IBM Security

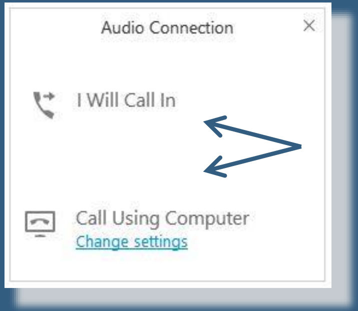
# Is Your Guardium Environment Secure & Supportable?

IBM SECURITY SUPPORT OPEN MIC, presented by Ian Kelly, Sr. Adv. Guardium Support Engineer

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

*You will not hear sound until the host opens the audio line.*

For more information, visit:
**http://ibm.biz/WebExOverview_SupportOpenMic**



**<u>NOTICE</u>:** BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.

26 October, 2017

IBM®

# Introduction

- Guardium Security
  - Configurations that affect security
  - Keeping your data safe
- Supportability
  - The customer part of the partnership
  - Access to your system when needed

# Agenda

- Shared Secret
  - What is the ‘Shared Secret’ and why is it important?
- User ID’s & Password
  - What ID’s exist on my system and who uses them?
- Ports and Firewalls
  - Which Ports do I need open and why?
- Backups and Archives
  - Once data leaves the Guardium Appliance is it still secure?
- Supportability Options
  - Making sure the correct diagnostics can be collected when / if needed

# Shared Secret

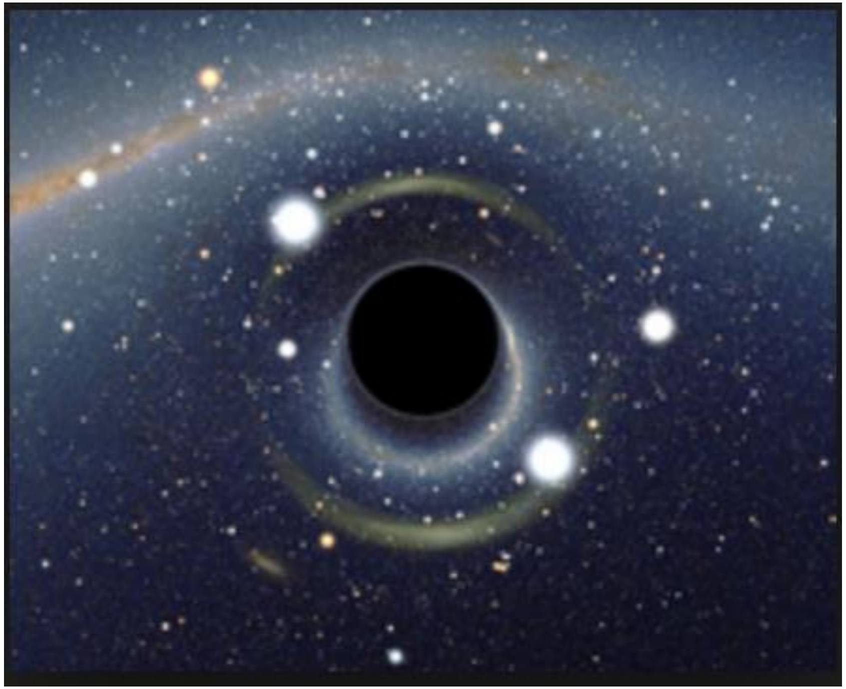
- Customer part of the encryption key
  - This makes your system unique and secure to you (Critical)

- “I don’t need to worry about this as I only have a standalone appliance”
  - Wrong, still critical !!!

# What is NULL?

- Is it Blank?
- Is it a Space?
- Is it a NULL?

- All of the above !



# Guardium keeps track of Shared Secrets

- Is this the Role of Guardium or the Users?

- Key Point :
  - Make sure you are aware of all the shared secrets your environment has ever used, including standalone !

