特權帳號管理

深入探討特權帳號管理系統整合運用

August 2024

鉉迪資訊

介紹

鍾迪 Andy Chung

- 現職：
  - 鋐迪資訊股份有限公司-資深技術顧問
- 學歷：
  - 加州長堤大學 CSULB 碩士
- 專案建置經歷 (20年)：
  - 政府、電信、航空、學校、海外：50個專案+
- 專業能力：
  - 身份管理系統規劃與建置
  - 帳號整合同步規劃與建置
  - 單一簽入系統規劃與建置
  - 特權管理系統規劃與建置
  - 多因素認證系統規劃與建置
  - Java / Linux Shell / SQL/ LDAP 開發
- 專業證照：
  - Access Manager Certified Professional Exam
  - Certified NetIQ Identity Manager Administrator (CNIMA)
  - Micro Focus Access Manager Specialization
  - IBM DB2 UDB Family Fundamentals
  - CompTIA LINUX+
  - Novell Certify Engineer (CLE)
  - Novell Certify Linux Professional (NCLP)
  - Security and Identity Management Technical Specialist
  - Novell Certify Linux Administrator (NCLA)
  - Access Management Technical Certification
  - Identity and Access Management Knowledge Check
  - Security Operations Knowledge Check

課程大綱

1. PAM概念
2. 代登與測錄
   - Windows與Linux與應用程式
   - 展示 – 自做教學影片
3. 密碼生命週期
   - 定期自動改密碼
   - 展示 – 密碼設定畫面
4. 應用程式整合
   - 應用系統連線帳密整合
   - 展示 – 不同語言整合，借特權密碼
5. PAM擴展的運用
   - 展示 – SFTP操作記錄側錄

PAM概念

電腦密碼歷史

CTSS 操作系統（1961年）
第一個實現密碼保護功能的電腦系統。用戶都有自己的賬戶和密碼

MULTICS 操作系統（1965年）
提供一個高度安全的計算環境。設計中包含了多用戶、多級安全的概念，並且使用密碼來控制對系統的訪問

UNIX 操作系統（1970年代）
加入密儲存密碼的概念，將密碼以加密後的形式儲存在系統的密碼文件（如 /etc/passwd）中。

商業電腦和個人電腦（1980年代）
操作系統如 MS-DOS、Windows 和 Macintosh 系統都開始提供基於密碼的登錄機制

網路和互聯網時代（1990年代及以後）
隨著網路和互聯網的普及，密碼保護變得更加重要。這一時期還引入了雙重認證和其他增強的安全措施。

為何一直使用密碼

1. 簡單且易於理解
2. 成本效益高
3. 普遍接受和廣泛應用
4. 靈活性
5. 可控性
6. 兼容性
7. 廣泛的支持和基礎設施
8. 相對的隱私性
9. 應用範圍廣泛

到處都是密碼

資訊安全歸納

使用新技術防止駭客入侵

保護高權限帳號密碼

IPS　IDS　WAF　防毒　防火牆

特權帳號管理系統

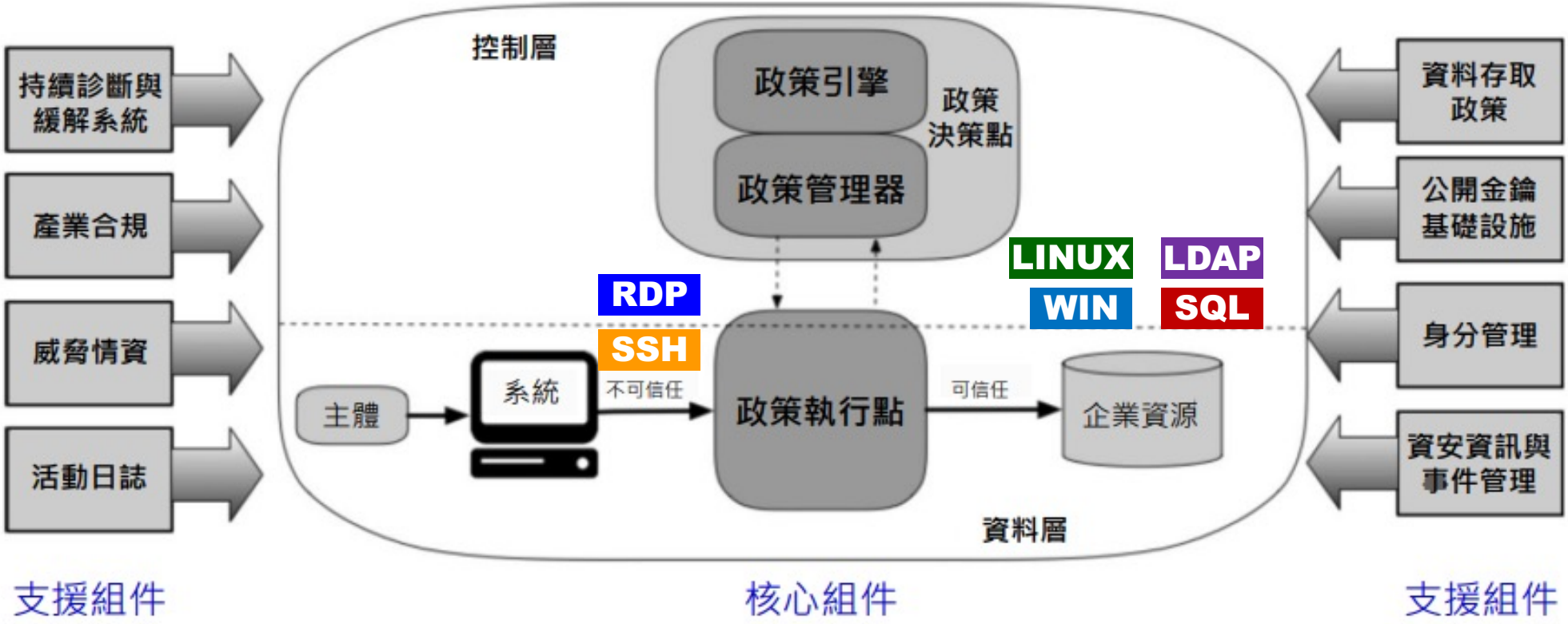
PAM知名的品牌

1. CyberArk
2. BeyondTrust
3. IBM Security Verify Privilege Manager
   (Thycotic, Centrify, Delinea)
4. One Identity Safeguard
5. ManageEngine PAM360
6. Wallix
7. Osirium
8. Hitachi ID Bravura Privilege

為什麼需要特權帳號管理系統

- **防止內部威脅** -> 未受控的特權帳號可能被惡意員工濫用，造成重大損失。
- **合規要求** ->法規要求對特權帳號進行嚴格管理和監控。
- **最小權限原則** ->確保僅擁有完成工作所需的最低權限，減少風險。
- **活動審計與監控** ->可提供記錄和監控特權帳號的所有活動。
- **防止特權濫用** ->防止特權帳號被未授權的人員濫用。
- **應對外部攻擊** ->減少攻擊成功的機會。
- **自動化和精簡管理** ->減少手動操作錯誤並提高效率。
- **跨平台管理** ->統一管理特權帳號，提供一致的安全控制。
- **應急響應** ->發生安全事件時，可以迅速撤銷特權帳號的訪問權限，減少損失。

