Mainframe Virtual User Groups

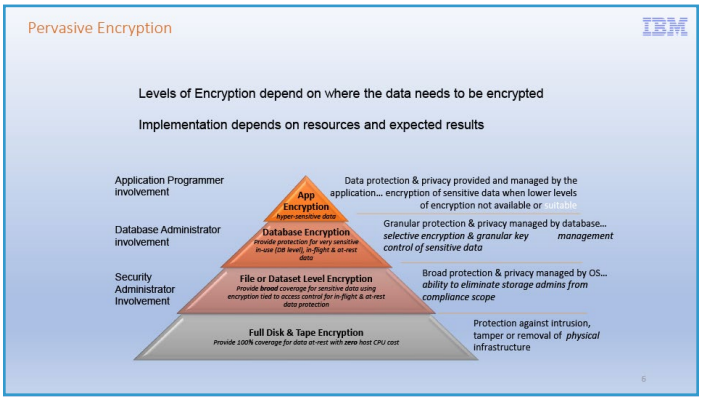
VIRTUAL IMS USER GROUP

NEWSLETTER 98 | SEPT. 2024

Virtual IMS User Group Presentation

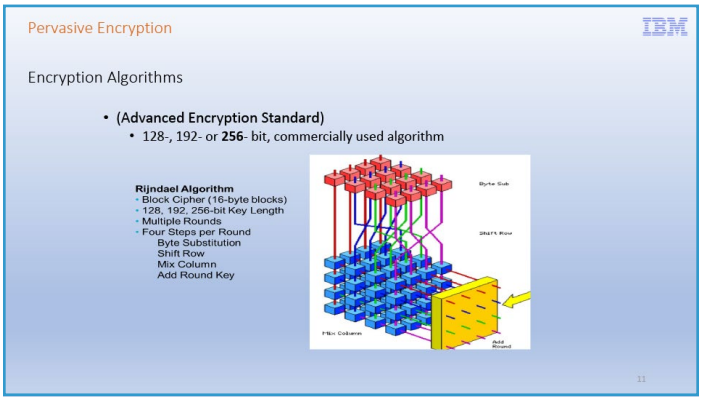
ENHANCING IMS PERFORMANCE WITH DATASET-LEVEL ENCRYPTION

In a recent virtual user group session, Dennis Eichelberger, a veteran with over 45 years of mainframe and database systems experience, presented an insightful discussion on implementing dataset-level encryption for IMS (Information Management System). Hosted by Amanda Hendley, Managing Editor at Planet Mainframe, the session delved into the nuances of transitioning IMS OSAM datasets to VSAM linear datasets and the broader benefits of pervasive encryption. This blog post aims to encapsulate the essence of Eichelberger's presentation and provide a comprehensive understanding of the subject while exploring the implications for enterprises today.



The session began with an overview of pervasive encryption, a concept that is becoming increasingly critical in today's regulatory and competitive landscape. As organizations face mounting pressure to protect sensitive data, Eichelberger highlighted encryption as a proactive measure against data breaches, which can often go undetected for months or even years. The importance of encryption lies in its ability to render data unreadable, even if it falls into the wrong hands, thus ensuring that personal, financial, and other sensitive information remains secure.

Eichelberger further elaborated on the specific encryption algorithms that are foundational to this process, particularly the Advanced Encryption Standard (AES) with a 256-bit key, which is widely recognized for its strength and reliability. He also discussed the different types of keys involved in the encryption process, including master keys, which are used to protect other keys, and user keys, which are applied directly to the data. This detailed examination underscored the layered approach required to implement effective encryption, ensuring data security at every level.