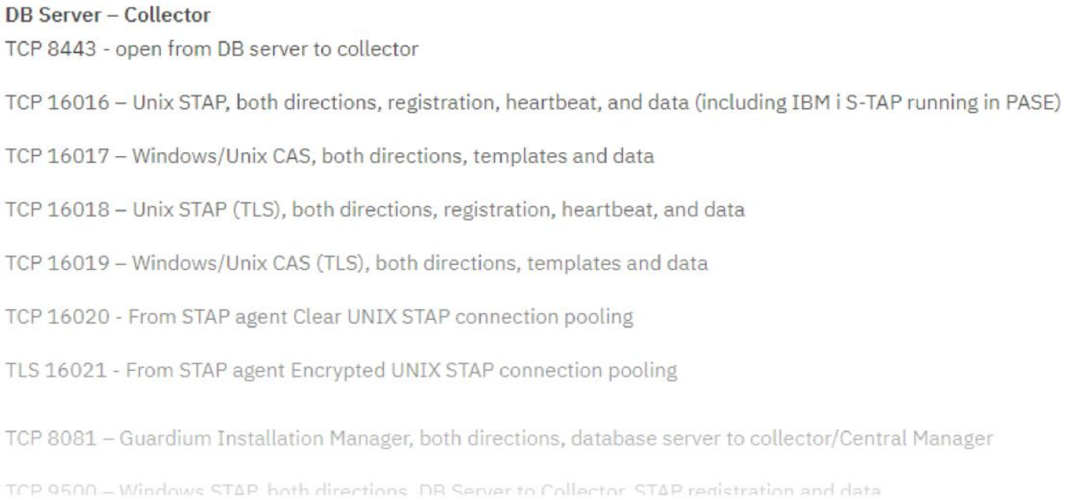
# User ID’s and Passwords

- **Via SSH**
  - CLI - The most common user login via SSH
    - Very important to keep restricted but known
    - Normal mode / recovery mode
  - guardcliX - Used to provide alternatives to CLI
    - ( guardcli1 / guardcli2 …. guardcli5)
  - Root - Restricted to support usage
    - Customer MUST to keep note of passkey away from the appliance
  - Mysql - Restricted to internal processes
  - Aggregator - Restricted to internal processes
  - Tomcat - Restricted to internal processes
- **Via GUI**
  - Accessmgr
  - Admin
  - GUI USERS with CLI privileges
  - INV_1 / 2 & 3
  - Customer user ID’s

# Ports and Firewalls

## Guardium v10.0/10.1/10.1.2/10.1.3 and v9.0/9.1/9.5 Open Ports

- https://www-01.ibm.com/support/docview.wss?uid=swg21973188



**DB Server – Collector**

TCP 8443 - open from DB server to collector

TCP 16016 – Unix STAP, both directions, registration, heartbeat, and data (including IBM i S-TAP running in PASE)

TCP 16017 – Windows/Unix CAS, both directions, templates and data

TCP 16018 – Unix STAP (TLS), both directions, registration, heartbeat, and data

TCP 16019 – Windows/Unix CAS (TLS), both directions, templates and data

TCP 16020 - From STAP agent Clear UNIX STAP connection pooling

TLS 16021 - From STAP agent Encrypted UNIX STAP connection pooling

TCP 8081 – Guardium Installation Manager, both directions, database server to collector/Central Manager

TCP 9500 – Windows STAP, both directions, DB Server to Collector, STAP registration and data

# Backups and Archives

- Where do I store backup and archives, and are they secure ?
  - What is the difference between a backup and an archive?
  - Why would I need to store backups in a secure place?

# Supportability Options

- Support of Guardium appliance
- Methods of communication with support
  - Phone & Email
  - WEBEX
  - Support Execute
- Must Gathers
  - Run must gathers from time to time for your own use and get to know them
- Root access
  - Know your passkey without needing CLI Command at the time

# What we have covered today

- Shared Secret
  - The ‘Shared Secret’ and why is it important
- User ID’s & Password
  - ID’s on my system and who uses them
- Ports and Firewalls
  - Ports I need open and why
- Backup’s and Archives
  - Is data secure after it leaves the Guardium Appliance
- Supportability Options
  - Making sure the correct diagnostics can be collected when and if needed

