Technical white paper

HPE NonStop security overview

CONTENTS

Introduction 3
HPE NonStop security fundamentals 4
Groups and users 4
Access modes 4
Memory protection 4
Process ownership 5
On-platform security 5
Guardian 5
Safeguard 6
SQL 10
SQL/MP security 10
SQL/MX security 10
Additional on-platform security products 11
XYGATE Merged Audit 11
XYGATE User Authentication 11
XYGATE Access Control (optional product) 11
XYGATE Compliance PRO (optional product) 11
Other subsystems 12
HPE NonStop data in motion security 12
HPE NonStop SSH 12
SSL and TLS 13
IPSec (IP CLIMs only) 13
IPTables and IP6Tables (IP CLIMs only) 13
HPE NonStop data at rest security 14
HPE NonStop Volume Level Encryption 14
Data sanitization 14
Partner products 14
Conclusion 14
Resources 15
HPE NonStop security manuals and white papers available at HPE NonStop technical library 15
HPE NonStop security partners 15

Introduction

HPE NonStop servers have been designed from the ground up to be both available and scalable. These fundamental system design properties also form an excellent architecture for system security because they provide a clear separation of function, starting at the lowest levels of the system. This white paper provides an overview of the HPE NonStop system's security architecture and capabilities, which are the foundation for implementing your security policies.

Guardian security provides a two-level group/user model, authentication, basic user management, and authorization. **Safeguard**, which is also a part of the base HPE NonStop Operating System (HPE NonStop OS), adds flexible authentication, authorization, and audit services based on a subject/object access control model that allows you to appropriately restrict authenticated users' access to HPE NonStop Guardian system resources.

Safeguard supports both traditional Guardian user names and, for additional flexibility and accountability, user name aliases. Safeguard gives you a wide range of controls over user account configuration. Safeguard allows you to define appropriate access controls, including Access Control Lists (**ACLs**), for objects such as disk files, volumes, and subvolumes; devices such as printers, tape drives, and communications lines; and named and unnamed processes and subprocesses. Safeguard **audits** logon attempts, access to objects, and changes to their security settings. Its audit criteria can be tailored to provide the information required by your security policies. Its audit controls allow your security administrators to detect unauthorized system access, detect unauthorized security setting changes, discourage users from abusing their authorized power and verify that your policies are being followed.

As noted above, Safeguard is part of the base OS for all systems. HPE also offers several security products that it delivers as standard products for **commercial** (non-Telco) systems and optional products for **Telco** systems, and additional security products that are optional for all systems.

A standard product for commercial systems, XYGATE User Authentication (**XUA**), and an optional product, XYGATE Access Control (**XAC**), extend Safeguard's capabilities by introducing features such as integration with an enterprise's Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) environment, multi-factor authentication, keystroke logging and command-level and subcommand-level control.

Partners and customers can add custom extension modules to Safeguard by configuring them as Security Event Exit Processes (**SEEPs**) that participate in evaluating authentication, authorization, and password changes. XUA is an example of an authentication SEEP.

XAC controls command-level security rather than file-level security, and effectively front-ends command-level interfaces to the system and system utilities.

The POSIX-based element of the HPE NonStop OS, Open System Services (**OSS**), uses the POSIX security model as would be expected. Its tight integration into the HPE NonStop OS allows it to also leverage the underlying HPE NonStop security infrastructure.

HPE NonStop servers support multiple file systems and databases. **Enscribe** files are protected through Guardian security and, if present, Safeguard ACLs. **OSS** files and directories use the POSIX security model and, where present, POSIX-style OSS ACLs. HPE NonStop **SQL/MP** objects are protected through Guardian security and, if present, Safeguard ACLs. HPE NonStop **SQL/MX** follows the ANSI GRANT/REVOKE model.

You almost undoubtedly have corporate requirements to audit your systems' security events and monitor them through both alerts at the time of occurrence and reports. To meet this need, your new-system purchases of commercial systems include XYGATE Merged Audit (**XMA**), which greatly enhances Safeguard audit reporting capabilities with a GUI-based interface and a series of standard reports that are focused on managing exceptions and help you demonstrate compliance with security regulations such as the Payment Card Industry Data Security Standard (PCI DSS). XMA also can aggregate audit from multiple sources, issue configurable alerts based on reported security events, and export audit information to many types of Security Incident Event Management (SIEM) systems.

Your HPE NonStop systems must cooperate with other systems to protect sensitive data in transit—both user credentials such as user names and passwords and user data. HPE bundles support for Secure Shell (**SSH**) and Secure Socket Layer (**SSL**) with new HPE NonStop commercial system purchases. HPE NonStop SSH uses the SSHv2 protocol to protect data in transit. It includes support for Secure File Transfer Protocol (**SFTP**). HPE NonStop SSL encrypts data sent or received by servers over TCP/IP using Transport Layer Security (**TLS**). A number of HPE NonStop products have built-in TLS/SSL support, and you can use HPE NonStop SSL's proxy modes to provide protection for other TCP/IP-based subsystems. SSL and SSH libraries and the SFTP API are available as optional products. HPE NonStop networking infrastructure based on IP Cluster I/O Modules (CLIMs) also can be configured to use **IPSec** to protect data in transit.

