針對整個系統安全性的建議方案

針對你三節點 Nutanix AHV 叢集的「**整體系統安全性建議方案**」。我把重點分成：身分與存取、網路防護、主機/平台強化、加密與金鑰、更新與弱點、紀錄監控、備份與復原、交換器與實體安全、運營治理。每段都附上最關鍵可查證的官方依據。

**一、身分與存取（IAM）**

* **SSO + MFA**：Prism Central 以 **SAML** 串接企業 IdP（Entra ID/Azure AD、Okta、Duo、RSA 等），在 IdP 端啟用 MFA，落實單一登入與條件式存取。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Amul-security-authentication-pc-iam-c.html?utm_source=chatgpt.com)[Duo Security](https://duo.com/docs/sso-nutanix-prism?utm_source=chatgpt.com)[RSA Community](https://community.securid.com/s/article/Nutanix-Prism-Central-IDR-SSO-Configuration-using-SAML-RSA-Ready-Implementation-Guide?utm_source=chatgpt.com)
* **RBAC**：以最小權限建立「平台管理、網路、儲存、租戶/專案」分權角色；變更權限需走變更管制流程（變更單、雙人覆核）。
* **離職/異動流程**：權限綁 AD 群組，定期（每月）盤點管理員與特權帳號。

**二、網路防護**

**1) 東西向（叢集內部）**

* **Flow Network Security（FNS）微分段**：依應用（App/DB/Web）與環境（Prod/Dev）建「應用導向」安全群組與政策，預設 **deny**，只開放所需通訊（least privilege）。FNS 在 AHV vSwitch 層執行，被動與主動偵測（下一代版）需符合最低 AOS/AHV 版本。[Nutanix Portal+2Nutanix Portal+2](https://portal.nutanix.com/page/documents/solutions/details?targetId=TN-2094-Flow%3ATN-2094-Flow&utm_source=chatgpt.com)
* **版本門檻**：FNS Next-Gen 5.2 需 **AOS 7.3+、AHV 10+**；規劃升/新建時一併對齊。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Flow-Network-Security-Guide-v5_2_0%3Afns-security-policy-requirements-r.html?utm_source=chatgpt.com)

**2) 南北向（資料中心邊界）**

* **邊界防火牆/IPS**：所有對外服務（含 Prism/PC）走 L3 邊界防火牆；只暴露所需管理埠，建議以 **跳板/堡壘** 存取。
* **SDN/ACI 整合（選項）**：若採 Cisco ACI，可用官方整合指引簡化 AHV 邊界控管。[Cisco](https://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/kb/cisco-aci-nutanix-integration.html?utm_source=chatgpt.com)

**3) L2/L3 與交換器基線**

* **VLAN 隔離**：Mgmt、Storage、Live-Migration 與 Guest VLAN 分離；Storage 僅 L2，不跨路由。
* **高可用**：主機上使用 **LACP**，交換器啟用 **MLAG/VPC**；Storage/Migration VLAN 啟用 **MTU 9000**。
* **安全保護**：Port-Security、BPDU Guard/Root Guard、Storm-Control、DHCP Snooping、ARP Inspection；管理 VRF/Out-of-Band 隔離。

**三、主機 / 平台強化（Hardening）**

* **AHV/CVM 強化**：依 Nutanix 安全強化指南啟用 **AIDE 完整性檢查**、限制 SSH、設定日誌與 Banner、移除不必要服務。[Nutanix Portal+1](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Asec-ahv-configuration-c.html?utm_source=chatgpt.com)
* **Prism 存取**：只允許管理子網與堡壘主機存取；替換預設 TLS 憑證、禁止舊版 TLS/加密套件。
* **作業基線**：對映 **AHV Best Practices** 做為平台標準建置檢核表。[Nutanix Portal](https://portal.nutanix.com/page/documents/solutions/details?targetId=BP-2029-AHV%3ABP-2029-AHV&utm_source=chatgpt.com)

**四、資料加密與金鑰管理**

* **靜態資料加密（DARE）**：啟用 Nutanix **軟體式 AES-256** 或硬體 SED；金鑰可用 **Native KMS（本地/遠端）** 或 **外部 KMIP KMS**（Thales/Vormetric 等），並支援 KMS 類型切換。[Nutanix Portal+2Nutanix Portal+2](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Awc-security-data-encryption-wc-c.html?utm_source=chatgpt.com)[Nutanix](https://www.nutanix.com/products/security/encryption?utm_source=chatgpt.com)[NutanixBible.com](https://www.nutanixbible.com/4b-book-of-aos-security.html?utm_source=chatgpt.com)
* **金鑰控管**：KMS 高可用、與 IdP 分權；輪替/備援/復原流程文件化與演練。
* **傳輸加密**：API/Prism/PC 對外只允許 HTTPS；CVM 間通訊維持預設保護並限制來源網段。

