, ECHO. While this has not been the case for some time, if configuration files within the organization have been migrated “as is” during system upgrades, it is possible that these entries may remain. Typically echo and finger are not required and should be removed or commented out. FTP should only be enabled on IP stacks where there is an authorized need (noting that FTP in itself is an insecure protocol). Different portconf files should be used for different listener processes if required so as to achieve this. These files should be strongly secured and audited for any changes where possible. • Examine the complete list of all processes running on the system to verify that only required processes are running on the system. All required processes should be documented, i.e. the process name (where applicable), the function of the process, the userid that the process should be running as, and the program file that is being run and the number of instances of the process being run (where known) should be specified • All open ports should be documented indicating the program, process and the reason why they are in use. See Services and Protocols for more information on this requirement.
	2.2.2.b	For this requirement, a QSA will typically: • Examine all open ports for all TCP/IP processes using SCF (state of LISTEN or ESTAB) • Examine PORTCONF and SERVICES files in the Guardian environment and the inetd.conf file in the OSS environment. In earlier versions of NonStop OS, the default PORTCONF file included entries for FTP, FINGER, ECHO. While this has not been the case for some time, if configuration files within the organization have been migrated “as is” during system upgrades, it is possible that these entries may remain. Typically echo and finger are not required and should be removed or commented out. FTP should only be enabled on IP stacks where there is an authorized need. Different portconf files should be used for different listener processes if required so as to achieve this. These files should be strongly secured and audited for any changes where possible. • Any insecure services or protocols running (e.g. Telnet, FTP) must be documented and justified as to why they are necessary. • All appropriate security features must be applied to insecure services to mitigate any risk associated with the protocol. These measures must all be documented. For example, if FTP is enabled, the reason for its use must be documented, and security features such as restricting access so that no critical and sensitive information can be accessed with this service, must be in place. See Access Control System for more information on ways to restrict user access. See Services and Protocols for more information on this requirement.

PCI DSS Requirement	Testing Procedure	Remark
2.2.3	2.2.3.a	For this requirement, a QSA will typically: • Examine all open ports for all TCP/IP processes using SCF (state of LISTEN or ESTAB) and identify which of these are insecure protocols (e.g. Telnet, FTP). • Examine PORTCONF and SERVICES files in the Guardian environment and the inetd.conf file in the OSS environment. In earlier versions of NonStop OS, the default PORTCONF file included entries for FTP, FINGER, ECHO. While this has not been the case for some time, if configuration files within the organization have been migrated “as is” during system upgrades, it is possible that these entries may remain. Typically echo and finger are not required and should be removed or commented out. FTP should only be enabled on IP stacks where there is an authorized need. Different portconf files should be used for different listener processes if required so as to achieve this. These files should be strongly secured and audited for any changes where possible. • Any insecure services or protocols running must be documented and justified as to why they are necessary. • All appropriate security features must be applied to insecure services to mitigate any risk associated with the protocol. These measures must all be documented. For example, if FTP is enabled, the reason for its use must be documented, and security features such as restricting access so that no critical and sensitive information can be accessed with this service, must be in place. See Access Control System for more information on ways to restrict user access. See Services and Protocols for more information on this requirement.
	2.2.3.b	For this requirement, a QSA will perform the testing procedures as per Appendix A2. This relates to any session encryption mechanism using SSL or early versions of TLS as these are no longer considered secure. On the HPE NonStop server, this may apply to NonStop SSL configuration (secure telnet, secure FTP) and any corresponding terminal emulation software, iTP webserver, application related sessions and so on.
2.2.4	2.2.4.a	For this requirement, a QSA will typically: • Interview the System Manager of the relevant NonStop server to determine if they understand the security setup of the system. This will include Safeguard, Guardian and OSS security configuration where applicable.

PCI DSS Requirement	Testing Procedure	Remark
	2.2.4.b	For this requirement, a QSA will typically view that all common security parameters are included in the organization's documentation. This will include items such as: • Safeguard globals • Safeguard objecttype protection records • Safeguard security groups • Security of system subvolumes and old system subvolumes ($SYSTEM.SYSTEM, $SYSTEM.SYSnn) • OSS environment security settings where applicable. If OSS is not running on the system, this should be stated. • The security relevant commands and utilities in Guardian, Safeguard, and OSS, which user accounts have the privileges to execute them, what the commands do, and so on. Where possible (for example, for "what the commands do") it is acceptable to reference out to relevant HPE documents such as the Safeguard Reference Manual (HPE NonStop Technical Library). Likewise for any other security related software such as SECOM, CSP Passport, XAC, XUA etc. • Cipher suites that are used for session encryption • Refer to Requirement 7.2.3 for more info on items to be included in this documentation. • It is not possible to have too much documentation associated with this requirement. If in doubt, document it.
	2.2.4.c	For this requirement, a QSA will typically: • Analyze all of the relevant configuration settings on the system • Verify that the configuration matches the settings that are documented as per section 2.2.4.b • Ensure that all configured and documented settings are justified and follow industry best practices. As a part of this, a QSA will typically require a list of all subvolumes, OSS directories, processes and devices on the system(s). For key subvolumes/directories the list will need to include details of all files. The subvolumes/directories listed should include at least the following: • System subvolumes ($system.system, $system.sysnn, relevant $system.z* type subvolumes) • Startup/Shutdown subvolumes for the system and subsystems (tmf, spooler, tcpip, database replication and so on). • Application subvolumes (Pathway, startup/shutdown, configuration, logs, programs, libraries, and so on) • Database Subvolumes • Subvolumes on #PMSEARCHLIST • Batch related subvolumes e.g. subvols containing batch infiles See System Security Parameters for suggestions on which parameters to include.
2.2.5	2.2.5.a 2.2.5.b 2.2.5.c	For this requirement, a QSA will typically: • Check that all existing subsystems and features are documented. • Check that all configuration of enabled subsystems and features are documented as per section 2.2.4.b • Check that settings of all enabled subsystems and features match the documentation as per 2.2.4.c • Check that all subsystems such as OSS or iTP Webserver are disabled if they are not in use on the system and that this is documented.
2.3	2.3	

PCI DSS Requirement	Testing Procedure	Remark
	2.3.a	For this requirement, a QSA will typically want to see: • Evidence of session encryption by witnessing a user logon sequence. • A network trace of a user session using a tool such as Wireshark. • Evidence of what cipher suites are being used for the encryption. This will be in the configuration of the session encryption product. The available cipher suites must be documented as per 2.2.a and 2.2.4.b. See Session Encryption for more information.
	2.3.b	On a NonStop system, telnet is required for system command level access e.g. TACL or OSS. To satisfy this requirement, a QSA will typically want to see, that for example: • That the protocol is only used over a secure channel such as TLS v1.2. Strong cipher suites must be used. • Direct access to the telnet service is protected from external or unauthorized networks by use of a firewall See Session Encryption for more information. All of the controls put in place for telnet access must be documented in a Compensating Controls Worksheet and approved by the relevant acquirer. See the section on Template for ROC for further information.
	2.3.c	This requirement will include all connections into the NonStop system via web based tools such as the OSM, Web Viewpt etc. for administrative access. All access via such tools must be over an encrypted channel. For this requirement, a QSA will typically want to see: • Evidence of what cipher suites are being used for the encryption. This will be in the configuration of the session encryption product. The available cipher suites must be documented as per 2.2.a and 2.2.4.b. See Session Encryption for more information.
	2.3.d	For this requirement, a QSA will typically want to see: • Vendor documentation that describes the best practices method of configuring for strong session encryption. See Session Encryption for more information.
	2.3.e	For this requirement, a QSA will perform the testing procedures as per Appendix A2 if SSL and early version of TLS is used to protect non-console login sessions.
2.4	2.4.a	This requirement will include keeping an up to date inventory of the following components:

PCI DSS Requirement	Testing Procedure	Remark
	2.4.b	• All hardware (cpus, disks, CLIMs, SWANs, comms adapters, console, virtual tape etc.) • Operating System software (e.g. TMF, Safeguard, Spooler, TS/MP, TCP/IP, Measure, NTP, OSS, SSL, SSH, XMA etc.) • Console based software (Windows OS version, antimalware software etc.) • Optional HPE products (e.g. SQL/MX, SQL/MP etc.) • Data replication software (RDF, Goldengate, HPE Shadowbase, DRNet etc.) • Third party software applications (Prognosis, SecurData, XYGATE etc.) • Business application software (BASE24, CONNEX etc.) • Custom "home grown" software See Template for ROC for specific details on what a QSA will need for this requirement.
2.5	2.5	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.
2.6	2.6	If the HPE NonStop server is being used in a host sharing environment for multiple clients, the system must be compliant with all requirements in Requirement A1: of the PCI DSS.

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 3 of PCI DSS states:

> *Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.*

REQUIREMENT DESCRIPTION

This requirement relates to ensuring that cardholder data is not stored in a readable form. How to best approach this requirement is often dependent on the nature of the card application and how it processes, stores or transmits data. If the organization is using a software product such as BASE24 or CONNEX, it is recommended that the software vendor is contacted to determine if you are running the latest version of the software. It is possible that some of the issues regarding storage or protection of data may be addressed in a more recent version of the product.

For some software products (including BASE24) as well as customized or in-house applications, it may be necessary to take some steps to make stored cardholder data unreadable. If an application is PA-DSS validated, this does not necessarily mean that the cardholder data is protected as required by PCI DSS. There may need to be action taken by the organization running the software to ensure that this is so. For any PA-DSS validated applications, the software vendor should have a PA-DSS Implementation Guide for the software that describes what measures should be put in place to ensure that the implementation is PCI DSS compliant. Ultimately the responsibility lies with the organization running the application to ensure that cardholder data is protected in accordance with PCI DSS, so it is recommended that any measures to be implemented be discussed first of all with the organization’s QSA.

See the *PCI Data Storage Do’s and Don’ts* document for more information on PCI data storage (https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf). Note that this document was released as accompaniment to PCI DSS v2.0 but still maintains relevance and may be useful.

PROTECTION OF CARDHOLDER DATA

Some of the card processing applications used in the financial industry do not include protection of cardholder data. It is recommended that you consult with your application vendor to determine the current status of this, as circumstances in the software industry constantly change as does software functionality from one version to the next. Even if these applications are updated to protect cardholder data in accordance with PCI DSS, most organizations have a unique processing environment and have typically customized the application to suit their individual business needs. This may mean that even if an "off the shelf" application has been enhanced to provide protection for cardholder data by the vendor, the "home grown" parts of the application may still contain unprotected data. Or old unprotected data may still reside on the system in locations outside of the application. The onus is on the organization to determine all places where cardholder data is stored, processed or transmitted and ensure that protection is provided in accordance with this requirement.

Independent Software Vendor Products exist that can assist with finding all locations where cardholder data resides on the system. [Consider PANfinder]

A number of Independent Software Vendor Products can help organizations protect cardholder data, using a number of different methods.

comForte SecurData (called CF Data Security if purchased from HPE), XYGATE Data Protection (XDP) and SecureData (Voltage) provide the ability to tokenize application data without requiring any modification to the data files and without needing to recode the application.

A number of ISVs provide encryption library solutions that can be used to encryption-enable or tokenize applications such as BASE24 or in-house developed applications, databases and communications. Code modification is typically required to the card processing application to call the relevant software functions for loading encryption keys, performing encryption/ decryption operations and so on. The underlying application database structure may also need to change to accommodate information about encryption keys. [Consider comForte SecurLib, Greenhouse INSET, ACI Enterprise Security Services: Application Firewall, TANDsoft Sensitive Data Intercept (SDI)]

If encryption or tokenization is used, it is necessary to ensure that the encryption algorithms used in the application are those that satisfy the PCI DSS requirements for Strong Cryptography.

Whichever method is chosen, full and thorough testing of the application after tokenization/encryption should be undertaken so as to ensure that all data is fully readable by all required aspects of the application and all application functionality is maintained.

COMPENSATING CONTROLS AND REQUIREMENT 3.4

In the past, many organizations were using compensating controls to satisfy requirement 3.4. This was largely due to the lack of available solutions to protect the data without significant changes being required to the application and underlying database. This is no longer the case, so HPE NonStop organizations should now be looking to fully satisfy the requirement by implementing a tokenization or similar solution. [Consider comForte SecurData (called CF Data Security if purchased from HPE), TANDsoft Sensitive Data Intercept (SDI), XYGATE Data Protection (XDP) and HPE SecureData (Voltage)].

While various different compensating controls for requirement 3.4 may have been accepted by QSAs to this point, a number that the authors have seen don't appear to adequately protect cardholder data. There are a significant number of ways that a user could assume privileged userid capabilities on an HPE NonStop server if security settings are not exactly as they should be or procedures are not fully followed. While it is desirable of course for these settings and procedures to be perfect, many organizations, despite best efforts, fall short in this regard. Given the inability of session capture software to capture TACL macro activity as part of a user session, it is possible for a user to mask their actions (see Session Capture for more details). If a user is somehow able to find their way to stored cardholder data, at least if it is protected by tokenization or encryption, it will be of no use to the unauthorized user and will prevent any kind of data breach. See the section on The difference between compliant and secure systems for more discussion on this point.

It should be further noted that a QSA views a compensating control as a temporary measure. What may be acceptable for an assessment one year may not be acceptable the following year. The QSA may expect the organization to be moving forward to full compliance in the longer term. This will depend on the reason for and nature of the compensating control and the relevant QSA who is performing the PCI DSS assessment. Whether any measure of protection other than making the PAN unreadable is acceptable to a QSA will likely also depend on the nature of the application. For example, if it is possible from within the application to dump out a list of credit card details en masse, it is likely to be unacceptable for the PAN to remain readable. Ultimately, it is the relevant acquirer/card scheme that needs to be satisfied that the compensating control is a suitable measure for protecting cardholder information.

LOCATING CARDHOLDER DATA

As well as asking you to prove that known locations containing cardholder data have appropriate protection as per PCI DSS, a QSA will expect you to demonstrate how you ascertained that cardholder data does not exist in any other location on the system. This includes not only known locations within the application, but also areas outside of the application such as test and development environments. See the section on Cardholder Data Elements for a list of possible locations where cardholder data may exist.

Independent Software Vendor Products exist that can search your systems and help identify files suspected to contain unprotected or unauthorized PAN or Sensitive Authentication Data. [Consider PANfinder]

PROTECTING BACKUP DATA

If PAN data is not rendered unreadable in the database, consideration needs to be given to system/application backups to physical or virtual tape and also to TMF dumps. Storage of cardholder data in any of these forms needs to be protected.

Independent Software Vendor Products exist that can encrypt backup operations and TMF dumps. A number of hardware based virtual tape systems also contain encryption functionality for traditional tape based operations. [Consider comForte SecurTape, Greenhouse

BaReLib or a hardware based solution such as HPE NonStop BackBox Virtual Tape Controller (VTC) or HPE Virtual Tape Server (VTS) that includes encryption capabilities. Note that Strong Cryptography must be used]

DISK ENCRYPTION

For full-volume disk encryption to be an acceptable method used to satisfy PCI DSS protection of cardholder data there needs to be a method of authentication used, other than that used by the operating system. That is, when a user/program requires access to the encrypted volume, they should be authenticated by a mechanism other than the Guardian USERID file before gaining access.

In cases where disk encryption is used, the method of encryption and access must be fully documented including details of the cipher suites used and the authentication mechanism.

HPE NonStop volume level encryption (NSVLE), which is available from HPE for all NonStop machines that support storage CLIMs, will not satisfy this requirement, as authentication is performed at the operating system level. Once the encrypted volume is mounted its data is "in the clear" on the NonStop server and potentially accessible to users who have authenticated to the system. Protection of the data then relies solely on Guardian and Safeguard access rules, just like for any other non-NSVLE protected files on the system. While not satisfying this particular PCI DSS requirement, volume level encryption is still beneficial as it ensures that no data can be read from the disk once it has been physically removed from the system. HPE NonStop volume level encryption also supports certain types of NonStop tape devices and so may be suitable for ensuring that backups and TMF dumps are encrypted on tape.

WARNING! The *BASE24-eps PA-DSS Implementation Guide* (version 11.1, November 2011) indicates that "To be PA-DSS compliant, users must implement a disk level encryption solution or software to provide file level encryption". As stated above, there is no available disk level encryption solution on the HPE NonStop platform that satisfies requirement 3.4.

ENCRYPTION KEY CUSTODIANS

A part of this requirement is in regards to encryption key custodians. A good deal of consideration and planning is needed for this requirement. The fewest number of key custodians that satisfies the requirement for split knowledge must be used. Conversely the organization must make sure that there are sufficient custodians, so that the minimum number is always available to perform key management operations if required. If for some reason the required number of key custodians cannot be obtained, potentially the database can no longer be decrypted and the data may be effectively lost. To ensure that this doesn't occur, a sufficient number of key custodians must be chosen to cater for possible absentees due to termination of employment, holidays, illness and so on. A better option may be for the organization to set up a procedure to guarantee that the passphrases or other credentials of the custodians are always obtainable under controlled circumstances. This could be achieved, for example, by setting up two separate departments as the custodians, using split knowledge so that no individual knows any bit of the entire key, and storing the key components for each custodian department in separate safes, each requiring two people from the relevant department to gain access. Any such procedure needs to be well documented and would need to be approved by the assessing QSA as being satisfactory.

ENCRYPTION KEYS

A part of this requirement surrounds the generation, storage and management of encryption keys. It is necessary to ensure that encryption keys cannot be obtained in an unauthorized manner and used to decrypt cardholder data. To this end, any vendor who's encryption suite the organization is intending on using should be interrogated strongly to determine all aspects of encryption key storage and use to determine if it is possible under any circumstance to gain access to encryption keys.

Encryption key generation must meet the definition of strong cryptography as defined in the PCI DSS Glossary https://www.pcisecuritystandards.org/security_standards/glossary.shtml.

The components required for strong cryptographic storage are also well described on the OWASP web site (http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet).

THE REQUIREMENT - 3

PCI DSS Requirement	Testing Procedure	Remark
3.1	3.1.a	This requirement is not specific just to the HPE NonStop server and should be handled as part of the corporate data retention policy and procedure.
	3.1.b	
	3.1.c	
3.2	3.2.a	This requirement only applies to issuers and/or companies that provide issuing services. For this requirement, a QSA would typically: • Review the justification for storing Sensitive Authentication Data (SAD) • Interview the person responsible for providing the justification of storing SAD • Review the documentation that describes which SADs are stored and how they are protected.
	3.2.b	This requirement and sub-requirements are relevant to the card processing application running on the HPE NonStop server such as BASE24, CONNEX, in-house developed application and so on. For this requirement, a QSA would typically: • Validate that the storage location for SAD meets requirements 2, and 5 through 11. • Validate that the SADs are stored (by issuers and/or companies that provide issuing services) using strong cryptography as per 3.4, 3.5, 3.6, 3.7.
	3.2.c	This requirement and sub-requirements are relevant to the card processing application running on the HPE NonStop server such as BASE24, CONNEX, in-house developed application and so on where the organization has no business requirement to store Sensitive Authentication Data (SAD). For this requirement, a QSA would typically: Review the document that lists how Sensitive Authentication Data (SAD) are stored pre-authorization and how they are securely deleted.
	3.2.d	This requirement and sub-requirements are relevant to the card processing application running on the HPE NonStop server such as BASE24, CONNEX, in-house developed application and so on where the organization has no business requirement to store Sensitive Authentication Data (SAD). For this requirement, a QSA would typically: • Review the evidence that shows how Sensitive Authentication Data (SAD) has been securely deleted post-authorization.

