Privileged User Accounts under Control

Dr. Götz Güttich

Privileged user accounts, such as local administrator accounts, constitute a security risk. Also accounts of service providers, which can access systems of a company via remote management, encounter problems in practice. Attackers can hack these accounts and use the account-related rights to get access on the data of the affected organization. This threat is increasingly gaining importance considering the growing number of attempted attacks. Alongside with enhanced compliance requirements, the risks also increase due to the increased use of externally hosted applications and cloud services. Solutions on the management of privileged accesses address these issues. We have looked at what AdminBastion Suite from Wallix can provide in this context.

The AdminBastion Suite (WAB Suite) from Wallix is one of the solutions for a Privileged Access Management (PAM). It manages password administration, secures the access on important data and systems and monitors the activities running via privileged user accounts in real-time. And it does not matter whether these users are working internally or from external sources.

Specifically, the WAB Suite includes three key components, the Password Manager, the Session Manager and the Access Manager. These three components ensure that the correct users have access to the right resources at the right time during operation.

The WAB Password Manager stores the access data for administrator accounts, local accounts and database administrator accounts in a central vault, which has an ANSSI certification in France and an FSTEC certification in Russia. ANSSI works closely with the German authorities on cyber security and is the French counterpart for the German BSI (Federal Office for Information Security). There the data can be managed via a single console, i.e. created, hidden, displayed or changed. The end users do not get the passwords in normal operation, so it is possible to automatically use long, complex, random strings.

The WAB Session Manager handles and monitors all accesses of privileged users to devices and applications on the network while ensuring the auditing. Monitoring – and thus also alerting – are carried out in real time. Each access is always assigned to an unambiguous identity so that it is possible to take each user accountable for his or her actions.

After all, the WAB Access Manager is a web portal that allows users to access all the resources they need. The privileged access management functions across multiple sites, customers, or networks. This makes the product suita-

ble for use with cloud providers as well as for end users. Access to the desired systems is achieved by a single click during operation.

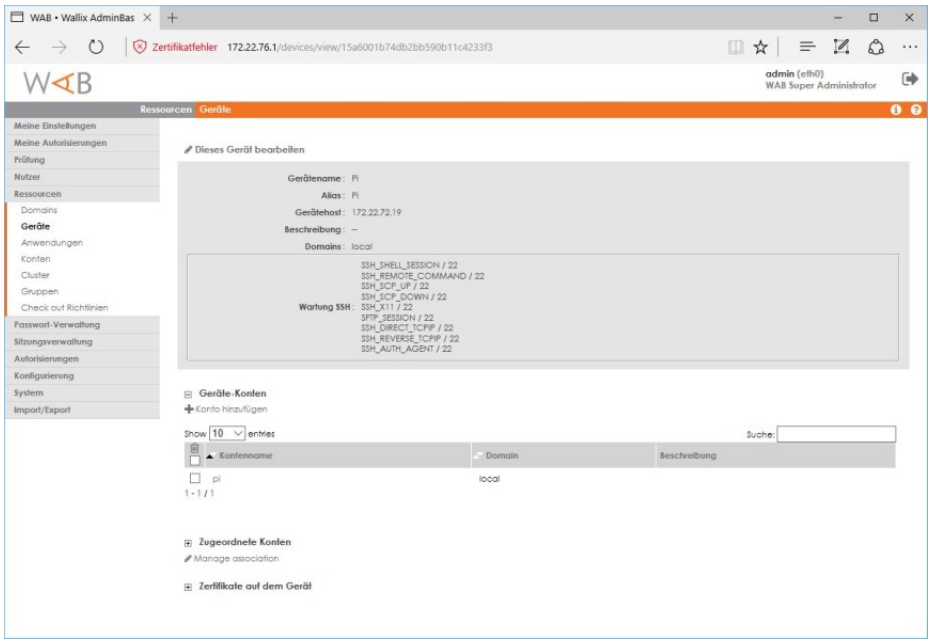
The test

For the test Wallix provided us with an appliance, on which the WAB Suite was preinstalled. We integrated this appliance into our environment, familiarized ourselves with the scope of the solution and managed privileged user accounts on our network. In addition, we recorded various sessions while using these accounts and tested the monitoring functions.