The optional HPE NonStop Volume Level Encryption (**VLE**) product provides transparent AES-256-based encryption for your CLIM-attached SAS drives, HPE XP and XP7 arrays, and LTO-4 and newer-model LTO tapes. When you no longer need sensitive data on disk, you can overwrite it on a file basis using Safeguard's "clear-on-purge" option for Guardian files or the shred utility for OSS files. You also can use the data sanitization feature in Open System Management (OSM) to overwrite an entire disk drive.

A number of partner products contribute to the extensibility and flexibility of the HPE NonStop security ecosystem.

HPE NonStop security fundamentals

The HPE NonStop OS is modular in design and based on a process-and-message model, as you would expect for a distributed system architecture. Much of the OS functionality is implemented as system processes that communicate through interprocess messages. This architecture ensures that individual processes—both system and user—are isolated from each other by default.

Groups and users

The basic HPE NonStop user paradigm is that each user is a member of a specific **administrative group**. Each user has a name in the form <group>.<user>, which has an underlying numeric representation. Each group may have a single member who is designated as the **group manager** who has special privileges relative to other members of the group.

The HPE NonStop user model supports basic delegation of authority by designating a specific group of users, the SUPER group, as having partial administrative privileges. Members of this group may perform most day-to-day system operations. A few privileges are reserved for the manager of the SUPER group, **SUPER.SUPER**, which is analogous to the UNIX®/Linux® root user.

Access modes

The HPE NonStop security model has two modes: nonprivileged (**user**) and privileged (**kernel**). Applications run in user mode, and may invoke system functions only through a defined set of **callable** procedures. Callable procedures in turn invoke lower-level system services by invoking privileged (**priv**) procedures. Callable procedures, which themselves run in priv mode, validate their user-supplied parameters before performing any privileged functions. This validation includes bounds checks on all reference parameters to prevent overwriting either the stack marker or other parts of the priv stack. Most lower-level system software runs in priv mode.

An object file (binary) that contains any callable or priv procedures must be explicitly **licensed** by SUPER.SUPER in order to be run by any user other than SUPER.SUPER.

Memory protection

Code and data are kept in separate memory segments, and **statically-compiled code segments** are read-only. Execution of code from **normal data segments** is disallowed, limiting the impact of buffer-overflow-based exploits. **Dynamically-generated code segments**, e.g., for Java, are read/write.

Each process has separate user and priv stacks, with no user-level access to priv stack contents. Defined segments of a user process' address space can be used by priv code to store its private data, but they are hidden from view (and therefore inaccessible) when the code is running in user mode.

Access to other processes' data is restricted: data sharing must be explicitly invoked, is limited to a defined part of a process' virtual address space (a **segment**), and is subject to security checking.

Only SUPER.SUPER can debug priv code; an ordinary user cannot step into privileged code and hence cannot view or modify priv data and/or manipulate execution paths to circumvent security.

Process ownership

A program normally executes with the user ID, and therefore privileges, of the user that started it. Optionally, an application program owner or SUPER.SUPER can set the **PROGID** flag on an executable (object) file. If PROGID is set, normal execute access checks are made before running the program; however, if the checks succeed, the process runs under the user ID and privileges of the program file's owner instead of as the user that started it. This model allows an application to open files that are accessible to the program file's owner even when that access would be denied to the user running the program. The typical use case is an application functioning as a server process that is applying its own fine-grained access control to the file contents based on the identities of its clients.

On-platform security

Guardian security provides the basic building blocks for defining users and file access permissions. **Safeguard** security software augments Guardian security with flexible authentication, authorization, and audit services based on a subject/object access control model that allows you to appropriately restrict authenticated users' access to Guardian system resources. Optional products that extend Safeguard's capabilities are available from HPE as well as from HPE NonStop security partners, including plug-in SEEP modules that participate in Safeguard's authentication, password quality, or authorization decisions. Security in the Open System Services (**OSS**) environment shares Safeguard's user management capabilities while providing a UNIX-based authorization model. It also leverages Safeguard's audit management infrastructure to provide granular control over OSS auditing. Guardian and OSS audit are aggregated in the same set of log files.

Guardian

The HPE NonStop OS has a built-in security model for Guardian authentication and authorization.

Authentication

As was described earlier, each user is assigned to a specific administrative security group that in turn has an optional group manager having a degree of authority over its group members. One distinguished group, the SUPER group, has extra operational privileges. The manager of that group, whose user name is SUPER.SUPER, by default has total access to resources within the local system—analogous to the root user in a UNIX or Linux environment.

