Microsoft

LIEBERMANSOFTWARE™

Automating Privileged Identity Management with Lieberman Software

Calum MacLeod
cmacleod@liebsoft.com
VP EMEA
Lieberman Software Corporation

What Are Privileged Accounts?

- Root and Admin
- Service and Process
- Application-to-Application
- Most powerful accounts in the organization
- Access sensitive information
- Rarely changed, known to many
- No individual user accountability

“Privileged Accounts Give System Wide Access”

“Shared superuser accounts — typically system-defined in operating systems, databases, network devices and elsewhere — present significant risks when the passwords are routinely shared by multiple users.” – Gartner, MarketScope for Shared-Account/Software-Account Password Management, 2009

The Privileged Identity Threat

- Most powerful accounts in organization
- Access to sensitive information
- Rarely changed, known to many
- No individual user accountability

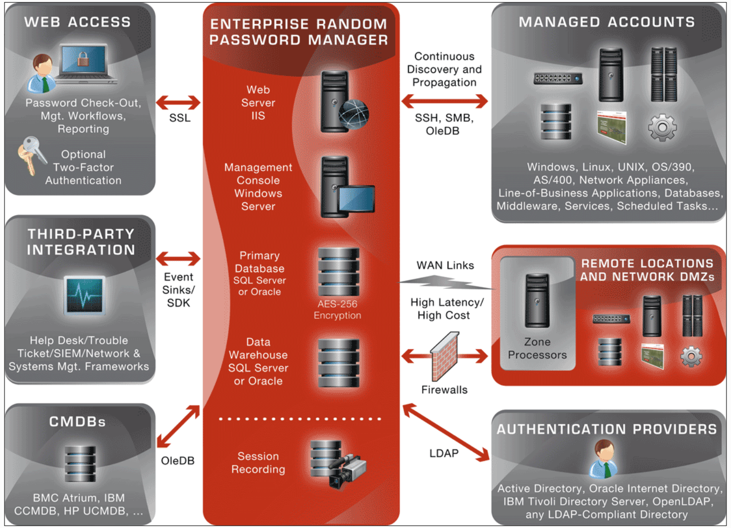
> **"Shared superuser accounts – typically system-defined in operating systems, databases, network devices and elsewhere – present significant risks when the passwords are routinely shared by multiple users."**
>
> *Gartner MarketScope for Shared-Account/Software-Account Password Management, 2009*

Mitigate Your Risks - *Through Automation*

1. **Identify** and **document** critical IT assets, their privileged accounts and interdependencies
2. **Enforce** rules for password strength, uniqueness and change frequency, synchronizing changes across dependencies
3. **Delegate** so that only appropriate personnel can access privileged accounts in a timely manner
4. **Audit** and **alert**

Solution Overview - *Enterprise Random Password Manager (ERPM)*

- Secures Windows, Linux / UNIX, mainframes, network appliances, databases, business applications, hypervisors, LOM cards, ..
- Multi-threaded, n-tier architecture scales to the **largest networks**
- Authenticates in **real time** with your directory services
- Built-in support for **multi-factor authentication**



WEB ACCESS

Password Check-Out, Mgt. Workflows, Reporting

Optional Two-Factor Authentication

THIRD-PARTY INTEGRATION

Help Desk/Trouble Ticket/SIEM/Network & Systems Mgt. Frameworks

CMDBs

BMC Atrium, IBM CCMDB, HP UCMDB, ...

SSL

Event Sinks/ SDK

OleDB

ENTERPRISE RANDOM PASSWORD MANAGER

Web Server IIS

Management Console Windows Server

Primary Database SQL Server or Oracle

AES-256 Encryption

Data Warehouse SQL Server or Oracle

Session Recording

Continuous Discovery and Propagation

SSH, SMB, OleDB

WAN Links

High Latency/ High Cost

Firewalls

LDAP

MANAGED ACCOUNTS

Windows, Linux, UNIX, OS/390, AS/400, Network Appliances, Line-of-Business Applications, Databases, Middleware, Services, Scheduled Tasks...

REMOTE LOCATIONS AND NETWORK DMZs

Zone Processors

AUTHENTICATION PROVIDERS

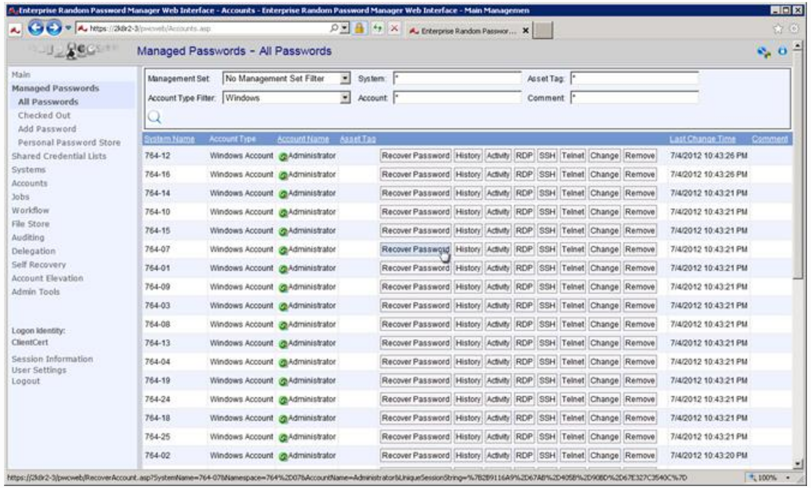
Active Directory, Oracle Internet Directory, IBM Tivoli Directory Server, OpenLDAP, any LDAP-Compliant Directory