Putting into operation

To put the product into operation, it is sufficient to integrate the appliance or the virtual appliance (the product is also available in this form) into the network and start it. We then logged on to the local console of Debian Linux, which uses the Wallix appliance as an operating system and adapted the network configuration of the system to our environment. As soon as this was done, we could connect to the web configuration tool of the solution via the new IP address. The configuration tool first pointed out that we would have to change the default password (admin) of the admin account. This makes sense to ensure that no products with default passwords enter the productive mode. After changing the password, we were able to start the practical work.

The appliance operates as a virtual proxy, which means that the users access the Wallix solution, which then connects to the desired target system. This makes the product equally suitable for service providers and internal administrators in medium-sized companies. The configuration of the individual target computers does not have to be changed necessarily, so that direct logins can still work, if needed. But there is also the option, as mentioned above, to automate the password administration and leave it completely to the WAB Suite; in that case, the accesses are only provided via the Wallix solution. We will go into that later.



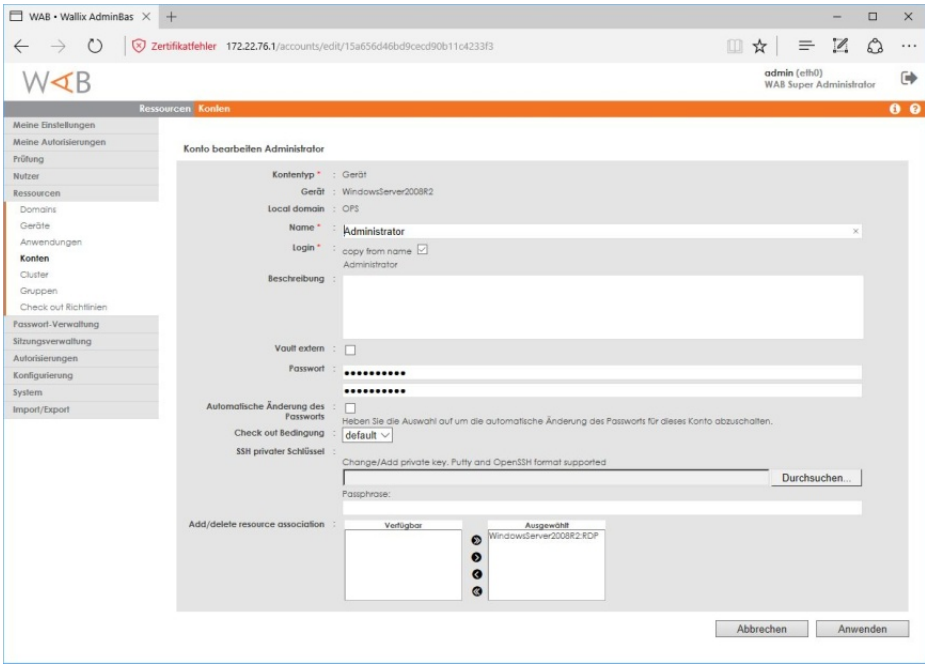
The device account for the SSH access at a Raspberry Pi under Linux

As part of our testing, we first took the opportunity to review the scope of the management tool. The solution works with a menu structure on the left, which makes all the functions of the Wallix product available. While we made ourselves familiar with the individual menu items, the connection to the appliance suddenly broke down. After a renewed login to the local console of the server, we realized that the solution had restored its old network configuration, which was located in a different subnet than our test environment. Therefore, we repeated the network configuration, once again logged in to the web interface and again adjusted the settings in the Network Settings. Afterwards the network connection remained stable.

The connection to a Windows server

After everything went as desired, we started to establish two connections - to a system running Debian Linux and a computer running Windows Server 2016. The Windows server was to be addressed via RDP, the Linux computer using SSH. To set up the RDP connection, we first changed to "Users / Accounts" and added a user account with normal user rights to the appliance. Through this account, the users could log on to the Wallix system later to access their assigned computers. After

that, we immediately set up a group into which our local user accounts were to be integrated. With the help of the groups, it is possible to grant specific users – e.g. the employees of the IT department or even external users – different rights than others on the network.