PCI DSS Requirement	Testing Procedure	Remark
3.2.1	3.2.1	This applies to card present transactions only and is typically relevant to the card processing application running on the HPE NonStop server rather than the HPE NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on. For this requirement, a QSA would typically: • Review the content of a sample of the types of files and database tables referenced in the requirement procedure to ensure that sensitive authentication data is not stored. See Locating Cardholder Data for further information on locating where PAN is stored on the system.
3.2.2	3.2.2	This applies to card not present transactions only and is typically relevant to the card processing application running on the HPE NonStop server rather than the HPE NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on. For this requirement, a QSA would typically: • Review the content of a sample of the types of files and database tables referenced in the requirement procedure to ensure that sensitive authentication data is not stored. See Locating Cardholder Data for further information on locating where PAN is stored on the system.
3.2.3	3.2.3	This applies to card present transactions only and is typically relevant to the card processing application running on the HPE NonStop server rather than the HPE NonStop server itself, for example BASE24, CONNEX, in-house developed card processing application and so on. For this requirement, a QSA would typically: • Review the content of a sample of the above types of files and database tables to ensure that sensitive authentication data is not stored. See Locating Cardholder Data for further information on locating where PAN is stored on the system.
3.3	3.3.a	This requirement does not apply specifically to the HPE NonStop server but is relevant to users who need to view PAN information as a part of their documented job role. See Template for ROC for details on what a QSA will require for this requirement.
	3.3.b	
	3.3.c	

PCI DSS Requirement	Testing Procedure	Remark
3.4	3.4.a	For this requirement, a QSA would typically: • Review documentation describing the method of PAN protection used. • Verify that the type of encryption method and the key length are satisfactory, if encryption is used. • Check system settings/application source code/scripts/processes to see if PAN protection has been implemented as per documentation. PANfinder can be used to assist in locating where cardholder data is stored on the system and whether it is adequately protected. See Locating Cardholder Data for further information on locating where PAN is stored on the system. See Protection of Cardholder Data for further information on protecting cardholder data in accordance with this requirement.
	3.4.b	This requirement refers to files or tables where the PAN is stored. For this requirement to be satisfied, the PAN must be stored in these locations in an unreadable form. For this requirement, a QSA will typically: • Examine the contents of a sample of tables or files storing the PAN to confirm that the PAN is not readable. A number of organizations in the past have used compensating controls to deal with requirement 3.4. While the compensating control may be accepted by a QSA, it does not necessarily mean that your cardholder data is truly secure. See the section on Compensating Controls and Requirement 3.4 for further discussion on this. If access control software is used as a compensating control for Requirement 3.4.a, a QSA would likely need a demonstration of attempts to access the PAN using programs such as FUP or SQLCI when logged on as the application owner userid or "owner" of the data or SUPER.SUPER. Such attempts to access the data by means other than through the application itself should fail with a security error (error 48). To truly protect cardholder data using this mechanism, an organization must have very strong general system security in place, highly controlled and audited procedures for use of privileged Userids and strong auditing and alerting in place. It is recommended that if an organization is planning on using compensating controls to satisfy requirement 3.4 that they engage in an independent review of their system security to ensure that there are no gaps in configuration or procedures that may make cardholder data vulnerable to unauthorized access. Contact Knightcraft Technology or see the Knightcraft website to find out how we can assist in this regard. See Protection of Cardholder Data for further information on protecting cardholder data in accordance with this requirement. See Locating Cardholder Data for further information on locating where PAN is stored on the system.

PCI DSS Requirement	Testing Procedure	Remark
	3.4.c	For this requirement, a QSA will typically: • Sample a number of removable media to ensure that the PAN is stored unreadable using one of the methods listed above. See Protecting Backup Data for further information.
	3.4.d	For this requirement, a QSA will typically: • Review the content of a sample of audit logs holding the PAN to confirm that PAN is not readable. See Protection of Cardholder Data for further information on protecting cardholder data in accordance with this requirement. See Locating Cardholder Data for further information on locating where PAN is stored on the system.
3.4.1	3.4.1.a	For this requirement, a QSA will typically: • Review the relevant system settings to ensure that appropriate logical access to the disk has been implemented • Verify that the method used and associated authentication has been fully documented. Note that HPE NonStop Volume Level Encryption (NSVLE) does not satisfy this requirement. See Disk Encryption for details. Independent Software Vendor Products exist that can encrypt backup operations and TMF dumps. A number of hardware based virtual tape systems also contain encryption functionality for traditional tape based operations [Consider comForte SecurTape, Greenhouse BaReLib or a hardware based solution such as HPE NonStop BackBox Virtual Tape Controller (VTC) or HPE Virtual Tape Server (VTS) that includes encryption capabilities. Note that Strong Cryptography must be used]
	3.4.1.b	This requirement is only relevant if disk encryption is the method used for protecting the PAN. For this requirement, a QSA will typically: • Review documentation describing how the cryptographic keys are stored and managed. • Review system settings and processes to ensure that cryptographic keys are stored and managed as described in the documentation. Note that HPE NonStop Volume Level Encryption (NSVLE) does not satisfy this requirement. See Disk Encryption for details. Independent Software Vendor Products exist that can encrypt backup operations and TMF dumps. A number of hardware based virtual tape systems also contain encryption functionality for traditional tape based operations [Consider comForte SecurTape, Greenhouse BaReLib or a hardware based solution such as HPE NonStop BackBox Virtual Tape Controller (VTC) or HPE Virtual Tape Server (VTS) that includes encryption capabilities. Note that Strong Cryptography must be used]

PCI DSS Requirement	Testing Procedure	Remark
	3.4.1.c	This requirement is only relevant if disk encryption is the method used for protecting the PAN. For this requirement, a QSA will typically: • Review the content of a sample of removable media holding PANs to confirm that the PAN is not readable. • Review documentation describing how data is protected on removable media. Note that HPE NonStop Volume Level Encryption (NSVLE) does not satisfy this requirement. See Disk Encryption for details. Independent Software Vendor Products exist that can encrypt backup operations and TMF dumps. A number of hardware based virtual tape systems also contain encryption functionality for traditional tape based operations [Consider comForte SecurTape, Greenhouse BaReLib or a hardware based solution such as HPE NonStop BackBox Virtual Tape Controller (VTC) or HPE Virtual Tape Server (VTS) that includes encryption capabilities. Note that Strong Cryptography must be used]
3.5	3.5	See Template for ROC for details on what a QSA will require for these requirements. See Encryption Key Custodians for further information.
3.5.1	3.5.1	
3.5.2	3.5.2.a	
	3.5.2.b	
	3.5.2.c	
3.5.3	3.5.3	See Template for ROC for details on what a QSA will require for these requirements.
3.6	3.6.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.b	
3.6.1	3.6.1.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.1.b	
3.6.2	3.6.2.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.2.b	
3.6.3	3.6.3.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.3.b	
3.6.4	3.6.4.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.4.b	
3.6.5	3.6.5.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.5.b	

PCI DSS Requirement	**Testing Procedure**	**Remark**
3.6.6	3.6.6.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.6.b	
3.6.7	3.6.7.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.7.b	
3.6.8	3.6.8.a	See Template for ROC for details on what a QSA will require for these requirements.
	3.6.8.b	
3.7	3.7	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

REQUIREMENT INTRODUCTION

The introduction for requirement 4 of PCI DSS states:

> *Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.*

REQUIREMENT DESCRIPTION

This requirement specifies the need for using session encryption to protect sensitive information. Encryption must be used where cardholder data is transmitted over a public network. It should also be noted that if an organization commissions private communications lines from a telecommunications company, it may be possible that the telecommunications company who owns the lines has the ability to view any unencrypted traffic.

The requirement covers only the sessions transmitting cardholder data. User sessions such as TACL, osh, ftp and so on, send userid and password information in the clear. To protect this information from being obtained by a network trace or sniffer utility, some form of session encryption is required.

See also the section on Session Encryption detailed in Requirement 2.

THE REQUIREMENT - 4

PCI DSS Requirement	Testing Procedure	Remark
4.1	4.1.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. In situations where SSL or early version TLS is being used, a QSA will perform testing procedures as per Appendix A2. See Session Encryption for further information.
	4.1.b	
	4.1.c	
	4.1.d	
	4.1.e	
	4.1.f	
	4.1.g	
4.1.1	4.1.1	This requirement is typically not applicable to the HPE NonStop server.
4.2	4.2.a	This requirement is typically not applicable to the HPE NonStop server.
	4.2.b	
4.3	4.3	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

REQUIREMENT INTRODUCTION

The introduction for requirement 5 of PCI DSS states:

> *Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.*

REQUIREMENT DESCRIPTION

Typically, the following operating systems are not commonly affected by malicious software: mainframes, and certain Unix servers (such as AIX, Solaris, and HP-Unix). However, industry trends for malicious software can change quickly and each organization must comply with Requirement 6.2 to identify and address new security vulnerabilities and update their configuration standards and processes accordingly[10].

HPE NonStop servers are not systems that are commonly affected by malware so this section is not applicable when strictly applied to HPE NonStop servers. However, HPE NonStop servers are regularly accessed by Windows workstations, including the system console, which are vulnerable to such attacks. Malicious programs such as software based key loggers, if installed on the system console, could potentially provide privileged userid and password information to unauthorized users. It is imperative that this is guarded against.

Any Windows based systems (or other client operating systems such as Linux) accessing an HPE NonStop server that stores, processes or transmits cardholder data are subject to requirement 5.

SECURING THE SYSTEM CONSOLE

For HPE's recommendations on how the system console should be protected, see the relevant section of the *HPE NonStop System Hardening Guide* document in the HPE NonStop Technical Library.

[10] From *Navigating PCI DSS:Understanding the Intent of the Requirements* (https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf)

The recommendations below and any comments in this section apply to the system console and any other Windows or client operating system based consoles connected to the HPE NonStop server, such as those used for system monitoring. Other Windows (or client operating system) based machines are likely to be subject to this requirement, but as this document focuses specifically on the HPE NonStop server environment, they are not in scope.

For the system console automatic updates of software may not be possible, as it is quite likely to be connected neither to the internet nor to a Windows Domain. In this case, anti-virus/anti-malware software and definitions will need to be updated manually. The process for updating the anti-virus/anti-malware software and definitions should be documented.

Automatic virus scans should be configured for all Windows workstations that provide access to the HPE NonStop server.

THE REQUIREMENT - 5

PCI DSS Requirement	Testing Procedure	Remark
5.1	5.1	The system console and any other dedicated consoles (e.g. Prognosis, XYGATE Compliance PRO – XSW etc.) must be hardened as per this requirement. For information on HPE supported software and configuration hardening for the console, see Securing the System Console. See Template for ROC for details on what a QSA will require for this requirement.
5.1.1	5.1.1	
5.1.2	5.1.2	While HPE NonStop servers are not prone to malware threats, organizations must continue to liaise with HPE in regard to any new malware threats that may develop to ensure that no changes in technology have introduced this as a potential vulnerability. See Template for ROC for details on what a QSA will require for this requirement.
5.2	5.2.a	The system console and any other dedicated consoles (e.g. Prognosis, XYGATE Compliance PRO – XSW etc.) must be hardened as per this requirement. For information on HPE supported software and configuration hardening for the console, see Securing the System Console. See Template for ROC for details on what a QSA will require for this requirement.
	5.2.b	
	5.2.c	
	5.2.d	
5.3	5.3.a	
	5.3.b	
	5.3.c	
5.4	5.4	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

REQUIREMENT INTRODUCTION

The introduction for requirement 6 of PCI DSS states:

> *Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.*
>
> *Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

REQUIREMENT DESCRIPTION

This requirement relates to ensuring that no software vulnerabilities exist and includes both system and application software. A large portion of the requirement focuses on establishing good coding, testing and application deployment practices.

Organizations should also have procedures in place to ensure that the security related configuration of their systems/subsystems is configured in a way to mitigate the possibility of non-privileged users gaining privileged access to utilities or data by exploiting known configuration vulnerabilities.

SECURITY UPDATES TO SOFTWARE

Any security related SPRs that are identified as critical need to be implemented within 30 days of being released. This also applies to any ISV security software that may be running on the system. Any critical patches released by the vendor should likewise be implemented within 30 days.

The organization must have a security policy that documents that all non-critical security related patches will be applied within the time period specified in the policy to the HPE NonStop servers.

It should be a part of documented procedures to go through all Hotstuffs, NonStop-related HPE security bulletins and SPR release notes and ensure that any SPRs related to security are applied.

To enroll in receiving HPE ExpressNotices so as to be alerted to newly discovered security vulnerabilities for the HPE Operating System and HPE products, a user should register via the HPE NonStop eService Portal which is located at https://h22204.www2.hpe.com/NEP/ e.

The link to HPE product security vulnerability alerts is http://www8.hp.com/us/en/business-services/it-services/security-vulnerability.html. From this site you can subscribe to alerts for the products that you use and also view HPE-wide security advisories for certain critical vulnerabilities and access the HPE Security Bulletin archive.

Contact independent software vendors to determine their procedure for alerting of security vulnerabilities and notification of new software patches and releases.

If the organization has no process in place for analyzing security related patches to determine which ones should be applied to the system, then all patches need to be installed within one to three months of release.

ROLE BASED APPLICATION ACCESS CONTROL

In regards to software applications, role-based access control typically relates to users only being authorized to perform functions or have access to screens required to fulfill their documented role within the organization. This type of functionality needs to be included in the design of the application. Only users with a specified and documented business requirement should be able to view cardholder details and only as per the requirements of PCI DSS.

Vendor applications such as BASE24 and CONNEX typically include the ability to configure which screens specified users can see. The responsibility is on the organization however to ensure that the application is appropriately configured to utilize this functionality.

SEPARATION OF TEST AND DEVELOPMENT FROM PRODUCTION

Test and Development environments must be separate from Production and Disaster Recovery (DR) environments. Ideally this means that they should not be on the same physical system or on the same Expand network.

Strong controls must be in place to ensure that there is no mixing of environments. There must be no possible access to production environments from development or test userids whether they are on the same system (if for example the DR system is also a test system) or from separate physical development or test systems. Such measures that would assist in keeping environments separate include the following:

- No sharing of userids between the environments. That is, no developmen/test userids should be able to access a production or DR environment.
- Unique subvolumes for each environment with appropriate Safeguard protection in place to enforce access control and auditing. Using dedicated volumes (or virtual volumes) for each of Production/DR and Test/Dev may make this easier to manage.

- Unique directories for each OSS environment with strong access security applied.
- Real (production) cardholder data must not be used on the development/test systems for test or development purposes.
- Production/DR application userids should not exist on the Dev/Test systems.
- Privileged userids on the Dev/Test system, such as SUPER.SUPER, should not have privileged capabilities on the Production/DR system.
- No shared communication lines between Prod/DR and Test/Dev.

Documentation must describe the process used for ensuring that test data and accounts are never ported to the production environment.

Different roles, for example testing and production support may be performed across the production and development/test environments by the same person. The different roles must however be performed by separate userids/aliases with different passwords. Each role performed must be fully documented.

If userids or aliases are common across production and development/test systems (not recommended), the passwords for these userids/aliases must be different.

If test users do exist on the production system due to shared physical systems, for example DR and test, they must be completely segregated as described above.

The organization must be able to show that test cardholder data on test or development systems is not production data. This may include demonstrating to the QSA the procedure used for creating the test data.

Independent Software Vendor Products exist that can assist in determining if production PAN data is being used in test or development environments. [Consider PANfinder]

CHANGE CONTROL

It needs to be shown that proper change control procedures are fully documented and are followed for the implementation of any changes to the system. Such change procedures should include impact analysis, security testing, back-out procedures and management sign-off.

GAINING PRIVILEGED ACCESS THROUGH SECURITY CONFIGURATION GAPS

It should be noted that while security vulnerabilities don’t tend to occur very often in HPE NonStop operating system software, there are a significant number of security vulnerabilities that can be exploited if systems/subsystems are not configured optimally. Methods exist for a non-privileged userid to assume the powers of a privileged userid such as SUPER.SUPER by exploiting such gaps. Requirement 6.1 states that an organization must “*establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information*”. While notification and publications from HPE and security software vendors will typically cover the requirement in regards to vulnerabilities within software, organizations should consider using external expertise to regularly review their HPE NonStop security environment to ensure that gaps in configuration, auditing and procedures don't exist. The need for this should be viewed as even greater for organizations that do not have all occurrences of cardholder data protected by encryption or tokenization and are instead using compensating controls to satisfy Requirement 3.4. As many QSAs typically don't have a high level of expertise in the HPE NonStop platform, relying on a PCI Assessment by a QSA, to determine if systems are secured adequately, is unlikely to provide a true picture of how secure the organization's cardholder data actually is. The organization may receive a "tick of compliance" but may have an insecure system leaving it exposed to a potential data breach.

Contact Knightcraft Technology or see the Knightcraft website to find out how we can assist you with a review of your HPE NonStop security environment.

For extra information on areas to look at for securing your system, see http://www.knightcraft.com/common-hp-nonstop-security-hacks-and-how-to-avoid-them.

THE REQUIREMENT - 6

PCI DSS Requirement	Testing Procedure	Remark
6.1	6.1.a	For this requirement, a QSA will typically: • Interview relevant personnel to determine the method that they use for reviewing and applying security related SPRs and ISV security software patches. It should be noted that while security vulnerabilities don't tend to occur often in HPE NonStop operating system software, there are a number of vulnerabilities that can exist in configuration. See the section on Gaining privileged access through security configuration gaps for further discussion on this. See Security Updates to Software for further information.
	6.1.b	For this requirement, a QSA will typically require evidence of the method of receiving the information and applying relevant patches provided to the QSA as per 6.2.a. a QSA will typically examine the following: • Documentation indicating the process for receiving and reviewing SPR Notifications, Hotstuffs, HPE Security Bulletins and release documents from HPE and ISVs respectively. • Evidence of received SPR Notifications, Hotstuffs and HPE Security Bulletins • Evidence of a method used for analyzing release notices to determine if they need to be applied, such as a security incident register or spreadsheet detailing all released relevant SPRs, which ones need to be applied to the systems and when they were applied. It should be noted that while security vulnerabilities don't tend to occur often in HPE NonStop operating system software, there are a number of vulnerabilities that can exist in configuration. See the section on Gaining privileged access through security configuration gaps for further discussion on this. See Security Updates to Software for further information.
6.2	6.2 .a	For this requirement, a QSA will typically examine the following: • SYSINFO to show current OS version • SYSTIMES to show when the system was last cold loaded • List of all installed SPRs and OS file versions • List of all latest releases of SPRs from HP • List of all installed ISV software • List of all in-house developed software • List of all latest releases from ISVs See Security Updates to Software for further information.

PCI DSS Requirement	Testing Procedure	Remark
	6.2.b	The organization must have a security policy that documents that all security related critical SPRs as per 6.1.a will be applied within 30 days to the HPE NonStop servers. All non-critical security related patches will need to be applied within time period specified in the organization’s security policy. For this requirement, a QSA will typically: • Examine the documentation to confirm that the process for installing SPRs is included and is satisfactory. See Security Updates to Software for further information.
6.3	6.3.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	6.3.b	
	6.3.c	
	6.3.d	
6.3.1	6.3.1	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
6.3.2	6.3.2.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	6.3.2.b	
6.4	6. 4	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. See Separation of Test and Development from Production for further information.
6.4.1	6.4.1.a	
	6.4.1.b	
6.4.2	6.4.2	For this requirement, a QSA will typically: • Request to witness a user logging on to a sample userid that exists on both systems and show by demonstration that the passwords are different. • Request to witness a user attempting to access the production environment from a test or development userid. • For further details of QSA requirements see the Template for ROC. See Separation of Test and Development from Production for further information.
6.4.3	6.4.3.a	See Template for ROC for details on what a QSA will require for this requirement.