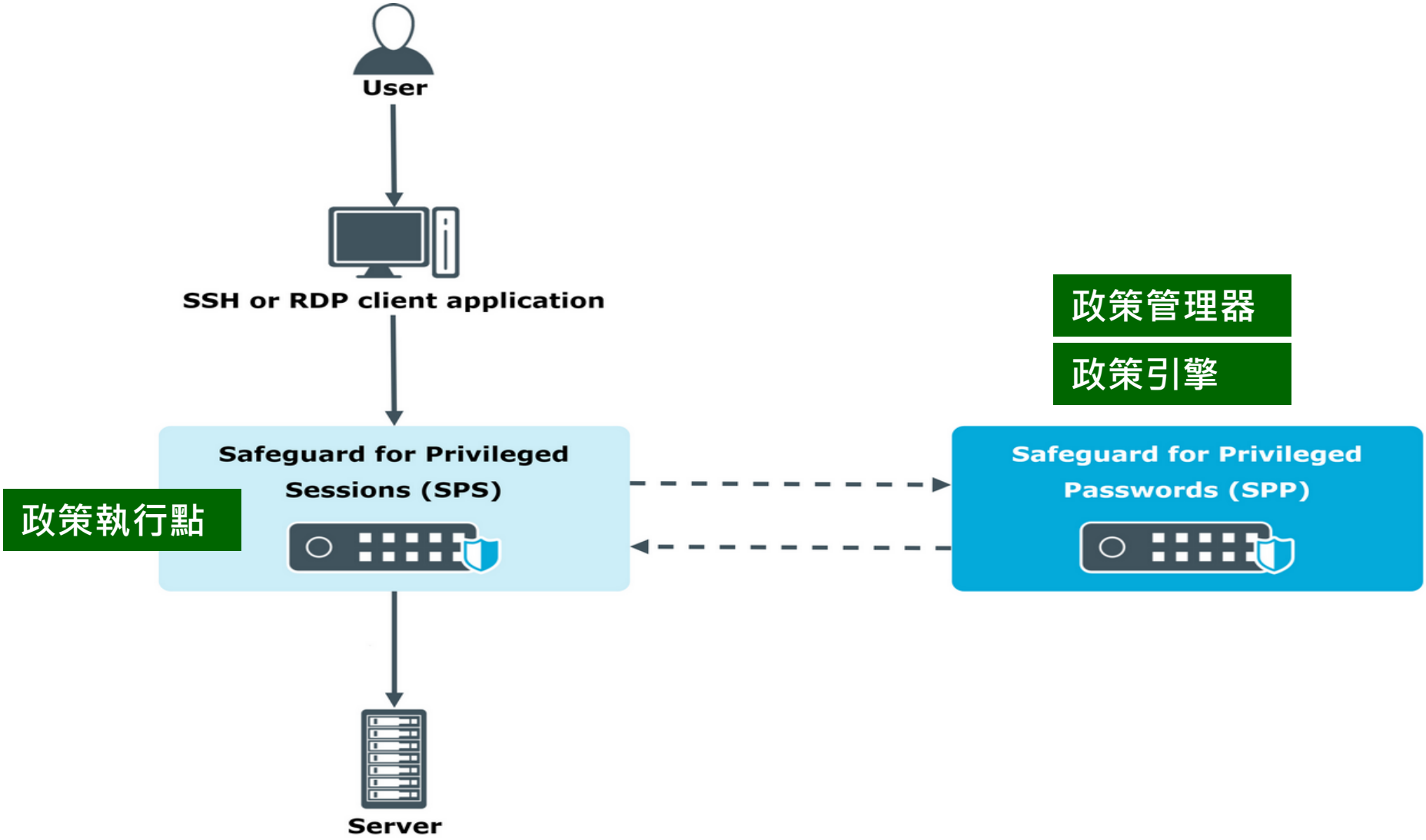
國家資通安全研究院 -政府零信任架構說明文件



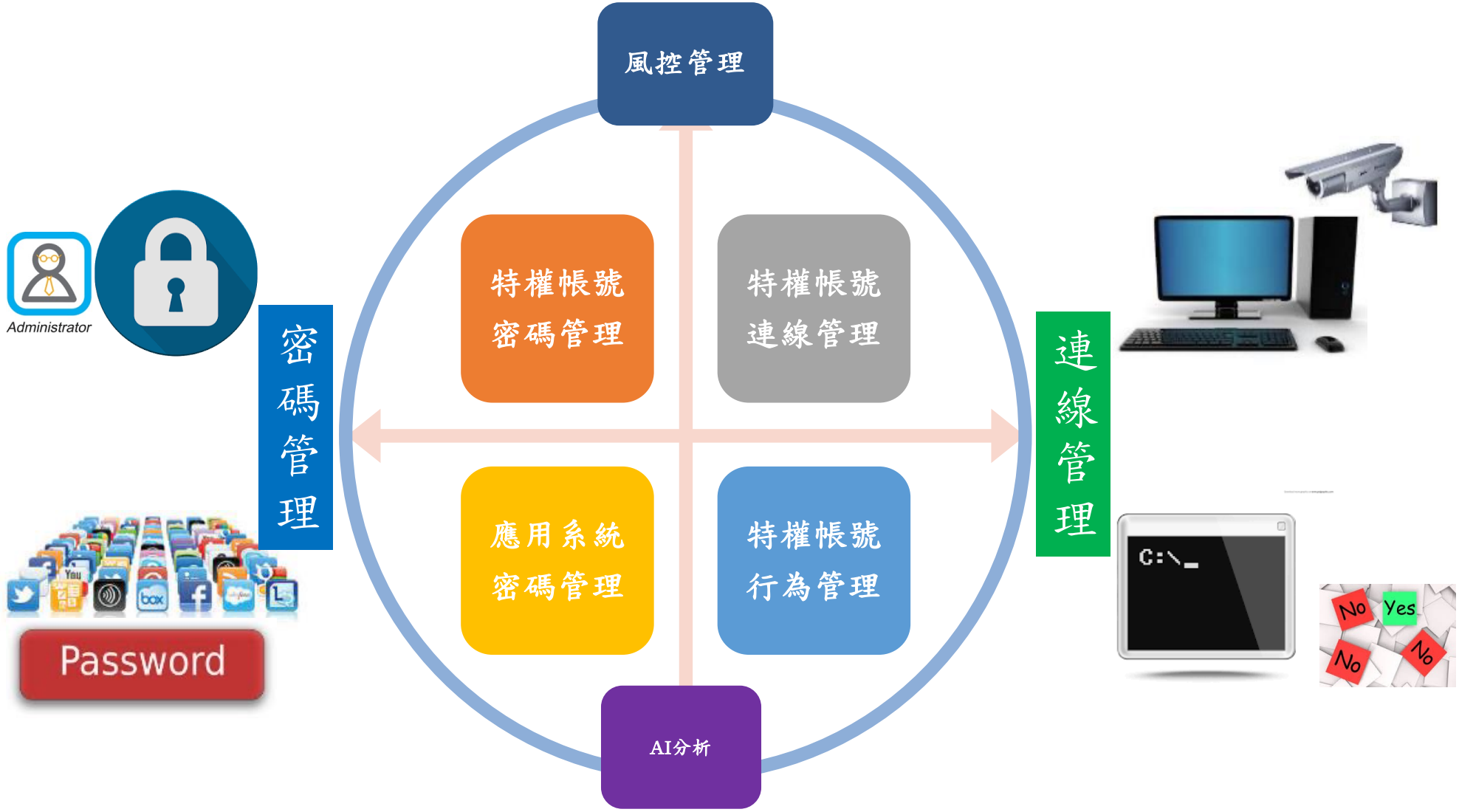
政府零信任架構說明文件 – 第6頁

NIST SP 800-207

特權管理架構

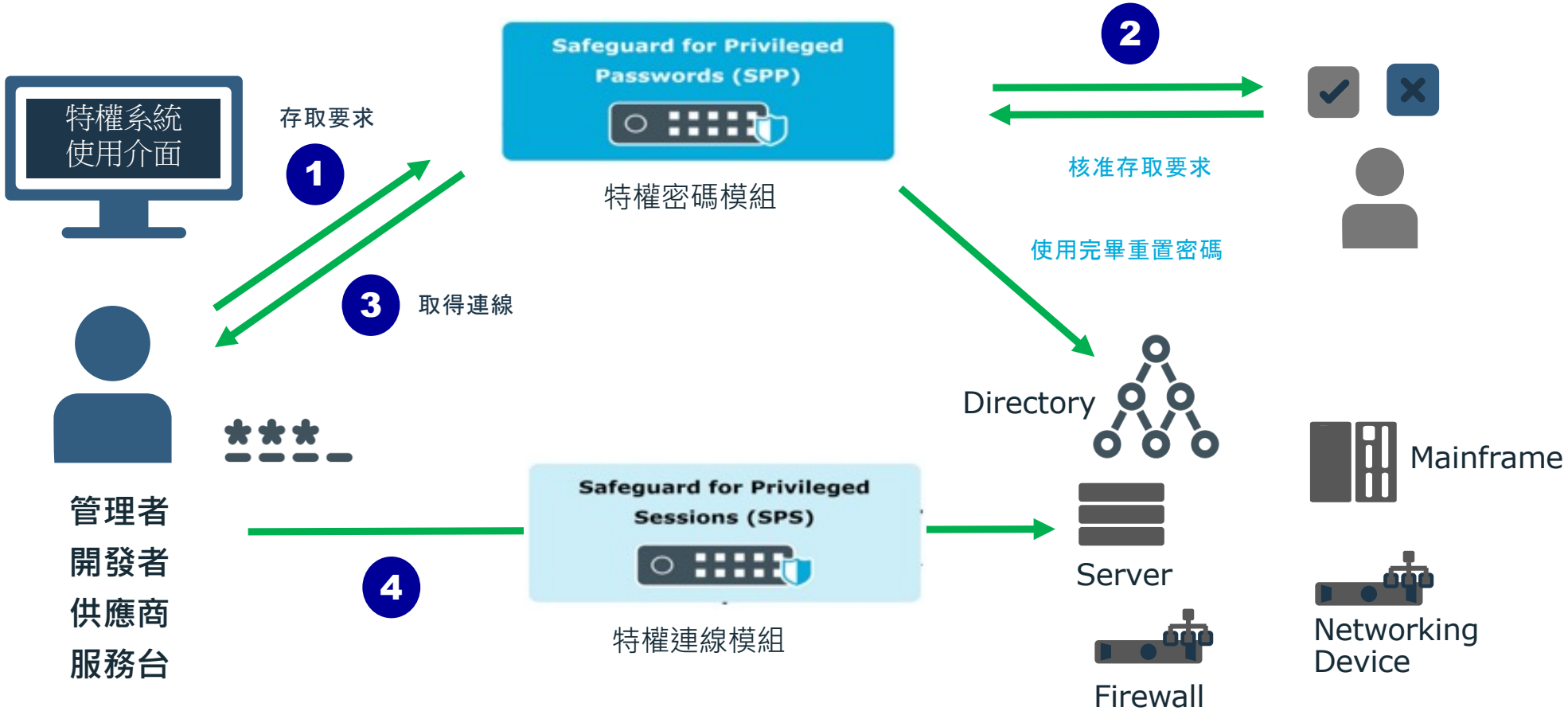

User
SSH or RDP client application
政策管理器
政策引擎
Safeguard for Privileged Sessions (SPS)
政策執行點
Safeguard for Privileged Passwords (SPP)
Server

PAM主要功能


風控管理
特權帳號
密碼管理
特權帳號
連線管理
應用系統
密碼管理
特權帳號
行為管理
AI分析
密碼管理
連線管理
Administrator
Password
C:_
No
Yes
No
No