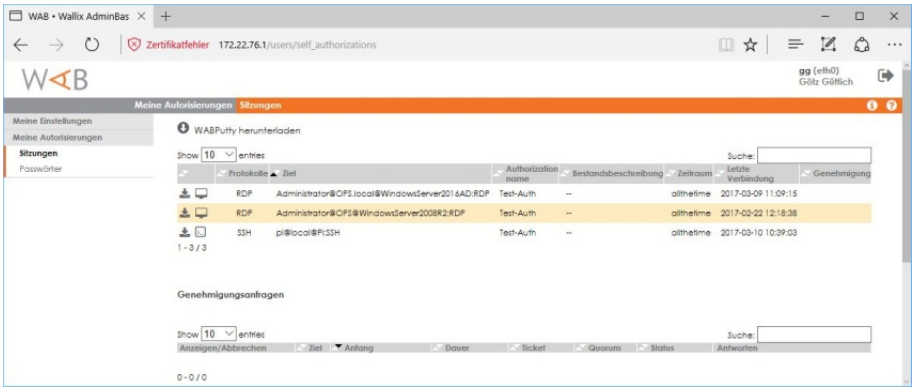


A Windows administrator account for RDP accesses

Then we turned to "Resources / Devices" and set up a new device there. We gave it the name "Windows2016AD" because it was an Active Directory Controller. We also added the IP address and the domain.

In a next step, we selected the required RDP protocol. At this point, the system supports Telnet, RLOGIN and VNC in addition to RDP and SSH. If necessary, the relevant employees are able to specify the ports used and the like when configuring the protocols. Once the device existed, we were able to switch to "Resources / Accounts" and set up a device account for the new device. This was used to perform the login on the end device. Since we wanted to secure our privileged accounts with the Wallix solution, we used the administrator account of the Windows server for this purpose. At this point, it is also possible to store private keys, for example for SSH accounts or passphrases, in addition to passwords. After we set up our account with password and description, we assigned it directly to our device. As part of the device account configuration, there is also the option to activate the already mentioned automatic password change. This makes it possible to completely leave the password management for the privileged accounts (or, if desired, also for all accounts, but for the privileged accounts it makes the most sense) to the Wallix solution.

To do this, you only have to configure the complexity of the passwords and activate the automatic password change. After this, AdminBastion generates the corresponding passwords for all affected accounts at regular intervals - the interval is definable - and stores them in its password vault and activates them on the relevant target systems. In this case, the passwords are no longer known to the users and they can access their computers exclusively via the Wallix product. After defining the device account, we set up a new group under "Resources / Groups" and added the new account to make it usable for the users. Finally we moved to the " Authorizations / Manage Authorizations" section, also set up a group and released the RDP proto-



After logging in with a user account, the systtem presents a list containing the available clients

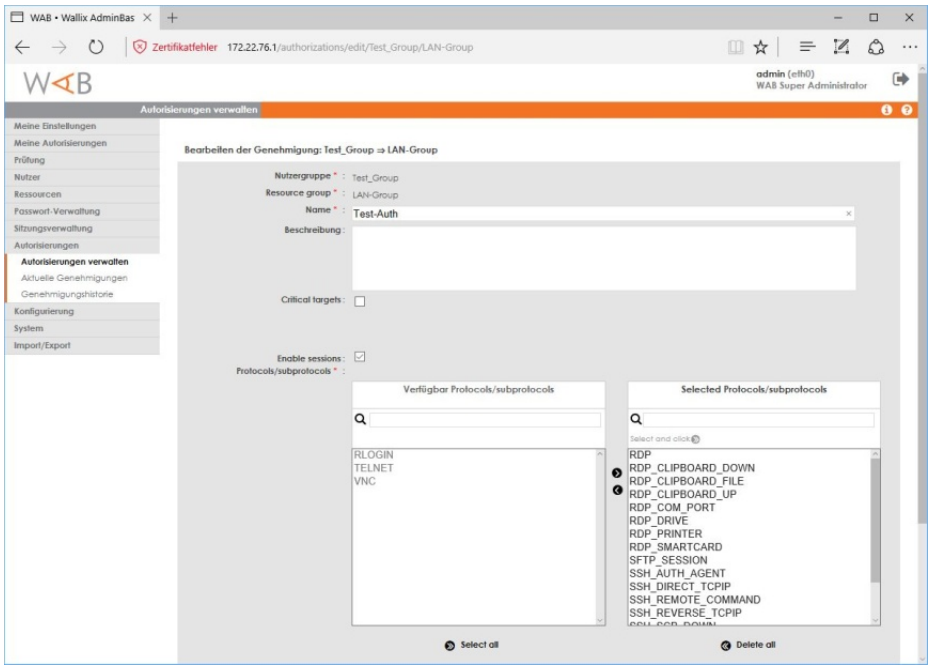
col for it. At the same time, we activated the Session Recording - one of the highlights of the Wallix product, which will be discussed in more detail later. The first connection was thus ready for use.