ERPM Architecture

LIEBERMANSOFTWARE

Privileged Account Security - *Enterprise Random Password Manager (ERPM)*

- Enforces cryptographically strong, sufficiently unique, frequently changed credentials
- Propagates new credentials to all places used to prevent service disruptions
- Stores passwords in an AES-256 encrypted MS SQL database



Managed Passwords - All Passwords

Management Set: No Management Set Filter
System: *
Asset Tag: *
Account Type Filter: Windows
Account: *
Comment: *

System Name	Account Type	Account Name	Asset Tag		Last Change Time	Comment
764-12	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:26 PM	
764-16	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:26 PM	
764-14	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-10	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-15	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-07	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-01	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-09	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-03	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-08	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-13	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-04	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-19	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-24	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-18	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-25	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:21 PM	
764-02	Windows Account	Administrator		Recover Password History Activity RDP SSH Telnet Change Remove	7/4/2012 10:43:20 PM	

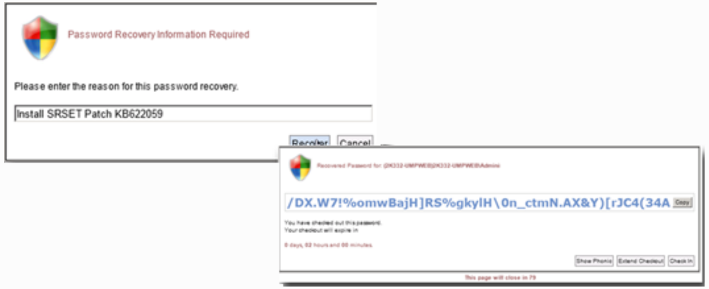
https://2k8r2-3/pwcweb/RecoverAccount.asp?SystemName=764-07&Namespace=764%2D07&AccountName=Administrator&UniqueSessionString=%7B2B9116A9%2D67A8%2D4058%2D90BD%2D67E327C3540C%7D

Password Recovery Console

LIEBERMANSOFTWARE

Automation and Workflows - *Enterprise Random Password Manager (ERPM)*

- Enforces **secure authentication**, **authorization** and **workflows** to retrieve credentials
- Documents **every requestor, location, and reason** for privileged access
- Changes passwords **immediately after they're disclosed** to prevent reuse



Password Recovery Information Required

Please enter the reason for this password recovery.

Install SRSET Patch KB622059

Recovered Password for: (2K332-UMPWEB)2K332-UMPWEB\Admin

/DX.W7!%omwBajH]RS%gkylH\0n_ctmN.AX&Y)[rJC4(34A

You have checked out this password.
Your checkout will expire in

0 days, 02 hours and 00 minutes.