PCI DSS Requirement	Testing Procedure	Remark
	6.4.3.b	Without using an automated scanning tool such as PANfinder to look for PANs, data may be missed. Detected PANs should be analyzed as to the process under which they came to the development system to ensure it is not production data. If production data is brought to a development system, all PANs must be masked. See Separation of Test and Development from Production for further information.
6.4.4	6.4.4.a	For this requirement, a QSA will typically: • Interview relevant personnel to determine the process for ensuring that test data and accounts are never ported to the production environment. • Review documentation to ensure that it describes the process used for ensuring that test data and accounts are never ported to the production environment. • Examine change control documents to ensure that test data and accounts are not ported from development/test environments. • Examine production data files or tables to ensure that there is no test data included (for example “Greg’s Test Record”) and a list of userids/aliases to ensure that there are no test users on the production system. See Separation of Test and Development from Production for further information.
	6.4.4.b	
6.4.5	6.4.5.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. See Change Control for further information.
	6.4.5.b	
6.4.5.1	6.4.5.1	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
6.4.5.2	6.4.5.2	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
6.4.5.3	6.4.5.3.a	This requirement relates to any system changes that may affect the security of the system. If there have been any changes to subsystems such as Safeguard or ISV security software, TCP/IP etc., testing should be performed to ensure that security has not inadvertently been compromised.
	6.4.5.3.b	This requirement relates to any changes to the application that may affect security. It is necessary to ensure that no changes to the code have compromised the security in any way, specifically regarding the requirements specified in Req. 6.5.
6.4.5.4	6.4.5.4	For this requirement, a QSA will typically: • Request to see a sample change control document that shows a description of the back-out procedures for the change.

PCI DSS Requirement	**Testing Procedure**	**Remark**
6.4.6	6.4.6	This requirement relates to any significant changes that that may affect the security of the system or application environment. Any such change must also consider all components on the periphery that may be affected, for example, documentation, procedures referenced in the system hardening guide, log integration, and so on, may need to be updated. All other subsystems should be considered to see whether or not they are affected. Significant changes would include actions such as operating system or security software upgrade, new application introduced to the system, changes to encryption methods used, and so on. See Template for ROC for details on what a QSA will require for this requirement.
6.5	6.5.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	6.5.b	
	6.5.c	
6.5.1	6.5.1	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
6.5.2	6.5.2	
6.5.3	6.5.3	
6.5.4	6.5.4	
6.5.5	6.5.5	
6.5.6	6.5.6	
6.5.7	6.5.7	
6.5.8	6.5.8	
6.5.9	6.5.9	
6.5.10	6.5.10	
6.6	6.6	A document must exist that describes how this requirement is met for publicly facing web-based applications. See Template for ROC for details on what a QSA will require for this requirement.
6.7	6.7	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

REQUIREMENT INTRODUCTION

The introduction for requirement 7 of PCI DSS states:

> *To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.*
>
> *"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.*

REQUIREMENT DESCRIPTION

There are a number of ways that non-privileged userids can gain privileged user abilities on an HPE NonStop server if security is not configured correctly. By obtaining this level of privilege, a user may be able to access areas of the system that they are not authorized to access, potentially including cardholder data or applications. See Gaining privileged access through security configuration gaps for further discussion on this and also http://www.knightcraft.com/common-hp-nonstop-security-hacks-and-how-to-avoid-them.

The basis of this requirement is that users accessing the system should be provided only with the access privileges required to perform their specific (and documented) job role. This refers to both the use of privileged userids and also the access rights that are provided for users on the system.

In an HPE NonStop server environment, a number of common tasks require SUPER group level access. This includes tasks that may fit regularly into a user's job role. For example, operations staff may be given the authority to bounce communications lines as a part of their authorized role. To perform this task in SCF, they would require super level access, yet if a SUPER userid is provided, this provides those staff with powers far in excess of just being able to bounce communications lines. Similarly if a progid version of SCF is provided for such users, they would be able to perform a wider range of activities than they may be authorized for. These factors must be considered when determining how to achieve compliance with this requirement.

In regards to accessing of files on the system, users should only be provided with the access that they require for their documented job role. Sensitive data should be restricted accordingly.

Note: If Off Box Authentication is used for authenticating to the HPE NonStop server, for example LDAP authentication against Windows Active Directory, all of the requirements listed in Requirement 7 must be met on the authenticating server as well as the HPE NonStop server.

ROLES AND RESPONSIBILITIES

There must be documentation describing the roles and responsibilities of the various users/groups that have access to the systems. The following should be included in the documentation:

- Identification of all departmental groups/userids that have access to the systems.
- For each user group, a brief description of their role as it relates to the HPE NonStop servers.
- Tasks authorized for each group defined at a functional level. This should include:
  - Authorized day to day activities that can be performed from a user's personal userid/alias without any extra level of authority being required.
  - Authorized day to day activities that need to be performed from a userid/alias with elevated privileges such as, for example, SUPER.SUPER, another SUPER group member or application userids.
  - Activities that need to be performed periodically from a userid/alias with elevated privileges but that need to be authorized in accordance with the organization's change management procedures.
  - Activities that need to be performed from a userid/alias with elevated privileges in an emergency support situation.

USE OF PRIVILEGED USERIDS

The usage of privileged userids must be documented and must include a description of how and when these userids are used. Elevated privileges should not be provided to users without proper controls. In regards to an HPE NonStop server, for example, system managers should not be provided with SUPER group privileges for their day to day operations, as this provides a greater level of access than will typically be required. Elevated privileges should only be made available on an as needs basis under a documented control mechanism.

Userids with elevated access privileges on the system (e.g. super users, Safeguard Security-Groups, ISV security software owner userid, application userids etc.) need to be identified. For each of these userids the following should be detailed:

- Purpose for the userid and typical tasks that require use of the userid.
- Role groups who are authorized to access the userid under appropriate controls.
- Circumstances under which the userid will be made available to authorized users.
- Password ownership of the userid and password requirements. System level password controls applied to the userid.
- Procedure for obtaining the authority to access the userid and for obtaining passwords.
- Any system level logon controls applied to the userid (e.g. those applied through ISV products).

The various userids detailed in the Privileged Userids section should be included.

SAFEGUARD SECURITY-GROUPS

A number of security related privileges can be provided to specified users through Safeguard Security-Groups. Through this mechanism, users can be designated powerful abilities such as controlling the Safeguard subsystem, managing OSS file security, managing persistent processes and so on. For a full list of Safeguard Administrator Groups and their privileges, see the Safeguard Administrator's Manual in the HPE NonStop Technical library. Any userid that is provided extra security capabilities due to their membership of a Security-Group should be considered a privileged user on the system and treated as such in regards to the requirements of PCI DSS.

USER ACCESS PRIVILEGES

User access privileges on the system must be documented. This should align with the roles as described above and should include details of the types of files/subvolumes that a user has access to on the system. The following types of files should be taken into account:

- Operating system objects
- Startup/Shutdown files for system and OS subsystems
- Configuration files for system and OS subsystems
- System and subsystem logfiles
- Security configuration, including for vendor security products such as CSP Passport, SECOM, XYGATE etc.
- Security audit logfiles, including for vendor security products such as CSP Passport, SECOM, XYGATE etc.
- Application object programs
- Application program source code/libraries/DDLs
- Application data subvolumes/directories
- Application reports
- Application configuration files
- Application startup/shutdown files
- Application logfiles
- Batch related files
- Any files containing cardholder data

If any Role Based User Access software products are in use, any privileged commands provided to individuals should be fully documented.

ACCESS CONTROL SYSTEM

The NonStop platform comes with an access control system that provides the following functionality:

- Users must enter a userid and password to gain access to the system.
- Guardian, Safeguard and OSS provide controls that allow the restriction of access to files based on the userid attempting the access and the type of operation being performed (read, write, execute, purge).

The HPE *Security Management Guide*[11] states, "Although the Guardian tools provide basic authentication and authorization services, Safeguard features add auditing services and also extend the authentication and authorization capabilities. Safeguard features also allow segregating of administration tasks. Safeguard's access control lists allow specifying access to a greater level of detail [than Guardian security strings allow]".

An automated mechanism should be used for restricting which users are allowed to logon to privileged userids. Neither Guardian nor Safeguard provides this level of access control. It is possible to control logon to TACL sessions by customizing the TACLLOCL file or by using a custom CMON program so that users are forced to logon to their own personal userid prior to being able to logon to privileged userids. The same mechanism can also control which userids are permitted to logon to privileged userids. This approach however does not easily translate to OSS unless users are forced to logon to TACL first and then enter an OSH session.

Alternately, ISV software tools exist that can control user logons. [Consider XYGATE User Authentication (XUA), XYGATE CMON (XCM), CSP Passport]

The following points should also be considered in regard to this requirement:

- If an OSS telnet service is configured then users would be able to login to the OSS environment without going through the Guardian shell. If no OSS telnet service exists, users must login to the Guardian environment and then use the OSH command to login to the OSS environment.
- Access to OSS files is controlled by OSS file-permission bits and access control lists (ACLs are supported by Version 3 OSS catalog filesets).
- As a command monitor process, $CMON controls user requests such as logons and execution rules for processes (priority, CPU). If a CMON process is not used, the process name $CMON should be protected, for example by using an OBJECTTYPE PROCESS under Safeguard.

"NEED TO KNOW" ACCESS

A part of Requirement 7 refers to the implementation of security on the system that ensures users do not have access to any component that they are not specifically authorized to access. For this to be achieved access needs to be denied by default.

[11] Security Management Guide (HPE NonStop Technical Library)

Use of aliases does not inherently satisfy the Least Privilege requirement, as the privileges of the alias are exactly the same as those of the underlying userid. For example, configuring different system administrators so that each has their own alias of SUPER.SUPER, gives each of those users the power of SUPER.SUPER from their own logon.

An example of a "deny all" implementation in Safeguard is as follows:

Safeguard Globals:

- Safeguard configured with SUPER.SUPER DENIABLE (SYSGEN parameter)
- DIRECTION-DISKFILE = FILENAME-FIRST
- COMBINATION-DISKFILE = FIRST-ACL
- CHECK-VOLUME = ON
- CHECK-SUBVOLUME = ON
- CHECK-FILENAME = ON

For each VOLUME:

- SUPER.SUPER or Application userid access only (depending on what is stored on the volume)
- Configured with no access to other userids.

For each SUBVOLUME:

- Required access configured for all relevant Userids.

DISKFILE Records:

- Only required where the security required for a file is different to the access provided by the Subvolume record.

OBJECTTYPE Records:

- Ensure that all objecttypes (including objecttype objecttype) are secured so that only authorized users are able to add Safeguard records.

This ensures that if a Safeguard Subvolume record is not specifically defined, no access will be granted to users other than SUPER.SUPER.

It would be possible to use other methods to achieve the above, such as by using Safeguard DISKFILE-PATTERNs or SAVED-DISKFILE-PATTERNs.

"Deny all" default security should likewise be set in the OSS environment. OSS cannot be secured using Safeguard. OSS security needs to be set within the OSS environment itself at the file and directory level.

A number of Independent Software Vendor Products exist that can simplify management of Safeguard through the use of a GUI based interface. These often provide not only the ability to manage and view Safeguard configuration records, but also OSS and/or SQL/MX security configuration. As setting up "deny all" security requires a significant effort in Safeguard and OSS, these tools can assist in making the task a lot simpler and provide much greater visibility of existing configuration than is possible with native tools.

[Consider CSP Protect X, comForte Safepoint, XYGATE Safeguard Manager (XSM)]

Independent Software Vendor Products exist that utilize the OSS SEEP, enabling them to control authorization requests to both Guardian and OSS files and directories.

[Consider XYGATE Object Security (XOS)]

ROLE BASED USER ACCESS

Apart from access to system objects such as subvolumes, files/tables etc. system users should only be provided with the ability to perform functions and tasks in accordance with their defined and documented role. A number of ISV software products can be used to set up a role based security model so that users have the ability to perform authorized actions, including those tasks normally requiring privileged userid access, from their own non-privileged personal userid. Typically this will include the ability to start a utility running as a privileged userid and restrict the commands that the user can perform to only those functions for which they are authorized. This means that users can be provided with exactly the level of privilege that they require for their job role, without being provided any greater privilege than they need and without needing to be given passwords for privileged userids. Any privileged access or commands that are configured using such software must be fully documented.

[Consider XYGATE Access Control (XAC), CSP Passport, Greenhouse SECOM]

THE REQUIREMENT - 7

PCI DSS Requirement	Testing Procedure	Remark
7.1	7.1	For this requirement, a QSA will typically: • Request to see the documentation to determine if all relevant items are included. • Require a demonstration that displays that proper procedures are being followed in the process of providing access to the system. This may include a request to see a signed Access Request Form or equivalent to show that this is the case. • Request to see a demonstration of the use of the automated access control system that is in place. See Use of Privileged Userids for further information. See Safeguard Security-Groups for further information. See Access Control System for further information.
7.1.1	7.1.1	See Template for ROC for details on what a QSA will require for this requirement. See Use of Privileged Userids for further information. See Safeguard Security-Groups for further information. See Access Control System for further information.
7.1.2	7.1.2.a	
	7.1.2.b	
7.1.3	7.1.3	

PCI DSS Requirement	**Testing Procedure**	**Remark**
7.1.4	7.1.4	For this requirement, a QSA will typically: • Match the user authorization forms with privileges assigned to users on the system. • Examine the access configuration of the system. • Examine access authorization forms and privileges that are detailed in the forms for each user. • Ensure that access provided to a particular user on the system matches what is defined in the authorization form and documentation. • Examine security of all cardholder data - whether the files are readable or not by unauthorized users. • Examine user menu screens to ensure users can't "break" out and get back to a prompt if not authorized. • Verify whether there seems to be a good rationale as to why userids/aliases/groups and their corresponding access have been set up in the manner in which they have. • Check which userid(s) the system manager logs on to on a day to day basis. • Check what SUPER.SUPER is used for, how often, and if this use is as reflected in user access forms. • Check usage of aliases. • Check all types of access around files containing any sensitive cardholder data.
7.2	7.2	For this requirement a QSA will typically look to see how access control and a default "deny all" setting are implemented on the system as per items 7.2.1 through 7.2.3.
7.2.1	7.2.1	For this requirement, a QSA will typically: • Check whether or not Safeguard is running on the system • Check if any other access control mechanisms such as ISV security software modules are running. See Access Control System for further information.
7.2.2	7.2.2	For this requirement, a QSA will typically: • Check that a document exists describing roles and access requirements to the system • Check that any user groups configured match the roles defined in the document • Verify that functions permitted for each group are documented • See a demonstration of how the functions described for each user group are configured on the system. This could be in the form of checking XAC configuration and commands. See "Need to Know" Access for further information.

PCI DSS Requirement	Testing Procedure	Remark
7.2.3	7.2.3	For this requirement, a QSA will typically examine security configuration settings of critical Guardian and OSS based system files and any files that store cardholder data, such as the following, to determine if this requirement has been satisfied: • All operating system files ($system.system, $system.sysnn, DSV subvols, ISV subvols) • Any files that store cardholder data • System and OS subsystem startup/shutdown/configuration files • Security subsystem related files (including ISV security software as well as Safeguard/Guardian). • Pathway configuration. Netbatch security including security of all of the job "infiles" and the NetBatch program files. • Spooler configuration. • User default subvolume security. These should not be shared and should be secured so that only the owner can create or modify any files. • Subvolumes on common pmsearchlists. • Process security for $CMON. • Default security for users. See "Need to Know" Access for further information.
7.3	7.3	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

REQUIREMENT INTRODUCTION

The introduction for requirement 8 of PCI DSS states:

> *Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized user and processes.*
>
> *The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.*
>
> *Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance).*

REQUIREMENT DESCRIPTION

Requirement 8 deals largely with the use and management of userids and passwords on the system. A main essence of the requirement is that every logon to the system must be directly traceable to a specific individual. If multiple personnel within the organization use the same userid, in the case of a potential security breach, it is not easy to determine which specific person has performed the relevant actions. By enforcing individual userids and non-sharing of passwords, user actions can be more easily determined.

The only exception permitted for shared logons under this requirement is for logon to shared userids that are not a security concern. For example, userids with no power or privilege such as those used only for monitoring may be allowed.

Compensating Controls are required for the existence of any shared userids on the system. This includes standard HPE NonStop server userids such as SUPER.SUPER.

All users of the system with userids or aliases providing access to cardholder data need to be familiar with corporate password procedures and policies.

Note: If Off Box Authentication is used for authenticating to the HPE NonStop server, for example authentication by LDAP to Windows Active Directory, all of the requirements listed in Requirement 8 must be met on the authenticating server as well as on the HPE NonStop server.

ACCOUNTABILITY OF USER SESSIONS

On an HPE NonStop server, some generic privileged userids will typically exist. These include userids such as SUPER.SUPER, SUPER.CE, application owner userids and so on. It is a specific aim of this requirement to ensure that all logons to the system must be tied to an individual. If generic/shared userids such as SUPER.SUPER exist, there must be some mechanism to ensure that all uses of such userids are traceable to a unique individual. There is no standard way through Safeguard of achieving this objective, so some other mechanism will need to be used. This mechanism must be documented and will form the basis of the compensating control. Use of aliases, TACL macros and procedures may assist in providing a compensating control for this mechanism, but considerations need to be taken for all user sessions on the system including osh, ftp, rsc, dsm/scm and so on, as well as TACL.

While use of aliases can achieve the result of ensuring that all sessions are accountable to an individual, it does not meet the requirement of providing users with minimum privilege based on “Need to Know” Access.

Note that application specific userids such as those required to logon to applications such as BASE24, CONNEX etc. are also subject to this requirement and will typically also be reviewed by a QSA for compliance.

Where shared userids are in place, a policy document must exist that defines which generic (or shared) userids exist on the system, what they are used for and what compensating control is in place. For example, “*SUPER.SUPER is a shared privileged userid that is only used for emergency support situations. Users must logon to their personal userid prior to logging on to SUPER.SUPER as enforced by controls within the TACLLOCL file*”.

A number of different mechanisms can help provide the required accountability of user sessions in an HPE NonStop environment. See the sections on Two Step Authentication, Off Box Authentication and Role Based User Access.

TWO STEP AUTHENTICATION

One solution to forcing users to logon to their own personal userid prior to logon to a privileged userid is through the TACLLOCL file. It is a relatively simple TACL operation to check which user is currently logging on and if the user is a privileged userid, simply output an appropriate message and terminate the user session. As the TACLLOCL is only invoked on an initial logon, subsequent logons to a privileged userid would be permitted but Safeguard would record who was logging on to that userid. In this way, it will be possible to associate all user sessions with a specific individual. If OSS is being used on the system, users would either need to be forced to logon first through TACL before entering OSH or the .profile file would need to be modified to perform similar checks by invoking the appropriate gtacl commands.

