Technische Anforderungen zum Erfassen

Da LOGINventory prinzipiell agentenlos arbeitet, ist stets die Grundvoraussetzung, dass eine Schnittstelle vorhanden ist, die zur Erfassung abgefragt werden kann. Dies ist in der Regel bei fast allen Geräten der Fall; es gibt jedoch Ausnahmen wie z.B. unmanaged Switches.

1 Windows Rechner

1.1 Remote Scan

Der Remote Scan von Windows Rechnern wird in LOGINquiry über eine Definition vom Typ **„Asset Inventory“** konfiguriert und ausgeführt.

Da es in Windows leider keine „ReadOnly-Admins“ gibt, muss dazu immer ein Account verwendet werden, der auf den zu erfassenden Rechnern **lokale Administrator-Rechte** hat. Dies ist z.B. bei einem Domain-Admin der Fall.

Die notwendigen APIs sind in Windows Home Editionen nicht vorhanden, bei allen anderen Windows Editionen muss zumindest der Dienst „Server“, bzw. „Datei und Drucker-Freigabe“ gestartet sein und selbstverständlich darf auch **keine Firewall** die Kommunikation behindern.

1.1.1 In gleicher Domain – oder mit Trust

Der Scan über innerhalb der gleichen Domain oder anderer Domain mit Vertrauensstellung (Trust) benötigt als Voraussetzungen zusätzlich lediglich:

Optimaler Weise:

- Voll-Zugriff auf Administrative Shares (C$, Admin$, …)

Oder:

- Den Dienst „Remote Registry“ (Startart: „Automatisch“ oder „Manuell“);
  Achtung: Dieser Dienst steht ab Windows 10 per Default auf „Deaktiviert“

1.1.2 In anderer Domain – ohne Trust

Prinzipiell funktioniert der Scan über non-trusted Domain-Grenzen nur unter folgenden Voraussetzungen:

- Voll-Zugriff auf Administrative Shares (C$, Admin$, …)

1.1.3 In Workgroup

Bei Workgroup Rechnern – oder beim Erfassen mittels lokalem Konto des Remote Rechners (auch in Domains):

- UAC-Remote muss aus sein, also entweder:
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, LocalAccountTokenFilterPolicy (DWORD) muss auf 1 gesetzt werden.
  - Oder: Lokale Richtlinien / Zuweisen von Benutzerrechten / *Zugriff vom Netzwerk auf diesen Computer verweigern*= Gast ~~, Lokales Konto~~
- Lokale Richtlinien / Sicherheitsoptionen / *Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten* = Klassisch
- Das Kennwort des Remote Administrators darf nicht leer sein.

1.2 Verwendete Ports und Protokolle bei Remote Scan

Verwendet wird zur Erfassung TCP/IP (IPv4 oder IPv6) und:

- ICMP Echo Request (Ping)
- Client für Microsoft Netzwerke
  - TCP Port 139 (NetBIOS Session Services)
  - UDP Port 137 und 138 (NetBIOS Name Server, NetBIOS Datagram)

- TCP Port 445 (RPC, WMI)

Als Zugriffs-Test empfohlen:

```
C:\> NET USE * \\RemotePc-or-IP\Admin$ /USER:Domain\AdminAccount AdminPassword
```

Und:

```
C:\> WMIC /NODE:RemotePc-or-IP /USER:Domain\AdminAccount /PASSWORD:AdminPassword CPU
```

1.3 Logon Skript

Bei der Ausführung der Erfassung im Logon- oder Startup-Skript müssen auf dem jeweiligen Rechner keine weiteren Voraussetzungen erfüllt werden.

Das ausführende Konto muss lediglich das Recht haben, die bei der Erfassung entstehende .INV Datei im „Datenverzeichnis“ des LOGINventory Rechners abzulegen, also Schreibrechte auf der Freigabe und im Filesystem haben.

Wir empfehlen:

- Authenticated Users (= Domain User + Domain Computers) mit Schreibrechten („Change“)

Beispiel für Logon-Skript:

```
START /B \\loginventory-server\LI7DATA\LOGINFO.EXE
```

1.4 Windows Offline Agent

Mit dem Offline Agenten können die Inventardaten sowohl über http/https an einen Webserver als auch an eine Datei-Freigabe geliefert werden.

Auch hier muss das verwendete Konto Schreibrechte auf der Freigabe und im Filesystem des „Datenverzeichnisses“ haben.

2 Exchange Organisation

Zur Inventarisierung einer komplette Exchange Organisation dient in LOGINquiry der Definitionstyp „MS Exchange Inventarisierung“. Das verwendete Konto benötigt in der Exchange Organisation die Mitgliedschaft in der **Rolle „View-Only Organization Management“** oder **„Organization Management“**. Als Quelle müssen Sie nur einen Exchange Server aus der vorgeschlagen Liste auswählen, und zwar den mit der höchsten Version, jedoch keine Edge-Rolle.

Gleichzeitig muss das Konto auf dem Exchange Server Rechner - wie stets bei Windows - lokale Administrator-Rechte besitzen.

3 VMware vSphere, ESXi

Für VMware ESXi und vCenter gibt es in LOGINquiry den Definitions-Typ „**vSphere Inventarisierung**“. Dieser benötigt allerdings zusätzliche PowerCLI v6.0 oder 6.3 **auf dem LOGINventory Rechner** installiert, welches Sie bei VMware direkt herunterladen können:

- https://my.vmware.com/group/vmware/get-download?downloadGroup=PCLI600R3
- https://my.vmware.com/group/vmware/get-download?downloadGroup=PCLI630R1

Das verwendete Konto benötigt hier lediglich **„Nur lesen“ Rechte**.

