Managing the Risk of Privileged Accounts and Privileged Passwords in Defense Organizations

Reduce Risk while Streamlining Administrative Workflows

Written by Dell Software

Abstract
Even IT environments that have two-factor authentication in place must still deal with passwords: service account passwords, local account passwords, Windows local administrator passwords and Unix/Linux root account passwords. Managing them in a way that meets requirements can be a tedious full-time job and can make even a “simple” job, like applying a hotfix, a complex, multi-step process that introduces far too much risk.

With Quest One™ Privileged Password Manager and Quest One™ Privileged Session Manager from Dell, managing privileged passwords is easy and far more secure. This white paper explains how.

Introduction
Even with two-factor authentication in place, passwords still present challenges.
The Defense community has come a long way with authentication. Instead of allowing users to authenticate with just usernames and passwords, organizations have implemented some form of two-factor authentication. Specifically, most of the Department of Defense (DoD) has moved to Common Access Card (CAC) integrated with public key infrastructure (PKI) to authenticate users, and even the administrators on these networks are starting to use dual certificates to perform administrative functions. This provides a solid level of assurance of who the users are and ensures nonrepudiation.

But even with the security infrastructure of CAC/PKI, there are many instances where passwords are still used on these networks. In particular, defense environments, like all IT environments, are full of service accounts and local accounts that are tightly woven into the functions of applications. Service
Maintaining compliance can require turning a highly-trained security engineer into a full-time password resetter.

**Maintaining compliance can require turning a highly-trained security engineer into a full-time password resetter.**

Accounts are used for applications that need to authenticate against either a domain or a local identity repository. These accounts may or may not be assigned any special permissions, but they authenticate with just a password. In addition, all Windows operating systems (servers and workstations) have a local administrator account and other local accounts, and platforms such as Red Hat Linux, Ubuntu, Fedora, Solaris, HP UX and even MacOS have root accounts. And all of these accounts have passwords.

Passwords exist in just about every environment. Some of them are buried in appliances or built into operating systems. These accounts and their passwords have been treated as incurring an “acceptable level of risk,” but that risk is becoming more and more difficult to accept. After all, we’re really just hoping: Hoping the people that know or have access to these passwords are honorable and will protect the passwords. Hoping that when they leave the organization, they magically erase the passwords from their memory. Hoping they change the passwords at the required intervals to meet compliance requirements. Hoping they use these accounts only for the purposes intended.

Managing passwords to meet requirements is a tedious and time-consuming job—but doing it right is critical to business continuity. Some organizations have delegated the management of service and administrative account passwords to a security team or even a single person. But these passwords must often meet requirements, such as DoD, Security Technical Implementation Guide (STIG) or DITSCAP/DIACAP requirements, that require regular password changes. Maintaining compliance can require turning a highly-trained security engineer into a full-time password resetter.

Why? When a service account password is reset in a typical Active Directory environment, it must also be entered everywhere the service is running; otherwise, the next time that service restarts, it will fail—which could affect hundreds of servers, cause an application outage and seriously hurt productivity. Most admins are accustomed to this problem and know that when a service account fails, they need to retrieve the password and reset it on the service to get the application going again. The larger the enterprise, the more pain this will cause. And, unfortunately, this task can be the first one overlooked in the heat of an application failure.

**The traditional way to manage privileged passwords**

Just applying a single hotfix is a multi-step process.

In an organization that puts some level of control around these privileged passwords, the daily life of an admin can get somewhat complicated. For example, suppose that in my organization, all passwords are managed by the security/auditing department. As an administrator, I need to apply a hotfix to an application, but this hotfix must be applied while I am logged on with the service account. Let’s look at all the steps required for this seemingly simple task:

1. I need to submit a request to the security/auditing department to justify my need for the password and the timeframe when I plan to use it.
2. A security auditor will consider my request.
3. Upon approval, the auditor will open a safe, retrieve the password and communicate it to me.
4. Now that I have the password, I can log on to the server running the application with the service account. I can then apply my hotfix (and do anything else I want to).
5. When I complete my task, I will notify the auditor.
The auditor will (or should):
6. Change the password in Active Directory.
7. Connect to each server where the service is running and enter the new password on the running service.
8. Document the new password and lock it back in the safe.

