Single Sign-On and Identity and Access Management Integration on NonStop Systems – A Feasibility Study –

connect2nonstop.com/single-sign-on-and-identity-and-access-management-integration-on-nonstop-systems-a-feasibility-study

comforte

Introduction

Every day, employees log in to many different software programs, from email to payment systems, and a myriad of other applications designed to help accomplish their daily tasks. Remembering all of the usernames and passwords associated with these products can be a real challenge with some users storing passwords insecurely, leading to serious data breaches. Single sign-on systems (SSO), i.e. moving to standardized services for digital identity, are crucial in alleviating the need for — and stress of — recalling a multitude of credentials. Providing a good SSO user experience has become more complex because the technical professionals responsible for implementing identity and access management (IAM) systems must balance user convenience against enterprise security risks.

As businesses strive to improve their security processes and procedures, an increasing number of HPE NonStop users are looking at ways to integrate access to their NonStop systems and applications into the overall authentication and access management environment.

This feasibility study is based on the experience drawn from several customer projects, and

its purpose is to describe how Single Sign-On (SSO) and Identity & Access Management (IAM) can be implemented on HPE NonStop systems. References to an existing IT environment, including Nonstop systems, tools and solutions are made with real-world customer scenarios in mind.

The Challenge

The “Nonstop Services” team has all necessary, privileged rights to carry out its tasks on the platform. However, a separation of user rights to achieve the “Segregation of Duties” between administrative sections that contain sensitive data (as often required by the security officers), is currently hard to do or infeasible.

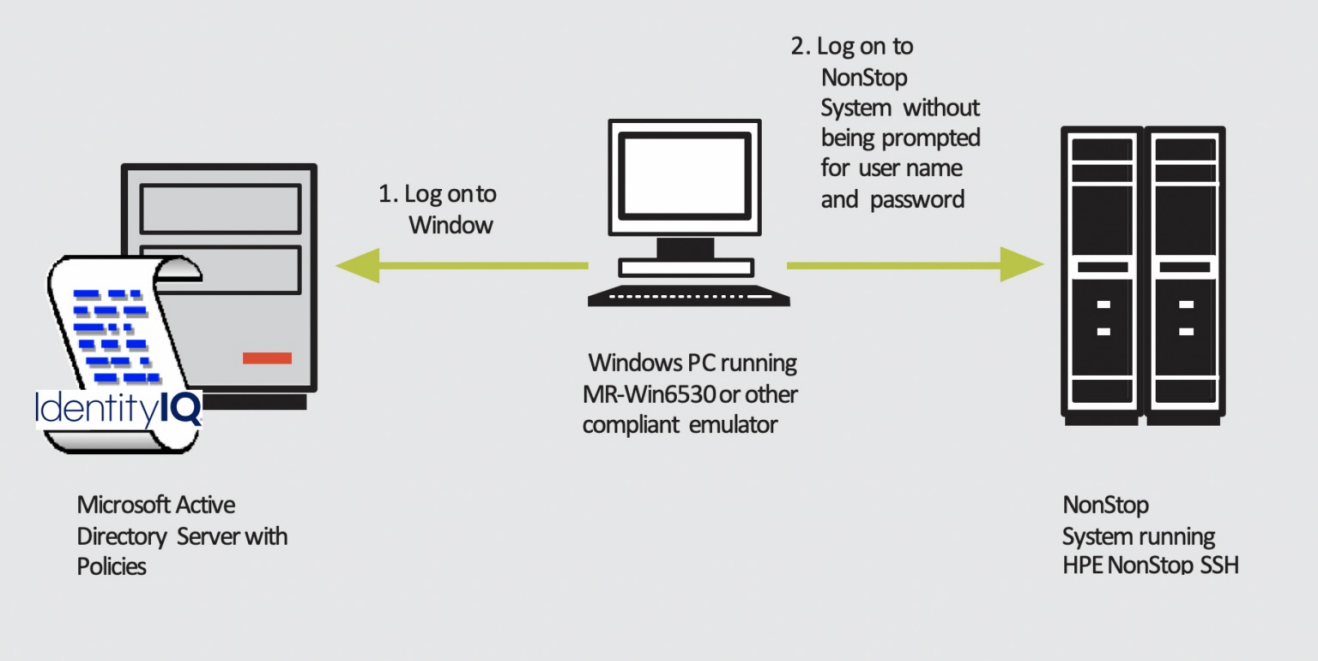
The Requirements

A suitable solution to the SSO problem, as outlined above, should meet the following key requirements:

1. Traceability of user permissions is provided, i. e. it can be determined at a later time which privilege rights were given (or withdrawn) to which user and when.
2. Have no impact on the availability of the NonStop platform.
3. Deliver seamless integration into the existing Enterprise environment. Integration, in this case, does not only mean the integration in the existing NonStop environment but also into the entire system landscape and IT system strategy. In particular, it should be noted that the customer could use a PAM solution like Sailpoint IdentityIQ for Privileged Access Management (PAM) throughout the rest of the company.
4. Be based on industry standards and make use of an available SSO solution on NonStop.

The Solution

The proposed approach is the implementation of a Single Sign-On solution **without any programmatic intervention** on the NonStop systems, enabling flexible, granular authorization management. The customer’s Enterprise Identity & Access Management (IAM) integration, under the control of Active Directory (AD) and additional components like Break Glass processes (in this case SailPoint IIQ), are used as a reference. Other AD-based PAM (Privileged Access Management) solutions are supported, which allow the use of a combination of Kerberos for authentication and LDAP for the role-based access control (RBAC), based on the LDAP group membership of the Kerberos user.



[Note: Identity IQ is shown as a reference AD plugin only.]

The recommended solution and its options are described in detail below.

As with all PAMs, (temporary) privileges are mapped to corresponding roles using memberships in (LDAP) groups, which means that when granting privileges, such as administrative access, the respective user is (temporarily) added to a corresponding group. Conversely, when the privileges are withdrawn, the user is removed from the privileged group.

With current Microsoft Server versions (as from v2016), group memberships can be given an expiration date as they are added, a functionality that was previously provided through active (but also automated) deletion of group membership by solutions such as IdentityIQ.

In this approach to IAM system integration, an HPE NonStop Server is integrated into the enterprise environment in a way, that allows users to authenticate based on their Windows Active Directory accounts and authorization based on their Active Directory group membership.

Therefore, if administrative privileges are to be granted (temporarily), the corresponding user account is simply added to the Administrators group. Once this is done, the user can log on with the administrator access (e.g., SUPER.SUPER).

Solution Options

This chapter provides an in-depth insight into the most effective solutions, as follows:

- Connection for classic 6530 applications with authorization at the application level

- Connection for command line, telnet and file transfer interactions by system users
- Connections for Web-based NonStop Applications with Application Level Authorization
- Connections via SSH Tunneling
- Connections via Jump Server

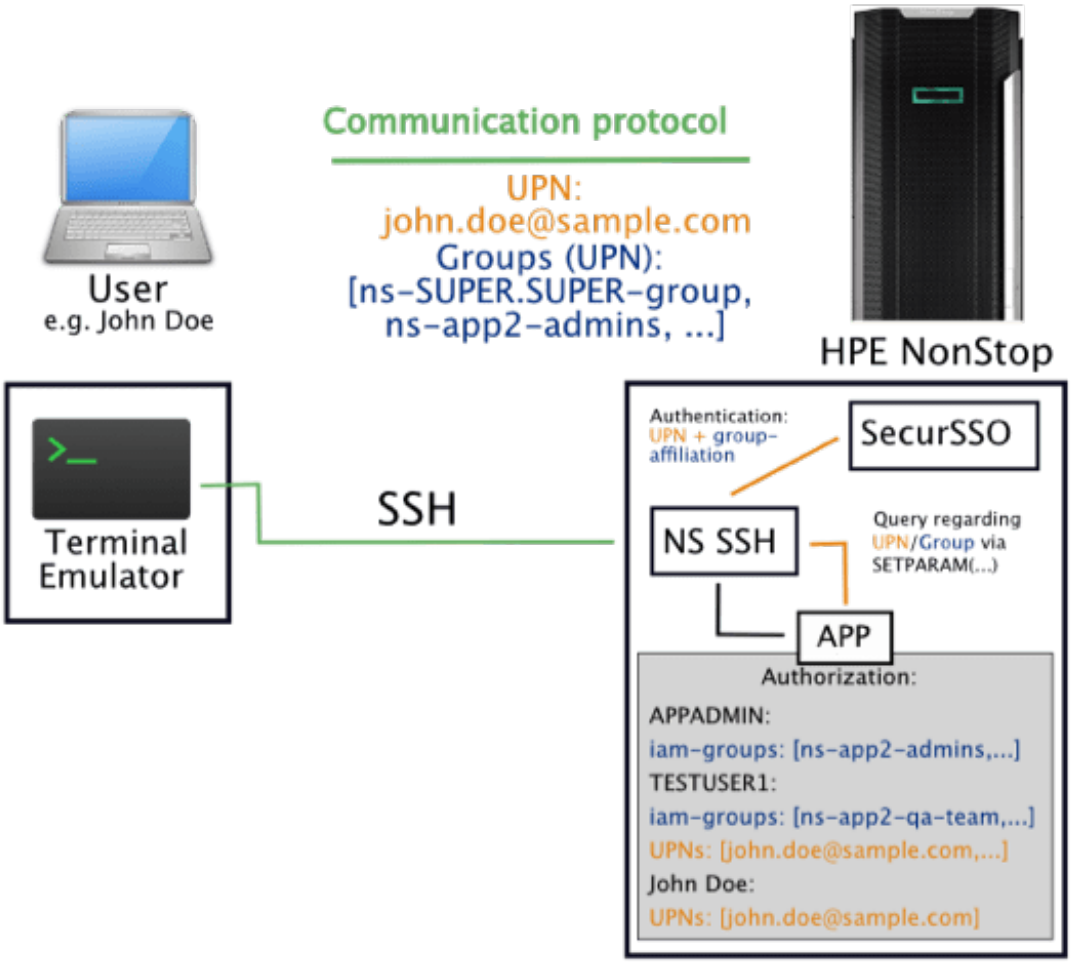
1. Connection for classic 6530 applications with authorization at the application level