You can configure a number of global **user management** attributes. As an example, you can configure minimum and maximum password lengths, with support for up to 64-character passwords and pass phrases. You also establish password quality requirements, such as a minimum number of uppercase, lowercase, alpha, numeric, or special characters. User passwords are stored as hashes on disk, calculated using the HMAC-SHA256 algorithm.

Authorization

If you own an object such as a Guardian file, you can authorize access to it by configuring its **read, write, execute**, and **purge** access settings, sometimes referred to as its **Guardian security vector**. These controls are similar, but not identical, to UNIX file permissions. You may configure additional attributes, including running a program under the user ID of its owner and a "clear contents on purge" option for Guardian disk files to help protect your sensitive data. You also can give ownership of the file to another user.

Permissions are given to seven user types:

- User (owner)—local or remote
- User's group—local or remote
- All users—local or remote
- Super ID—local only

A user who exists on multiple HPE NonStop systems connected by an Expand network can create matching **remote passwords** between pairs of systems, which allow transparent remote access to system resources subject to the usual security checks.

The security model among networked (Expand-connected) HPE NonStop systems distinguishes between **locally-authenticated** and **remotely-authenticated** users. Security-related operations such as opening a file on a remote system require the user to have matching remote passwords in addition to appropriate access permissions. Remote passwords are distinct from the user's local password. Remote passwords are required for access to both Guardian and OSS objects.

Multiple HPE NonStop systems do not constitute a single security domain; the default paradigm is mutual suspicion. You can construct most aspects of a single security domain through appropriate user and access configuration and password management; however, there is no ability to configure a network-wide SUPER.SUPER user.

Safeguard

The Safeguard product builds on Guardian standard security, adding more flexible user naming through support for **user aliases**, extensive user management, and much more granular access control to objects, and auditing. Safeguard is a standard product for HPE NonStop L-series, J-series, and H-series systems. Safeguard must be explicitly started and configured in order to take advantage of its capabilities.

Authentication

Safeguard supports both traditional Guardian users and, for additional flexibility and accountability, user aliases. Each user alias is linked to an underlying Guardian user, and a single Guardian user can have multiple aliases.

Safeguard gives you the ability to configure additional **user account** management attributes, including:

- Password history depth
- Required password change intervals
- Automatic user account suspension after excessive log-on failures
- Temporary access suspension and restoration
- Account expiration
- Assignment of users to administrative or file-sharing groups
- Audit generation controls for authentication, user account management, and authorization

You can reduce your help desk calls by configuring Safeguard to issue a warning to users when their password expiration date approaches, and by extending a post-expiration grace period to users. The authentication service allows users to change passwords as part of the logon sequence.

User record contents track the times of the user's last successful and unsuccessful logons, and include a text description field that you can use to hold user-specific data such as contact information.

A user can be a member of one or more configurable **file-sharing groups**. You can use file-sharing groups to provide access control flexibility beyond the confines of a user's administrative group membership. Safeguard also supports a set of **reserved groups** for particular roles such as Safeguard administrator, Safeguard operator, OSS administrator, and security auditor that you can create and populate with the appropriate users if desired.

Some applications have a legitimate requirement to authenticate themselves as different users at different times so that they can perform tasks on behalf of multiple users. To meet this need, Safeguard provides an authorized **Privileged Logon** feature that allows designated applications to authenticate themselves as any user in the system without either password checks or delays in the case of authentication failures, but with the appropriate audit generated. This design allows an application to control which services it makes available to a given user without having to maintain its own parallel user database. Only SUPER.SUPER can authorize the use of the Privileged Logon feature for a program.

Authorization

Authenticated Safeguard users can define appropriate **access controls** for a variety of Guardian objects including disk files, volumes, subvolumes, devices, subdevices, users, aliases; and named and unnamed processes and subprocesses. Different object types have different rules about who can define controls. You establish protection for an object by creating an Access Control List (**ACL**) for it. ACLs are also referred to as **protection records**. An ACL contains subjects or groups of subjects (users) and the access rights that they are granted for the object. Access categories include **read, write, execute, create, purge,** and **ownership**. ACLs also can explicitly deny access to designated individuals and groups, including the super ID if it is configured as DENIABLE.

If an ACL exists for an object, its ruling takes precedence over the object's standard Guardian security permissions. Safeguard allows different authorization privileges for an object to be assigned to the same user, depending on whether the user is authenticated locally or remotely. Safeguard allows definition at the individual user level of both a **default Guardian security vector** and a **default protection record** that is applied automatically whenever that user creates a new file.