Independent Software Vendor Products also exist that enforce two-step logon to privileged userids. [XYGATE User Authentication (XUA)]

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) involves authentication using combinations of two or more of something you know (e.g. a password), something you have (e.g. a SecurID token), or something you are (e.g. fingerprint). With the advent of PCI DSS 3.2, all non-console privileged userid access to the system must be authenticated using MFA. That means that any user who accesses the system as SUPER.SUPER, a security administrator userid, application owner userid and so on, must have authenticated using a MFA mechanism. The MFA need not necessarily occur on the HPE NonStop itself. The following are appropriate methods of authentication using MFA:

- At the network level. It is acceptable, for example, for a user to authenticate using MFA at the time that they connect in to the network to gain access to the HPE NonStop server.
- Using a jump box to access the HPE NonStop server, where access to the jump box is controlled by MFA. For example, access from a Citrix server where authentication has been previously established using MFA.
- Single Sign On (SSO) using a mechanism such as Kerberos is acceptable as long as the initial sign on (authentication) is performed using MFA.
- Use of SSH private key/public key pair and passphrase to satisfy the MFA requirement may not be acceptable anymore as this method is more susceptible to compromise than the methods listed above, particularly as Tandem terminal emulator software often allows the storing of the private key passphrase. Individual QSAs may have different opinions on whether or not this truly satisfies the requirement.

Note that whichever method is used will need to be confirmed as satisfactory by your QSA.

The requirements around MFA refer to non-console access of privileged userids. It should be specifically noted that console access implies that the user is physically located at the system console, inside an access controlled and monitored room. It does **NOT** include remotely accessing a console session over the network using RDP or other means. In cases where the user is remotely connecting in to the console, all of the requirements related to MFA and privileged access apply.

[Consider comForte SecurSSO, CSP Authenticator, CSP NIMS, Greenhouse **SECOM**, XYGATE User Authentication (XUA)]

OFF BOX AUTHENTICATION

A number of Independent Software Vendor Products provide a facility for authenticating users against Windows Active Directory (AD), an LDAP server or by use of other Single Sign On mechanism such as Kerberos. By using software of this nature, the lock out facility as specified in this requirement could potentially be provided by the authenticating server. Note that if privileged userid access to the system is through this mechanism, then the user must also perform multifactor authentication before access is provided.

[Consider comForte SecurSSO, CSP Authenticator, CSP NIMS, XYGATE User Authentication (XUA)]

PASSWORD ENCRYPTION

Userid and alias passwords must be encrypted both in storage and also in transmission.

Safeguard provides the facility to encrypt passwords in storage and this should be appropriately configured. The legacy encryption algorithm used in older versions of Guardian and Safeguard was DES. This setting is not appropriate as the DES encryption algorithm is no longer considered strong. Furthermore, it is only with the stronger algorithm of HMAC256 that passwords/passphrases longer than 8 characters are possible.

While passwords can be stored encrypted on an HPE NonStop server using Safeguard, userid and password information is transmitted unencrypted as standard by some subsystems on an HPE NonStop server. It is therefore essential to use an appropriate Session Encryption mechanism, as discussed in Requirement 2.

PASSWORD MANAGEMENT

Organizational procedures must be in place for verifying the identity of individuals before they have their password remotely reset by security or help desk personnel. For example, if an individual has forgotten their password or it has expired after returning from vacation, it may be necessary to have the password reset remotely by the help desk. On such occasions, the person resetting the password must have a procedure for validating the identity of the person requesting the password change and must be able to match the individual to their authorized userid. The procedure may be a manual procedure or it may be a part of a user password management program.

A number of the Independent Software Vendor Products contain a mechanism for storing personal information about users on the system that can be used to verify the identity of an individual when resetting userid/alias passwords. Alternately, the Userid file can store optional data that can be used by organizations to store information themselves about the users configured on the system.

[Consider CSP Netpass, XYGATE Password Quality (XPQ)]

NEW PASSWORDS FOR USERS

When userids or aliases are added to the system via Safecom, they should be added with their password expired, and with a Password-Expiry-Grace period set. This will force the individual to change their password when they first logon. Likewise, if a password is changed for an existing user by an administrator, the password should be automatically expired so that the user must change it when they next logon.

It is acceptable (in small organizations, for example) for a system administrator to add new users to the system via Safecom and for the individual to come over and change their password at the time by running the Password program. Blind Password must be enforced via TACL configuration (#SETCONFIGURATION) and Safeguard.

REVOKING OF USERIDS

Any user no longer employed by the organization should have their userid removed. This is important so that it is not possible for the ex-employee to gain access to the system, but also so that no existing employees are able to masquerade as that user by performing actions using the defunct userid. See the NonStop Security Hardening Guide for details on steps that must be taken to completely remove a userid.

Independent Software Vendor Products exist that will provide a facility for reporting on "orphaned" Safeguard ACLs. This means that when a userid/alias is removed from the system, Safeguard configuration can be updated to remove corresponding access rules for that userid/alias.

[Consider comForte Safepoint KSL, CSP Protect X, XYGATE Safeguard Manager (XSM), XYGATE Compliance PRO (XSW)]

PASSWORD EXPIRY

It is a part of Requirement 8 that a mechanism is in place to ensure that user passwords are changed every 90 days at a maximum. This requirement can typically be satisfied if userids/aliases are configured so that the sum of the values set for Password-Must-Change and Password-Expiry-Grace is less than 90 days in total. In such cases, a userid/alias will be frozen with a status of password-expired if they have not logged on for 90 days.

A compensating control is required for any userid or alias configured with a non-expiring password. For example, if the SUPER.SUPER password is non-expiring, a suitable compensating control may be the secure holding of the password by a group who do not have the ability to use the password to logon as SUPER.SUPER. The procedure or mechanism used to enforce this needs to be documented.

Independent Software Vendor Products exist that will report on userids/aliases that have not logged on in the last 90 days or any other specified time period. They typically can also report on users with expired passwords, userid/alias password change settings, passwords not changed for a specified period and so on.

[Consider XYGATE Safeguard Manager (XSM), XYGATE Compliance PRO (XSW), CSP Protect X, comForte Safepoint KSL]

VENDOR OR THIRD PARTY USERIDS

Vendor userids such as those used by HPE for remote support, or application software vendors where applicable, should be frozen when not in use. They should be thawed only as required and re-frozen when the relevant task has been completed. Consider changing the passwords after each use.

When a service account is used (such as SUPER.CE), an authorized member of the organization needs to be present to witness the session of the engineer. If it is not possible or practical for somebody to be present in this capacity, there is a need to capture the session and review the logs to ensure no unauthorized actions were performed. Note that there is an issue with capturing user sessions on HPE NonStop servers. See the section on Session Capture below for details.

SERVICE PROVIDER ACCESS TO SYSTEMS

A growing number of organizations are outsourcing management of their HPE NonStop servers or components of their application to third party service providers. Typically in these situations, the service provider will have a number of people who require access to the system to perform support or maintenance functions. It is important under PCI DSS for each individual from any service provider who accesses the system in this capacity to have their own userid and password. This is to ensure that specific individuals within a service provider organization can be held accountable for their actions on the system. For example, on organization systems that are managed by HPE, each HPE person accessing the system should have their own individual logon to the system with their own password.

For organizations who are managing their own systems, consideration still needs to be given to service provider access. See the section on Vendor or Third Party Userids for further information.

SESSION CAPTURE

A range of Independent Software Vendor Products provide the ability to capture user interactive sessions. Functionality that may be required from this type of software includes capture of conversational and block mode sessions, Guardian and OSS sessions, input and output of user commands, FTP and other types of interactive sessions. The tool should provide associated reporting capabilities making it possible to determine which actions a user has performed during any given session.

There is however one problem with session capture on the HPE NonStop server. Due to the workings of TACL, there is currently no way of fully capturing what occurs within a TACL macro that is executed from a TACL session. None of the session capture solutions offered by software vendors is able to address this issue. In some situations, depending on the software product being used for session capture and/or the configuration of the product, the contents of OBEY files may also not be fully logged. This means that organizations should not be relying exclusively on using session capture technology to ascertain what activities have taken place. A malicious user could potentially cover their tracks by using these known vulnerabilities in session tracking (see http://www.knightcraft.com/2014-hp-nonstop-advanced-technical-boot-camp for details of how this can be achieved). It is important therefore to ensure that appropriate Safeguard auditing and alerting is configured and reports of audit data are analyzed accordingly, along with tools providing File Integrity Monitoring capabilities. Minimizing the use of privileged userids on the system and ensuring appropriately tight security configuration will reduce exposure to this issue. If organizations do not contain the expertise in-house to determine if their security and auditing are configured appropriately, it is recommended that they seek an independent review of their security to help determine what needs to be done. Contact Knightcraft Technology or see the Knightcraft website to find out how we can assist in this regard.

PASSWORD LENGTH AND COMPLEXITY

The longer and more complex a password, the more difficult it is for somebody to either guess or crack using brute force techniques. A part of Requirement 8 specifies that passwords must be a minimum of 7 characters long and complexity must be enforced, so that all users must be configured with passwords containing both numeric and alphabetic characters. Both of these requirements can be achieved using Safeguard.

It should be noted that the greater the length of a password/passphrase, the average time to crack using a brute force attack increases exponentially. Longer passphrases typically provide greater protection than a shorter password/passphrase configured with complexity. Safeguard supports passwords/passphrases up to 64 characters. Note that the PASSWORD-COMPATIBILITY-MODE parameter must also be set to OFF to allow for passwords/passphrases longer than 8 characters. If passphrases with spaces are allowed, the PASSWORD-SPACES-ALLOWED parameter must be set to ON.

A range of Independent Software Vendor Products provide enhanced password strengthening capabilities, though recent releases of Safeguard can be used to satisfy this requirement.

AUTHENTICATE FAIL FREEZE

Action must be taken to reduce the likelihood of anybody successfully logging on to the system by guessing the password of a valid userid or alias. Requirement 8 states that a userid or alias must be frozen if there are six consecutive invalid logon attempts. The mechanism within Safeguard for performing this action involves setting the values for AUTHENTICATE-MAXIMUM-ATTEMPTS to 6 and AUTHENTICATE-FAIL-FREEZE to ON. This however is **not recommended** on an HPE NonStop server. The problem is that the Authenticate-Fail-Freeze parameter is a global setting. If it is set on, it is very easy for anybody to freeze out critical users such as SUPER.SUPER or other privileged userid by continually attempting to logon with an incorrect password. If an organization loses SUPER.SUPER on the system, recovery is potentially a very difficult and time consuming procedure, perhaps requiring system down time or a complete rebuild of the system disk.

The requirement further states that a userid or alias must be locked (frozen) after the invalid logon attempts for a period of 30 minutes. Short of freezing the user permanently, with the associated problems as described above, this cannot be achieved by Safeguard. The Safeguard Global parameter AUTHENTICATE-FAIL-TIMEOUT freezes the user session, not the user account.

There are Independent Software Vendor Products that can be configured with parameters such as Authenticate-Fail-Freeze set on a user by user basis so that it would be possible to have all users other than SUPER.SUPER configured to be frozen after 6 failed authentication attempts and if desired, thaw the user again after a specified time period has elapsed as per requirement 8. [Consider Greenhouse REPRIEVE, XYGATE User Authentication (XUA)]

XYGATE Merged Audit (XMA) (which is now distributed as standard with the Operating System) has the ability to run a TACL macro based on the occurrence of a specified Safeguard security event. To satisfy this requirement, XMA could detect the Safeguard event detailing that user's failed logon count has been changed from 5 to 6 and then invoke a TACL macro that freezes the userid. The XMA event could be configured to perform this operation for all userids/aliases with the exception of SUPER.SUPER (and perhaps the security manager userid). As XMA ships free with the operating system, this may provide an easy and cost effective solution. The userids in question would however need to be manually thawed to re-activate them, though this could also be performed by use of an appropriate TACL macro, perhaps triggered by a Netbatch job.

USER SESSION INACTIVITY TIMEOUT

If a user leaves their session inactive for 15 minutes, it is required that the session be automatically locked so that another user cannot perform actions on the system using that session. This requirement is to assist in ensuring that all user actions can be tied to a specific individual. It is possible to satisfy the requirement in general by using a Windows screensaver with a password set. At a shared console workstation however, if a generic userid with a shared password is being used for some reason, controls must be applied at the Guardian/OSS level.

If the system console screensaver password is shared, any TACL/OSS sessions must have autologoff or session locking after 15 minutes or less of session inactivity. As the console is often the workstation used by HPE engineers to access the system, typically using a privileged userid, it is imperative that if the session is left logged on, that no other user will find it active and be able to enter commands.

Automatic termination of a TACL session after 15 minutes of session inactivity can be set in TACL using #SETCONFIGURATION. It can however be "fooled" if the user has entered a utility such as FUP or Viewpt. When the user exits the utility, the TACL session will still be alive and logged on. If for example, somebody has logged on to the system console as SUPER.SUPER, run Viewpoint and forgotten to exit and logoff, when another user comes along to the console, they will find a logged on session running as SUPER.SUPER.

For osh sessions in the OSS environment, session timeout should be configured using the TMOUT env variable.

It is possible to use Telnet process timeout parameters to enforce session timeouts, but this may not exit the session in a clean manner and can also be "fooled" by users starting a Viewpt session, or equivalent, to keep the session alive.

A number of the Independent Software Vendor Products that provide Role Based User Access also provide the ability to lock user sessions after a period of inactivity.

APPLICATION USERIDS

It is a part of Requirement 8 that application userids are not used by individuals for interactive logons to the system. This includes for purposes of managing the application, such as startup and shutdown. A mechanism such as Netbatch could potentially be used to assist in meeting this requirement.

A number of the Independent Software Vendor Products that provide Role Based User Access could be configured to allow authorized users to start up or manage application processes from their own non-privileged userid.

THE REQUIREMENT - 8

PCI DSS Requirement	Testing Procedure	Remark
8.1	8.1.a	See Template for ROC for details on what a QSA will require for this requirement.
	8.1.b	
8.1.1	8.1.1	For this requirement a QSA will typically interview relevant personnel, check documentation (for example, company security policy) and examine system configuration settings such as the following: • List of userids/aliases. • Check configuration of application userids to ensure they are not shared and that all are current e.g. BASE24 userid configuration. • HPE or ISV software configuration of any modules that provide Single Sign On functionality via LDAP or Windows Active Directory authentication (e.g. XUA, SecurSSO, CSP NIMS etc.) • Mechanisms used for enforcing two step logon i.e. ensuring logon to personal userid prior to logon to privileged userid. • Users/aliases on the system should match the relevant documentation. See Accountability of User Sessions for more information.
8.1.2	8.1.2	For this requirement, a QSA will typically: • Match the user authorization forms with privileges assigned to users on the system. • Examine the access configuration of the system. • Examine access authorization forms and privileges that are detailed in the forms for each user. • Ensure that access provided to a particular user on the system matches what is defined in the authorization form and documentation. • Examine security of all cardholder data - whether the files are readable or not by unauthorized users. • Examine user menu screens to ensure users can't "break" out and get back to a prompt if not authorized. • Verify whether there seems to be a good rationale as to why userids/aliases/groups and their corresponding access have been set up in the manner in which they have. • Check which userid(s) the system manager logs on to on a day to day basis. • Check what SUPER.SUPER is used for, how often, and if this use is as reflected in user access forms. • Check usage of aliases. • Check all types of access around files containing any sensitive cardholder data.

PCI DSS Requirement	Testing Procedure	Remark
8.1.3	8.1.3.a 8.1.3.b	For this requirement, a QSA will typically: • Review that a procedure for revoking access for terminated users is documented as specified. • Examine a current set of all userids and aliases on the system. • Verify that all userids and aliases on the list belong to currently employed personnel. See Revoking of Userids for further information.
8.1.4	8.1.4	For this requirement, a QSA will typically: • Review that a procedure for removing inactive user accounts is documented as specified. • Request to see evidence that the procedure is followed as documented. See Password Expiry for further information.
8.1.5	8.1.5.a	For this requirement, a QSA will typically: • Confirm that vendor service userids/aliases are frozen. • Verify that the procedures used for monitoring actions performed by these userids are adequate and are as documented. See Vendor or Third Party Userids for further information.
	8.1.5.b	Any remote sessions to the system by vendors such as HPE or other software providers for example, must be recorded. See the section on Session Capture for further information. Logs of any sessions must be reviewed by security administrators or a person filling that designated role within the organization.
8.1.6	8.1.6.a	For this requirement, a QSA will typically: • Examine the system configuration that enforces the locking out of users after the invalid password attempts. • Observe the mechanism in effect to ensure it corresponds with the documentation. See the section on Authenticate Fail Freeze for further information.
	8.1.6.b	This requirement refers to organizations that act as service provider to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HPE NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.1.6.a.
8.1.7	8.1.7	For this requirement, a QSA will typically: • Examine the system configuration that enforces the locking out of users after the invalid password attempts. • Observe the mechanism in effect to ensure it corresponds with the documentation. See the section on Authenticate Fail Freeze for further information.

PCI DSS Requirement	Testing Procedure	Remark
8.1.8	8.1.8	For this requirement, a QSA will typically: • Examine the system configuration enforcing the inactivity timeout of user sessions. • Observe the mechanism in effect to ensure it corresponds with the documentation. See the section on User session inactivity timeout for further information.
8.2	8.2	For this requirement, a QSA will typically: • Confirm that all users logging on to the system require a userid and a password • Verify that this fact has been documented. • Observe a sample logon to the system to ensure that a password is entered at the prompt. If the user logs on and does not enter a password, the logon should fail.
8.2.1	8.2.1.a	For this requirement, a QSA will typically check the following: • In Safeguard, the PASSWORD-ALGORITHM = HMAC-256. • Examination of the USERID file to ensure that all passwords are encrypted. • For password transmission, requirement 2.3.a through 2.3.c must be met i.e. that strong session encryption is being used for all user sessions to the HPE NonStop server. See the sections on Session Encryption and Password *Encryption* for further information.
	8.2.1.b	
	8.2.1.c	
	8.2.1.d	This requirement refers to organizations that act as service provider to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HPE NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.2.1.a, 8.2.1.b and 8.2.1.c. See the section on Service Provider Access to Systems for more information.
	8.2.1.e	
8.2.2	8.2.2	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. See Password Management for further information.
8.2.3	8.2.3.a	For this requirement, a QSA will typically • Confirm that the value set in Safeguard for PASSWORD-MINIMUM-LENGTH is at least 7. • Check Safeguard configuration to ensure that password complexity is in use and that it satisfies the rules stated in the requirement. • Check any ISV software enforcing password rules to make sure that it satisfies the rules stated in the requirement and is consistent with Safeguard settings. See Password Length and Complexity for further information.

PCI DSS Requirement	Testing Procedure	Remark
	8.2.3.b	This requirement refers to organizations that act as service provider to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HPE NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.2.3.a. See the section on Service Provider Access to Systems for more information.
8.2.4	8.2.4.a	For this requirement, a QSA will typically: • Examine Safeguard configuration to determine that user passwords are set to expire as per the requirement. • Ensure that a suitable compensating control is in place for userids with non-expiring passwords. See Password Expiry for further information.
	8.2.4.b	This requirement refers to organizations that provide cardholder services to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HPE NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.2.4.a. See the section on Service Provider Access to Systems for more information.
8.2.5	8.2.5.a	For this requirement, a QSA will typically: • Confirm that the value set in Safeguard for PASSWORD-HISTORY is at least 4.
	8.2.5.b	This requirement refers to organizations that provide cardholder services to multiple customers. For example, organizations running a payment gateway type of environment. It is not generally applicable to the HPE NonStop server environment unless the users of the service application also have access to the operating system. If they do, this requirement is covered under 8.2.5.a. See the section on Service Provider Access to Systems for more information.
8.2.6	8.2.6	See Template for ROC for details on what a QSA will require for this requirement. See New Passwords for Users for further information.
8.3	8.3	See Template for ROC for details on what a QSA will require for this requirement.
8.3.1	8.3.1.a	This requirement relates to any non-console privileged userid access to the system performed by an individual (i.e. it excludes automatic accounts). See the section on Privileged Userids for further information on which types of userids this requirement is likely to apply to.