Traditional 6530 applications on the NonStop, which are addressed through the terminal emulator, and where application-level authorization occurs, can also be linked to the break-glass process based on IAM-based group memberships.

For this use case, only the authentication of the requesting user, including the determination of the group memberships of the solution components is performed. The application itself must perform the actual authorization, i.e. determining if an incoming user may log on as a particular application user (based on their username) or memberships.

For this purpose, the solution presented here offers appropriate programmatic interfaces; with the aid of which, the respective application can request the necessary information on usernames and group memberships from the solution components in a simple manner (e.g. via a SETPARAM call).

The following graphic illustrates the solution for classic 6530 applications with application-level authorization.



As shown in the graphic above, user authentication and group memberships continue to be authenticated by SSO. However, the authenticated connection is then forwarded by NonStop SSH to the actual application. The application must then make the programmatic call to get UPN (User Principal Name) and group memberships. The application must continue to provide a database for authorization (e.g., by adding a database field, additional configuration file, and the like), based on which the authorization decision can then be made.

In this way, as exemplified in the graphic, a user who is (temporarily) assigned to the group “ns-app2-admins” has access to the administrative user of the application, here, e.g. “APPADMIN”. Of course, in addition to group-based access, the associations may also allow access to particular users (UPNs) when appropriately configured.