The first access

To use the new connection, we logged on to the appliance with our previously created user account and landed in a web interface, which had two menu items. The first is called "My Settings" and allows you to specify the language to be used for the account and to enter the email address of the user. SSH and GPG keys can also be stored here.

validity. Both methods worked right away in the test.

RDP protocol. After that we had to define the device ac-



For our test group, we released the protocols RDP and SSH

More interesting is the menu item "My authorizations", because it contains a list of all the systems that the respective user account is allowed to access, in our case it was naturally only the Windows server at this time.

In addition to the name of the system, the mentioned list includes information such as, for example, the protocol to be used and the last connection. In addition, it provides two icons for each target system. One allows you to download an RDP configuration file, which allows you to call up the connection via a single click. If a user selects this path, he must always enter his password in order to establish the connection. Alternatively, the responsible persons can make an immediate connection via the second icon. No password is required, but the access only works within 30 seconds, after which it loses its

By the way, RDP accesses can not only be realized via the web interface. It is also possible to log on directly to the appliance with an RDP client. The Wallix solution then details in a list those RDP target systems, which can be accessed by the respective account, and establishes the connection at the touch of a button. If necessary, there is also the option of making individual applications available via RDP on the network using a Windows Jump Server with installed terminal services or remote desktop roles using the WAB Suite.

The configuration of the SSH access

Next, we dealt with the configuration of the SSH access to our Debian server. The procedure is similar to the RDP configuration. First, we set up the device with IP address and name. Here we naturally activated SSH instead of the

count with password and the like; at this point we used the root account of the server and also deactivated immediately the automatic password change. After we added the new account to the Debian device and added it to the group, we released the SSH protocol in the authorizations, after which the connection was available.

SSH access as user

The SSH access in practice is somewhat different than working with RDP. Users can access the SSH target system via the list of their authorizations, but the connection setup for Windows works only with a special version of the putty client called WABputty, which can be downloaded directly from the user interface of the appliance. As soon as this has been installed on the used client computer, SSH accesses are possible without problems. Otherwise users have the op-

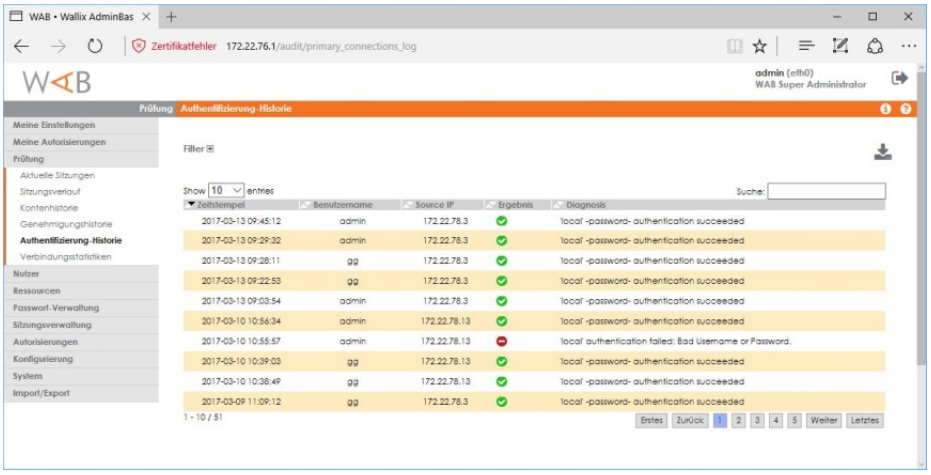
tion to connect to the Wallix appliance via SSH. This works both from Linux, as well as with putty under Windows. Similar to accesses with the RDP client, the appliance then presents the users with a list of the available target systems and establishes the connection after selecting an entry.