OBJECTTYPEs

Safeguard includes an **OBJECTTYPE** model that allows higher-level control over who can create authorization records for objects of a given type. By default, only SUPER group members can create authorization records for volumes, devices, and subdevices; however, by default any user can create authorization records for processes, subprocesses, subvolumes, and disk files. OBJECTTYPE commands allow you to change these default permissions by designating a specific set of users who can add new subjects and objects to the Safeguard database. With the OBJECTTYPE commands, you can specify:

- Who can protect individual objects of a given type
- Who can add users, aliases, and groups to the system
- Who can add an OBJECTTYPE record to the Safeguard database
- Who has owner authority of an OBJECTTYPE record
- What auditing is applied to an OBJECTTYPE

Diskfile ACLs

You can protect a disk file in multiple ways: with a **diskfile ACL** specific to that file, a **subvolume or volume ACL** that applies to all files within the subvolume or volume, or a **diskfile pattern**. Diskfile patterns and **saved diskfile patterns** are more flexible than other types of ACLs, as their permissions apply to all files whose names match the pattern. Where multiple ACLs apply to the same file, Safeguard gives you control over the **evaluation rule order**. For example, a volume ACL may override the ACL associated with an individual file on that volume, or vice versa.

Safeguard provides a **persistence** option for diskfile ACLs. This feature allows you to create an ACL for a file before the file exists and to retain the ACL even after the file is purged, which is useful in situations in which files are deleted and recreated with the same name during each run of an application.

Testing new ACLs

You can configure **ACL warnings** at the individual protection record level to test security settings for new applications or files without affecting security for applications and objects already in production on the same system. Guardian security settings control access to any object that has the Warning Mode attribute enabled in an ACL. Safeguard software then unconditionally audits the new access decision even if the ACL would deny the access. This allows the security administrator to easily and safely tune new ACLs.

Auditing

Safeguard audits logon attempts, access to objects, and changes to the security settings for those objects. Control over what gets audited is highly configurable. Safeguard audit logs can be reviewed by management and auditors to detect anomalies and verify that activity on the system conforms to established security management policies.

Audit controls allow your security administrators to:

- Detect unauthorized system access
- Detect unauthorized security setting changes
- Discourage users from abusing their authorized power
- Verify that policies are being followed

Safeguard is used to configure audit controls for both the Guardian environment and the OSS environment. Your security administrators can specify the objects and types of access to be audited. You can configure Safeguard to log each attempt to access an object, as well as the establishment of communication between client or server application processes. Each audit record includes the object name, date, and time of the access attempt, and whether the attempt was authorized or denied. You can control whether audit is generated for authorized access (**pass**), access denial (**fail**), or both. You also can configure Safeguard to log information about specific user activity such as logging on and logging off.

Safeguard also logs changes made to user authentication records. It unconditionally audits changes to its own configuration attributes, including attempts to alter or stop the subsystem itself, manage audit services, manage terminals, and manage the configuration of partner Security Event Exit Processing (SEEP) modules, described below under “Safeguard extensions”.

Individual users can specify auditing on protection records that they own, subject to system-wide audit controls. There are restrictions on who can control auditing of:

- Users
- Disk volumes
- Devices and subdevices
- OBJECTTYPEs

Both Safeguard and certain other HPE NonStop subsystems can generate audit records, but Safeguard has the system-wide responsibility for security-related audit logging and log management. Safeguard handles **audit log rollover**, and has several options for recovery actions should it become unable to write audit to disk, including recycling the oldest unreleased audit file, suspending audit, and denying audited authorization and authentication requests unless they are issued by a member of the Safeguard administrator or operator groups.

Safeguard-controlled terminals

You can add a terminal definition to give Safeguard control over that terminal. When a terminal definition is added, Safeguard can perform the following additional security functions at the terminal:

- Start a specific command interpreter automatically after the user is authenticated
- Allow the user who is logged on at the terminal to have exclusive access to it

Terminal definitions can be added selectively for some or all the terminals on your system. Safeguard's user authentication controls are enforced for all terminals regardless of whether they are under Safeguard control.

Safeguard configuration

You can configure Safeguard using the **SAFECOM** command-line interface. Safeguard also has a rich set of documented application program interfaces (APIs), so you can write your own programs to customize the software according to your needs and improve administrative productivity by simplifying complex and repetitive tasks. By default, the SUPER.SUPER user has access to all system resources. Safeguard can be configured to **restrict SUPER.SUPER access** in various ways, including explicit denial in ACLs, to improve separation of duties.

Safeguard extensions

You can configure Safeguard to consult with a Security Event Exit Process (**SEEP**) when making decisions on user authentication, password quality, or access control. Multiple security partners offer SEEP-based products, and you can write your own SEEP if desired—the interfaces and processing requirements are documented in the Safeguard Reference Manual.

Open System Services

If you are used to working with UNIX or Linux security, you will find that OSS has a familiar security model. There is a superuser similar to root, namely the SUPER.SUPER user and its Safeguard aliases. Every file has a user (owner) and a group associated with it. These can be changed through the **chown** or **chgrp** utilities or via the chown() API. OSS, like most UNIX systems, restricts their use to privileged users—only the super user or an OSS security administrator can change file ownership for an OSS file, and the user can change the group membership of files only to one of the supplementary groups. When chown, chgrp and chown() are used against Guardian files, the Guardian security rules apply.