2. Connection for command line, telnet and file transfer interactions by system users

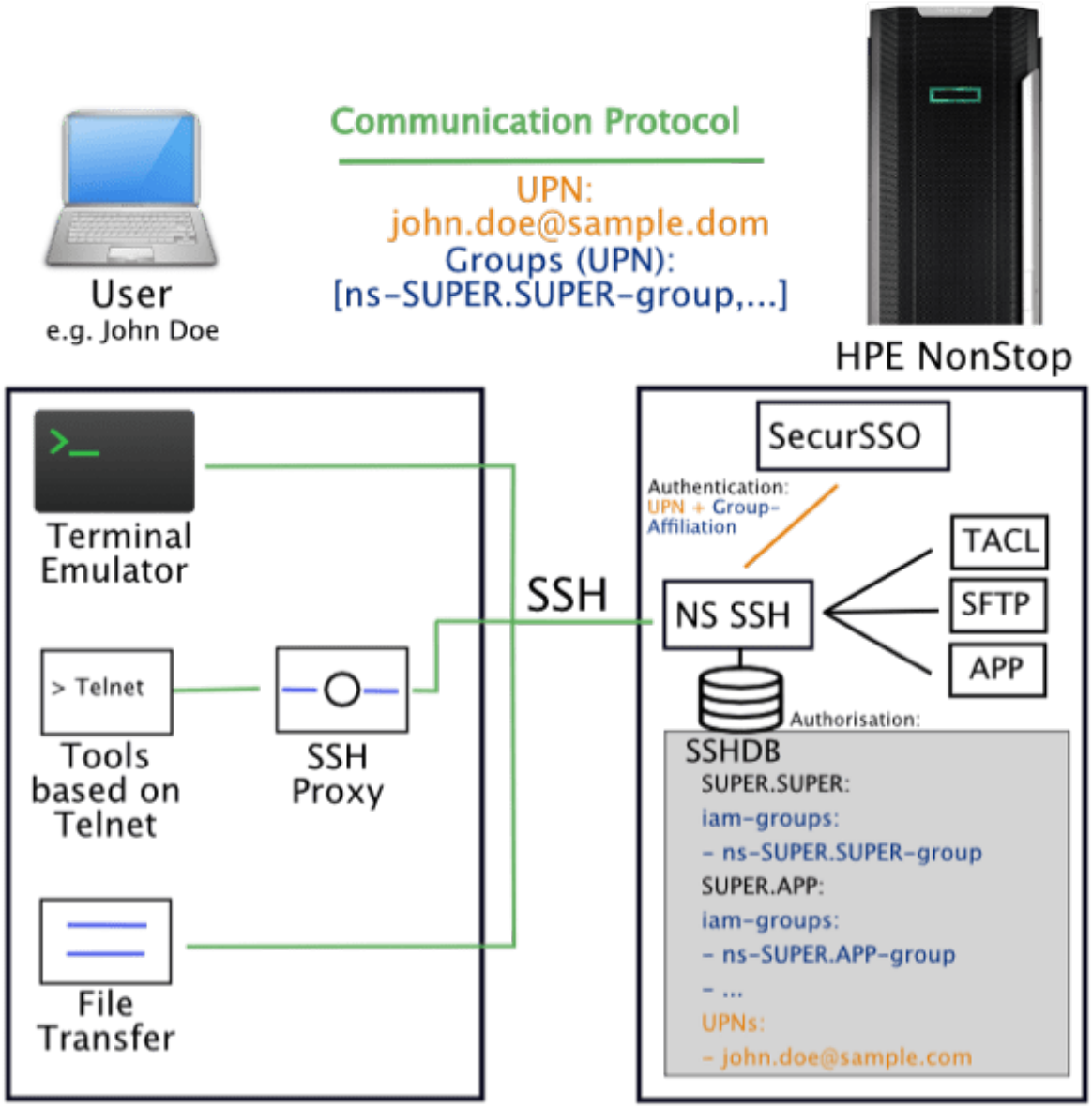
For classic NonStop command-line or file-transfer accesses, modern HPE NonStop terminal emulations have Kerberos native integration over the SSH protocol and typically SSH-based Kerberos-enabled file transfer capabilities (SFTP) as well.

In addition to the Kerberos functionality, the SSH protocol is generally better suited for these purposes than SSL / TLS; especially for secure file transfer (SFTP). It is easier to manage, as no separation of a control channel and data channel or dynamic opening of connection channels – as in FTPS – is performed. Also, SSH / SFTP has fewer vulnerabilities than SSL / TLS or FTPS and can be much more easily secured via a firewall.

Accordingly, it is highly recommended to investigate the current use of SSL / TLS based connections. Security will improve by switching using SSH for command line and SFTP for file transfers.

As part of the solution described here, the advice is to simplify the same-purpose product landscape and to focus on terminal emulation or file transfer tools that already provide native support for Kerberos. Examples of such tools are MR-Win6530, OpenSSH, Putty, WinSCP and several others.

For non-replaceable tools with command-line functionality via (SSL/TLS-encrypted) Telnet, an SSH proxy should be used for the connection. The resulting connection is shown in the following diagram:

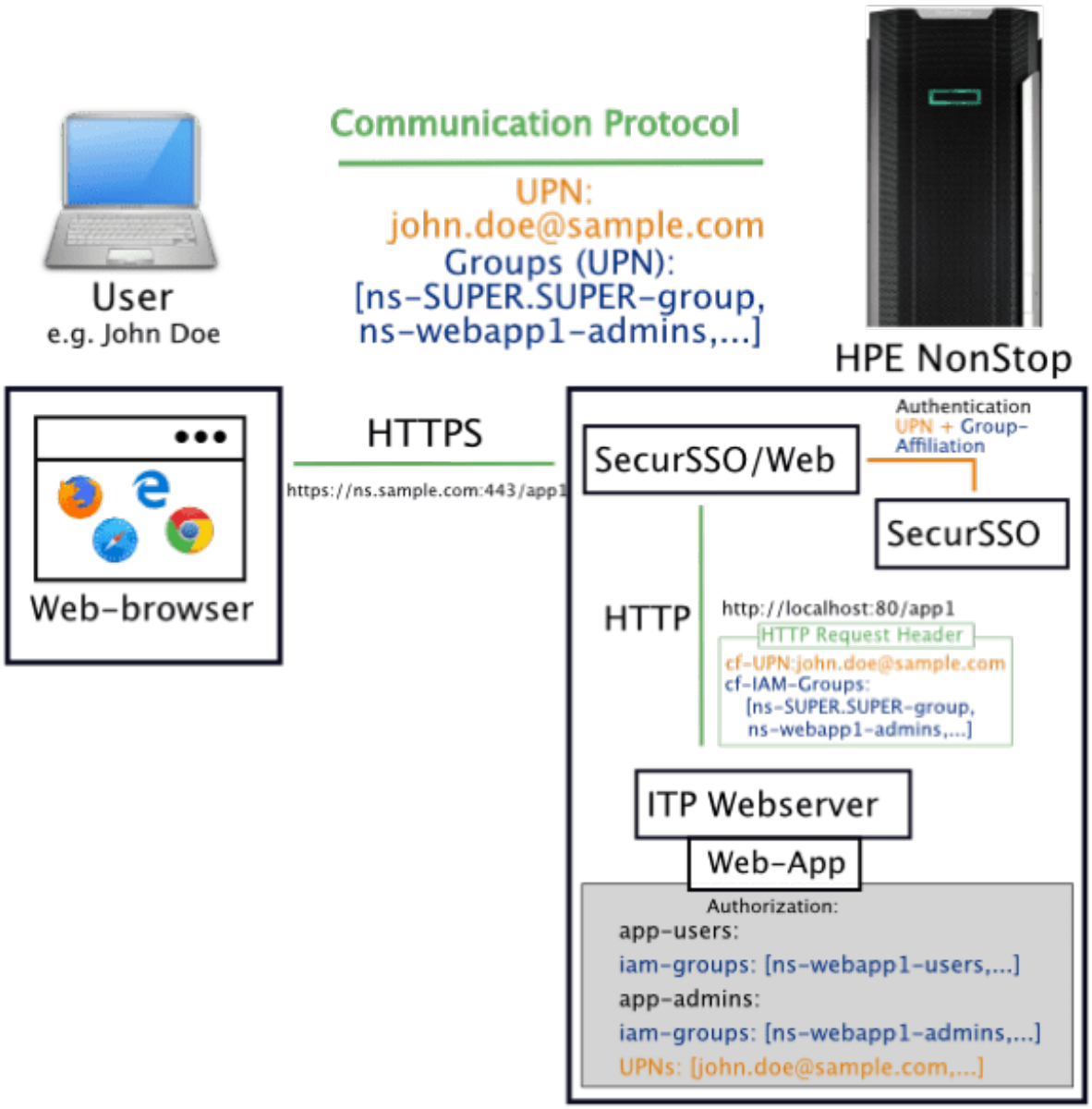


3. Connections for Web-based NonStop Applications with Application Level Authorization

The connection of web-based applications to the NonStop can be carried out using the SPNEGO protocol[1] standardized for web-based Kerberos authentication. The SPNEGO protocol allows Kerberos to perform the necessary interactions for Kerberos based authentication over HTTP (S) and is native to all non-standard web browsers and servers.

On the NonStop the corresponding SSO/Web module offers the corresponding server-side component for the implementation of SPNEGO. Thus, the use of group-based authentication to implement the PAM like “break glass”[2] process for web applications on the NonStop can then be made possible.

The following graphic illustrates the connection using SSO and the SSO/Web module:



On the client-side, web browsers can still use any standard web browser, as they all support native Kerberos. The necessary client-side changes are limited to possible configuration adjustments in the browser to switch on Kerberos-based authentication explicitly.