Die Standard-Einstellung der Windows PowerShell ist es, die Ausführung von Skripts zu verhindern! Sie müssen diese Funktion erst freischalten, z.B. über

```
C:\> Powershell
PS C:\> Set-ExecutionPolicy ByPass
```

Typischerweise erhalten Sie in LOGINquiry bei Erfassen von ESXi oder vCenter eine Nachricht: „**Warnung: Ungültiges SSL Zertifikat**“, und zwar dann wenn Sie die von VMware automatisch erstellten „SelfSigned“ Zertifikate verwenden und noch keine vertrauenswürde Zertifizierungsstelle verwendet haben. Diese Warnung beeinträchtigt die Inventarisierung nicht.

4 XenServer

Diese Geräte werden nicht über die Methode „Asset Inventory“ sondern über „**XenServer Inventarisierung**“ erfasst. Auch hier wird ein Konto mit Administrator-Rechten auf dem XenServer benötigt.

5 XenApp Server

Für den Zugriff auf die XenApp Daten auf einem entsprechenden Windows Server muss das verwendete Konto in der Methode „**XenApp Inventory**“ sowohl auf Windows als auch auf XenApp Administrator-Rechte besitzen.

6 Unix, Linux, MacOS

Die Erfassung dieser Systeme mittels „**Asset Inventory**“ geschieht über eine Secure Shell Verbindung, über die das Erfassungs-Skript und die Ergebnisdaten übertragen werden.

Die Voraussetzungen dafür sind generell:

- Installation/Aktivierung des SSH-Daemon (inklusive Freigabe des Port 22)
- Konto mit „root“ Rechten (nur damit können Hardware-Informationen gelesen werden)
- Programmpaket `perl` (ab Version 5.8)
- Notwendige vorhandene Kommandos:
  - **`which perl chmod cp gzip mkdir mv rm rmdir tar`**
  - **`cut date head last uname`**

Die Authentifizierung des Benutzers für SSH kann alternativ über:

- Benutzername und Passwort;
- Benutzername und Schlüsseldatei sowie Passphrase identifiziert werden (Details siehe Administrator Handbuch Kapitel 13.2.2).

Bei manchen Systemen muss die Passwort Authentifizierung extra freigeschaltet werden, die Authentifizierung über Schlüsseldatei mit Passphrase ist prinzipiell immer möglich.

6.1 Mac mit OS X

Der SSH-Daemon ist per Default aktiviert.

In der Datei */etc/ssh/sshd_config* muss ggf. der Eintrag für *`PasswordAuthentication`* aktiviert und auf den Wert ***`yes`*** gestellt werden:

`#PasswordAuthentication no` →
`PasswordAuthentication yes`

Nach einer Änderung ist ein Restart des Systems oder Neustart des Daemons nicht notwendig.

6.2 SuSe Linux

Zur SSH-Aktivierung muss folgende Aktionen durchgeführt werden:

- NetServices: sshd enable
- Firewall → Service → SSH-Daemon freigeben

Zur Passwort-Authentifizierung muss in der Datei */etc/ssh/sshd_config* der Eintrag geändert werden:

`PasswordAuthentication no` → ***`yes`***

Nach einer Änderung ist ein Restart des Systems oder Neustart des Daemons notwendig.

6.3 Ubuntu Linux

Hier muss der SSH-Daemon explizit aktiviert werden.

Die Aktivierung des Daemons erfolgt über:

```
sudo apt-get install openssh-server
```

Die Passwort Authentifizierung ist hier per Default aktiviert.

6.4 Red Hat Linux

Der SSH-Daemon ist per Default aktiviert.

Die Passwort Authentifizierung ist hier per Default aktiviert.

6.5 Oracle Solaris

Der SSH-Daemon ist per Default aktiviert.

Die Passwort Authentifizierung ist hier standardmäßig aktiviert. Für die Benutzung der Benutzerkennung »root« muss jedoch die Konfiguration des SSH-Daemon angepasst werden:

- In der Datei */etc/ssh/sshd_config* muss der Eintrag für `PermitRootLogin` auf den Wert ***yes*** gestellt werden:

  `PermitRootLogin no` → `PermitRootLogin` ***yes***
- In der Datei */etc/default/login* muss der Eintrag für `CONSOLE` auskommentiert werden:

  `CONSOLE=/dev/console` → ***#****CONSOLE=/dev/console*
- In der Datei */etc/user_attr* muss der Eintrag `;type=role` aus dem ‚root'-Eintrag entfernt werden. Dies kann durch folgendes Kommando erfolgen:

  rolemod -K type=normal root
- Nun muss der SSH-Daemon neu gestartet werden:

  svcadm restart svc:/network/ssh:default

7 Drucker, Router, Switches

Diese Geräte werden üblicherweise mittels „**Asset Inventory**" mittels SNMP v1 oder v3 erfasst.

Die SNMP v1 API ist standardmäßig in Windows vorhanden und funktioniert ohne weitere Konfigurationsschritte.

Die meisten Drucker haben einen SNMP v1 ReadOnly-Community-String „public" voreingestellt, mit deren Verwendung sich die Konfiguration einfach auslesen lässt.

Bei Routern und Switches ist dies meist nicht der Fall und muss dann manuell konfiguriert werden. Wir empfehlen die Verwendung eines unterschiedlichen Community-Strings um beim Erfassen über diesen Weg bestimmte Geräte-Typen zu selektieren.

Eventuell muss auch der Default View angepasst werden (sollte die OID 1 sein) sowie die IP der zulässigen Management Station(s), also des LOGINventory Rechners (0.0.0.0 = alle Rechner).

Soll SNMP v3 benutzt werden, sind zusätzlich Schritte notwendig. Diese sind ausführlich beschrieben im Administrator Handbuch, Kapitel 12.