PCI DSS Requirement	Testing Procedure	Remark
	8.3.1.b	Console access is excluded from this requirement, because it is assumed that console access means that the user is accessing the system from a console in a tightly controlled and monitored computer or operations room. Console access does **NOT** include a user accessing the system from the console via a remote desktop session, as is common in the HPE NonStop environment. Such access to the console must be controlled by multifactor authentication. See the section on Multi-Factor Authentication for further information. See Template for ROC for details on what a QSA will specifically require for this requirement.
8.3.2	8.3.2.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	8.3.2.b	
8.4	8.4.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	8.4.b	
	8.4.c	
8.5	8.5.a	This requirement is essentially the same as Requirement 8.1. The remarks under that section apply directly to this section also. • Verify that a compensating control is in place for any shared/generic userids such as SUPER.SUPER. • See Accountability of User Sessions for further information.
	8.5.b	For this requirement, a QSA will typically: • Examine the documentation to ensure that shared userids and their use are explicitly prohibited. • Verify that a compensating control is in place for any shared userids. See Accountability of User Sessions for further information.
	8.5.c	For this requirement, a QSA will typically: • Interview the system administrator to ensure that no passwords are shared for generic userids. • Verify that a compensating control is in place for any shared userids. • See Accountability of User Sessions for further information.
8.5.1	8.5.1	This requirement is to ensure that separate userids exist for service provider users logging on to the customer system. See Template for ROC for details on what a QSA will require for this requirement. See the sections on Vendor or Third Party Userids and Service Provider Access to Systems for more information.

PCI DSS Requirement	Testing Procedure	Remark
8.6	8.6.a	See Template for ROC for details on what a QSA will require for this requirement. See the sections on Multi-Factor Authentication and Off Box Authentication for more information.
	8.6.b	
	8.6.c	

PCI DSS Requirement	Testing Procedure	Remark
8.7	8.7.a 8.7.b 8.7.c	For this requirement, a QSA will typically require the following: • A list of all database users. Users with access to the database will typically be matched with their user roles as defined in documentation to see if they should have access. • Confirmation that all database users are authenticated against the system before accessing the database. • Confirmation that all application access to the database contains appropriate authentication mechanisms. For this the QSA may want to analyze the application code to see the authentication mechanism used and access method to the database. • Confirmation that only userids with a DBA function are permitted direct access to the data files by mxci, SQLCI, Enable etc. Users with this type of access to the database will typically be matched with their user roles as defined in documentation.
	8.7.d	For this requirement, a QSA will typically check that: • Application owner userids are frozen. • Application startup is set up so that nobody needs to logon to the application owner userid itself, but startup of the application processes is via some other mechanism such as by use of Pathway owner settings, Netbatch initiated startup, progid processes or a third party tool that allows specified users to start authorized processes as a privileged userid. This requirement also has a component regarding network/firewall access. For this, a QSA will typically: • Check which ports are open on the system (for example, by running nmap scan) and whether or not firewalls prevent unauthorized access to the system from within the network. • Check open ports to see if it is possible to access the system through the port using an application userid, without authenticating, to access cardholder data.
8.8	8.8	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 9 of PCI DSS states:

> *Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.*

REQUIREMENT DESCRIPTION

Requirement 9 predominantly deals with the physical security required for systems and for media containing cardholder data. HPE NonStop servers are typically stored in an organization facility that may house other system or network components used by the organization. As such, policies and procedures surrounding the facility are often not specific to the HPE NonStop server environment and are more likely to be a part of overall organization policies and procedures. While all requirements in this section must be met for an organization to be PCI DSS compliant, often it is the role of a different area of the organization to ensure that this is the case.

Areas that may apply specifically to the HPE NonStop server have been detailed where relevant.

SYSTEM CONSOLE PHYSICAL SECURITY

The system console should be physically secured as well as logically secured, such as by being locked in a cabinet. If somebody is able, for example, to attach a keystroke logging hardware device, it is quite likely that it is just a matter of time before they will be able to capture SUPER.SUPER or other privileged userid's password information giving them unauthorized privileged powers on the HPE NonStop server.

Note that many organizations now access the system console via Remote Desktop Protocol (RDP) or similar remote access technology. Appropriate measures must be taken to ensure that any such sessions are encrypted as per requirement 2.3. If consoles are accessed in this way, access to them must be controlled by Multi-Factor Authentication in accordance with requirement 8.3.1.

REMOVABLE MEDIA

A large part of this requirement refers to removable media that contains cardholder data. When considering what is required to satisfy this requirement, consideration should be given to tapes and other removable media containing not only database backups, but also backups of system or application trace files, saveabend files, CPU dumps, TMF dumps and so on.

A number of Independent Software Vendor Products provide the ability to encrypt backup or TMF operations. See the section on Protecting Backup Data.

CLEARONPURGE PARAMETER

The file attribute CLEARONPURGE should be set on any cardholder data files. When a database file/table is purged or dropped from a database with the CLEARONPURGE option set, the data on the disk space is overwritten with zeroes to physically destroy the data space.

CLEARONPURGE increases security for sensitive data or programs. It should be noted that the time for deletion of the file will be increased with this attribute set. ISV product Greenhouse DiskWipe can securely "clean up" empty disk space when files have been deleted. The OSM also has disk wiping capabilities that can be used for cleaning disks when they are to be removed from the system, for example when a system is being decommissioned.

When disks are physically removed from the system, they need to be securely destroyed unless all data has been securely erased.

Obsolete tape media needs to be physically destroyed.

THE REQUIREMENT - 9

PCI DSS Requirement	Testing Procedure	Remark
9.1	9.1	For this requirement, a QSA will typically observe that the appropriate security requirements are in place. This will normally involve a visit to the data center and an examination of the security implemented for the datacenter itself, the HPE NonStop server, the console, network connections and any other relevant components. See System Console Physical Security for further information.
9.1.1	9.1.1.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	9.1.1.b	
	9.1.1.c	
9.1.2	9.1.2	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
9.1.3	9.1.3	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
9.2	9.2.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	9.2.b	
	9.2.c	
9.3	9.3.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	9.3.b	
	9.3.c	
9.4	9.4	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
9.4.1	9.4.1.a	
	9.4.1.b	
9.4.2	9.4.2.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	9.4.2.b	
9.4.3	9.4.3	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
9.4 .4	9.4.4.a	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	9.4.4.b	

PCI DSS Requirement	Testing Procedure	Remark
9.5	9.5	A document must exist that describes the policies and procedures for physically securing backup media. This should include backup tapes, DVDs, CDs, TMF media and so on. For this requirement, a QSA will typically: • Review the documentation to ensure that the procedure specified in the requirement is adequately documented. See Removable Media for further information.
9.5.1	9.5.1	A document must exist that describes the policies and procedures for storing backup media. This should include backup tapes, DVDs, CDs, TMF media and so on. For this requirement, a QSA will typically: • Examine evidence showing that the storage location is reviewed at least annually to ensure that the location is secure. See Removable Media for further information.
9.6	9.6	A document must exist that describes the policies and procedures for distribution of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on. For this requirement, a QSA will typically: • Review the documentation to ensure that the procedure specified in the requirement is adequately documented. • Applies to requirement 9.7.1 through 9.7.2 See Removable Media for further information.
9.6.1	9.6.1	A document must exist that describes the policies and procedures for classification of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on. For this requirement, a QSA will typically: • Review the documentation to ensure that the procedure specified in the requirement is adequately documented. See Removable Media for further information.

PCI DSS Requirement	Testing Procedure	Remark
9.6.2	9.6.2.a 9.6.2.b	For this requirement, a QSA will typically: • Interview personnel responsible for sending media outside the facility. • Examine documents showing the date and time that any media has been sent outside of the facility. • Ensure that all media movement entries have been authorized. • Examine courier documentation or other evidence proving that all media is sent via secured courier or other traceable delivery method. This should include movement of backup tapes, DVDs, CDs, TMF media and so on. See Removable Media for further information.
9.6.3	9.6.3	A document must exist that describes the policies and procedures for transferring backup media to offsite storage locations. This should include not only backup tapes, DVDs, CDs and so on, but also TMF media. For this requirement, a QSA will typically: • Examine the documentation to ensure that this requirement is covered. • Examine a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization See Removable Media for further information.
9.7 9.7.1	9.7 9.7.1	A document must exist that describes the storage and handling of backup media. This should include backup tapes, DVDs, CDs, TMF media and so on. For this requirement, a QSA will typically: • Examine the documentation to ensure that this requirement is covered. • Review the media inventory log to verify that periodic media inventories are performed at least annually. See Removable Media for further information.
9.8	9.8	A document must exist that describes the secure destruction of any media that contains cardholder data. This should include backup tapes, DVDs, CDs, TMF media, etc. For this requirement, a QSA will typically: • Examine the documentation to ensure that this requirement is covered. • Applies to requirement 9.10.1 through 9.10.2 See Removable Media for further information.
9.8.1	9.8.1.a 9.8.1.b	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.

PCI DSS Requirement	Testing Procedure	Remark
9.8.2	9.8.2	For this requirement, a QSA will typically request to see the following: • Evidence that the CLEARONPURGE attribute is set or used as part of purge operations. • Evidence of secure destruction of disks such as media movement documents, logs etc. • Evidence of secure destruction of obsolete/faulty backup media (including TMF media), faulty/obsolete hard disk that may contain any cardholder data. • A document that describes the secure destruction of any media that contains cardholder data. This should include physical disks, backup tapes, TMF media, DVDs, CDs and so on. See Clearonpurge Parameter for further information.
9.9	9.9	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
9.9.1	9.9.1.a	This requirement refers to Point Of Interaction devices such as PIN pads and as such is not applicable specifically to the HPE NonStop server.
	9.9.1.b	
	9.9.1.c	
9.9.2	9.9.2.a	
	9.9.2.b	
9.9.3	9.9.3.a	
	9.9.3.b	
9.10	9.10	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

REQUIREMENT INTRODUCTION

The introduction for requirement 10 of PCI DSS states:

> *Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.*

REQUIREMENT DESCRIPTION

Requirement 10 deals with the necessity to maintain audit logs used to track actions and user activity performed on the system. It also covers what the logs must contain and how the logs should be protected to ensure that they are not tampered with in any way.

It is of limited value if logs are captured but never reviewed, so this requirement deals not only with the capturing of logs but also which type of system events need to be reviewed on a regular basis. PCI SSC has published a document called Information Supplement: Effective Daily Log Monitoring (https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf) that should be viewed for further details on best practices in how to go about setting up a structured approach for analyzing security logs.

NOTE: This requirement does not necessarily cover all types of audit logs and audit events that need to be captured. Most system administrator and DBA access will likely be covered by audit logs referred to in this section. All of the different log types referred to in the section Security Audit Logs should be taken into consideration.

A QSA will be able to assist in determining what type of events need to be captured if there are any additional to those described here due to the varied nature of environments.

ACCESS TO SYSTEM COMPONENTS

It is a part of this requirement to be able to determine what actions a user has performed while accessing the system. This is particularly important for users with elevated system or application privileges. Mechanisms must be in place to ensure that all access to the system can be associated with a specific individual and that these actions can be captured and reported upon.

Safeguard has the ability to capture user access to system objects such as files or devices, but does not have the ability to record exactly what actions a user has performed during a session. For example, if a user were to perform an action within SCF such as modifying the attributes of an object, Safeguard could be configured to provide information detailing that the user had executed the SCF program, but could not tell what the user did once they were inside of SCF.

A number of Independent Software Vendor Products provide the ability to capture user interactive sessions, making it possible to determine which actions a user has performed during any given session. Note that there are limitations with session capture software on the HPE NonStop platform. See the section on Session Capture for further details.

If generic userids are in use, a mechanism must be in place to ensure that all user sessions are accountable to a specific individual. See the sections on Two Step Authentication, Off Box Authentication and Role Based User Access.

INDIVIDUAL ACCESS TO CARDHOLDER DATA

All individual access to cardholder data must be recorded. This would typically be access occurring outside of the application, for example, copying the contents of a file using FUP. For this requirement to be satisfied, all Enscribe files and SQL/MP subvolumes containing cardholder data should be configured in Safeguard with appropriate audit settings. Where possible Safeguard protection of Enscribe files and SQL/MP should be configured at the subvolume level. Safeguard diskfile records should be added for Enscribe files that have differing security requirements to that configured at the subvolume level. SQL/MP tables cannot be individually protected at the Safeguard diskfile level. All relevant subvolume and diskfile protection records should be configured so that:

- AUDIT-ACCESS-PASS = ALL
- AUDIT-ACCESS-FAIL = ALL

WARNING! Depending on the nature of the application environment, a setting of AUDIT-ACCESS-PASS = ALL may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for all relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

Independent Software Vendor Products exist that can provide more granular audit for accessing system objects at the file level, such as only auditing access attempts made by non-specified programs.

[Consider XYGATE Object Security (XOS)]

Independent Software Vendor Products exist with the ability to audit access and any changes made to individual records within a file/table, providing application level auditing to existing applications, without the need for any application changes.

[Consider comForte SecurData, TANDsoft Sensitive Data Intercept (SDI)]

SQL/MX tables cannot be protected by Safeguard. This means that if cardholder data is stored in SQL/MX tables, another mechanism must be used to audit access to the tables.

Independent Software Vendor Products such as those indicated in the section on Role Based User Access could be used to audit all user access to SQL/MX tables via interactive MXCI sessions. Likewise, this software could potentially be used to audit interactive SQLCI sessions for SQL/MP access, and FUP, Enable, DBAccess and so on for access to Enscribe files.

RECORDING PRIVILEGED USER ACTIONS

A part of Requirement 10 is to capture all actions taken by any individual with administrative privileges. This would require capturing sessions for the SUPER.SUPER userid at a minimum but should include capture of sessions for all userids or aliases identified as privileged (see the section on Privileged Userids for more details). As described above, it is not possible for Safeguard to log all actions performed by users on the system.

See the section on Session Capture for details of how privileged user actions can be captured.

ACCESS TO AUDIT TRAILS

Unauthorized access attempts to security audit logs may indicate an attempt to tamper with logs or an attempt to see which activities have been recorded, so as to determine whether an action may be detected or not. Requirement 10 specifies that access attempts to security audit trails must be recorded and reported upon. Safeguard can be used to capture such access attempts. To configure Safeguard to capture this information, set the relevant Safeguard records for the Safeguard Audit Pool subvolume, other security software audit log subvolumes and application security related logfiles (for example BASE24 OMF data) so that:

- AUDIT-ACCESS-PASS = ALL
- AUDIT-ACCESS-FAIL = ALL

WARNING! A setting of AUDIT-ACCESS-PASS = ALL may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for all relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

FAILED LOGON ATTEMPTS

All failed logon attempts to the system by userids or aliases must be audited. To achieve this, configure Safeguard so that:

- AUDIT-AUTHENTICATE-FAIL= ALL

USERID MANAGEMENT ATTEMPTS

All creation, deletion and modification of userid or alias records must be audited. To achieve this, configure Safeguard so that:

- SUBJECT-MANAGE-PASS= ALL
- SUBJECT-MANAGE-FAIL= ALL

SECURITY MANAGEMENT EVENTS

If a user is able to manipulate the security subsystems or audit trails, they potentially could hide activities that have occurred on the system that would normally be captured by the security logs. If Safeguard were stopped, for example, not only would security of objects revert back to the Guardian level security, but system or object access attempts would not be logged. To ensure that such occurrences do not go undetected, Requirement 10 specifies that a number of critical events surrounding the security subsystems must be captured. Inherently, Safeguard satisfies the requirement by logging the following events:

- Starting and stopping of the Safeguard subsystem causes an event to be raised to the EMS subsystem and a record to be written to the Safeguard audit logs.
- Rollover or changing of Safeguard audit logs causes an event to be raised to the EMS subsystem and a record to be written to the Safeguard audit logs.

Initialization of audit logs and audit log rollover must be logged for any other security related audit logs (ISV security software logs).

SYSTEM LEVEL OBJECTS

Attempts to create and delete system level objects must be logged. For this requirement to be satisfied, all operating system subvolumes should be configured in Safeguard with appropriate audit settings

- AUDIT-ACCESS-PASS = ALL
- AUDIT-ACCESS-FAIL = ALL

WARNING! As described for requirement 10.2.1 above, a setting of AUDIT-ACCESS-PASS = ALL may add significant processing overhead to the system. With this setting, Safeguard will write an audit log event (actually 2 or 3 records) every time the object in question is opened. Implementation of this setting should be fully tested for relevant objects before being applied to a production environment to ensure that there is no significant impact to system or application performance.

OSS FILE AUDITING

To audit operations in the OSS environment such as MKDIR, CHMOD, CHOWN etc., Safeguard must be configured with the following setting:

- AUDIT-CLIENT-OSS

Note that for this parameter to take effect, the OSS filesets to be audited need to have the AUDITENABLED flag set to ON. In SCF:

- ALTER FILESET $ZPMON.<*file set*>, AUDITENABLED ON
  e.g. ALTER FILESET $ZPMON.ROOT, AUDITENABLED ON

Note also that this may cause a significant increase in Safeguard audit data. You should test thoroughly to determine performance impact before applying on a production machine and should also monitor the sizing of the Safeguard audit pool to ensure that audit logs do not rollover too quickly.

Independent Software Vendor Products exist that can audit access to OSS files and directories. [Consider XYGATE Object Security (XOS) which provides a much more granular logging capability than Safeguard as well as being able to secure OSS files.]

SYNCHRONIZATION OF SYSTEM TIME

The system time is logged as part of system or security related events and typically also as part of application related events. It may be difficult to ascertain what has occurred on the system at an exact time if the system clocks across various system or network components are different. Requirement 10 states that all system clocks must be synchronized.

HPE provides TIMESYNC software which enables the synchronization of the system clock on an HPE NonStop server with a time source on the network.

Given the typical applications running on an HPE NonStop server, it is not recommended for the HPE NonStop server to be connected to a time source outside of the organization’s corporate network. The network time should be obtained from a time source within the network.

ACCESS TO AUDIT LOGS

As the audit logs on the system provide the record of what has occurred on the system, it is imperative that they are protected and that access is monitored so as to detect any unauthorized access attempts. Such attempts may indicate a potential security breach.

A Safeguard subvolume record should be configured to protect the Safeguard audit pool from access to unauthorized persons. By default, SUPER.SUPER owns the Safeguard audit files and has full access. Other users that require access to the audit log files, such as security administrators who need to run security reports, should be configured with read only access to the Safeguard Audit Pool.

By default, most security software logs are owned by the user that the software runs under. This userid will need full access to the audit trails to be able to create logs, write to the logs etc. As such, this userid should be treated as a privileged userid on the system. Access requirements for security audit logs should be analyzed and Safeguard ACLs put in place providing read only access to relevant authorized users, such as security administrators, as for Safeguard.