**五、更新與弱點管理**

* **LCM 生命週期**：以 **LCM** 滾動更新 AOS/AHV/CVM/韌體，先做非生產驗證；重大安規通告採快軌修補。[Nutanix Portal+1](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3ANutanix-Security-Guide-v7_3?utm_source=chatgpt.com)
* **弱點掃描**：月更例行掃描（含主機管理介面與 Prism），關鍵漏洞（CVSS≥9）限時修補；例外需風險接受書。

**六、紀錄、監控與稽核**

* **集中化日誌**：Prism/PC 事件、審計與 FNS 事件送往 **SIEM/Syslog**；設定保存/完整性與告警門檻。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3ANutanix-Security-Guide-v7_3?utm_source=chatgpt.com)
* **安全監控**：定義指標（異常登入、政策命中、封包異常、資源暴衝），與 on-call 排程對應。
* **變更稽核**：所有網路/安全政策與 RBAC 變更需留有工單與審核紀錄。

**七、備份、災難復原與勒索防護**

* **平台與配置**：匯出/備份 PC 設定、Flow 政策與 Runbook。
* **資料面**：啟用快照與複寫（NearSync/Async），異地保存；備份庫採 **WORM/物件鎖**（若使用 Objects/NAS）。
* **演練**：每季做應用層復原演練與勒索感染情境演練（隔離網段、只讀恢復）。

**八、交換器與實體安全**

* **AAA/集中認證**：交換器接 **TACACS+/RADIUS** 與 MFA；命令稽核開啟。
* **硬體**：機櫃上鎖、雙路電源、獨立 OOB；序號與維保資訊納入 CMDB。

**九、治理與流程（Zero-Trust 觀點）**

* **零信任原則**：身分為中心、微分段預設拒絕、裝置與狀態評估通過才放行；策略隨應用生命週期自動化。[Nutanix](https://www.nutanix.com/products/flow?utm_source=chatgpt.com)[nutanix.dev](https://www.nutanix.dev/learn-how-to-secure-your-hybrid-multi-cloud-in-30-mins-part-1/?utm_source=chatgpt.com)
* **文件化**：安全基線（Host/Network/PC）、事件回應手冊、權限與金鑰輪替表、DR/BCP 計畫；每年至少一次桌上推演。

**快速落地清單（可直接執行）**

1. **接 IdP + MFA** 到 Prism Central，關閉本地共用帳號。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Amul-security-authentication-pc-iam-c.html?utm_source=chatgpt.com)
2. **開 FNS**，先套用 **觀察模式** 建模，再切換強制。[Nutanix Portal](https://portal.nutanix.com/page/documents/solutions/details?targetId=TN-2094-Flow%3ATN-2094-Flow&utm_source=chatgpt.com)
3. **啟用 DARE + KMS**，完成金鑰輪替/備援演練。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Awc-security-data-encryption-aos-wc-t.html?utm_source=chatgpt.com)
4. 依 **AHV Hardening** 套 AIDE、SSH 控制與最小服務。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3Asec-ahv-configuration-c.html?utm_source=chatgpt.com)
5. 建 **SIEM 轉送** 與告警；把 LCM 納入每月維護視窗。[Nutanix Portal](https://portal.nutanix.com/docs/Nutanix-Security-Guide-v7_3%3ANutanix-Security-Guide-v7_3?utm_source=chatgpt.com)

如果你要，我可以把這份建議轉成「**安全基線檢查表（Excel）**」與「**Flow 微分段範例策略**（含 L3/L4 規則樣板）」方便你直接套用到專案交付。

**You said:**

轉成「安全基線檢查表（Excel）」與「Flow 微分段範例策略（含 L3/L4 規則樣板）」

**ChatGPT said:**

✅ 已完成轉換：

1. **安全基線檢查表（Excel）**  
   👉 下載 Nutanix\_Security\_Baseline.xlsx
2. **Flow 微分段範例策略（L3/L4 規則樣板）**

# Nutanix Flow 微分段範例策略 (L3/L4)

1. 管理平面保護 (Prism / CVM)

- Source: 管理員端 IP (10.1.10.0/24)

- Destination: CVM/PE/PC (Mgmt VLAN)

- Ports: TCP 9440 (Prism), TCP 22 (SSH), ICMP

- Action: Allow

2. Storage Backend 保護

- Source: Cluster CVMs

- Destination: Cluster CVMs

- VLAN: Storage VLAN (不可跨 L3)

- Ports: 全部 (內部通訊必要)

- Action: Allow

3. VM 區隔 (Web / App / DB 三層)

- Web Tier:

- Allow: 0.0.0.0/0 → TCP 80, 443

- Deny: 其他

- App Tier:

- Allow: Web Tier → TCP 8080

- Deny: 其他

- DB Tier:

- Allow: App Tier → TCP 3306 (MySQL)

- Deny: 其他

4. 基礎安全策略

- Deny Any Any 作為預設策略 (最後一條規則)

要不要我幫你把 **Flow 策略規則** 也整理成 Excel 格式，方便直接上傳到 Prism Flow 當成規則樣板？

**You said:**

Flow 策略規則 也整理成 Excel 格式

**ChatGPT said:**

✅ 已完成整理 Flow 策略規則 Excel  
👉 下載 Nutanix\_Flow\_Policies.xlsx