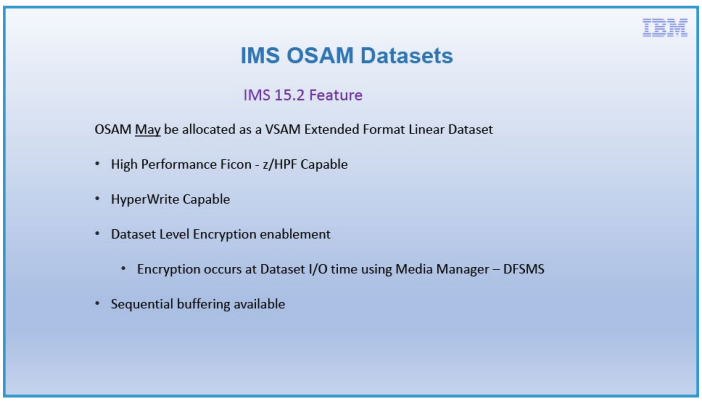


Enhancing IMS Performance with Dataset-Level Encryption

Continued

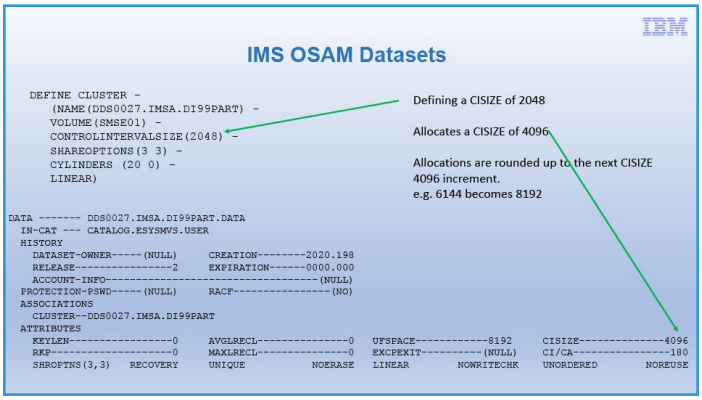
A pivotal part of the presentation focused on the transition of IMS OSAM datasets to VSAM linear datasets, a shift that became possible with the release of IMS 15.2 in March 2020. OSAM, an access method traditionally used by IMS, is known for its high-speed processing capabilities, making it a preferred choice for many organizations. However, OSAM's limitation was its inability to be encrypted using DFSMS, a critical drawback in today's security-conscious environment.

The introduction of IMS 15.2 brought a significant change by enabling OSAM datasets to be reallocated as VSAM linear datasets. This transition not only allows the use of DFSMS for encryption but also opens the door to additional benefits, such as high-performance FICON (Fibre Connection) and Hyperwrite capabilities. These enhancements contribute to improved performance and reliability, making the transition an attractive option for organizations looking to bolster both security and efficiency.



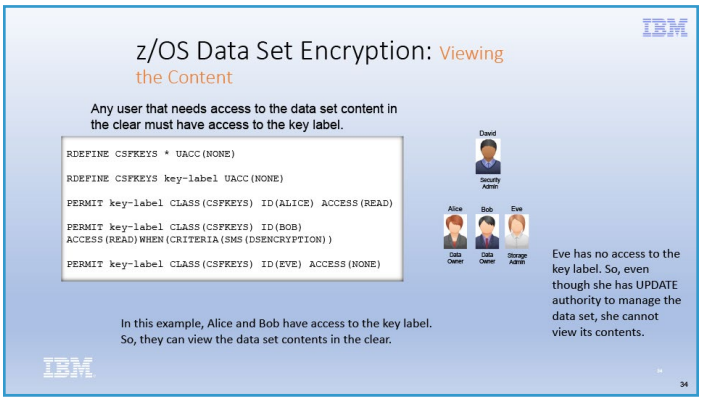
Eichelberger didn't shy away from discussing the technical intricacies of this transition. He delved into the changes required in dataset allocations and the necessity for database outages during the reallocation process. These outages, while potentially disruptive, are a necessary step in ensuring that the transition is smooth and effective. Eichelberger also emphasized the importance of control interval size, a critical factor that can significantly impact performance and storage efficiency.