OSS filesets are analogous to UNIX file systems.

OSS users and groups

The OSS environment does not provide common UNIX default user names and user IDs unless they are explicitly created by a site administrator. However, equivalent OSS user names and user IDs do exist. For example, the privileges normally associated with the UNIX user name root and the user ID of 0 exist for the OSS user ID (UID) of **65535** (the **super ID**), which is the user SUPER.SUPER and its aliases.

The following OSS environment conventions are equivalent to UNIX user and group conventions:

- The super ID login name, with an OSS user ID (scalar view of the HPE NonStop operating system user ID) of 65535, is the same as the UNIX user name root with a UNIX UID of 0.
- The super group, with an OSS group ID (group number from the structured view of the HPE NonStop operating system user ID) of 255, is the same as the UNIX group name **wheel** with a UNIX GID of 0.
- Using root as an alias of the OSS user ID 65535 (which usually has the login name SUPER.SUPER) is the same as using root for the UNIX user name of the super ID.
- Using wheel as an alias for the OSS group ID 255 (the specially privileged super group, usually with the group name SUPER) is the same as using wheel for the UNIX group name of the trusted administrator group.

OSS file and directory security

File permissions correspond to UNIX file permissions, with a few HPE NonStop-specific extensions to enable features such as enhanced data integrity. Three access modes are supported: **read, write,** and **execute** (**rwx**). Execute also has options for set user and group ID on execution.

Permissions are given to three user types (POSIX model):

- User (owner)
- Group
- Others

OSS Access Control Lists (ACLs)

To allow more flexible control over file access, OSS supports ACLs. ACL rulings take precedence over standard OSS security settings. For better performance, OSS ACLs are implemented as a part of the OSS environment rather than as Safeguard ACLs. OSS also supports a fileset-level **Restricted Access** attribute, which allows users to explicitly deny SUPER.SUPER (root) access to resources within the fileset that are protected by OSS ACLs.

OSS ACL functionality is based on the POSIX 1003.1e draft standard. All OSS system calls that include pathnames are subject to the ACLs on any directory or file in the path. If an ACL does not exist, the standard OSS file permissions are used.

sudo

OSS supports the sudo program, which allows a permitted user to run some (or all) OSS commands as the super ID or another user as specified by the sudoers security policy. Sudo audits the command that it explicitly runs.

OSS auditing

OSS supports very granular controls over **audit generation**, including user and operation type. You configure OSS audit controls through Safeguard.

The audit service can record the outcome of requests for permission to create, open, or delete files; change file content, permissions, or ownership; add or alter filesets; and create or delete directories. You also can audit actions that create or change the state of OSS processes, such as the kill command or any of the tdm_exec, tdm_spawn, exec, and tdm_fork() or fork() function calls. In addition, many OSS shell commands—including mkdir, chmod, chown, kill, rmdir, and setfilepriv—cause audit records to be generated by the OSS name server when auditing is enabled. The contents of each audit record depend on which operation is being performed.

OSS extensions

You can configure OSS to consult with an **OSS SEEP** when making decisions on access control. Multiple security partners offer SEEP-based products, and you can write your own SEEP if desired—the interfaces and processing requirements are documented in the Open System Services (OSS) Programming Guide. OSS SEEP support is implemented in the OSS Name Server processes rather than in Safeguard for performance reasons. OSS SEEP attributes are configured on a per-fileset basis.

SQL

Both the **SQL/MP** database and the **SQL/MX** database have been engineered to be well-integrated components within the overall HPE NonStop security ecosystem, and both leverage the HPE NonStop OS security features described above. As an example, sensitive SQL code runs in priv mode, but ordinary users are prevented from stepping into priv mode code when debugging. These controls permit debugging of SQL applications while protecting SQL execution flow and local data. SQL's in-memory data is contained in hidden segments, and only the data that the user has permission to access is made visible outside the priv boundary. The debugger prevents ordinary users from viewing SQL's private data.

Both databases rely on the HPE NonStop OS and Safeguard for user management. They do not have the overhead associated with having to create and manage a separate set of database users and administrators. The HPE NonStop OS recognizes SQL objects and protects them from data file access outside of the SQL environment.

SQL/MP security

SQL/MP security now relies on a combination of Guardian security and Safeguard ACLs. SQL/MP objects can be protected through DISKFILE and DISKFILE-PATTERN ACLs. SQL/MP catalog objects currently cannot be protected with Safeguard ACLs.

The SQL/MP database executes within the Guardian environment, and its database tables reside within the Guardian environment.

SQL/MX security

Overview

SQL/MX supports the **ANSI SQL GRANT/REVOKE** authorization model rather than being integrated tightly with Safeguard.