Test continued

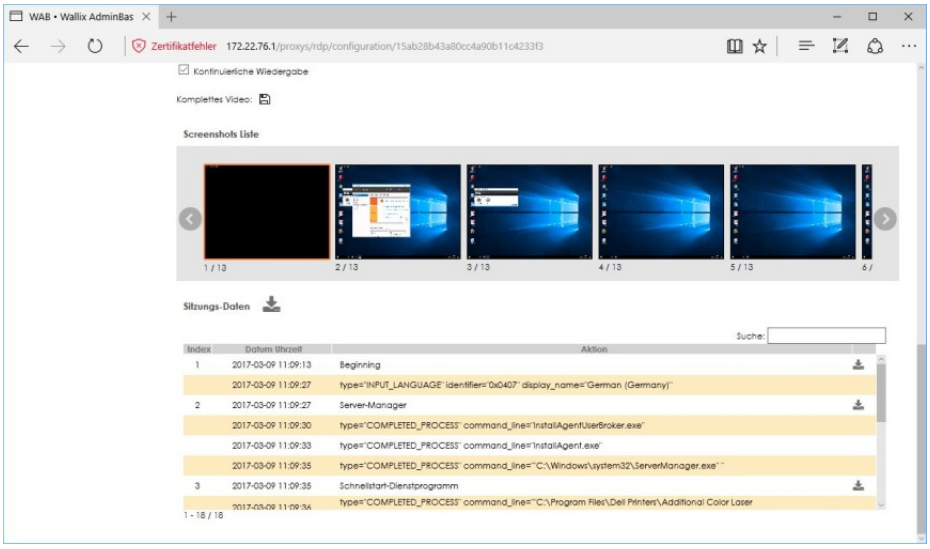
In the further course of the test, we became familiar with the functionality of the Wallix solution in detail, worked with the recording features for the sessions, and added to our environment other target systems, for example Windows server 2008 R2 and Fedora Linux. It would go beyond the scope of the test to go into every single feature of the solution, but it makes sense to point out the recording features of the product.

If an authorized user logs in to the appliance, he has the option of switching to the "Review" area. There he can view a list of the current sessions and the session history in the past.

If the corresponding function has been activated, there is an option for each session to analyze the history in detail. For SSH, this is available as text and ttyrec files. In this context, we must particularly emphasize the support of ttyrec, since this tool not only makes it possible to read the commands entered, but can also output them in real-time on a console so that the administrator always sees what exactly when has happened. For RDP connections, the WAB-Suite creates flash videos that can be viewed and downloaded directly from the web interface. In addition, it also provides screenshots generated from the videos, which are created on the basis of identified actions. Here, too, it is clear at any time which actions were carried out at what time, which helps to carry out audits and to ensure their compliance. Comprehensive statistics on the connections, which, for example, visualize the number of WAB connections per user as well as the target connections by duration or by date, complete the scope of information offered by the appliance.



Comprehensive statistics, such as the history of login and login attempts in this example, help to keep an eye on all activities



A recorded RDP session

Conclusion

The test of the Wallix AdminBastion left a remarkably good impression. The product not only enables easy and secure access to the privileged user accounts of the existing network components, but also handles the password management and, if desired, provides applications on the network. Comprehensive functions for auditing, which clearly show who has done what and when, round off the range of services provided by WAB Suite.