代登與測錄

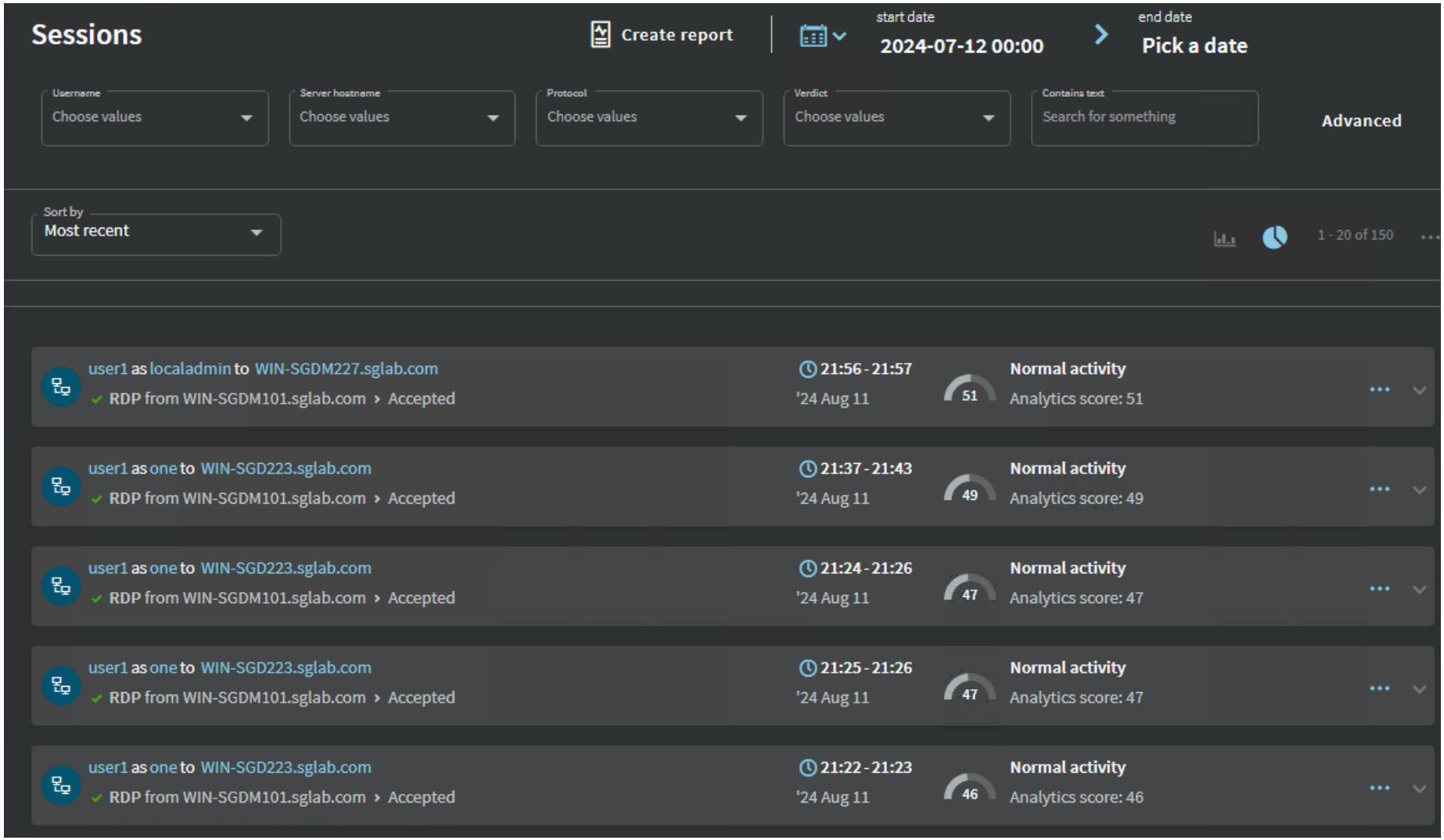
特權申請流程簡介


特權系統
使用介面
存取要求
1
Safeguard for Privileged
Passwords (SPP)
特權密碼模組
2
核准存取要求
使用完畢重置密碼
3
取得連線
管理者
開發者
供應商
服務台
4
Safeguard for Privileged
Sessions (SPS)
特權連線模組
Directory
Server
Firewall
Mainframe
Networking
Device

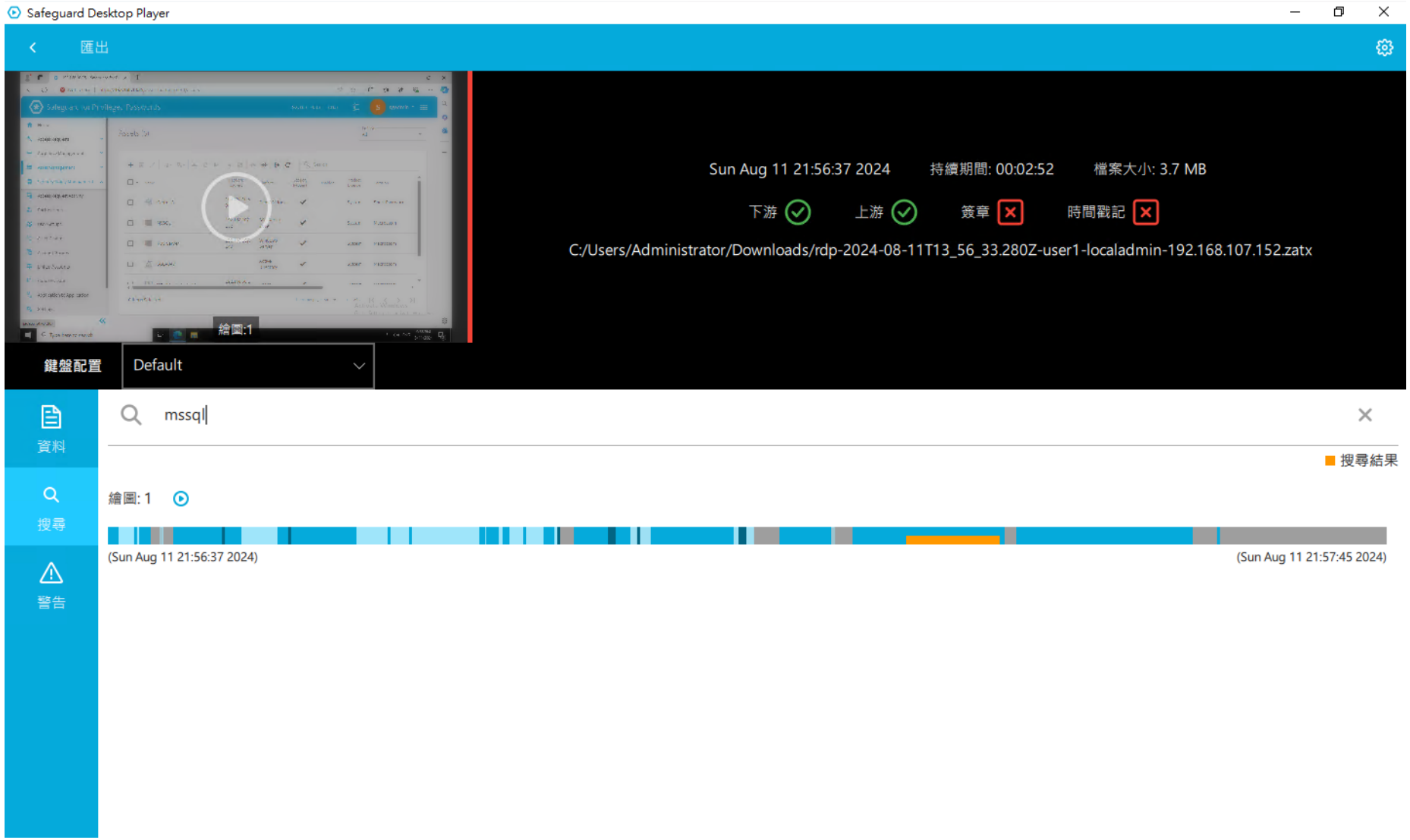
代登連線與測錄-展示


資產
帳戶
存取類型
Centos 8
192.168.10.50
user1
SSH
MSSQL
192.168.107.152
apcon
RDP 應用程式
vm_192_168_66_11
192.168.66.11
sysadmin
RDP 應用程式
Windows Server
192.168.107.152
localadmin
RDP
Windows Server
192.168.107.152
aduser
sglab.com
RDP
Windows Server
192.168.107.152
我的認證
RDP

測錄收尋與播放-展示


Sessions
Create report
start date
2024-07-12 00:00
end date
Pick a date
Username
Choose values
Server hostname
Choose values
Protocol
Choose values
Verdict
Choose values
Contains text
Search for something
Advanced
Sort by
Most recent
1 - 20 of 150
user1 as localadmin to WIN-SGDM227.sglab.com
RDP from WIN-SGDM101.sglab.com › Accepted
21:56 - 21:57
'24 Aug 11
51
Normal activity
Analytics score: 51
user1 as one to WIN-SGD223.sglab.com
RDP from WIN-SGDM101.sglab.com › Accepted
21:37 - 21:43
'24 Aug 11
49
Normal activity
Analytics score: 49
user1 as one to WIN-SGD223.sglab.com
RDP from WIN-SGDM101.sglab.com › Accepted
21:24 - 21:26
'24 Aug 11
47
Normal activity
Analytics score: 47
user1 as one to WIN-SGD223.sglab.com
RDP from WIN-SGDM101.sglab.com › Accepted
21:25 - 21:26
'24 Aug 11
47
Normal activity
Analytics score: 47
user1 as one to WIN-SGD223.sglab.com
RDP from WIN-SGDM101.sglab.com › Accepted
21:22 - 21:23
'24 Aug 11
46
Normal activity
Analytics score: 46

