Need to know details of Windows Server 2012 Kerberos

Essential knowledge about Microsoft Kerberos with Claims

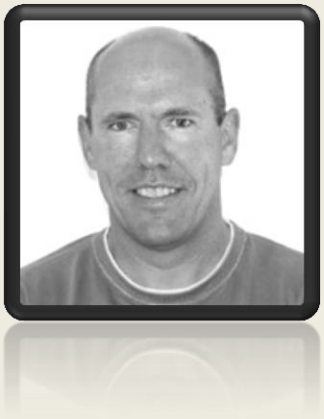
Author

Tony Murray

Cayosoft | Need2Know

About the Author

Tony has been working in the IT industry in the area of messaging and directory services for over 20 years. He currently lives and works in New Zealand and runs the popular "Active Directory Discussions" mailing list at www.activedir.org and blogs at www.open-a-socket.com. While waiting to become a captain of industry he somehow stumbled into computers (not always figuratively). He thinks this has something to do with unresolved emotional trauma from having broken the plastic keypad on his Sinclair ZX81 while in his teens. Despite later having been exposed to an early Microsoft Exchange Server 4.0 Beta, he somehow made the switch from Unix to the world of Windows and started to get involved with Exchange and, more recently, Active Directory. Tony has been a Microsoft MVP (Directory Services) since 2002.



Email: tony@fish-eagle.net
LinkedIn: www.linkedin.com/pub/tony-murray-smith
Twitter: @MrTweetTastic

Introduction

- **Kerberos protocol**
- **Token used for authorization**
- **Contains SIDs**
- **Seamless access to network resources**

Kerberos is a highly secure authentication protocol that allows two parties to verify their identity to one another. Kerberos tokens are issued to users during Active Directory user authentication. The user's token contain the necessary authorization information for Windows to make decisions about granting access to network resources, e.g. files, shares, Exchange, IIS web sites. Token include the domain security identifier (SID) of the user account, together with the SIDs of all the groups that the user is a member of (both directly and transitively). The token may also include the SIDs contained within the user's SIDHistory attribute, to support seamless access to resources in legacy domains from which the user account has migrated. The token can accommodate a maximum of 1024 SIDs.

Strengths

- **Standards-based**
- **Secure**

The Kerberos protocol is highly secure as it uses the AES encryption standard. The authentication mechanism used within Active Directory is also compliant with Kerberos V5 (see RFC4120), which means that it can be used to gain access to non-Windows resources that are Kerberos-enabled.

Weakness

- **Token bloat**
- **Built-in limits**
- **Interoperability**
- **Complexity**

Problems can occur when the size of the token exceeds the member buffer allocated by the system hosting the resource being accessed. Typically, this is due to the token containing too many groups and is exacerbated by the use of SIDHistory.

The phenomenon, known as "token bloat", can generally be avoided by modifying the MaxTokenSize registry value, which effectively increases the buffer size to handle larger tokens. Microsoft has increased the default MaxTokenSize from the Windows 2000 default of 8KB to 12KB in Windows 2000 SP2 and to 48KB in Windows Server 2012.

Opportunities

- **Claims**
- **GPO Setting**

Windows Server 2012 has changed the game somewhat in that claims information used by Dynamic Access Control (DAC) is stored within the token. The increased token size is offset to a certain extent by the larger MaxTokenSize default of 48KB. There are also useful Group Policy settings that can be used to configure the MaxTokenSize value (above 48KB if required) as well as to set warnings when the token size for a specific user is close to the MaxTokenSize value.

Threats

- **Open to exploits**
- **Compatibility**

The problems generated when either the number of SIDs in the token exceeds 1024, or when the token is larger than the buffer size can be difficult to diagnose (especially pre-Windows 2012). While this is not a security vulnerability itself, the complexity can potentially open infrastructures to potential exploits and increased support costs.

By default Windows Server 2012 Domain Controllers implement resource SID compression, whereby the token size is reduced by removing repeating information common to SIDs from resource domains. While all Windows systems from 2000 onwards support the resource SID compression, other non-Windows systems, including some NAS devices may not support it. The feature can however be turned off using Group Policy.

Conclusion

Kerberos tokens are central to the Windows domain authentication process and provide essential authorization information for accessing network resources. Constraints such as the maximum number of SIDs that can be stored in the token, as well as the default buffer size allocated to handling the token, have historically created problems for organizations that have a large number of groups and use SIDHistory to facilitate domain migrations. Windows Server 2012 increases the size of the token (to support DAC) and yet decreases the likelihood of token size becoming issue through a range of methods, including: increasing the default MaxTokenSize; allowing the value to be easily configured using Group Policy; providing warning events for large token use; and implementing Resource SID compression by default.

Cayo | Software™

To get additional practical whitepapers from Cayo | Software, please visit www.cayosoft.com.

WARRANTY

The information contained in this document is subject to change without notice. Cayo|Software makes no warranty of any kind with respect to this information.

Cayo | SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cayo | Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

Cayo | and Cayo | Software are trademarks of Cayo | Software, LLC. in the United States of America and other countries. Other trademarks and registered trademarks used in this document are property of their respective owners.

For additional information please see our web site at (www.cayosoft.com)