As the access requirements for security audit trails are typically different to the access requirement to other files in the security software subvolumes (e.g. program executables, configuration files), the audit trails should be configured to be in separate dedicated subvolumes where possible.

No user other than SUPER.SUPER should have Write access to the Safeguard Audit Pool. No user other than the owner userid of other security software modules should have Write access to the security Audit Trails for that software. Relevant subvolumes should be controlled through the use of Safeguard subvolume records with appropriate ACL configuration. Likewise for any security related application audit trails, and so on.

STORAGE OF AUDIT LOGS

It is a requirement for security logs to be sent to a centralized audit log repository. This is typically a device or system on the network whose sole purpose is to collect security logs for storage and for running of reports and raising alerts.   Safeguard does not have the facility to write audit trail data to a centralized server.

XYGATE Merged Audit (XMA) can send audit trail data in real time from Safeguard, XYGATE, EMS, BASE24 and a number of other subsystems/applications to a centralized server , for example HPE ArcSight or RSA enVision®.

Other Independent Software Vendor Products exist that can send HPE NonStop security events off-box. [Consider comForte Safepoint KSL, CSP Alert-Plus]

AUDIT LOG RETENTION

Security policy documentation must include details of audit log retention. The time period specified must be a minimum of 12 months.

The audit trails to be kept should include those from Safeguard, any ISV software security logs, EMS logs (which contain events such as system time changes) and application related security logs.

It is advisable that security audit trails are monitored to ensure that they are not rolling over too quickly causing events to be overwritten prematurely. If Safeguard is sized incorrectly or if something goes wrong and unexpected events flood the Safeguard logs, it is possible that audit data could be lost when log files rollover, depending on how Safeguard audit management is configured. Likewise, audit logs from the other sources should be sized appropriately.

SECURITY REPORTS

The whole point of capturing the events that occur on the system is so that reports can be run to determine what has happened and when. Requirement 10 specifies how often particular security events need to be reviewed.

In the past, Safeguard did not come with a useful reporting tool, just the Safeguard Audit Reduction Tool (SAFEART) which is in essence a tool for dumping complete audit records and is not very user friendly (no GUI, no reporting by exception). XYGATE Merged Audit (XMA) (which comes as standard with the operating system) can be used to report and alert on events from Safeguard, EMS, XYGATE software modules, iTP Web Server, BASE24, log files from some ISV security software products and logs from a number of different payment applications. XMA also has the ability to raise alerts from these subsystems or ship the events off to a SIEM device such as HPE ArcSight.

Other Independent Software Vendor Products that report and/or alert on Safeguard and other security events are also available.

[Consider comForte Safepoint KSL, CSP Auditview]

Note that all other security related logs must also be regularly reported on and reviewed. These include logs from SSL, SSH and any other ISV product security related logs.

Details on log monitoring are available from PCI SSC in the *Information Supplement: Effective Daily Log Monitoring*[12].

[12] *PCI SSC Information Supplement: Effective Daily Log Monitoring https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf*

THE REQUIREMENT - 10

PCI DSS Requirement	Testing Procedure	Remark
10.1	10.1	For this requirement, a QSA will typically analyze the exact mechanism used for tracking user system activities and will typically want evidence of the following: • That Safeguard is running and fully operable. • That appropriate Safeguard audit settings are configured. That is, Safeguard globals or individual userids/aliases are set as follows ○ AUDIT-AUTHENTICATE-PASS = ALL • That appropriate auditing is turned on for any ISV security tools. • That application level security auditing is configured and operable. See Access to System Components for further information.
10.2	10.2	
10.2.1	10.2.1	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged e.g. sample log file). See Individual Access to Cardholder Data for further information.
10.2.2	10.2.2	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file). See Recording Privileged User Actions for further information.
10.2.3	10.2.3	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file). See Access to Audit Trails for further information.
10.2.4	10.2.4	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file).

PCI DSS Requirement	**Testing Procedure**	**Remark**
		See Failed Logon Attempts for further information.
10.2.5	10.2.5.a 10.2.5.b 10.2.5.c	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file). See Userid Management Attempts for further information.
10.2.6	10.2.6	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file). See Security Management Events for further information.
10.2.7	10.2.7	For this requirement, a QSA will typically require the following: • An interview to ask how the event is captured. • Evidence of the relevant configuration settings. • Evidence of the event being logged (e.g. sample log file). See System level Objects for further information.
10.3	10.3	

Requirement 10.3 describes what information must be captured in all security related events. Prior to the J06.15 version of the operating system, Safeguard did not satisfy all of the requirements for 10.3, as it did not include the session IP address in its audit records. In this case, a mechanism needs to be used to match the timestamp, terminal ID and/or logon userid with those recorded in other logs. For example SSH session connection audit logs can be matched with Safeguard logs to provide the session IP address.

Check that any other audit trails such as those listed in the section on Security Audit Logs also contain the required information.

Various Safeguard audit reports generated using SAFEART are provided as a sample for requirements 10.3.1 through 10.3.6 with comments indicating how each requirement is met. For information on reading Safeguard audit trails using SAFEART and for a description of the various Safeguard audit record fields, see the *HPE Safeguard Audit Services Manual* in the HPE NonStop Technical Library. While the SAFEART tool is not recommended by the authors for day to day reporting, due to the volume of information provided, it provides the complete Safeguard audit record so has been used here to provide examples.

PCI DSS Requirement	**Testing Procedure**	**Remark**
10.3.1 User identification.	10.3.1 Verify user identification is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows that the user who performed the logon operation was alias root-gs (alias of SUPER.SUPER) with a user number of 255,255 on the \KNIGHT1 system.

```
------------------------------------------------------------------------------------
Auditnumber              =FFFF02F21B08E068E857
TimeReported             =2014/05/16 22:06:45 TimeReceived                 =2014/05/16 22:06:45
Operation                =VerifyUser          Outcome                      =UserValid
ObjectType               =GuardianUser        Veracity                     =Tr
OwnerUsername            =SEC.SUPER           OwnerUsernumber              =254,255     OwnerIsRemote                =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255             SubjectSystemName            =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER         SubjectCreatorNumber         =255,255     SubjectSystemNumber          =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                                SubjectAuthlocName           =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                        SubjectAuthlocNumber         =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.LOGIN
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255             CreatorSystemName            =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER         CreatorCreatorNumber         =255,255     CreatorSystemNumber          =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                                 CreatorAuthlocName           =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                       CreatorAuthlocNumber         =254
GuarduserUserName        =                    GuarduserUserNumber          =255,255
UserAliasName            =root-gs                                                       UserPrivLogonOper            =False
UserCreatorNumber        =255,255             UserCreatorName              =SUPER.SUPER
UserCreatorIsAlias       =False               UserCreatorNodeNumber        =254
UserCreationTime         =2012/04/17 08:46:59
------------------------------------------------------------------------------------
```

PCI DSS Requirement	**Testing Procedure**	**Remark**
10.3.2 Type of event.	10.3.2 Verify type of event is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows that the operation performed was a Verifyuser operation performed on a Guardian user, that is, a user logging on to the system. Note that there are several types of authentication procedures used for "logging on" to an HPE NonStop server. These are logon, authenticate, verifyuser, privlogon.

```
-----------------------------------------------------------------------------------
Auditnumber              =FFFF02F21B08E068E857
TimeReported             =2014/05/16 22:06:45 TimeReceived                 =2014/05/16 22:06:45
Operation                =VerifyUser           Outcome                      =UserValid
ObjectType               =GuardianUser         Veracity                     =Tr
OwnerUsername            =SEC.SUPER            OwnerUsernumber              =254,255    OwnerIsRemote                =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255              SubjectSystemName            =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER          SubjectCreatorNumber         =255,255    SubjectSystemNumber          =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                               SubjectAuthlocName           =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                       SubjectAuthlocNumber         =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.LOGIN
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255              CreatorSystemName            =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER          CreatorCreatorNumber         =255,255    CreatorSystemNumber          =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                                CreatorAuthlocName           =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                      CreatorAuthlocNumber         =254
GuarduserUserName        =                     GuarduserUserNumber          =255,255
UserAliasName            =root-gs                                                      UserPrivLogonOper            =False
UserCreatorNumber        =255,255              UserCreatorName              =SUPER.SUPER
UserCreatorIsAlias       =False                UserCreatorNodeNumber        =254
UserCreationTime         =2012/04/17 08:46:59
-----------------------------------------------------------------------------------
```

PCI DSS Requirement	Testing Procedure	Remark
10.3.3 Date and time.	10.3.3 Verify date and time stamp is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows the time that the logon event was generated and the time that it was written to the log.

```
-----------------------------------------------------------------------------------
Auditnumber              =FFFF02F21B08E068E857
TimeReported             =2014/05/16 22:06:45 TimeReceived                 =2014/05/16 22:06:45
Operation                =VerifyUser          Outcome                      =UserValid
ObjectType               =GuardianUser        Veracity                     =Tr
OwnerUsername            =SEC.SUPER           OwnerUsernumber              =254,255    OwnerIsRemote                =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255             SubjectSystemName            =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER         SubjectCreatorNumber         =255,255    SubjectSystemNumber          =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                               SubjectAuthlocName           =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                       SubjectAuthlocNumber         =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.LOGIN
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255             CreatorSystemName            =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER         CreatorCreatorNumber         =255,255    CreatorSystemNumber          =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                                CreatorAuthlocName           =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                      CreatorAuthlocNumber         =254
GuarduserUserName        =                    GuarduserUserNumber          =255,255
UserAliasName            =root-gs                                                      UserPrivLogonOper            =False
UserCreatorNumber        =255,255             UserCreatorName              =SUPER.SUPER
UserCreatorIsAlias       =False               UserCreatorNodeNumber        =254
UserCreationTime         =2012/04/17 08:46:59
-----------------------------------------------------------------------------------
```

PCI DSS Requirement	**Testing Procedure**	**Remark**
10.3.4 Success or failure indication.	10.3.4 Verify success or failure indication is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows that the outcome of the operation was "UserValid". This is described in the HPE *Safeguard Audit Services Manual* as "the user was successfully authenticated".

```
-----------------------------------------------------------------------------------
Auditnumber              =FFFF02F21B08E068E857
TimeReported             =2014/05/16 22:06:45 TimeReceived                 =2014/05/16 22:06:45
Operation                =VerifyUser          Outcome                      =UserValid
ObjectType               =GuardianUser        Veracity                     =Tr
OwnerUsername            =SEC.SUPER           OwnerUsernumber              =254,255    OwnerIsRemote                =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255             SubjectSystemName            =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER         SubjectCreatorNumber         =255,255    SubjectSystemNumber          =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                               SubjectAuthlocName           =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                       SubjectAuthlocNumber         =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.LOGIN
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255             CreatorSystemName            =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER         CreatorCreatorNumber         =255,255    CreatorSystemNumber          =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                                CreatorAuthlocName           =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                      CreatorAuthlocNumber         =254
GuarduserUserName        =                    GuarduserUserNumber          =255,255
UserAliasName            =root-gs                                                      UserPrivLogonOper            =False
UserCreatorNumber        =255,255             UserCreatorName              =SUPER.SUPER
UserCreatorIsAlias       =False               UserCreatorNodeNumber        =254
UserCreationTime         =2012/04/17 08:46:59
-----------------------------------------------------------------------------------
```

PCI DSS Requirement	Testing Procedure	Remark
10.3.5 Origination of event.	10.3.5 Verify origination of event is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows that the IP Address of the user session was 10.21.5.12. This is contained in a secondary record for the event.

It should be noted that some SSL/TLS/SSH proxies return the IP Address of 127.0.0.1 so it may be necessary to match up user sessions in those logs with the corresponding Safeguard logon records using the terminal name. See the section on Session Encryption for details.

```
-----------------------------------------------------------------------------------
Auditnumber              =FFFF02F21B08E068E857
TimeReported             =2014/05/16 22:06:45 TimeReceived                 =2014/05/16 22:06:45
Operation                =VerifyUser          Outcome                      =UserValid
ObjectType               =GuardianUser        Veracity                     =Tr
OwnerUsername            =SEC.SUPER           OwnerUsernumber              =254,255    OwnerIsRemote                =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255             SubjectSystemName            =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER         SubjectCreatorNumber         =255,255    SubjectSystemNumber          =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                               SubjectAuthlocName           =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                       SubjectAuthlocNumber         =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.LOGIN
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255             CreatorSystemName            =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER         CreatorCreatorNumber         =255,255    CreatorSystemNumber          =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                                CreatorAuthlocName           =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                      CreatorAuthlocNumber         =254
GuarduserUserName        =                    GuarduserUserNumber          =255,255
UserAliasName            =root-gs                                                      UserPrivLogonOper            =False
UserCreatorNumber        =255,255             UserCreatorName              =SUPER.SUPER
UserCreatorIsAlias       =False               UserCreatorNodeNumber        =254
UserCreationTime         =2012/04/17 08:46:59
-----------------------------------------------------------------------------------
SecondaryAuditnumber         =FFFF02F21B08E068E857
SecondaryTimeReported        =2014/05/16 22:06:45 SecondaryTimeReceived        =2014/05/16 22:06:45
SecondaryVeracity            =Tr                  SecondaryRecordType          =Other
SecondaryTextAreaType        =ClientIPAddress
IpAddress                    =10.21.5.12
```

PCI DSS Requirement	Testing Procedure	Remark
10.3.6 Identity or name of affected data, system component, or resource.	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.	For this requirement, a QSA will typically: • Examine evidence in the form of audit event logs or samples.

The example below shows that the file $DATA1.GREG.TESTFILE was created by the userid SUPER.SUPER.

```
-----------------------------------------------------------------------------------
Auditnumber              =000002F1D448178701DF
TimeReported             =2014/05/16 22:13:35 TimeReceived             =2014/05/16 22:13:35
Operation                =Create              Outcome                  =Granted
ObjectType               =Diskfile            Veracity                 =Tr
OwnerUsername            =SEC.SUPER           OwnerUsernumber          =254,255    OwnerIsRemote              =Local
SubjectUserName          =SUPER.SUPER
SubjectUserNumber        =255,255             SubjectSystemName        =\KNIGHT1
SubjectCreatorName       =SUPER.SUPER         SubjectCreatorNumber     =255,255    SubjectSystemNumber        =254
SubjectProcessName       =\KNIGHT1.$X1V1Y                                           SubjectAuthlocName         =\KNIGHT1
SubjectTerminalName      =\KNIGHT1.$ZTN0.#PTKBXMZ                                   SubjectAuthlocNumber       =254
SubjectProgramName       =\KNIGHT1.$SYSTEM.SYS03.TACL
CreatorUserName          =SUPER.SUPER
CreatorUserNumber        =255,255             CreatorSystemName        =\KNIGHT1
CreatorCreatorName       =SUPER.SUPER         CreatorCreatorNumber     =255,255    CreatorSystemNumber        =254
CreatorProcessName       =\KNIGHT1.$ZSMP                                            CreatorAuthlocName         =\KNIGHT1
CreatorTerminalName      =\KNIGHT1.$ZTNP1.#PTUTDDA                                  CreatorAuthlocNumber       =254
ObjectName               =$DATA1.GREG.TESTFILE

SecondaryAuditnumber     =000002F1D448178701DF
SecondaryTimeReported    =2014/05/16 22:13:35 SecondaryTimeReceived    =2014/05/16 22:13:35
SecondaryVeracity        =Tr                  SecondaryRecordType      =Other
SecondaryTextAreaType    =PatternSearch
PatternTSStart           =2014/05/16 22:13:35 PatternTSEnd             =2014/05/16 22:13:35
PatternNumSearch         =1
PatternAuthzMethod       =NormalFirst         PatternReductionLevel    =Initial
PatternAuthzResult       =NoRecord
PatternAuthzSpec         =
-----------------------------------------------------------------------------------
```

PCI DSS Requirement	Testing Procedure	Remark
10.4	10.4	For this requirement, a QSA will typically want to see evidence that an automated time Synchronization mechanism such as TIMESYNC (from HP) is running on the system and that it is documented. They will likely want to see evidence of the configuration to confirm that it is set appropriately and that it is configured as described in the documentation. Typical configuration items that a QSA may look for are: • The TCP/IP process that the time synchronization process communicates through. • The name and IP address of the NTP time server used for time synchronization. The QSA will also likely want to see evidence of a successful synchronization of the system time, for example, from an event log. This should indicate the time that the synchronization took place and the time difference before the reset. HPE Timesync writes such events to EMS. See Synchronization of System Time for further information.
10.4.1	10.4.1.a 10.4.1.b	This requirement is not typically applicable to the HPE NonStop server. It refers to central time servers.
10.4.2	10.4.2.a	For this requirement, a QSA will typically: • Verify configuration and operation of utilities such as TIMESYNC to ensure that only authorized users can change the system time.
	10.4.2.b	For this requirement, a QSA will typically: • Check logs to ensure that any system time changes are recorded., monitored and reviewed. TIMESYNC logs both to EMS and to its own dedicated logs.
10.4.3	10.4.3	This requirement is not specific to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement. See Synchronization of System Time for further information.
10.5	10.5	This requirement applies to the central log server. Storing logs locally is likely to fail this requirement. Logs that are initially written to disk on the HPE NonStop server e.g. Safeguard, some ISV security software audit trails, application security audit trails (for example BASE24 OMF audit data) need to satisfy requirements 10.5.1 to 10.5.5 also. These logs should be sent as quickly as technically possible to the central log server using a tool such as XMA. See Access to audit logs for further information.
10.5.1	10.5.1	This requirement applies to the central log server. Storing logs locally is likely to fail this requirement. However, for log files that are written to the HPE NonStop prior to transmission to a central log server (via XMA or similar mechanism), a QSA will typically: • Examine Safeguard records that protect the relevant audit trail subvolumes to ensure that they are satisfactory. See Access to audit logs for further information.

PCI DSS Requirement	**Testing Procedure**	**Remark**
10.5.2	10.5.2	This requirement applies to the central log server. Storing logs locally is likely to fail this requirement. However, for log files that are written to the HPE NonStop prior to transmission to a central log server (via XMA or similar mechanism), a QSA will typically: • Interview relevant personnel to discover how audit trails are protected. • Examine Safeguard records that protect the relevant audit trail subvolumes to ensure that they are satisfactory. See Access to audit logs for further information.
10.5.3	10.5.3	This requirement applies to the central log server. Storing logs locally is likely to fail this requirement. However, for log files that are written to the HPE NonStop prior to transmission to a central log server (via XMA or similar mechanism), a QSA will typically: • Interview relevant personnel to discover the process for satisfying the requirement. • Examine the configuration to ensure that the mechanism has been implemented as stated. • Observe sample audit trail data being written to a centralized server. See Storage of Audit Logs for further information.
10.5.4	10.5.4	This requirement is only relevant if the HPE NonStop server is running a web server from within the DMZ of the organizational network. This is not a typical role for an HPE NonStop server and so this requirement is typically not applicable.
10.5.5	10.5.5	This requirement applies to the central log server. Storing logs locally is likely to fail this requirement. However, for log files that are written to the HPE NonStop prior to transmission to a central log server (via XMA or similar mechanism), a QSA will typically: • Ask for a description of what mechanism is in use to ensure the integrity of the security audit trail. • Require a demonstration of the mechanism used to ensure the integrity of the security audit trail. • Examine evidence of the configuration settings used to fulfill this requirement. See Storage of Audit Logs for further information.
10.6	10.6	This requirement is a procedural item not specific to the HPE NonStop Server. See Security Reports for further information. See Template for ROC for details on what a QSA will require for this requirement. See the PCI SSC Information Supplement: Effective Daily Log Monitoring (*https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf*) for further details.
10.6.1	10.6.1.a	
	10.6.1.b	
10.6.2	10.6.2.a	
	10.6.2.b	
10.6.3	10.6.3.a	
	10.6.3.b	
10.7	10.7.a	This requirement is a procedural item not specific to the HPE NonStop Server.