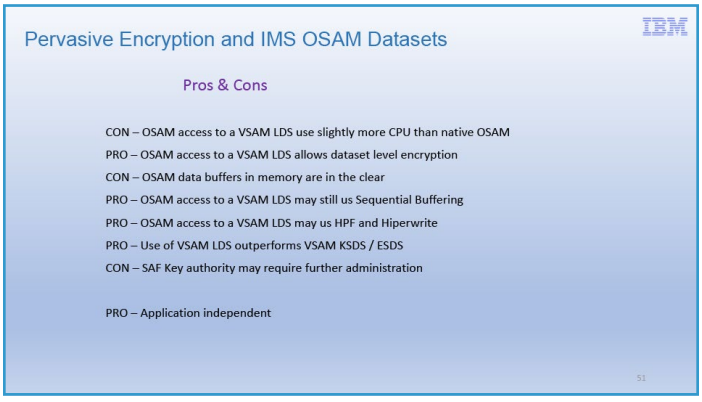
To facilitate the transition, Eichelberger explained the process of allocating a linear dataset using IDCAMS input, a method that, while technically detailed, is often simplified through the use of Storage Management Subsystem (SMS) data classes. These data classes provide a more user-friendly approach, allowing organizations to streamline the implementation process without sacrificing control over the encryption settings.



Security considerations were another crucial aspect of the presentation. Eichelberger elaborated on the significance of managing key labels, which are essential for accessing encrypted datasets. He stressed the importance of ensuring that all relevant jobs and tools have the necessary access to these keys, as failure to do so can lead to operational disruptions. For instance, Eichelberger shared a real-world example where a lack of access to the key label resulted in a job failure, highlighting the practical challenges that can arise if security configurations are not meticulously managed.

Enhancing IMS Performance with Dataset-Level Encryption
Continued





This example served as a practical reminder of the potential pitfalls and the need for vigilance in managing encryption keys. Proper key management not only ensures smooth operations but also enhances the overall security posture of the organization by preventing unauthorized access to sensitive data.