Idea: 教學影片

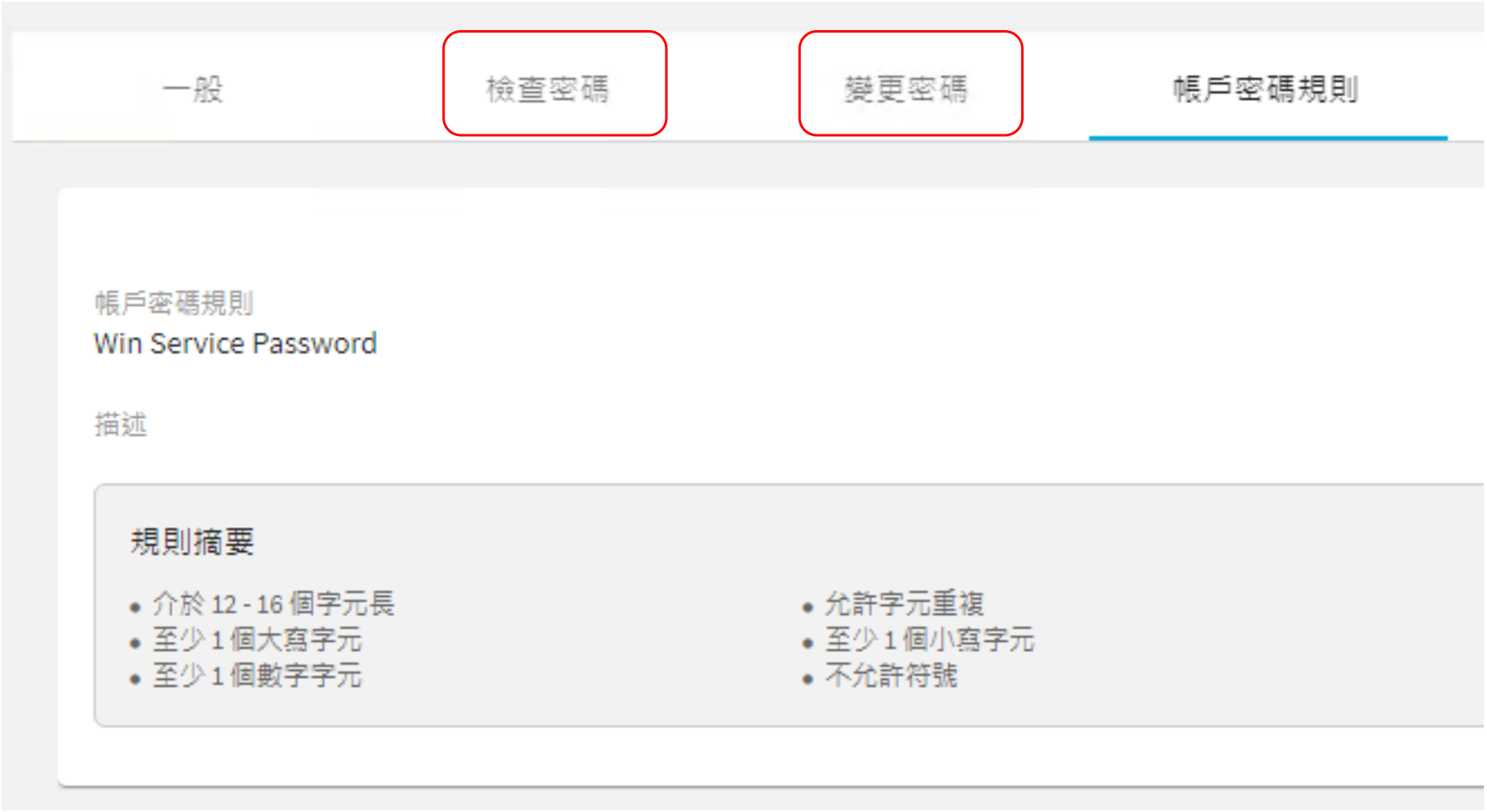

Safeguard Desktop Player
匯出
Sun Aug 11 21:56:37 2024
持續期間: 00:02:52
檔案大小: 3.7 MB
下游
上游
簽章
時間戳記
C:/Users/Administrator/Downloads/rdp-2024-08-11T13_56_33.280Z-user1-localadmin-192.168.107.152.zatx
繪圖:1
鍵盤配置
Default
資料
搜尋
警告
mssql
搜尋結果
繪圖: 1
(Sun Aug 11 21:56:37 2024)
(Sun Aug 11 21:57:45 2024)

密碼生命週期

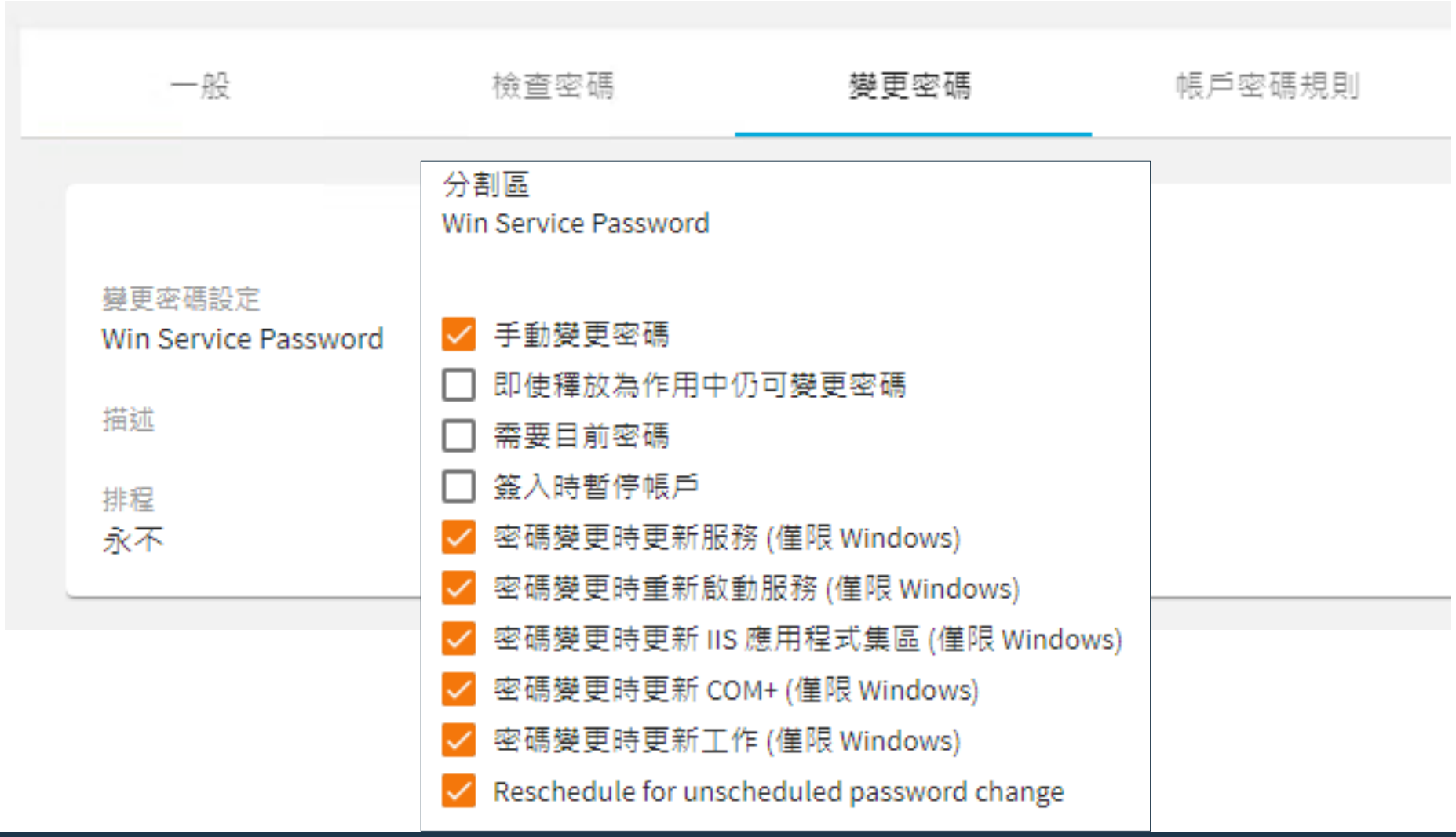
特權密碼

- 可以依據各種平台需求特別設定密碼原則
- 密碼允許使用大寫英文、小寫英文、數字、特殊符號組合
- 可做排程修改Windows「元件服務」上的指定帳號密碼
- 可做排程修改Windows「工作排程器」上的指定帳號密碼
- 可做排程定期檢查密碼正確性
- 可排程定期修改大權限密碼
- 可察看之前改成功的密碼

設定密碼生密週期


一般
檢查密碼
變更密碼
帳戶密碼規則
帳戶密碼規則
Win Service Password
描述
規則摘要
介於 12 - 16 個字元長
至少 1 個大寫字元
至少 1 個數字字元
允許字元重複
至少 1 個小寫字元
不允許符號

設定排程變更密碼

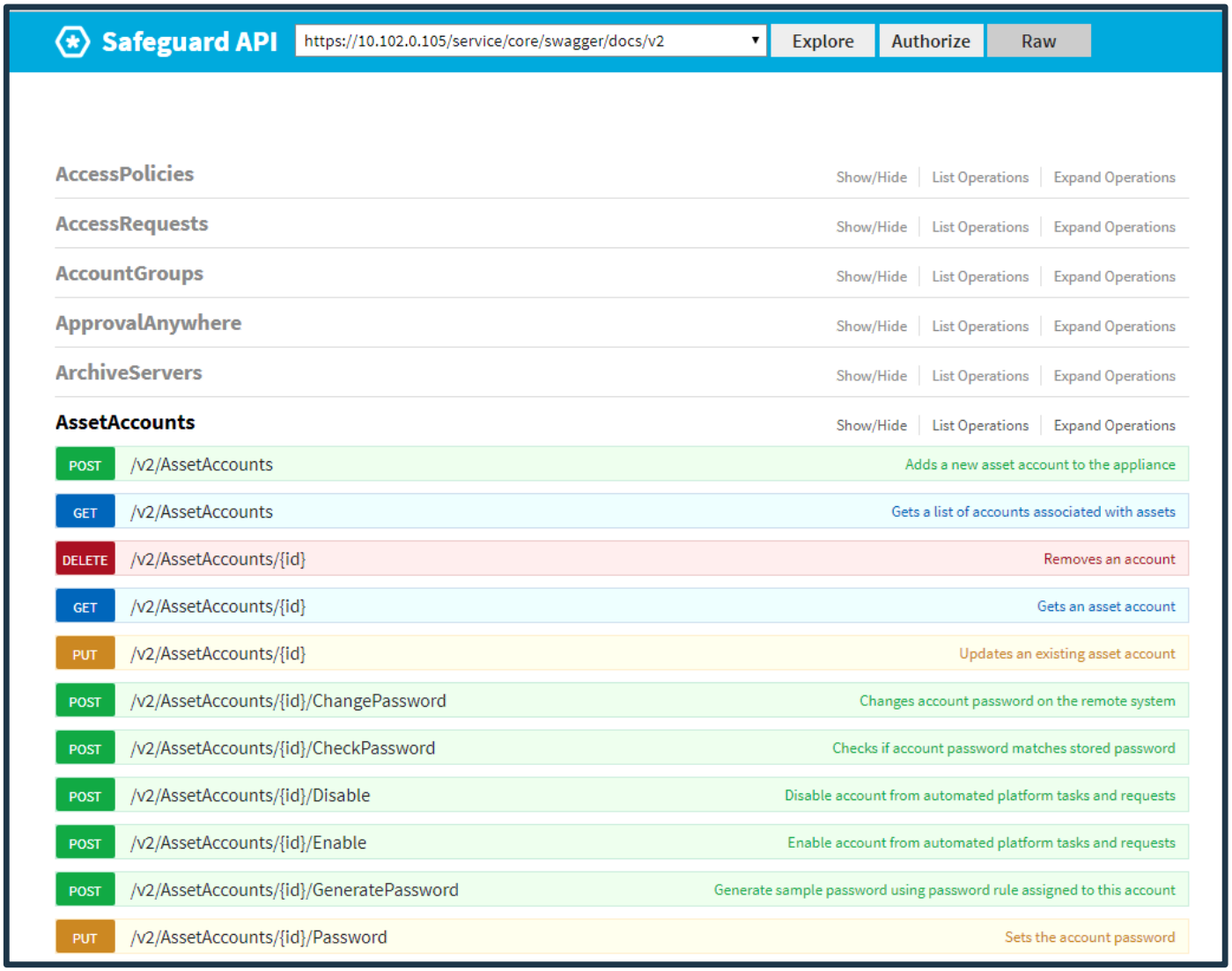

一般
檢查密碼
變更密碼
帳戶密碼規則
變更密碼設定
Win Service Password
描述
排程
永不
分割區
Win Service Password
手動變更密碼
即使釋放為作用中仍可變更密碼
需要目前密碼
簽入時暫停帳戶
密碼變更時更新服務 (僅限 Windows)
密碼變更時重新啟動服務 (僅限 Windows)
密碼變更時更新 IIS 應用程式集區 (僅限 Windows)
密碼變更時更新 COM+ (僅限 Windows)
密碼變更時更新工作 (僅限 Windows)
Reschedule for unscheduled password change