PCI DSS Requirement	Testing Procedure	Remark
	10.7.b 10.7.c	See Template for ROC for details on what a QSA will require for this requirement. See Audit Log Retention for further information.
10.8	10.8	This requirement applies specifically to service providers who host and manage payment systems on behalf of other organizations but it is a best practice recommendation for all organizations as it provides a sound guideline for the timely detection and reporting of any potential security breaches. Organizations who process payment card data should be not only trying to achieve compliance, but making their systems as secure as they possibly can, so should look to implement this recommendation even though it may not be required for compliance.
10.8.1	10.8.1.a 10.8.1.b	This requirement is not typically applicable to the HPE NonStop server. It refers to central time servers.
10.9	10.9	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

REQUIREMENT INTRODUCTION

The introduction for requirement 11 of PCI DSS states:

> *Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.*

REQUIREMENT DESCRIPTION

It is imperative to ensure that what is running on the system is what should be running on the system. Requirement 11 deals with the need for monitoring and regular testing against vulnerabilities so as to ensure the integrity of the system and application.

FILE INTEGRITY MONITORING

Part of this requirement is to ensure that there are no unauthorized changes to critical files on the system. This means that such files need to be monitored for any change by use of a File Integrity Monitor.

For suggestions of file types to include as monitored "critical files", see the file types listed under requirement 7.2.3.

A number of Independent Software Vendor Products provide the ability to perform File Integrity Monitoring, some in real time and some in batch.

[Consider Integrity Detective, CSP File Integrity Checker, XYGATE Compliance PRO (XSW)]

REVIEW OF SECURITY CONFIGURATION

All security related configuration should be periodically reviewed to ensure that as the operational, system or application environment, procedures or work practices change, any alternate required settings can be configured accordingly. This does not apply only to Safeguard or dedicated security subsystems such as SSH, SSL, XYGATE etc. All typical configuration vulnerabilities should be examined to ensure that no gaps in security exist or have emerged. This is particularly pertinent to areas of the system that if not configured correctly would allow a user to potentially gain unauthorized privileged user access, such as the Netbatch, Pathway, Spooler or TACL environments etc. This task should be performed by personnel who are not also responsible for managing the security of the system, so as to ensure separation of duties.

Contact Knightcraft Technology or see the Knightcraft website to learn how we can help review your security related configuration.

See http://www.knightcraft.com/common-hp-nonstop-security-hacks-and-how-to-avoid-them and http://www.knightcraft.com/2014-hp-nonstop-advanced-technical-boot-camp for some further information that will assist in ensuring that your HPE NonStop systems are secured appropriately.

THE REQUIREMENT - 11

PCI DSS Requirement	Testing Procedure	Remark
11.1	11.1.a	This requirement is generally not applicable to the HPE NonStop server. Requirements related to wireless access points are typically the responsibility of networking personnel within the organization.
	11.1.b	
	11.1.c	
	11.1.d	
11.1.1	11.1.1	
11.1.2	11.1.2.a	
	11.1.2.b	
11.2	11.2	As well as traditional port scans, security configuration should be independently reviewed to ensure that no known security gaps exist. See the section on Review of Security Configuration.
11.2.1	11.2.1.a	HPE NonStop Servers must be included in any internal vulnerability scans. See Template for ROC for details on what a QSA will require for this requirement.
	11.2.1.b	
	11.2.1.c	This requirement applies to both internal and external vulnerability scans. As such it applies to ports on all TCP/IP subnets configured on the HPE NonStop server. For this requirement, a QSA will typically: • Examine documentation that covers the requirement. • Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation. • Confirm that testing was performed by a qualified internal resource (independent) or a qualified external 3rd party. The QSA will question the qualification of the tester if they feel it is required.
11.2.2	11.2.2.a	HPE NonStop Servers must be included in any external vulnerability scans. See Template for ROC for details on what a QSA will require for this requirement.
	11.2.2.b	
	11.2.2.c	An external network vulnerability scan is a scan of ports on public facing IP addresses and needs to be performed by an Approved Scanning Vendor (ASV). This scan will include access to any public facing IP interface (i.e. configured TCP/IP subnets) on the HPE NonStop server. For this requirement, a QSA will typically: • Examine documentation that covers the requirement.

PCI DSS Requirement	**Testing Procedure**	**Remark**
		• Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation. • Examine dated scan results (clean scan results) to see that the scan has been performed at least every quarter.
11.2.3	11.2.3.a	HPE NonStop Servers must be included in any internal and external scans following a significant change. See Template for ROC for details on what a QSA will require for this requirement.
	11.2.3.b	
	11.2.3.c	This requirement applies to both internal and external vulnerability scans. As such it applies to ports on all TCP/IP subnets configured on the HPE NonStop server. For this requirement, a QSA will typically: • Examine documentation that covers the requirement. • Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation. • Confirm that testing was performed by a qualified internal resource (independent) or a qualified external 3rd party. The QSA will question the qualification of the tester if they feel it is required.
11.3	11.3	This requirement applies to both internal and external penetration testing. As such it applies to any subsystem on the HPE NonStop server that may potentially allow unauthorized access. This includes any potential vulnerability within the HPE NonStop, such as communications ports as well as application level or system configuration vulnerabilities. Testing should be performed after any significant change in the network, operating system, application, security subsystems (including ISV security products). e.g. rolling out new version of the OS, installation of SPRs, adding new software etc. Segmentation controls MUST be tested as part of penetration tests. Testing should include the following components: • Management LAN (for example the ability to remote desktop to the console from unauthorized locations). • Expand network (for example how is segregation between production systems and test/development systems controlled? E.g. NOPASSTHROUGH param, remote passwords etc.) • Configuration of subsystems such as Pathway, Netbatch, Spooler, TACL environment etc. See Review of Security Configuration for further details. For this requirement, a QSA will typically: • Examine documentation that covers the requirement. • Interview security personnel to see how the requirement is met and to confirm that the methods used align with the documentation. • Confirm that testing was performed by a qualified internal resource (independent) or a qualified external 3rd party. The QSA will question the qualification of the tester if they feel it is required. See Template for ROC for full details on what a QSA will require for this requirement.

PCI DSS Requirement	**Testing Procedure**	**Remark**
11.3.1	11.3.1.a 11.3.1.b	This requirement applies to external penetration testing. Typically this will not apply to the HPE NonStop server in isolation but as there may be links or access to the HPE NonStop from other external facing servers, this needs to be taken into consideration. See Template for ROC for details on what a QSA will require for this requirement.
11.3.2	11.3.2.a 11.3.2.b	This requirement applies to internal penetration testing performed as per requirement 11.3 and in essence is an examination of the evidence to show that the required testing has taken place as documented. See Template for ROC for details on what a QSA will require for this requirement.
11.3.3	11.3.3	This requirement is to ensure that any vulnerabilities detected in the testing associated with requirement 11.3 have been appropriately remedied. See Template for ROC for details on what a QSA will require for this requirement.
11.3.4	11.3.4.a 11.3.4.b 11.3.4.c	This requirement will be relevant in cases where nodes that are not part of the Cardholder Data Environment are connected to those that are e.g. where development or test systems are connected to production systems by Expand. Note that segmentation means complete isolation (e.g. nodes not connected at all by Expand), it does NOT mean controlled access (e.g. userid access controlled by use of remotepasswords). See Template for ROC for details on what a QSA will require for this requirement.
11.3.4.1	11.3.4.1.a 11.3.4.1.b	This requirement is essentially the same as requirement 11.3.4 except that it applies specifically to service providers. See Template for ROC for details on what a QSA will require for this requirement.
11.4	11.4.a 11.4.b 11.4.c	This requirement is generally not applicable to the HPE NonStop server. Requirements related to intrusion-detection or intrusion-prevention systems are typically the responsibility of networking personnel within the organization.
11.5	11.5.a 11.5.b	See Template for ROC for details on what a QSA will require for this requirement. See File Integrity Monitoring for further information.
11.5.1	11.5.1	
11.6	11.6	This requirement is not specific to the HPE NonStop server. In essence it means that all items and associated procedures identified as part of the sub-requirements above have been fully documented and that the associated documentation is kept up to date and is used actively by personnel where relevant. See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

REQUIREMENT INTRODUCTION

The introduction for requirement 12 of PCI DSS states:

> *A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.*

REQUIREMENT DESCRIPTION

The requirements in this section are all in regards to documentation. In reality, this section is the ideal place to start the process of approaching PCI DSS compliance. As all aspects of configuration, policies and procedures contained in the other 11 requirements need to be documented, starting with this section may help provide an overview of what is required for the organization to comply with PCI DSS.

A large number of the requirements in this section will typically be related to the policies and procedures of the organization in general. Some may apply specifically to the HPE NonStop server environment. This will vary from one organization to another depending on individual business practices and circumstances.

For all requirements listed in this section, a QSA will typically:

- Review the documentation and ensure that the required information is included
- Observe processes and procedures to ensure that they are followed as specified in the documentation.
- In some cases, a QSA will also interview relevant personnel to ascertain further information or to confirm that the processes and procedures are followed as documented.

All PCI DSS requirements for this section of the specification are listed for the sake of completeness. For requirements where there is more likely to be specific relevance to the HPE NonStop server environment, notes and recommendations have been included.

Knightcraft Technology can assist with PCI DSS required documentation. Please see http://www.knightcraft.com to see how we can assist you with your compliance and NonStop security requirements.

THE REQUIREMENT - 12

PCI DSS Requirement	Testing Procedure	Remark
12.1	12.1	This requirement is not applicable specifically to the HPE NonStop server and should be implemented by the relevant personnel within the organization.
12.1.1	12.1.1	For this requirement, a QSA will typically: • Review documentation to ensure that the document history shows that version updates have occurred in the past 12 months. • Examine documentation to ensure that it includes changes that have occurred in the previous 12 months.
12.2	12.2.a	Note that HPE NonStop Servers are included in the scope of this requirement. See Template for ROC for details on what a QSA will require for this requirement. See the PCI SSC paper on risk assessment for more information. https://www.pcisecuritystandards.org/documents/PCI_DSS_v2_Risk_Assmt_Guidelines.pdf
	12.2.b	
12.3	12.3	
12.3.1	12.3.1	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.3.2	12.3.2	
12.3.3	12.3.3	
12.3.4	12.3.4	
12.3.5	12.3.5	
12.3.6	12.3.6	
12.3.7	12.3.7	
12.3.8	12.3.8.a	Automatic disconnect should be configured for the HPE NonStop server as described under requirement 8.5.15. The mechanism used should be fully documented.
	12.3.8.b	
12.3.9	12.3.9	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.3.10	12.3.10.a	
	12.3.10.b	
12.4		

PCI DSS Requirement	Testing Procedure	Remark
12.4.1	12.4.1	This requirement, which is not applicable specifically to the HPE NonStop server, applies to service providers, such as those who host computing services for organizations that process card payments. The purpose is to ensure that somebody within the service provider organization is ultimately accountable for the PCI DSS compliance of the environments that they host. See Template for ROC for details on what a QSA will require for this requirement.
12.5	12.5	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.5.1	12.5.1	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.5.2	12.5.2	The mechanism used and the processes for analyzing alerts/reports must be fully documented. The documentation must include: • The delivery mechanism of alerts/events • Personnel responsible for analyzing alerts/reports XYGATE Merged Audit (XMA) provides the ability to send alerts based on security events from Safeguard, EMS, BASE24, XYGATE and a number of other sources to SIEM devices such as HPE ArcSight or RSA enVision. Reports on events from these subsystems can also be obtained via XMA.
12.5.3	12.5.3	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.5.4	12.5.4	
12.5.5	12.5.5	
12.6	12.6.a	
	12.6.b	
12.6.1	12.6.1.a	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	12.6.1.b	
	12.6.1.c	
12.6.2	12.6.2	
12.7	12.7	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.8	12.8	
12.8.1	12.8.1	This requirement refers to HPE and any other organization that provides services such as copying or translating of media, secure destruction of media, vendor support with system access etc.
12.8.2	12.8.2	

PCI DSS Requirement	Testing Procedure	Remark
12.8.3	12.8.3	It also includes any external organization that has remote access to the system. See Template for ROC for details on what a QSA will require for this requirement.
12.8.4	12.8.4	
12.8.5	12.8.5	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
12.9	12.9	This requirement will apply in situations where management of the HPE NonStop server has been outsourced to an external party such as HP. See Template for ROC for details on what a QSA will require for this requirement.
12.10	12.10	
12.10.1	12.10.1.a	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement.
	12.10.1.b	
12.10.2	12.10.2	
12.10.3	12.10.3	
12.10.4	12.10.4	
12.10.5	12.10.5	
12.10.6	12.10.6	
12.11	12.11.a	This requirement, which is not applicable specifically to the HPE NonStop server, applies to service providers, such as those who host computing services for organizations that process card payments. The purpose is to ensure that appropriate security and operational policies and procedures are being followed within the service provider organization and that documentation of these policies and procedures is kept up to date. See Template for ROC for details on what a QSA will require for this requirement.
	12.11.b	
12.11.1	12.11.1	

REQUIREMENT A1: ADDITIONAL PCI DSS REQUIREMENTS FOR SHARED HOSTING PROVIDERS

REQUIREMENT INTRODUCTION

The introduction for requirement A.1 of PCI DSS states:

> *As referenced in Requirement 12.8 and 12.9, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.*

REQUIREMENT DESCRIPTION

Requirement A.1 is only relevant if the HPE NonStop server is being used in a host-sharing environment for multiple clients, as per Requirement 2.6. That means that applications (that process, transmit or store cardholder data) for different customers are running on the same system. The requirements in this section are aimed at ensuring that each application environment is kept entirely separate.

SEGREGATION OF ENVIRONMENTS

The application environments for different customers must be kept entirely segregated. This means that each environment should be running under its own distinct userid and should be configured with its own customer application-specific subvolumes/directories and non-privileged userids/aliases. The following should be ensured at a minimum:

- No sharing of userids between the environments.
- Unique subvolumes for each environment with appropriate Safeguard protection in place to enforce access control and auditing.
- Unique directories for each OSS environment with strong access security applied.

RESOURCE ALLOCATION

One of the aims of this requirement is to ensure that no application environment negatively impacts on any other environment by using up all available resources. Certain protection is inherently provided by the HPE NonStop Server operating system due to its architecture. For example, non-shared memory space for processes, mechanism for reducing priority of looping processes and so on.

Use of a CMON, either custom written or from a software vendor, can help with allocation of resources by allocating specific CPUs for certain activities, restricting priority assignments and so on. [Consider XYGATE CMON (XCM)]

THE REQUIREMENT – A1

PCI DSS Requirement	**Testing Procedure**	**Remark**
A1.1	A1.1	
A1.1.1	A1.1.1	The application environments for different customers must be kept entirely segregated. This means that each should be running under its own distinct userid. See Segregation of Environments for further information.
A1.1.2	A1.1.2.a	For this requirement, a QSA will typically: • Interview security personnel so as to understand how they have ensured that none of the customer userids have access to any area of the system other than their own hosted environment. • Examine evidence of userid/alias access to the different environments to ensure that proper segregation is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases. See Segregation of Environments for further information.
	A1.1.2.b	For this requirement, a QSA will typically: • Interview security personnel so as to understand how they have ensured that customer userids have access to only their files, subvolumes and OSS directories. • Examine evidence of userid/alias access to the different environments to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases. See Segregation of Environments for further information.
	A1.1.2.c	For this requirement, a QSA will typically: • Interview security personnel so as to understand how they have ensured that customer userids do not have write access to system objects, for example $SYSTEM.SYSTEM, $SYSTEM.SYSnn and so on. • Examine evidence of userid/alias access to the system subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases. See Segregation of Environments for further information.
	A1.1.2.d	For this requirement, a QSA will typically:: • Interview security personnel so as to understand how they have ensured that customer userids can only read log entries associated with their specific customer application(s). • Examine evidence of userid/alias access to the log subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.

PCI DSS Requirement	**Testing Procedure**	**Remark**
		See Segregation of Environments for further information.
	A1.1.2.e	See Template for ROC for details on what a QSA will require for this requirement. See Segregation of Environments for further information.
A1.1.3	A1.1.3	For this requirement, a QSA will typically: • Interview security personnel so as to understand how they have ensured that each customer's audit data can only be read by the customer to whom it belongs. • Examine evidence of userid/alias access to the log subvolumes/directories to ensure that proper access restriction is in place. This may include an analysis of Safeguard access records, OSS directory/file security and relevant userids/aliases.
A1.1.4	A1.1.4	This typically applies to policies and procedures at the corporate level.

REQUIREMENT A2: ADDITIONAL PCI DSS REQUIREMENTS FOR ENTITIES USING SSL/EARLY TLS

REQUIREMENT INTRODUCTION

The introduction for requirement A2 of PCI DSS states:

> *Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits.*

REQUIREMENT DESCRIPTION

Requirement A2 addresses the need for organizations to migrate away from cryptographic protocols that are now known to be insecure. This includes SSL 3.0 and TLS 1.0 which are both known to be vulnerable to the POODLE exploit. Organizations should ensure that all software using the SSL/TLS mechanism contain the latest security patches and that the configuration is set to only allow secure cryptographic protocols.

SSL/TLS ENCRYPTION IN THE HPE NONSTOP SERVER ENVIRONMENT

SSL/TLS encryption is potentially used in a number of areas on an HPE NonStop server. These include the following:

- HPE NonStop SSL (comes with the NonStop OS Security Bundle).
- Session encryption software from ISVs such as CAIL, comForte, XYPRO that provide SSL/TLS encryption for sessions such as TACL, osh, FTPS etc.
- iTP secure web server.
- GUI based client/server applications.
- Data communications links such as ACI Ice-XS.
- Between system components.
- Virtual Tape Server.
- VTC
- Application based sessions including links to devices such as ATMs or EFTPOS terminals.

This is far from an exhaustive list. A full examination of the HPE NonStop operating environment should be performed to determine all implementations of SSL/TLS, whether the latest patches have been applied and whether the strongest possible encryption protocols are in use.

THE REQUIREMENT – A2

PCI DSS Requirement	**Testing Procedure**	**Remark**
A2.1	A2.1	See Template for ROC for details on what a QSA will require for this requirement.
A2.2	A2.2	See Template for ROC for details on what a QSA will require for this requirement.
A2.3	A2.3	See Template for ROC for details on what a QSA will require for this requirement.

REQUIREMENT A3: DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION (DESV)

REQUIREMENT INTRODUCTION

The introduction for requirement A3 of PCI DSS states:

> *This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Examples of entities that this Appendix could apply to include:*
>
> - *Those storing, processing, and/or transmitting large volumes of cardholder data,*
> - *Those providing aggregation points for cardholder data, or*
> - *Those that have suffered significant or repeated breaches of cardholder data.*
>
> *These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes, and increased validation and scoping consideration..*

REQUIREMENT DESCRIPTION

Requirement A3 provides extra requirements that a card scheme or acquirer may impose on an entity who they believe requires these extra measures. Typically this will be for an organization who has already experienced a breach or is found to be struggling in some way with achieving or maintaining compliance. If an organization becomes subject to this requirement, they should consult closely with their QSA to determine how they should best meet it.