On the server-side, the ITP web server is the default web application execution environment on the NonStop. Compared to standard web servers beyond the NonStop, the ITP web server is not native to Kerberos. In order to make the connection possible, a corresponding SSO/Web module is required for this purpose.

The SSO/Web module is an HTTPS to HTTP TCP/IP proxy with connection to the SSO core component, which accordingly retrofits the missing Kerberos capability for the ITP web server.

As shown in the graphic above, the group-based integration process takes place in the

following main steps:

1. The SSO/Web module accepts the incoming HTTPS request (HTTP request via SSL/TLS) from the client
2. If no corresponding session cookie has been set from a previous successful authentication, SSO Web uses SSO to perform Kerberos-based authentication including extraction of group memberships and set a corresponding session cookie.
3. SSO/Web adds into the header of the original HTTP request the UPN and group memberships extracted in step 2 as HTTP header attributes.
4. The modified HTTP request is forwarded via the local loopback to the ITP web server.
5. The application running in the ITP webserver context reads out the set HTTP Request Header attributes and authorizes based on an appropriate group/UPN-to-application user association maintained as part of the application.
6. Upon successful authorization, the user is granted access to the application.

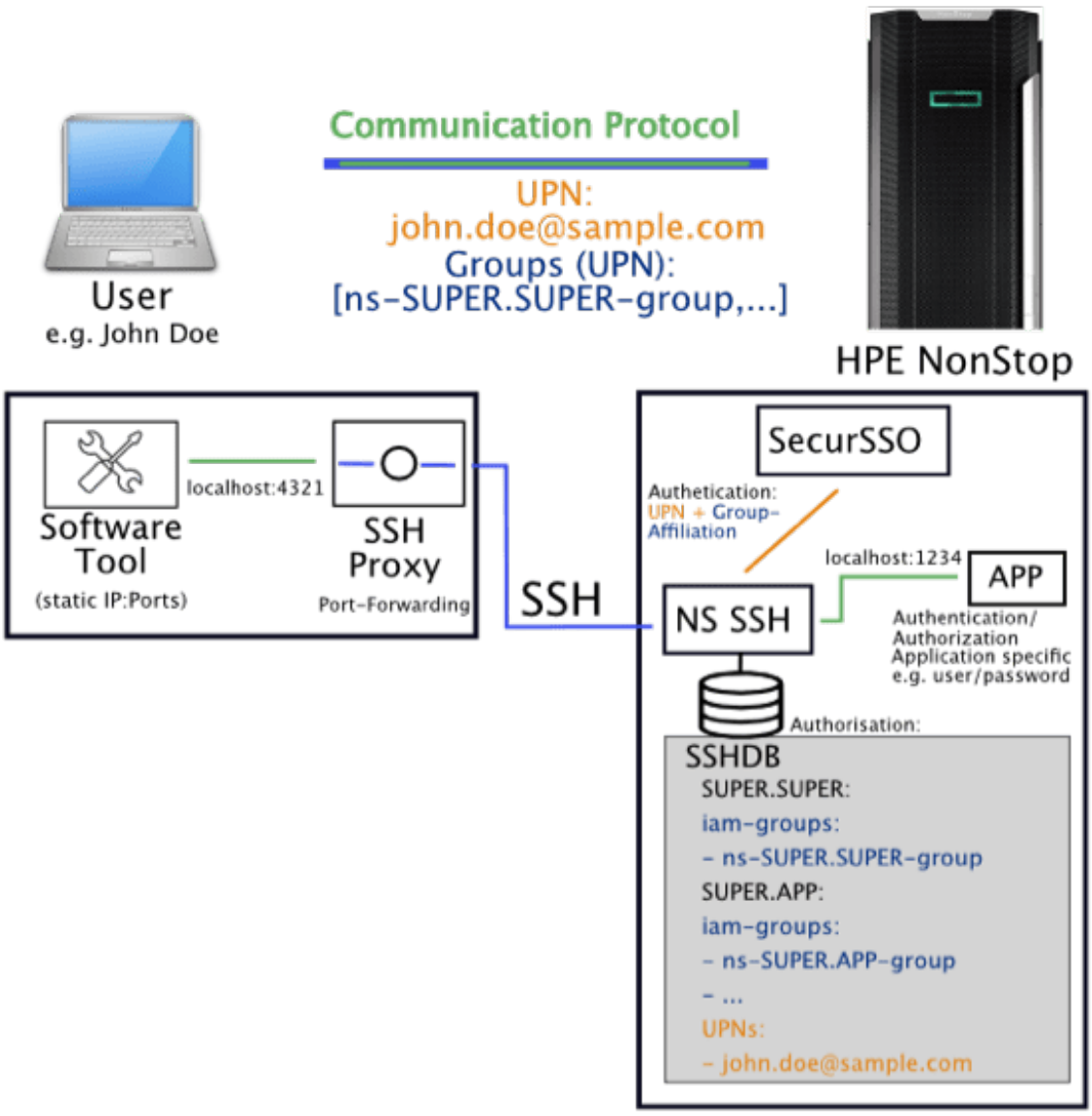
4. Connections via SSH Tunneling

For those applications which cannot be covered by the connection possibilities as described above, where neither native Kerberos support is available nor can it be changed, the binding can take place by means of SSH Tunneling. This would apply to predefined TCP/IP IP port connections.