Idea:破窗帳號

- 每一台伺服器，建議建立二組高權限帳號。
- 比如admin1, admin2
- admin1 與 admin2設定自動修改密碼時間需要錯開。
- 假如每180天修改密碼，admin1 與 admin2 錯開90天自動改密碼。

應用程式整合

提供Restful-API呼叫

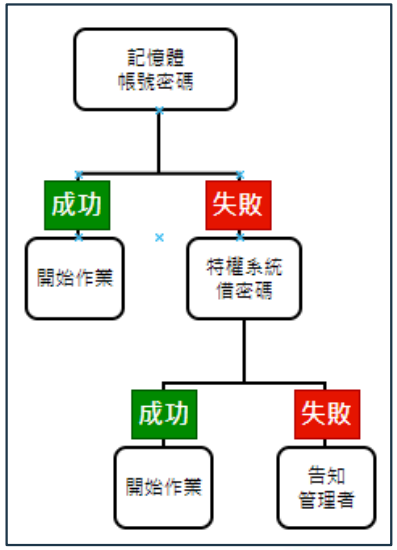


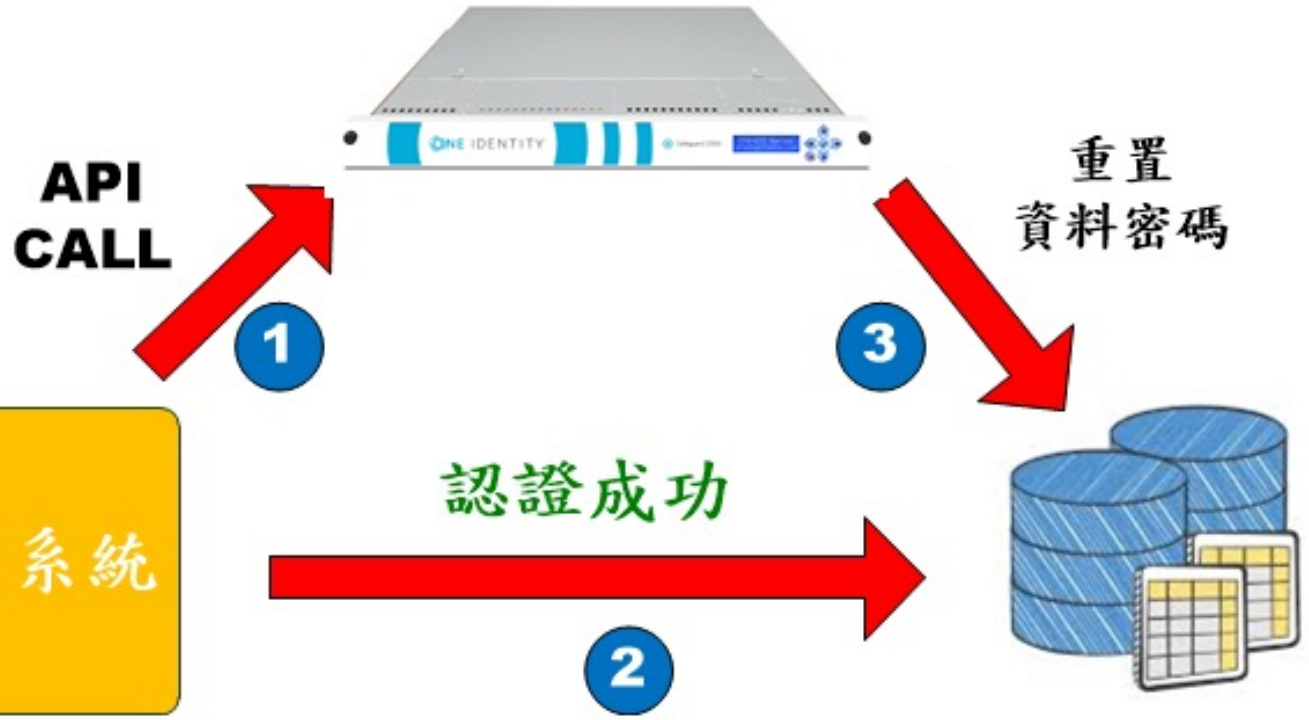
應用系統密碼的挑戰

- 帳密夾雜在應用程式或自動化管理腳本中
  - 程式開發者已知道帳號/密碼
  - 後門帳號/密碼
  - 應用系統密碼不能異動
  - 應用程式的需求
    - 連續式的A2A連接
    - 交易式的A2D連接

```
7  public class discovery {
8      private String computer, username, password;
9      private ActiveXComponent connection;
10
11     discovery() {
12         computer = "10.61.1.215";
13         username = "administrator";
14         password = "5k4g4AU$AU$";
15         connection = rcon();
16     }
17
18     private ActiveXComponent rcon() {
19         ActiveXComponent wmi = new ActiveXComponent("WbemScripting.SWbemLocator");
20         Variant variantParameters[] = new Variant[4];
21         variantParameters[0] = new Variant(computer);
22         variantParameters[1] = new Variant("root\\CIMV2");
23         variantParameters[2] = new Variant(username);
24         variantParameters[3] = new Variant(password);
25         ActiveXComponent axWMI;
26         try {
27             Variant conRet = wmi.invoke("ConnectServer", variantParameters);
28             axWMI = new ActiveXComponent(conRet.toDispatch());
29         } catch (ComFailException e) {
30             axWMI = null;
31         }
32
33         return axWMI;
34     }
```

應用系統密碼解決方案


記憶體
帳號密碼
成功
失敗
開始作業
特權系統
借密碼
成功
失敗
開始作業
告知
管理者


API
CALL
1
重置
資料密碼
3
應用系統
認證成功
2

連線retry範例

```
public class DatabaseConnectionRetry {

    public Connection getConnection() {

        while (attempt < MAX_RETRIES) {
            try {
                connection = DriverManager.getConnection(DB_URL, USER, PASS);
                System.out.println("Connection established successfully!");
                return connection; // 連線成功回傳連線
            } catch (SQLException e) {
                attempt++;

                //建立Safeguard連線
                ISafeguardA2AContext a2aContext = Safeguard.A2A.getContext(sppHostname, cert, certPwd,null, true);
                //ApiKey取出密碼
                PASS = a2aContext.retrievePassword(ApiKey);

                // 等待重試
                try {
                    Thread.sleep(RETRY_DELAY_MS);
                } catch (InterruptedException ie) {
                    Thread.currentThread().interrupt();
                    break;
                }
            }
        }
}
```

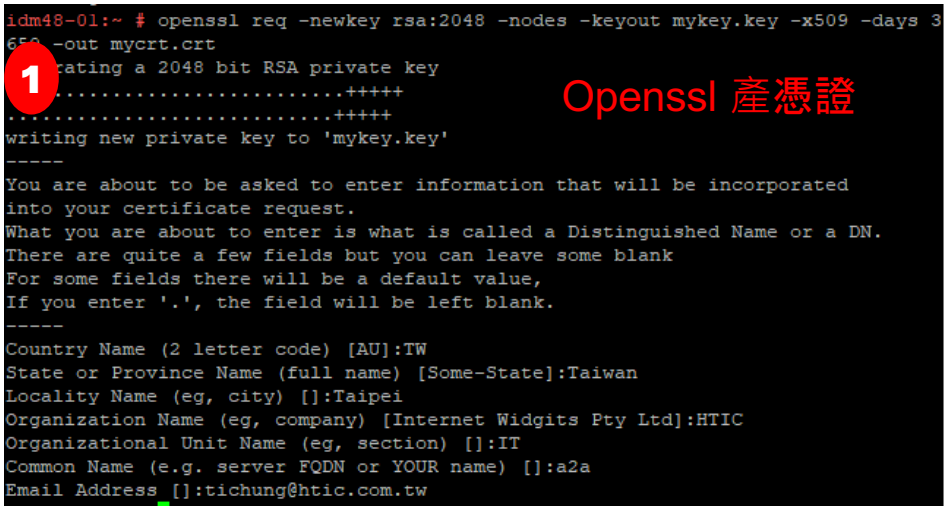
支援不同語言程式整合

Safeguard for Privileged Passwords

Add-Ons	SDKs	Scripting Resources
SCALUS session launcher	SafeguardDotNet	safeguard-ps
Safeguard Secrets Broker	SafeguardJava	safeguard-discovery
Active Roles Safeguard JIT Access	PySafeguard	safeguard-bash
Safeguard Custom Platform	safeguard.js	Safeguard API Tutorial
Safeguard Session Automation		safeguard-ansible