You can designate **security administrators** to manage SQL/MX security. These administrators manage GRANT/REVOKE privileges, but do not have access to the data itself.

SQL/MX executes within the OSS environment, but its database files reside within the Guardian environment.

Object and access management

Object management (**DDL**) and access to objects (**DML**) are controlled separately, but both use the ANSI model of granting or revoking privileges. Creation of objects is limited to the owner of the **schema** containing the objects or SUPER.SUPER (as of release 3.5, the owner also can specify schema-level privileges to individual users or user groups). Ownership of an object may be transferred using the GIVE command. Management of an object is limited to the object owner, the owner of the schema containing the object, or SUPER.SUPER. DML security controls access to the contents of objects, such as SQL SELECT, DELETE, INSERT, or UPDATE statements. An optional GRANT privilege (**WITH GRANT OPTION**) can be associated with each access privilege, allowing the holder to GRANT that privilege to other users as well. The creator/owner of an object inherently has ALL privileges WITH GRANT OPTION.

Privilege groups

As of release 3.5, SQL/MX supports the creation of user privilege groups that are arbitrary collections of users.

Security administrators

Security administrators are a class of users that can administer database object security through **privileges** without being explicitly GRANTed access to the objects (WITH GRANT OPTION), including schema-level privileges. They do not have access to the underlying data unless explicitly GRANTed access by an object owner (or designee) or through the use of **PUBLIC** access. Security administrators may not GRANT privileges to either security administrators or PUBLIC.

Initially, the set of security administrators is empty. Only SUPER.SUPER has the capability to designate an initial security administrator, but only an existing security administrator may designate additional security administrators. As long as the set of security administrators is non-empty, SUPER.SUPER does not have "super" GRANT/REVOKE privileges unless explicitly designated as a security administrator.

Multitenancy

As of release 3.5, SQL/MX supports database isolation in multitenant environments.

Additional on-platform security products

HPE offers several products that work in conjunction with Safeguard to help meet your security requirements, including:

- XYGATE Merged Audit for enhanced audit management
- XYGATE User Authentication for additional log-on controls and integration into LDAP and Active Directory environments
- XYGATE Access Control for command-level access control and audit, including keystroke logging
- XYGATE Compliance PRO for GUI-based security configuration management and compliance-oriented reporting for standards such as the **PCI DSS**

XYGATE Merged Audit

XYGATE Merged Audit (XMA), which is standard for new commercial systems, provides audit consolidation, reporting, alerting, and export. XMA integrates audit records and other information from multiple sources, including Safeguard audit, Event Management System (EMS) logs, CLIM logs, and Measure-collected information on running processes, into a single, SQL-based repository for consolidation and ease of reporting. You also can use XMA to consolidate audit from multiple HPE NonStop systems.

XMA's sophisticated **filtering** allows you to focus on the most important data in your environment. You can either use its predefined reports for compliance with regulations such as PCI DSS or define your own reports through its GUI-based tool. You can customize filters for near-real-time event monitoring, identify the events that require alerts, and configure **alert delivery**. XMA can deliver filtered audit to industry-leading SIEM devices.

If you use ACI BASE24, ACI BASE24-eps, HPE Home Location Register (HLR), AJB RTS, or GreenHouse SECOM software, you can purchase optional XMA plug-in products from HPE that integrate logs maintained by these products into the common XMA log database.

XYGATE User Authentication

XYGATE User Authentication (XUA), which is standard for new commercial systems, provides granular logon controls, including restrictions based on IP address or port, time of day and requesting user or group. Its flexible configuration allows you to configure individualized user management, including handling of failed authentication attempts. It also allows you to integrate your HPE NonStop users into your enterprise user management systems by acting as an LDAP, Active Directory, or RADIUS client. It supports two-factor authentication using RSA SecurID tokens.

XUA permits controlled user impersonation, e.g., logging on as SUPER.SUPER with the user's own password. This feature, in combination with its auditing capabilities, gives you a high level of accountability for your users' activities.

XYGATE Access Control (optional product)

XYGATE Access Control (XAC) supports Role-Based Access Control (RBAC). You'll find it particularly useful for its fine-grained control over which users can perform specific commands and subcommands within HPE NonStop utilities that otherwise allow any SUPER group member to perform most sensitive operations. You can configure XAC to effectively eliminate the need for shared user IDs. You also can configure keystroke-level logging to monitor activity at the user and/or function level.

XYGATE Compliance PRO (optional product)

XYGATE Compliance PRO streamlines the data-gathering effort to allow you to answer questions such as, "Does my system meet compliance regulations?" and "Do my system's current security settings conform to HPE NonStop server best practices?" Compliance PRO lets you easily review both current system settings and changes to your system's security baseline, pinpoint areas of concern that should be addressed, and get advice on how to address them. It has built-in reports for compliance against PCI DSS, the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX), and allows you to customize your own reports to match your company's security policies.