THE REQUIREMENT – A3

PCI DSS Requirement	**Testing Procedure**	**Remark**
A3.1	A3.1.1 through A3.1.4	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement and discuss with your QSA.
A3.2	A3.2.1 through A3.2.6	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement and discuss with your QSA.
A3.3	A3.3.1 through A3.3.3	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement and discuss with your QSA.
A3.4	A3.4.1	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement and discuss with your QSA.
A3.5	A3.5.1	This requirement is not applicable specifically to the HPE NonStop server. See Template for ROC for details on what a QSA will require for this requirement and discuss with your QSA.

INDEPENDENT SOFTWARE VENDOR PRODUCTS

The products in this list represent products that are available from ISVs which may assist an organization in achieving PCI compliance. Due to the changing nature of features and product sets, no claim is made that this is a complete list. Product information in many cases has been obtained from the relevant ISV. Vendor claims about the functionality of their software should be scrutinized closely before committing to any purchase. It is recommended that organizations become familiar with the offerings of all vendors and evaluate software functionality fully or undertake a POC (Proof Of Concept) to ensure that it fits in with their specific needs. ISVs typically are happy for a customer to test out the software for a defined period (typically 30 to 60 days) on their own system prior to committing to a purchase.

For detailed information about a particular product or ISV in the list below, click on the corresponding hyperlink.

See the section on Evaluating Security Software Products in this document for assistance in evaluating software in relation to PCI DSS (i.e. some questions to ask vendors about their products that may help you choose the most suitable fit for your organization and specific circumstance).

Company	Product	Category	Description
4tech Software	Integrity Detective	File Integrity Monitoring	Monitors selected files (Guardian and OSS) and subsystems such as Netbatch, Pathway for any changes in real time and raises alerts if a change is detected. Able to send alerts “off box” in syslog format to a SIEM device. (Available from 4tech Software and comForte)
4tech Software	PANfinder	Locating Cardholder Data	Scans a system and identifies which files contain suspected PAN data. Able to send reports “off box” in syslog format. (Available from 4tech Software and comForte)
ACI Worldwide	ACI Enterprise Security Services: Application Firewall	Enhanced Security	Ensures that only authenticated and authorized users are able to access protected resources, regardless of how those resources are accessed, or what those resources consist of.
ACI Worldwide	ACI Enterprise Security Services: SSL	Session Encryption	Provides SSL and TLS capabilities on the HPE NonStop server. Provides both SSL Client and SSL Server functionality as well as SFTP support.
comForte 21	PANfinder	Locating Cardholder Data	Scans a system and identifies which files contain suspected PAN data. Able to send reports “off box” in syslog format.
comForte 21	Safepoint	Security Configuration Mgmt Security Configuration View Security Reporting ‘Off Box’ Auditing	Provides GUI based management of Safeguard and reporting/alerting of Safeguard security events.

Company	Product	Category	Description
		Alerting	
comForte 21	Safepoint KSL	Role Based User Access Session Capture	Provides the ability to capture and report on user sessions (keystroke logging).
comForte 21	SecurCS	Session Encryption	Provides SSL/TLS encryption for any Telnet, FTP, RSC, ODBC server application or any TCP/IP communication session. Also provides SSL/TLS encryption capabilities for Expand traffic. **Ships as a standard part of the HPE NonStop Operating System**.
comForte 21	SecurData	Protection of Cardholder Data Auditing	Provides a framework to make sensitive data like Primary Account Numbers (PANs) unreadable and to log access to such sensitive data. Uses intercept libraries so no programmatic changes are required to integrate tokenization or encryption into application. Available also from HPE as HPE NonStop Cf Data Security.
comForte 21	SecurFTP	Session Encryption	Provides SSL/TLS or SSH encryption to any FTP session. **Ships as a standard part of the HPE NonStop Operating System**.
comForte 21	SecurLib	Protection of Cardholder Data	An encryption library that can be used to encryption-enable applications, databases and communications using strong encryption algorithms.
comForte 21	SecurOS	Session Encryption	SecurOS is a bundle of the comForte security solutions which HPE has incorporated into its HPE NonStop Operating System H and J series. Includes SecurCS, SecurFTP, and SecurSH. **Ships as a standard part of the HPE NonStop Operating System**.
comForte 21	SecurPrint	Printing Encryption	Provides SSL/TLS plug-in for FASTTCP to encryption enable sending of print jobs to spoolers or printers.
comForte 21	SecurSH	Session Encryption	Provides SSH implementation for the HPE NonStop server.
comForte 21	SecurSSO	Multi-Factor Authentication Off Box Authentication	Single sign-on functionality for the NonStop platform using the Kerberos standard.
comForte 21	SecurTape	Protecting Backup Data	Provides software-based encryption to secure the data at rest on NonStop backup and TMF tapes.
comForte 21	SecurTN	Session Capture	Provides enhanced Telnet sessions with encryption and auditing.
CSP	CSP Alert-Plus	Alerting 'Off Box' Auditing	Provides real time alerting on security events from Safeguard and a number of other subsystems as well as ability to send events to a centralized SIEM device such as HPE Arcsight, RSA envision etc.
CSP	CSP Auditview	Security Reporting Alerting 'Off Box' Auditing	Provides ability to analyze, extract, and integrate important audit information captured by Safeguard, CSP PassPort, and other CSP products.
CSP	CSP Authenticator	Multi-Factor Authentication Off Box Authentication	RSA SecurID agent software for HPE NonStop servers.
CSP	CSP Protect X	Security Configuration Mgmt Security Configuration View Password Management	Provides GUI based Security Management, Safeguard Audit Reporting, Security Compliance Reporting and Intrusion Detection.
CSP	CSP Passport	Role Based User Access Session Capture Password Length and	Controls user access to programs and restricts the user to specific commands based upon their profile. Also provides password quality enforcement and auditing of user sessions (keystroke logging).

Company	Product	Category	Description
		Complexity	
CSP	CSP CRM	Compliance Monitoring File Integrity Monitoring	Provides a Windows-based method to establish, monitor and report on compliance with your information security policy and inbuilt PCI DSS compliance checks. Provides a built in File Integrity Monitor and customizable PCI DSS compliance reports.
CSP	CSP NIMS	Multi-Factor Authentication Off Box Authentication	LDAP User ID management system for NonStop systems, allowing NonStop systems to form part of the corporate identity management system.
CSP	CSP Netpass	Password Length and Complexity	A solution for both enforcing password quality and for managing passwords across multiple HPE NonStop system.
CSP	CSP File Integrity Checker	File Integrity Monitoring	A file integrity monitor that detects any changes to critical files and raises alerts.
ETI-NET	BackBox	Protecting Backup Data	Hardware based solution for managing and encrypting NonStop tapes/virtual tapes such as those containing backups or TMF audit dumps.
Greenhouse	BaReLib	Protecting Backup Data	DES based encryption for BACKUP and RESTORE
Greenhouse	CURIOUS	Security Configuration View	Provides a Safecom interface for auditors so that they can view all Safeguard configuration without the ability to change anything.
Greenhouse	DiskWipe	Data Protection	Erases the contents of disk volumes
Greenhouse	FTPSERV-E	Session Control	Library for standard FTPSERV providing security enhancements to FTP server including audit logging and user access restrictions.
Greenhouse	INSET	Protection of Cardholder Data	Set of functions to provide field level encryption for application data.
Greenhouse	LISTLIB	Session Control	Library for standard LISTNER that prevents the LISTNER from supporting a DoS attack. Available as shareware.
Greenhouse	MPWD	Session Control	Authentication and session control for dial-up ports and TCPIP Telnet ports.
Greenhouse	MyLogin	Single Sign On	Single sign-on functionality for MR-WIN6530 emulator.
Greenhouse	Object Integrity (OBI)	File Integrity Monitoring	A file integrity monitor that detects any changes to critical files and produces reports on any files that have changed.
Greenhouse	PRCOSEEP	Enhanced Security	Authorization SEEP that controls all program executions and can limit the number of processes on a 'by user' and/or 'by object' basis.
Greenhouse	Password Quality Process	Password Length and Complexity	Provides the ability to FREEZE configured users for a set duration after a defined number of failed logon attempts.
Greenhouse	PS-Shell (PATHWAY Server Security)	Role Based User Access Enhanced Security	Provides enhanced security for Pathway servers. Stops PATHMON from being re-configured by unauthorized users, PATHWAY programs from being executed by unauthorized users and PATHWAY servers from being called by unauthorized PATHSEND communication events.
Greenhouse	REPRIEVE	Authenticate Fail Freeze	Provides the ability to FREEZE configured users for a set duration after a defined number of failed logon attempts.
Greenhouse	SECOM	Role Based User Access Session Capture	Provides role based security functionality where users can run designated privileged commands from their own non-privileged userid. Captures and logs user sessions (keystroke logging).

Company	Product	Category	Description
HPE	SecureData (Voltage)	Protection of Cardholder Data	Encryption and tokenization product. Requires either comForte SecurData (HPE NonStop Cf Data Security) or XYGATE Data Protection (XDP) to be implemented on the NonStop platform.
TANDsoft	Sensitive Data Intercept (SDI)	Protection of Cardholder Data	Protects sensitive data at rest by intercepting NonStop database access calls, encrypting data written to disk, and decrypting data read from disk. Supports Enscribe and SQL/MP, both native and non-native applications. No program changes are required.
TANDsoft	SDI/Log	Auditing	Provides intelligent interception and logging of all access to sensitive data. SDI/Log does not require any application modifications, works with all NonStop programs and can be used by auditors for regulatory compliance.
XYPRO Technology	XYGATE Access Control (XAC)	Role Based User Access Session Capture	Allows the functional properties of one NSK userid to be allocated and controlled for another userid (i.e. role based security) while the user's inputs and outputs are fully audited. Includes the ability to capture user sessions (keystroke logging). (Available also from HP).
XYPRO Technology	XYGATE CMON (XCM)	Authentication Control	Full featured CMON process that acts as a control center for Command Interpreter and TACL process startups, logins and alter priorities. Via these three interfaces CMON balances the loads of the CPUs.
XYPRO Technology	XYGATE Data Protection (XDP)	Protection of Cardholder Data	Provides encryption for data using tokenization and/or Format Preserving Encryption (FPE) to avoid the need for database changes.
XYPRO Technology	XYGATE Host Encryption (XHE)	Session Encryption	Provides SSL/TLS encryption for any Telnet, FTP, RSC, ODBC server application or any TCP/IP communication session.
XYPRO Technology	XYGATE Key Manager (XKM)	Key Management	Software based encryption key management subsystem.
XYPRO Technology	XYGATE Merged Audit (XMA)	Security Reporting Alerting 'Off Box' Auditing	Provides a facility to combine Safeguard, XYGATE, BASE24 and selected EMS Audit trails into a single SQL Database. Also provides real-time alerting functionality and the ability to send selected or all events to an "off box" audit logging appliance or server. **Ships as a standard part of the HPE NonStop H and J series Operating System**.
XYPRO Technology	XYGATE Object Security (XOS)	Enhanced Security	Enables pattern-oriented security, using rules to reduce ACL counts and streamline security maintenance. Allows for access authorization based on criteria other than object name and has the ability to secure SQL/MP tables/views and OSS files and directories.
XYPRO Technology	XYGATE Password Quality (XPQ)	Password Length and Complexity Password Management	Provides enhanced password controls such as dictionary checks.
XYPRO Technology	XYGATE Secure Shell (XSH)	Session Encryption	Provides SSH implementation for the HPE NonStop server.
XYPRO Technology	XYGATE Safeguard Manager (XSM)	Security Configuration Mgmt Security Configuration View Password Management	Windows interface to streamline management of Safeguard globals, users/aliases and Object ACLs. Also operates in the OSS environment supporting OSS file/directory level security vectors and ACLs and provides security management for SQL/MX Objects.
XYPRO Technology	XYGATE Compliance PRO (XSW)	Compliance Monitoring Safeguard Configuration View File Integrity Monitoring	Provides a Windows-based method to establish, monitor and report on compliance with your information security policy, inbuilt PCI DSS compliance checks and Best Practices. Provides a built in File Integrity Monitor with alerting capabilities, customizable PCI DSS compliance reports and user access matrix.

Company	Product	Category	Description
			(Available also from HPE).
XYPRO Technology	XYGATE User Authentication (XUA)	Authenticate Fail Freeze Off Box Authentication	Delivers granular failed logon management, logon-specific audit reporting, logon control by IP address or requestor program and multi-factor authentication (RSA SecurID) to associate all system logons to a specific person. Ships as a standard part of the HPE NonStop Operating System with NB56000 (and newer) systems. On other system types, available for purchase from HP as part of the upgraded security bundle.

GLOSSARY

Term	Description
ASV	Approved Scanning Vendor – approved by PCI SSC. List on website.
Cardholder	Customer to whom a card is issued or individual authorized to use the card
Cardholder Data	Full magnetic stripe or the PAN plus any of the following: * Cardholder name * Expiration date * Service Code
Cardholder Data Environment	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment
Card Validation Value or Code	(1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. (2)The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic.
CAV	Card Authentication Value (JCB payment cards)
CVC	CVC Card Validation Code (MasterCard payment cards)
CVV	Card Verification Value (Visa and Discover payment cards)
CSC	Card Security Code (American Express)
CID	Card Identification Number (American Express and Discover payment cards)
CAV2	Card Authentication Value 2 (JCB payment cards)
CVC2	Card Validation Code 2 (MasterCard payment cards)

Term	Description
CVV2	Card Verification Value 2 (Visa payment cards)
Enscribe	The proprietary file system running on all HPE NonStop servers. Enscribe files are managed by the FUP utility.
Event Management Service (EMS)	The event subsystem for the HPE NonStop server where system and subsystem events can be collected and viewed.
Guardian	The proprietary operating system on which HPE NonStop servers run. Guardian offers basic file level security with no auditing capabilities.
Netbatch	The batch scheduler typically running on HPE NonStop servers. The Netbatch environment is managed by the BATCHCOM utility.
NonStop SQL	SQL subsystems for the HPE NonStop. Could be either SQL/MP or SQL/MX.
OSS	The POSIX flavor of the operating system that runs on the HPE NonStop server. The OSS subsystem needs to be specifically started for OSS to be running on a system.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PCI SSC	Payment Card Industry Security Standard Council
PCI DSS	Payment Card Industry Data Security Standard
Pathway	The requestor/server based application environment for the NonStop.
Pathcom	The interactive utility for managing Pathway environments.
QSA	Qualified Security Assessor approved by PCI SSC. Listed on the PCI SSC website.
SAD	See Sensitive Authentication Data
SAFEART	Safeguard Audit Reduction Tool used for viewing Safeguard audit records.
Safecom	Interactive utility for controlling and managing the Safeguard subsystem.
Safeguard	Security subsystem that provides increased and more flexible access control than Guardian security. Has the ability to provide auditing of object access attempts and attempts to manage security configuration. Used also for user/alias maintenance. Provided as a standard product with all NS and NB series HPE NonStop servers.
SCF	Subsystem Control Facility used for managing hardware and a variety of subsystems on the HPE NonStop server.
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction
SQL/MP	SQL implementation that runs on the HPE NonStop server. SQL/MP runs in the Guardian environment and is managed by the SQLCI interactive utility.
SQL/MX	SQL implementation based on the ANSI standard that runs on the HPE NonStop server. SQL/MX runs in the OSS environment and is controlled through the mxci utility.
Strong Cryptography	General term to indicate cryptography that is extremely resilient to cryptanalysis. That is, given the cryptographic method (algorithm or protocol), the cryptographic key or protected data is not exposed. The strength relies on the cryptographic key used. Effective size of the key should meet the minimum key size of comparable strengths recommendations.

Term	Description
System Components	Any network component, server, or application included in or connected to the cardholder data environment

For PCI SSC definitions of PCI DSS related terms, see the PCI DSS Glossary (https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3.pdf)

RESOURCES

Resource	Location
PCI SSC Website	https://www.pcisecuritystandards.org/index.shtml
PCI DSS Specification PCI DSS Template for ROC PCI DSS Summary Of Changes PCI DSS Supporting Documents	https://www.pcisecuritystandards.org/security_standards/documents.php
PCI DSS Glossary	https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf
PCI Data Storage Do's and Don'ts	https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf
PCI SSC Information Supplement: Effective Daily Log Monitoring	https://www.pcisecuritystandards.org/documents/Effective-Daily-Log-Monitoring-Guidance.pdf
Prioritized Approach for PCI DSS Version 3.2	https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf https://www.pcisecuritystandards.org/documents/Prioritized-Approach-v3_2.xlsx
HPE NonStop Security Hardening Guide	See HPE NonStop technical Library
HPE NonStop Security – HPE resource page	http://www.hpe.com/info/nonstop-security
HPE NonStop System Console Security best practices	http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4aa2-2863enw&404m=secure-erc
HPE NonStop Technical Library	http://www.hpe.com/info/nonstop-jdocs (J-series) http://www.hpe.com/info/nonstop-ldocs (L-series) http://www.hpe.com/info/nonstop-hdocs (H-series)
HPE NonStop server Security- A Practical Handbook, By XYPRO Technology Corporation (ISBN: 1-55558-314-8)	http://www.elsevier.com/wps/find/bookdescription.cws_home/701262/description#description
Securing HPE NonStop servers in an Open Systems World, By XYPRO Technology Corporation (ISBN: 1-55558-344-X)	http://www.elsevier.com/wps/find/bookdescription.cws_home/708269/description#description
Security Management Guide	See HPE NonStop technical Library
Safeguard Administrator's Manual	See HPE NonStop technical Library
Safeguard Reference Manual	See HPE NonStop technical Library

Resource	Location
Safeguard User's Guide	See HPE NonStop technical Library
Safeguard Audit Service Manual	See HPE NonStop technical Library
ISO 8583 Financial transaction card originated messages — Interchange message specifications	http://en.wikipedia.org/wiki/ISO_8583
OWASP Top 10	http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
OWASP Cryptographic Storage Cheat Sheet	http://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet
Knightcraft Technology Website	http://www.knightcraft.com/
UL Website	http://industries.ul.com/transaction-security
4tech Software Website	http://www.4techsoftware.com
comForte 21 Website	http://www.comforte.com
CSP Website	http://www.tandemsecurity.com/
Greenhouse Software Website	http://www.greenhouse.de/
Integrated Research	http://www.ir.com/
TANDsoft	http://www.tandsoft.com/default.html
XYPRO Technology Website	https://www.xypro.com/

ACKNOWLEDGEMENTS

The authors would like to thank the following individuals and organizations for their contributions in reviewing the document, for providing technical assistance or for general assistance in making this document possible.

- Mario Sist, Andrew Jamieson (UL)
- Simon Siebert
- Ian Salter
- Dan Lewis (4tech Software)
- Wendy Bartlett, Gary Bender (HPE)
- Andy Simpson, Thomas Burg (comForte 21 GmbH)
- Carl Weber (Greenhouse Software and Consulting)
- Morné Conradie (NSK Systems Services)
- Computer Security Products (CSP)
- Integrated Research
- TANDsoft
- Terri Hill, Scott Uroff (XYPRO Technology Corporation)