Finally the job of applying the hotfix is complete!

This may seem like a tedious process but it’s (close to) the right way to do business. These are common procedures, and for the most part, they provide a slightly better security posture than sharing the passwords between admins.

The problems with the traditional process
Of course, there are huge holes in this process:
• The workload and time required to perform these functions—Security auditors are some of the most highly skilled people we have. Do we really want to burn hours of their day resetting passwords?
• Risk of application downtime—If the auditor changes the password but fails to enter it on any one of the servers where the service runs, the service will fail.
• Too much power—A second problem is that the auditor—who is tasked with meeting compliance requirements and keeping the network running—has no idea what the admin did with that password while he had it. All the auditor can hope is that the admin had honorable intentions.
• Lack of visibility and accountability—Probably the most serious problem is all the unknowns. In this scenario, the security auditor has access to the password. If something malicious is done with the account, we have to look to the people who might know the password. Most auditors would not want to be in that position. Moreover, if more than one person has access to the password, auditing is an exercise in futility.

The solution: Quest One Privileged Password Manager and Quest One Privileged Session Manager from Dell Software
Managing and security privileged passwords is easy with Quest One Identity Solutions.
Quest One Privileged Password Manager and Quest One Privileged Session Manager make managing privileged password easier and far more secure. For example, the process of applying my hotfix using a service account now looks like this:
1. I open a browser and connect to a web interface for Quest One Privileged Password Manager. I look for the service account password I need and request it with a few clicks.
2. A security auditor receives an email saying I have requested the service account, reviews my brief justification and approves the request.
3. When I receive notification that my request was approved, I reconnect to the web UI of Quest One Privileged Password Manager and am allowed to check out the password for the time specified. I can then log on to the server and do my administration.
4. When I'm done, I check in the password. This check-in will automatically:
   • Initiate a password change to a randomly generated password based on an organization policy (for example, a password that has 30 characters, including 8 uppercase, 8 lowercase and 7 special characters).
   • Change the password everywhere the service is running to make sure enterprise applications continue to operate.

Benefits
The advantages of this process are significant:
• Time savings—Quest One Privileged Password Manager streamlines the workflow for requesting and approving use of a privileged password, saving valuable time.
• Business continuity—Quest One Privileged Password Manager automatically resets the password and changes it everywhere it is
Dell’s end-to-end security solutions ensure that your users, applications, critical data and mission are protected against internal threats.

required, eliminating the risk of application failure due to password issues.

• **Real-time visibility and accountability** — The security auditor can decide my justification is valid but want to audit my actions while I have access. Instead of allowing me to check out the password, he or she can simply grant my session directly to the server. I will receive notification my session request has been approved. Then I will connect to the Quest One Privileged Session Manager console, where I will see my approved session request and will be connected directly to the console of the server when I need to do my administration.

• **Auditing** — When I wrap up my work, I simply log out of my session. The security auditor then has the option to review my work through a DVR-like playback.

• **Security** — If the auditor grants my session directly to the server, I won’t even need to know the password for the service account.

**Conclusion**

Dell Software’s solutions for privileged accounts reduce the risk of improper use of administrative and service accounts through tightly controlled access rules—and at the same time, they significantly reduce the manual effort required to manage these privileged identities. Dell’s end-to-end security solutions ensure that your users, applications, critical data and mission are protected against internal threats—giving you the power to do more.

For more information about Dell Software’s solutions for privileged account management visit software.dell.com.

---

**About Dell Software**

Dell Software makes it easy to securely manage and protect applications, systems, devices and data to help organizations of all sizes fully deliver on the promise of technology. Our simple yet powerful software – combined with Dell hardware and services – provides scalable, integrated solutions to drive value and accelerate results. Whether it’s Windows infrastructure, the cloud and mobile computing, or networks, databases and business intelligence, we dramatically reduce complexity and risk to unlock the power of IT. For more information, visit software.dell.com.
For More Information

© 2013 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.