Other subsystems

Many HPE NonStop subsystems have security aspects, and some (such as iTP WebServer, TS/MP, and Samba) have numerous security considerations. You can read the individual subsystems' documentation for details.

A note on viruses, malware, and security vulnerabilities

The HPE NonStop system has some inherent architectural advantages that greatly reduce both the potential for malevolent software to be imported and the effects if such software were introduced into the system. As you learned earlier, nonprivileged (user) processes cannot modify either their own object code (binaries) or those of other processes. As long as you have properly secured your HPE NonStop system, its object files also cannot be modified by a nonprivileged process. As a consequence, even if a virus written for a UNIX, Linux, or POSIX environment on any other platform were introduced into your HPE NonStop system, it could not have its intended effect. For example, common UNIX attacks that exploit buffer overflows to gain root access capabilities will not work on an HPE NonStop Server because a nonprivileged process cannot execute code from within a data segment and, even if that were possible, could not use execution of that code to escalate its privileges.

As an HPE NonStop customer, it is your responsibility to develop and implement a security policy to ensure that you use best practices to protect your HPE NonStop servers. You should keep your HPE, partner and custom software up to date to help minimize security risks, and make full use of the security products that HPE provides. Internet-facing systems should be protected with appropriate intrusion prevention and detection products, and unneeded ports and services should be disabled.

HPE NonStop data in motion security

HPE NonStop SSH

SSH or Secure Shell is a network protocol from the UNIX environment that allows data to be exchanged using a secure channel between two networked devices. It was designed to be a replacement for Telnet and other insecure remote shells.

HPE NonStop SSH fully complies with the SSHv2 protocol, including strong public key authentication with key lengths of up to 4096 bits and ciphers such as Advanced Encryption Standard (AES) and algorithms for message authentication code. It maintains its own central key store. It includes built-in user base support, allowing remote users to log on with virtual user names instead of a Guardian user ID to avoid exposure of system credentials to file transfer clients. Individual user access can be configured to be limited to a specific set of files and to a specific set of operations (e.g., only download) or services and connection can be restricted to specific IP addresses.

Other features include:

- Full-screen pseudo terminal access for administrators and developers
- TCP and FTP port forwarding, allowing secure tunneling both locally and remotely
- Advanced auditing capabilities, including audit of all operations initiated from remote clients

Unlike OpenSSH, which works only in the OSS environment, HPE NonStop SSH works in both the OSS and Guardian environments.

HPE NonStop SSH includes SFTP clients for both OSS and Guardian SFTP, as well as an SFTP server, with support for navigating the Guardian file system, specifying files using the OSS or Guardian file name syntax, and specifying file attributes. If you have programs that use the FTP API, you can easily convert them to use SFTP instead through the optional HPE SFTP API plug-in—with no or minimal code changes.

SSL and TLS

SSL or **Secure Socket Layer** is a cryptographic protocol developed to provide security for communicating over the internet, end-to-end encrypting the segments of network connections at the transport layer. The SSL protocol has been superseded by the **Transport Layer** Security (TLS) protocol. TLS is in widespread use for web browsing, email, instant messaging, and other applications. SSL, while deprecated, is still in use in some sites.

A number of HPE NonStop products, including iTP WebServer, HPE NonStop Servlets for Java Server, HPE NonStop Application Server for Java, ODBC/MX, HPE NonStop Software Essentials, and some OSM components, have native TLS support.

HPE NonStop SSL, which supports TLS, can be used to encrypt data sent or received over TCP/IP by other programs on HPE NonStop servers. Running as a proxy, it adds TLS to TCP/IP protocols that do not have built-in support of TLS or SSL on HPE NonStop, such as TELNET, FTP, or ODBC/MP. It also can encrypt Expand-over-IP traffic.

HPE NonStop SSL creates secure connections, offering TLS 1.2 and strong ciphers such as 256-bit AES. It supports the FTP-TLS standard (RFC 4217), providing compatibility with a wide range of SSL-enabled FTP solutions for PCs and other platforms. HPE NonStop SSL enforces both client and server authentication using Public Key Infrastructure (PKI) with X.509 certificates and RSA key sizes of up to 8192 bits.

HPE NonStop SSL includes basic firewall functionality, including disabling unencrypted protocol access and support for both allow lists and deny lists. It optionally can audit network traffic for protocols such as ODBC or TELNET when a complete byte-by-byte dump is desired.

Two optional products, **HPE NonStop cF SSL-LIB** and **HPE NonStop cF SSL-AT**, allow you to directly integrate TLS support into your applications and also provide visibility of the client IP address instead of the local loopback address as seen when using the HPE NonStop SSL proxy. You can integrate SSL-LIB into your native applications with minor code changes if you have access to their source code, or use the application-transparent SSL-AT library to add TLS support without any application or configuration changes—for example, to encrypt ATM traffic in an existing ACI BASE24 installation.