The application data is transmitted via an SSH tunnel using the SSH tunnel.

It should be emphasized that the actual application, cannot be addressed any longer directly from external, i.e. externally exclusively through the SSH tunnel.

The following graphic illustrates this connectivity using SSH Tunneling:



As illustrated in the graphic, the software tool is configured to connect to the user PC running SSH Proxy. The SSH Proxy must be configured using appropriate port-forwarding entries, i.e. to forward the incoming connection on a specific local port on the user's computer, then via NonStop SSH to the local port on the NonStop, where the application expects the incoming connections.

When connecting via SSH tunneling, both the authentication and authorization based on IAM-based users and groups take place, as well as the authentication/authorization according to the respective application. However, because Kerberos-based authentication and subsequent group-based authorization at the SSH level can be done without user interaction, there is no degradation, e.g. double password prompt for the user.

Operationally, to separate the SSH tunneling environment from general user access, it is advisable to use dedicated NonStop SSH and dedicated local TCP/IP subnet process environments for SSH tunneling purposes.

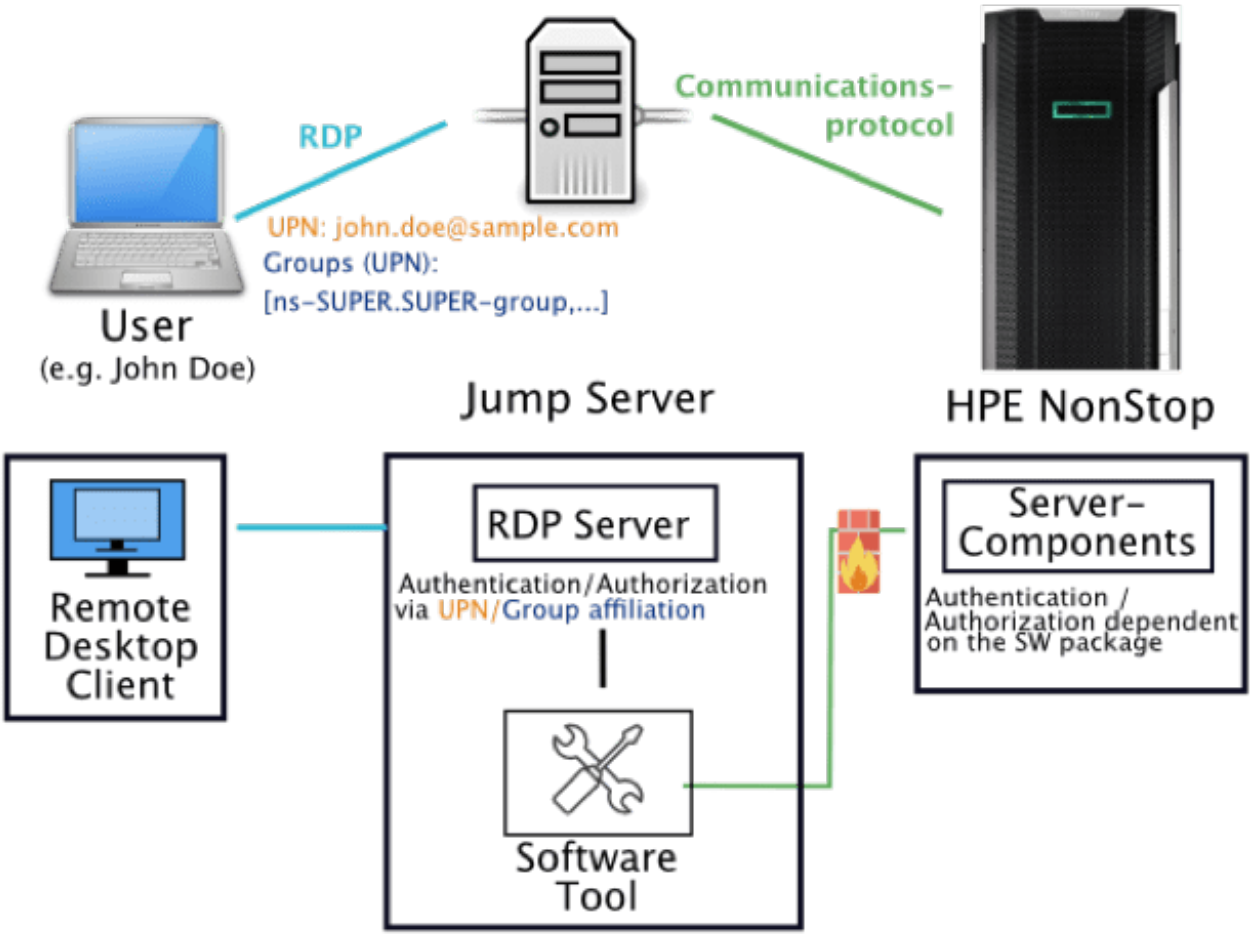
Furthermore, for performance reasons (where possible), the unencrypted variant of the respective application protocol should be used to avoid the expenditure for double encryption (for example SSL/TLS over SSH).