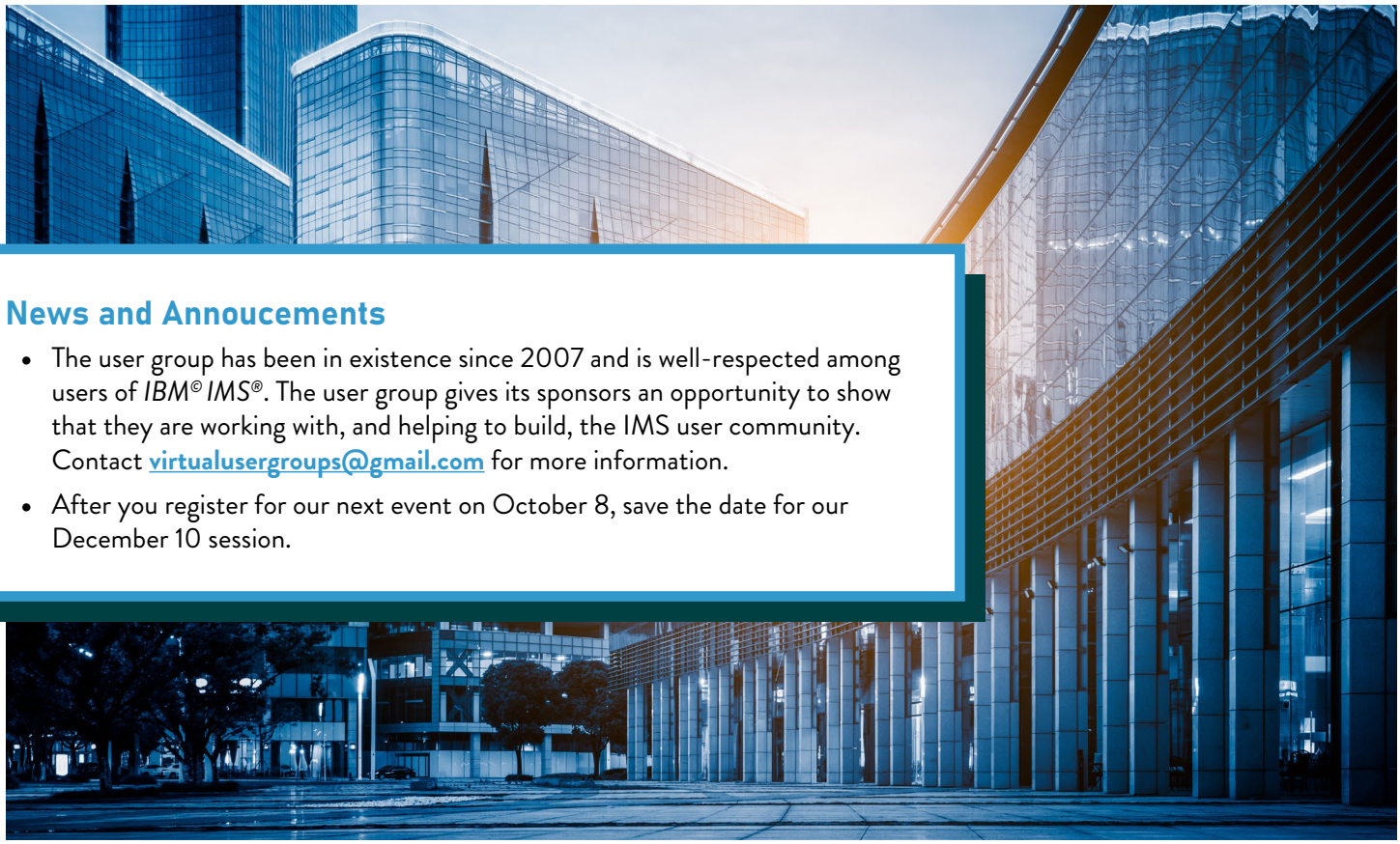
The session concluded with a balanced discussion on the pros and cons of dataset-level encryption. Eichelberger reaffirmed the benefits, such as application independence, enhanced security, and the ability to comply with stringent regulatory requirements. However, he also acknowledged the potential drawbacks, including the possibility of increased CPU usage, which can impact overall system performance.

Eichelberger shared an intriguing case study where a customer's transition from Guardian encryption to dataset-level encryption led to a significant increase in CPU and runtime. This was primarily due to the additional encryption of index datasets and IMS Log Data Sets (ILDS), which had not been fully accounted for in the initial planning stages. This case study underscored the importance of thorough testing and careful consideration of all factors before making the transition.

In summary, Eichelberger's presentation provided a thorough exploration of IMS dataset-level encryption, offering valuable insights into its implementation and benefits. For organizations looking to enhance their data security, the transition to VSAM linear datasets with encryption presents a compelling opportunity. By understanding the technical requirements, conducting thorough testing, and managing security considerations effectively, businesses can not only safeguard their data but also optimize IMS performance, ensuring a robust and secure environment for their operations.

Mainframe Virtual User Groups

NEWSLETTER 98 | SEPT. 2024



News and Annoucements

- The user group has been in existence since 2007 and is well-respected among users of *IBM© IMS®*. The user group gives its sponsors an opportunity to show that they are working with, and helping to build, the IMS user community. Contact virtualusergroups@gmail.com for more information.
- After you register for our next event on October 8, save the date for our December 10 session.

About the Virtual IMS User Group

The Virtual IMS User Group is an independently-operated vendor-neutral site run by and for the mainframe IMS user community. This is a mainframe IMS information website, not in any way related to, sponsored, or approved by IBM, which is the legitimate owner of the trademark, and any use of the mark in the URL or the body of the site is for information, education, and opinion expression purposes. The Virtual IMS user group was established as a way for individuals using IBM's IMS for z/OS database to exchange information, learn new techniques, and advance their skills with the product. Anyone with an interest in IMS for z/OS is welcome to join the Virtual IMS user group and share in the knowledge exchange.

SPONSOR

bmc