IPSec (IP CLIMs only)

Internet Protocol Security (IPSec) provides application-transparent encryption services for IP network traffic. You can set up IPSec on an IP-address-to-IP-address basis, and optionally on a UDP or TCP port, but you cannot establish IPSec on a per-physical-Ethernet-interface basis.

The IP CLIM has IPSec functionality enabled by default. You can use either the CLIMCMD **climconfig** tool or **HPE NonStop I/O Essentials** to configure the IPSec security policies, security associations, and dynamic Internet Key Exchange (IKE) functionality. The climconfig tool also allows configuration of the security policy (SP) and manual security association (SA). Manual SA uses a fixed secret key for the IPSec VPN. Since this poses a security risk over a period of time, HPE discourages this practice and recommends configuring automatic SAs instead.

The **IPSec** daemon establishes automatically keyed IPSec associations and supports authentication using pre-shared keys, X.509 certificates. Whenever an application sends network data, the CLIM kernel checks whether there are security policies in the security policy database (SPD) matching with the source and destination IP addresses. If a security policy is found, and there is no security association corresponding to this security policy, the kernel triggers the IPSec daemon to establish the security association. The application data is then transferred over the newly created IPSec connection.

The primary use of IPSec is to encrypt traffic between HPE NonStop systems and other hosts/endpoints. It also can be used to encrypt **Expand** traffic.

IPTables and IP6Tables (IP CLIMs only)

The Linux IPTables (IPv4) and IP6Tables (IPv6) packet filtering facilities allow you to establish a robust **firewall** capability. The IP CLIM supports a subset, allowing filtering of the INPUT chain (packets destined to local sockets).

HPE NonStop data at rest security

HPE NonStop Volume Level Encryption

HPE NonStop Volume Level Encryption (VLE) is a fully-integrated, application-transparent encryption solution for your **CLIM-based storage**, including SAS disks, HPE XP and XP7 disk arrays and LTO-4 and newer-model LTO tapes. You can perform initial disk encryption and key rotation online, with full data access during the operation. For disks, encryption and decryption take place within the storage CLIM. The VLE code in the storage CLIM is only a key management client for tape drives, with encryption/decryption taking place within the drives.

Encryption is under the control of designated security administrators. It is configurable on a device basis, and for disks you can choose between two NIST-approved AES-256 algorithms. HPE NonStop VLE has received FIPS 140-2 level 1 validation.

HPE NonStop VLE uses the highly available and scalable HPE Enterprise Secure Key Manager (ESKM) for its encryption key generation and management. The ESKM will become a Micro Focus product in August 2017. HPE ArcSight SIEM or another enterprise SIEM for centralized log management, security event monitoring, and compliance reporting. The ESKM has received FIPS 140-2 level 2 validation.

HPE also offers software-based encryption for all tape drive types through the optional HPE NonStop cF Secure Tape product. Its operation is transparent to HPE NonStop utilities such as BACK/RESTORE, BR2, BACKCOPY, and PAK/UNPAK, as well as to TMF audit online dump/restore operations. It has a built-in key server.

Data sanitization

You can use Safeguard to configure either individual files or the entire system for **clear on purge**, which writes zeroes over the file's contents on disk at the time it is purged. You also can use the shred command to sanitize files in the OSS environment. For direct-attached disks, you also can use OSM's **data sanitization** capabilities to overwrite an entire disk using a specified number of passes and sets of patterns before the disk is removed from the system.

Partner products

A number of HPE NonStop partner companies extend the HPE NonStop security ecosystem through their products, offering a wide range of functionality including enhanced password quality enforcement, file integrity monitoring, frameworks that support Enscribe and OSS field-level and SQL column-level data encryption, and Hardware Security Modules. For more information, visit their websites. The References section includes a list of partners.

Conclusion

System security in both the Guardian and OSS environments provides a strong foundation for protection of system data and resources, which is augmented as appropriate by security elements within individual subsystems. You may wish to incorporate HPE NonStop security partner products for additional enhancements.

You can visit the HPE NonStop website for additional information on HPE products, or dive directly into the HPE NonStop manuals collection for additional white papers, reference manuals and guides.

Resources

HPE NonStop security manuals and white papers available at HPE NonStop technical library

hpe.com/info/nonstop-docs

Suggested initial reading:

- HPE NonStop Security Hardening Guide
- Safeguard User's Guide
- Safeguard Administrator's Manual
- Open System Services (OSS) Management and Operation Guide
- HPE NonStop System Console Security Policy and Best Practices
- Security Management Guide

HPE NonStop security partners

Partner	URL
4tech Software	4techsoftware.com
ACI	aci.com
Bowden	bsi2.com
CAIL	cail.com
comforte	comforte.com
CSP	cspsecurity.com
ETI-NET	etinet.com
GreenHouse	greenhouse.de
Opsol Integrators	opsol.com
XYPRO Technology	xypro.com

Learn more at

hpe.com/info/nonstop