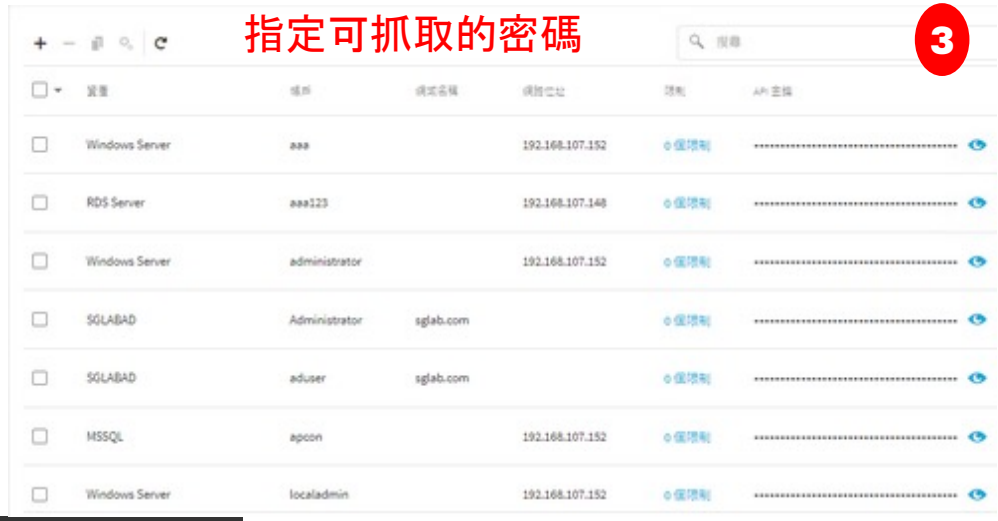
https://github.com/OneIdentity

取密碼前置作業


idm48-01:~ # openssl req -newkey rsa:2048 -nodes -keyout mykey.key -x509 -days 3
650 -out mycrt.crt
Generating a 2048 bit RSA private key
.....+++++
.....+++++
writing new private key to 'mykey.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:HTIC
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:a2a
Email Address []:tichung@htic.com.tw
1
Openssl 產憑證


指定可抓取的密碼
3
Windows Server aaa 192.168.107.152
RDS Server aaa123 192.168.107.148
Windows Server administrator 192.168.107.152
SGLABAD Administrator sglab.com
SGLABAD aduser sglab.com
MSSQL apcon 192.168.107.152
Windows Server localadmin 192.168.107.152


a2a-api
2
內容
使用者群組
權利
停用
身分識別
驗證
權限
驗證提供者
Certificate
指定帳號
憑證指紋 (SHA-1)
27C 7212

不同程式語言整合-展示

PowerShell

```
PS C:\safeguard_lab> Get-SafeguardA2aPassword -Appliance "10.101.2.105" -Insecure -CertificateFile "C:\safeguard_lab\mys
afeguardkey.pfx" -ApiKey "WB9s/oJuAUagGafxCH3VjOH8M74mdpTatMIIZX6kHD4="
B4sZr19
```

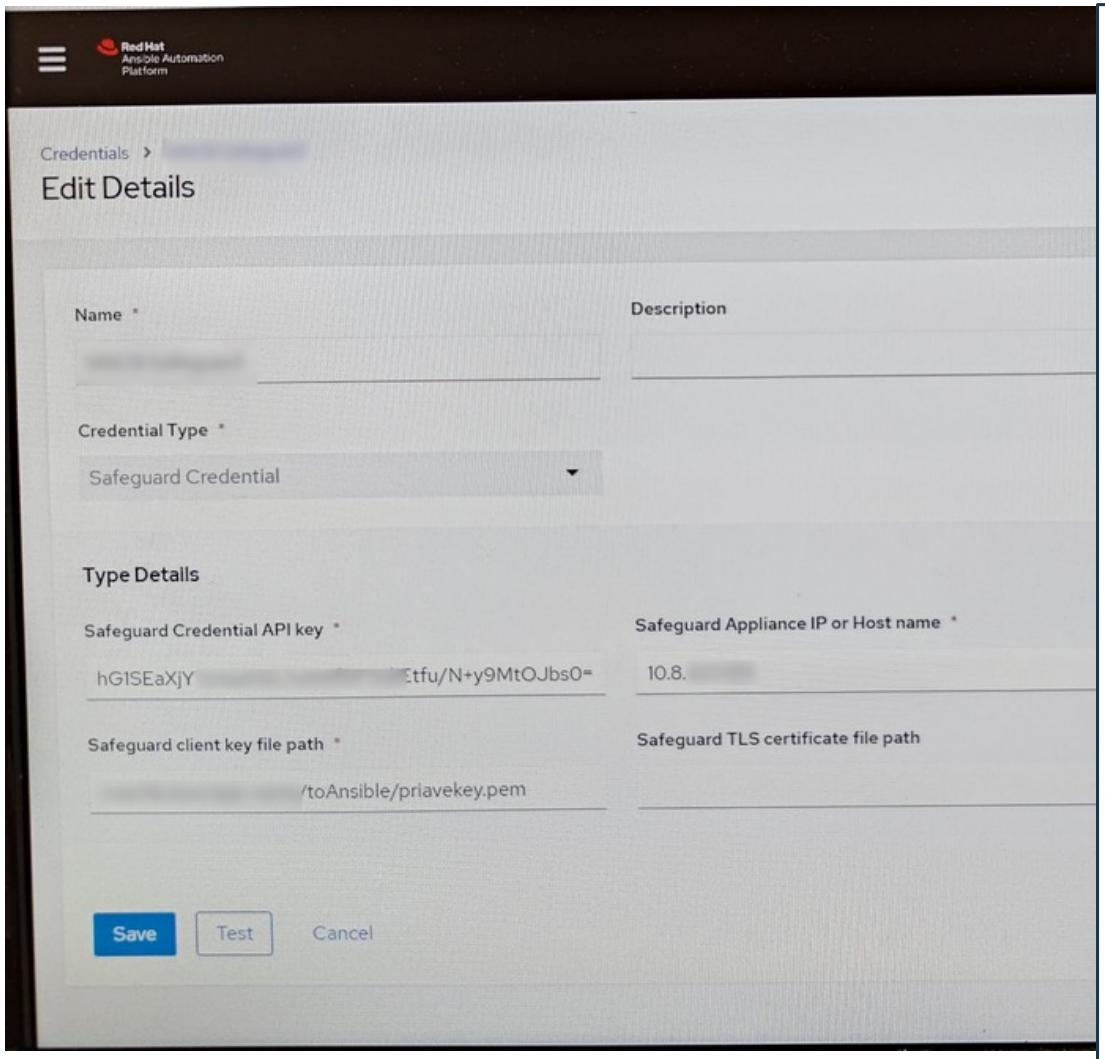
PythonI

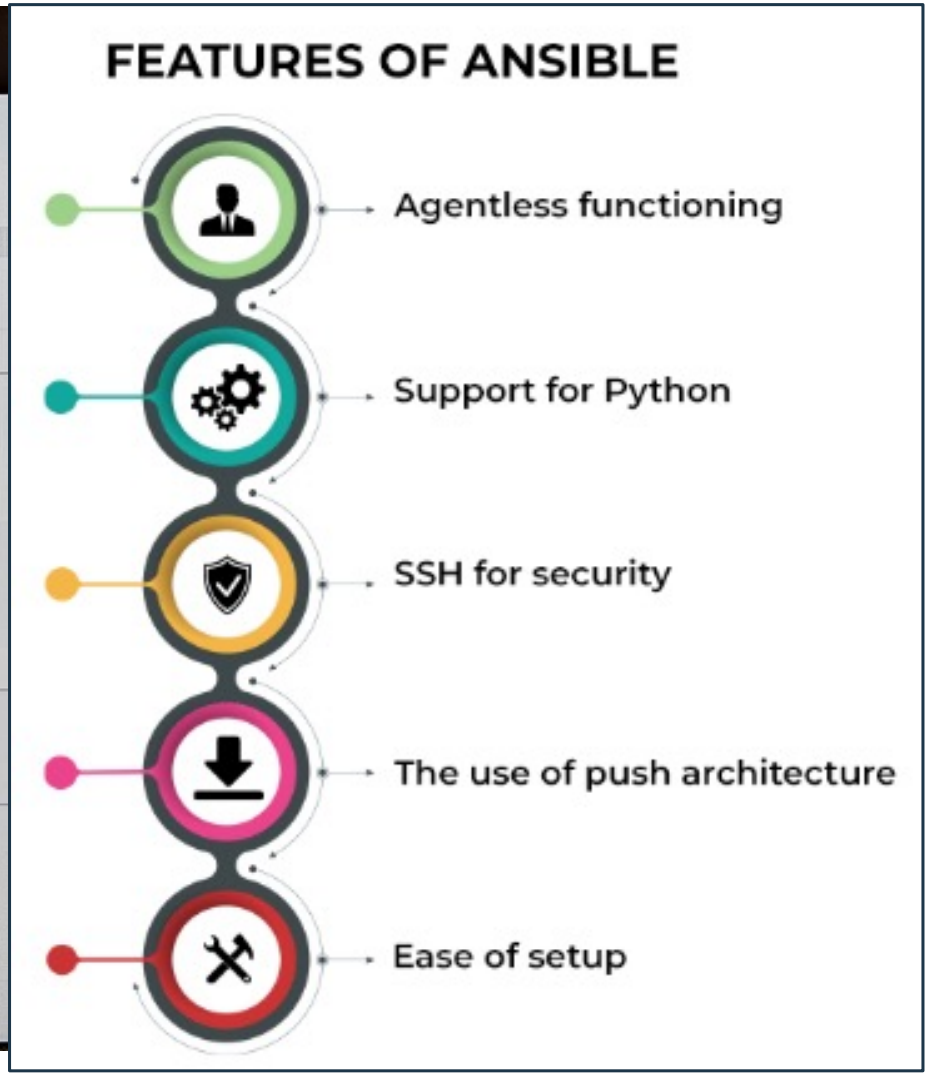
```
c:\Scripts\python>python a2a.py
mssql password: yGbZ#H6ymM4V%7
```

Java

IP:	10.8.210.145	**(A PART)**	10.8.210.145 - testadmin
系統名稱:	受信系統		
業務別:			
保管密碼:	A PART	1qaz@W	
帳號:	testadmin		
備註:	A PART		
IP:	10.8.210.145	**(B PART)**	10.8.210.145 - testadmin
系統名稱:	受信系統		
業務別:			
保管密碼:	B PART	SX3edc	
帳號:	testadmin		
備註:	B PART		