5. Connections via Jump Server

Applications that do not support native Kerberos or are not easily integrated using the previously described connections (for example third-party dynamic port applications) can be integrated into the IAM/PAM-based “break-glass” process using a “Jump Server” approach.

As is usual in Jump Server approaches, the access to the actual function and the software tools required for this is made available exclusively by a secure Jump Server. With the help of the Jump Server, the desired authentication, authorization and logging, based on the IAM mechanism, can then be implemented.

The connection via Jump Server is illustrated in the following graphic:



As shown in the graphic, the user connects to the Jump Server using Remote Desktop Protocol, RDP. Typically, the Jump Server used is a Windows Terminal Server, integrated into the company-wide Active Directory, which has all the usual

authentication/authorization functions, including Kerberos. After successful authentication and authorization based on the UPN and group membership, the Jump Server can then gain access to the corresponding software tool under a specific user account and connect to the NonStop.

The communication protocol used and the method for authentication/authorization in the direction of HPE NonStop are then dependent on the respective software tool.

On the NonStop users (aliases) should be created, to which the tool connects, and whose secret authentication information, e.g. the password used (if possible, not easily extractable) etc. is stored in the configuration of the software tool on the Jump Server.

Conclusion

This suite of solution provides the perfect answer for current and future privileged account management requirements demanding SSO in a hybrid IT environment, including NonStop. Features like robust immutable audit and integration into a SIEM are other must-have capabilities. Finally, the deep future-proof AD integration architecture of NonStop SSO supports any future AD-based changes without any product-specific changes in the NonStop environments.

[1] iETF RFC 4178 The Simple and Protected GSS-API Negotiation Mechanism (obsoletes RFC 2478).

IETF RFC 4559 SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows

[2] For a definition of a break glass procedure see https://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems

About the Authors

Thomas Gloerfeld

Thomas Gloerfeld is Director of Partner Development & Marketing NonStop Solutions at

comforte and has been associated with the NonStop community for 25 years. Before joining comforte, he held various management positions at ACI Worldwide in Germany and the UK. In his role at comforte he closely monitors topics such as data security, risk and compliance.

Helmut Bernhard

As an experienced senior solutions architect, Helmut Bernhard has seen various iterations of innovation, modernisation, digital enablement, security and customer focus. With over three decades of real-life, in-the-trenches business experience, his view on leading-edge projects and forward-looking solution areas in the finance and telecommunication ecosystems is profound and radical.

Before joining comforte AG, Helmut has served as a business development manager, program manager, consulting and software sales manager in the US and EMEA, working for leading companies like HPE, Tandem Inc., a Nortel affiliate, Oracle and a Western/Central European payment service provider.