# Questions for the panel

***Now is your opportunity to ask questions of our panelists.***

**<u>To ask a question now:</u>**

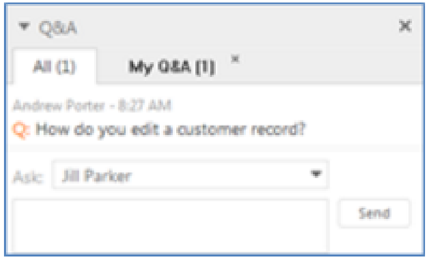
**Raise your hand by clicking Raise Hand.** The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

**or**

**Type a question in the box below the Ask drop-down menu in the Q&A panel.**

**Select *All Panelists* from the Ask drop-down-menu.**

**Click Send.** Your message is sent and appears in the Q&A panel.



Andrew Porter - 8:27 AM

Q: How do you edit a customer record?

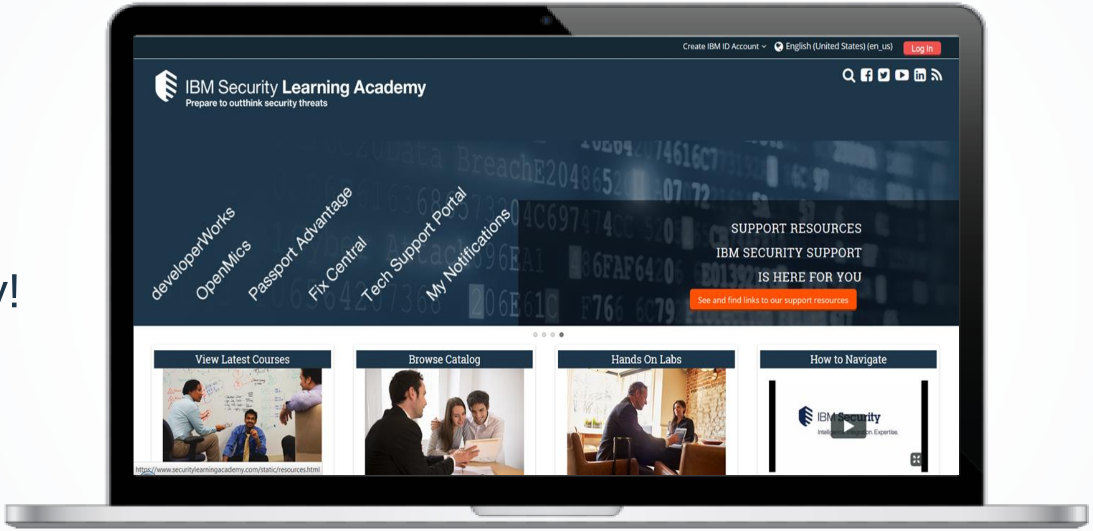
**<u>To ask a question after this presentation:</u>**

- **You are encouraged to participate in the dW Answers forum:** [http://ibm.biz/guardiumforum](http://ibm.biz/guardiumforum)

# IBM Security Learning Academy

www.SecurityLearningAcademy.com

New content published daily!



Learning at no cost!

Learning Videos ● Hands-on Labs ● Live Events

# Where do you get more information?

- **Questions on this or other topics can be directed to the product forum:** http://ibm.biz/guardiumforum

- **Technote** Guardium v10.0/10.1/10.1.2/10.1.3 and v9.0/9.1/9.5 Open Ports https://www-01.ibm.com/support/docview.wss?uid=swg21973188

- **Security Learning Academy:** www.SecurityLearningAcademy.com
- **Get started with IBM Security Support:** ibm.biz/Security-Support-Start-Here
- **IBM Support Portal:** ibm.com/support
- **Sign up for My Notifications:** ibm.com/software/support/einfo.html

- **Follow us:**

IBM Security

# THANK YOU

FOLLOW US ON:

facebook.com/IBMSecuritySupport

youtube/user/IBMSecuritySupport

@askibmsecurity

SecurityLearningAcademy.com

securityintelligence.com

xforce.ibmcloud.com

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®