Idea: Ansible自動化平台整合





Idea:AB密碼函

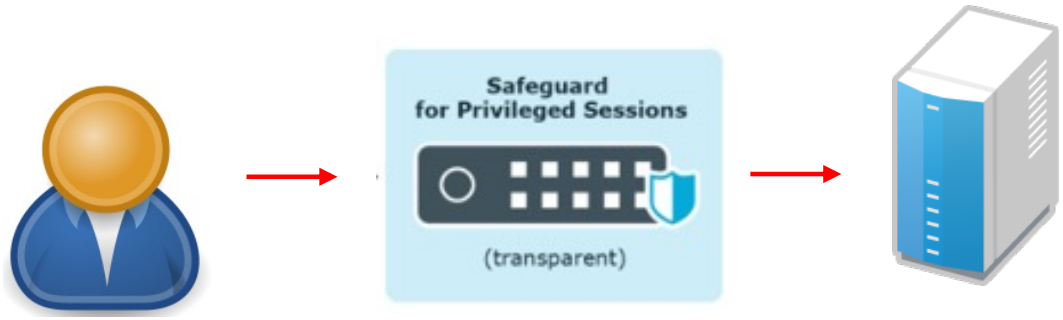
特權
系統

IP:	10.8.210.145	**(A PART)**	10.8.210.145 - testadmin
系統名稱:	受信系統		
業務別:			
保管密碼:	A PART	1qaz@W	
帳號:	testadmin		
備註:	A PART		
IP:	10.8.210.145	**(B PART)**	10.8.210.145 - testadmin
系統名稱:	受信系統		
業務別:			
保管密碼:	B PART	SX3edc	
帳號:	testadmin		
備註:	B PART		

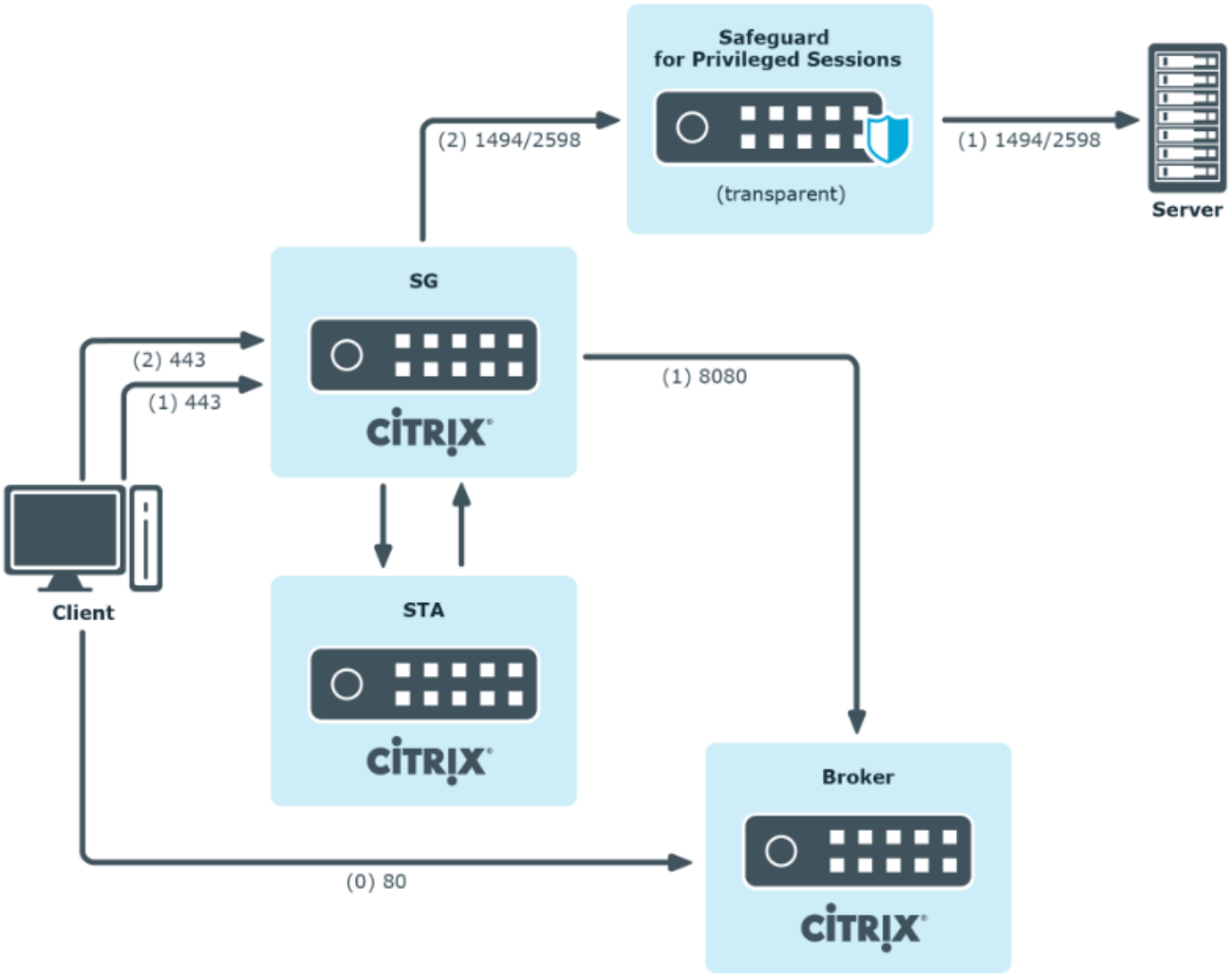
PAM擴展的運用

可測錄與紀錄不同類別的連線

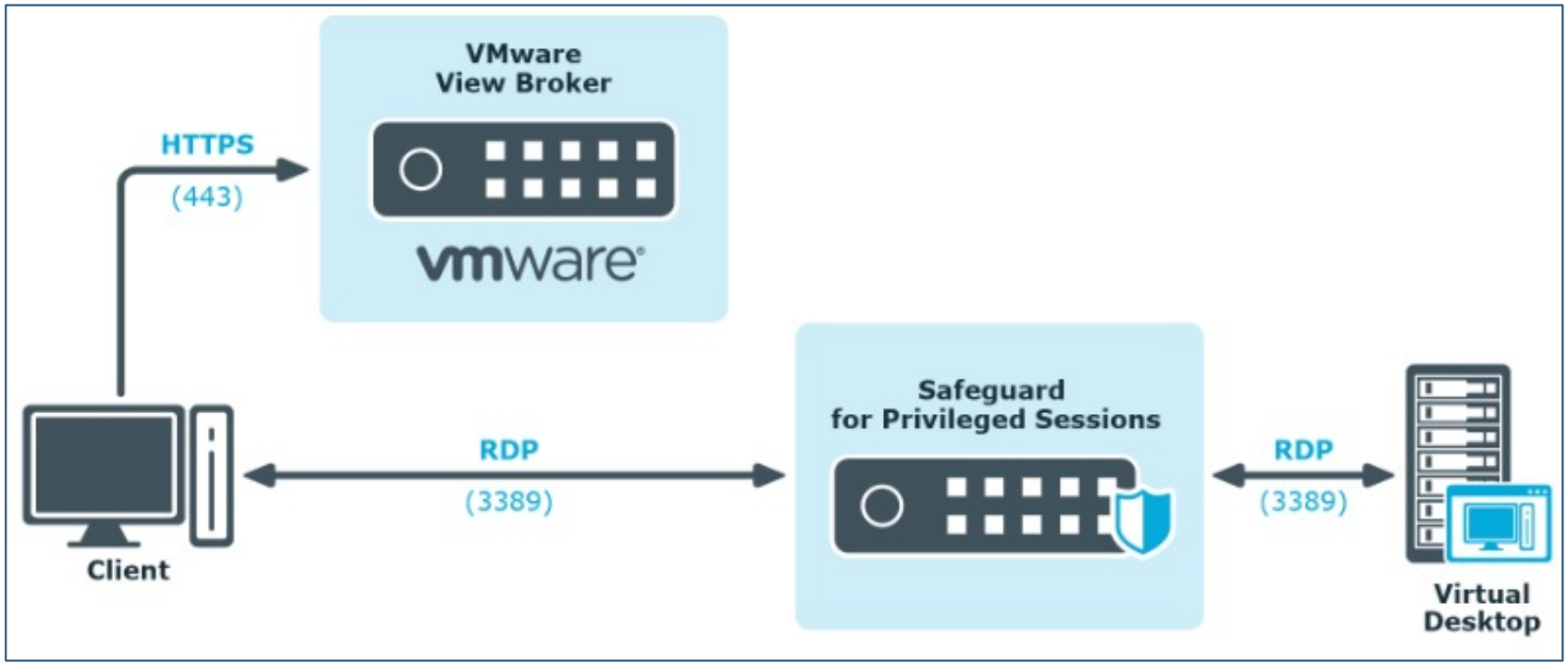
- HTTP Control
- ICA Control
- MSSQL Control
- RDP Control
- SSH Control
- Sudo iolog Control
- Telnet Control
- VNC Control

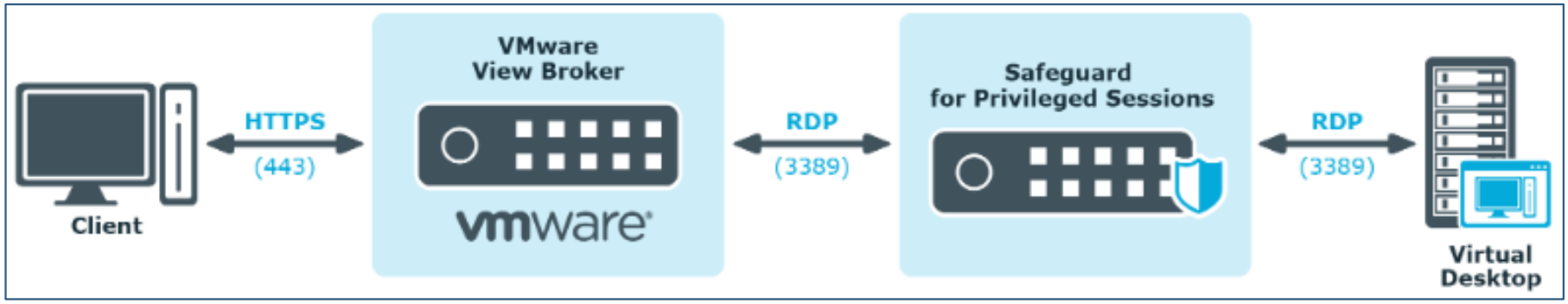


Idea: ICA連線紀錄

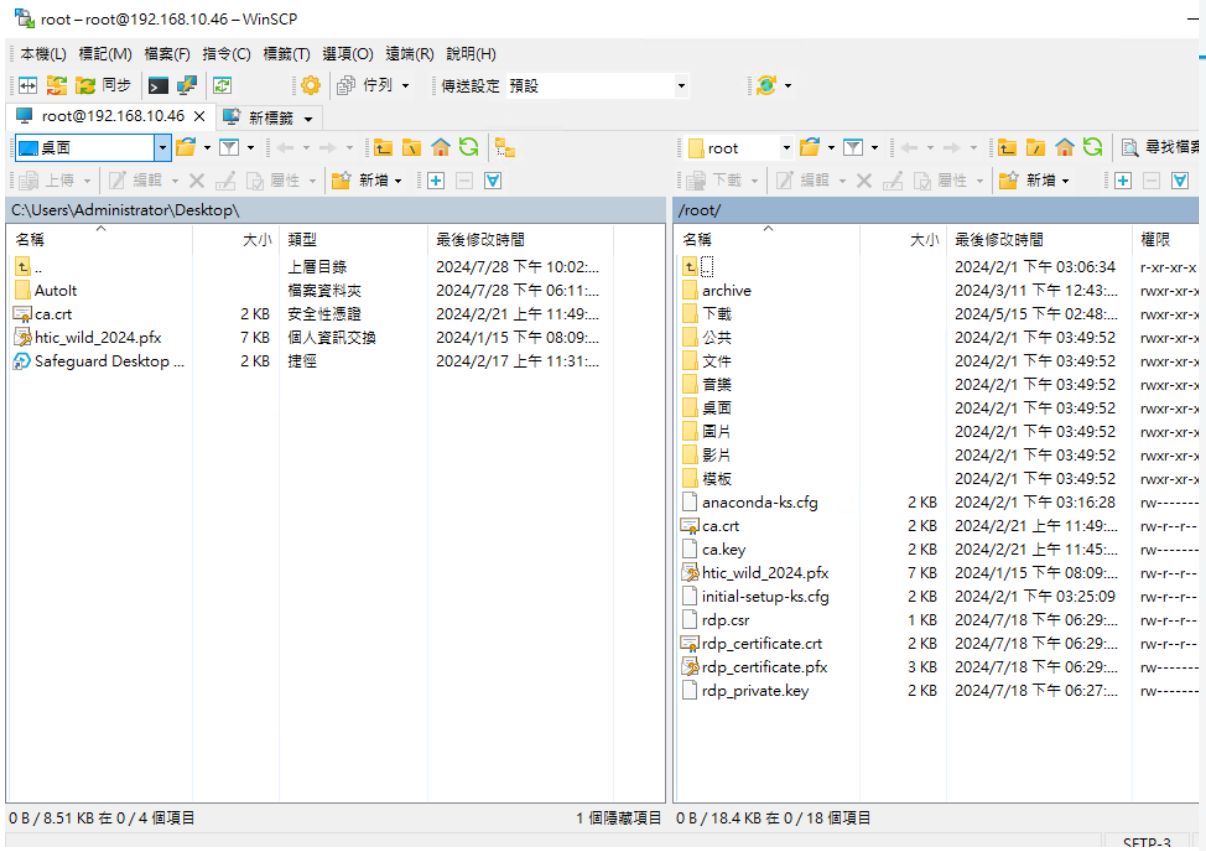


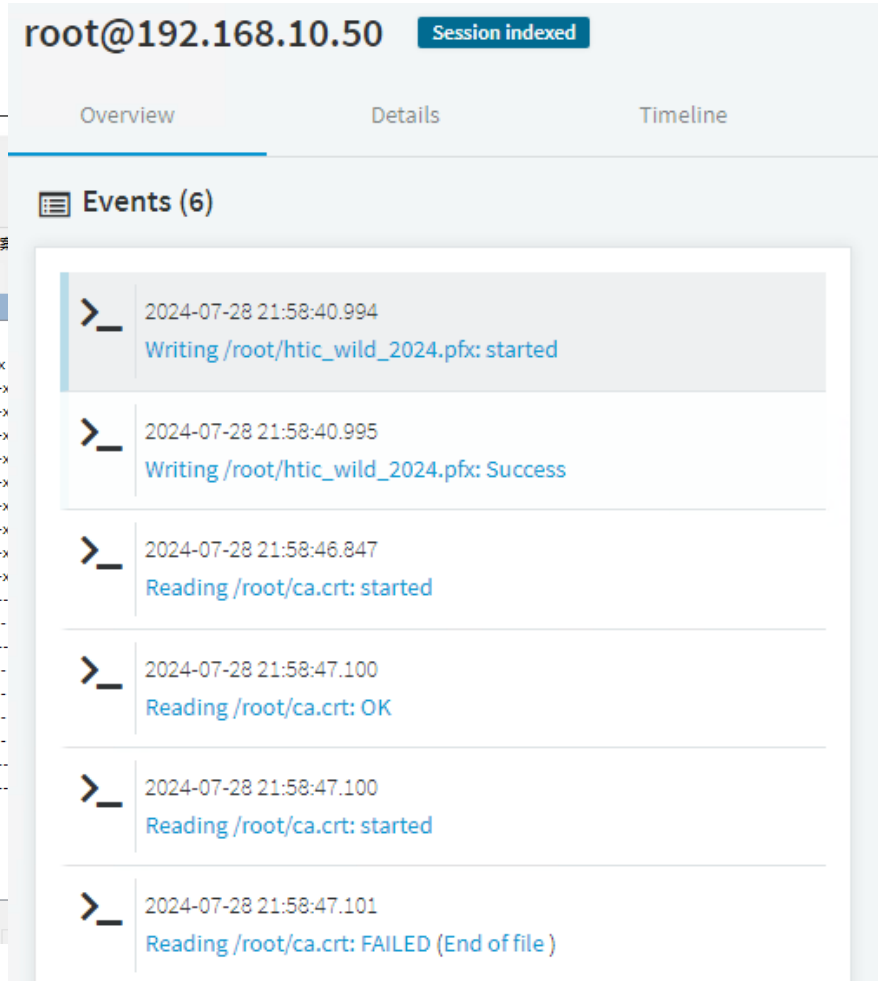
Idea: VMware Horizon View 連線紀錄



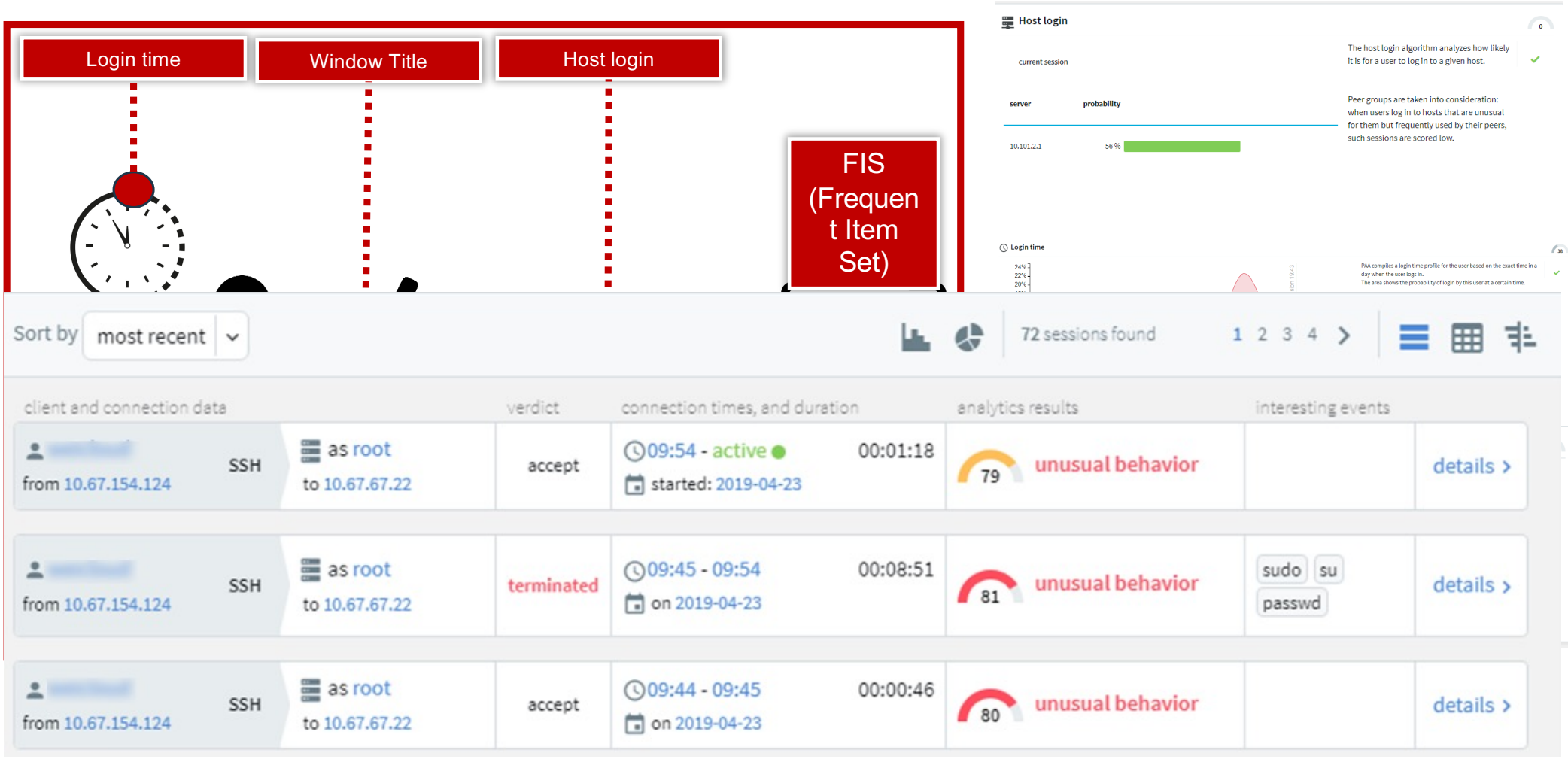


Idea: SSH-SFTP or SCP操作紀錄 - 展示





Idea: 異常行為偵測 – 機器學習分析



部署：特權管理注意事項

1. 簽核流程制訂與規劃
2. 特權密碼自動變更時機（使用完畢與定期）
3. 稽核記錄與影片保留時間5年
4. 稽核記錄如果是Windows需要有影片，如Linux需要有指令
5. 使用者登入需雙因子認證
6. 建議有Common Criteria Certificate認證

單一簽入解決方案

THANK YOU

如果給我6個小時砍下一顆樹，我會用前面4個小時把斧頭磨利。

Give me six hours to chop down a tree and I will spend the first four sharpening the axe.

Abraham Lincoln

鋐迪資訊