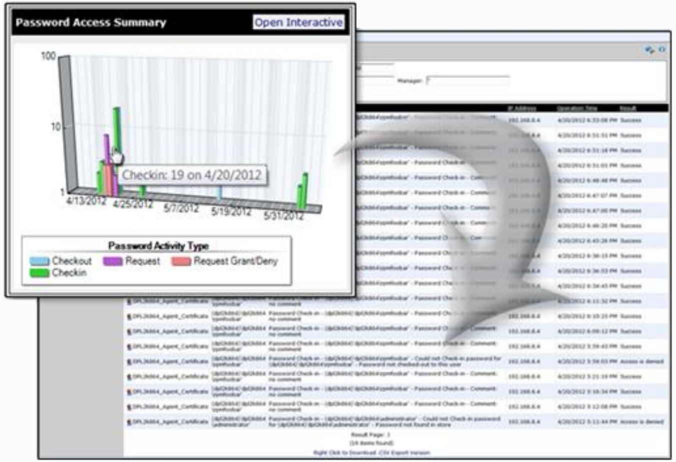
This page will close in 79

Audited Password Check Out

LIEBERMANSOFTWARE

Auditing, Reporting, & Analytics - *Enterprise Random Password Manager (ERPM)*

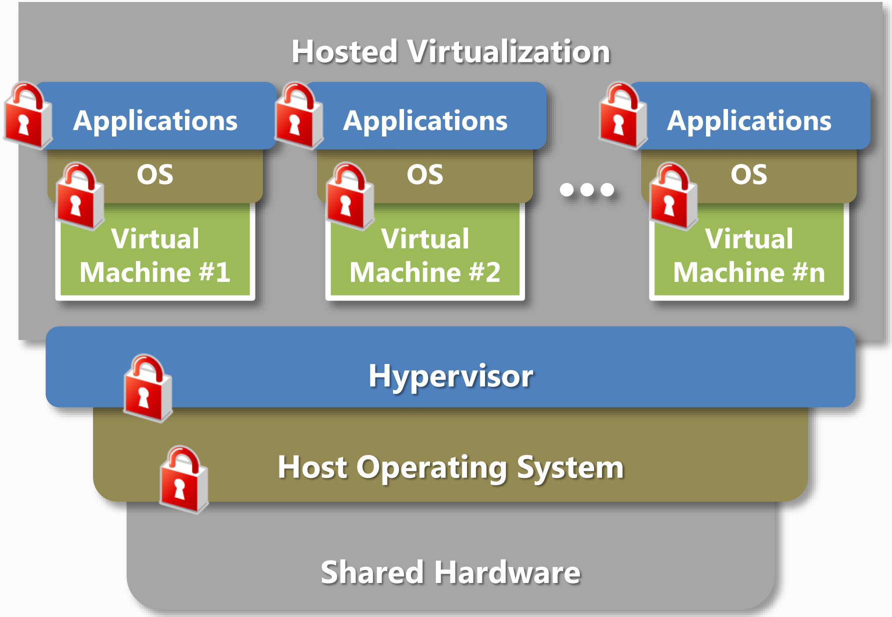
- Logs **all password and system activity**
- Provides **comprehensive auditing and compliance reports**
- Displays **real-time business intelligence** with drill-down to the underlying data



Dashboard Drill Down

LIEBERMANSOFTWARE

Secure Physical and Virtual Stacks

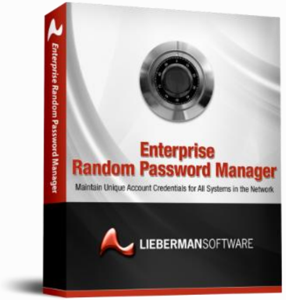


Every privileged identity – in every host OS, guest OS, and application – presents a potential security threat if unsecured.

Enterprise Random Password Manager (ERPM)

Automated Credential Management

- **Discovers** machines, process accounts, local and fire call accounts, services and tasks – and wherever accounts are referenced
- **Randomizes privileged account passwords** and propagates those changes everywhere accounts are used to avoid lockouts
- **Stores complex, random passwords** in encrypted **repository**
- **Enforces role-based provisioning** of password access and delegation
- **Audits and reports** every password request, use and change

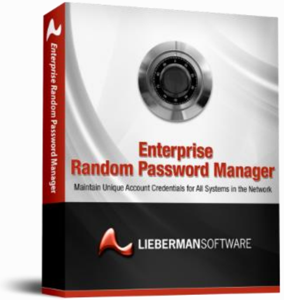

Enterprise Random Password Manager
Enterprise
Random Password Manager
Maintain Unique Account Credentials for All Systems in the Network
LIEBERMANSOFTWARE

LIEBERMANSOFTWARE

Enterprise Random Password Manager

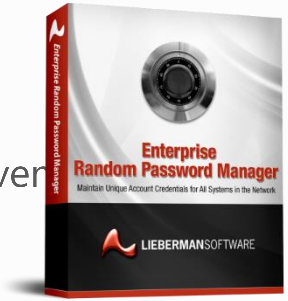
Controls the Entire Life Cycle of Privileged Accounts

- Always keeps **up-to-date, accurate** systems and account lists
- Immediately **removes knowledge** of shared credentials
- Provides **quick access** to credentials on a need to know basis for the shortest time possible
- **Automatically changes** disclosed passwords
- Allows organizations to change sensitive passwords – including **process and service account credentials** - without fear of outages
- Automates as much as possible for **low TCO and fast deployment**


Enterprise Random Password Manager
Enterprise
Random Password Manager
Maintain Unique Account Credentials for All Systems in the Network
LIEBERMANSOFTWARE

What Differentiates ERPM?

- **Rapid, complete deployments (days, not months)**
  - User installable and configurable - no need for scripting, customization, professional services
  - Easy to upgrade and manage over time
- **Superior technology**
  - Auto-discovery and correlation, propagation
  - Unsurpassed service account management
  - N-tier deployment architecture
- **Open standards: no proprietary technology**
- **Enterprise-ready** for scale, scope, and complex, dynamic infrastructures
  - Resilient solution: without constant IT interven
- **Comprehensive and open documentation**


Enterprise Random Password Manager
Enterprise
Random Password Manager
Maintain Unique Account Credentials for All Systems in the Network
LIEBERMANSOFTWARE

System Center Integrations

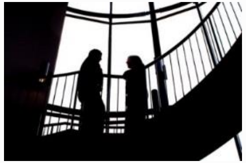
LIEBERMANSOFTWARE

What We Have Historically Done With System Center

- **Grant Access to Privileged Credentials** within SCOM/SCCM Interface
- **Update SCOM Credentials**
- **Provide Trouble Ticket Integration** with SCSM

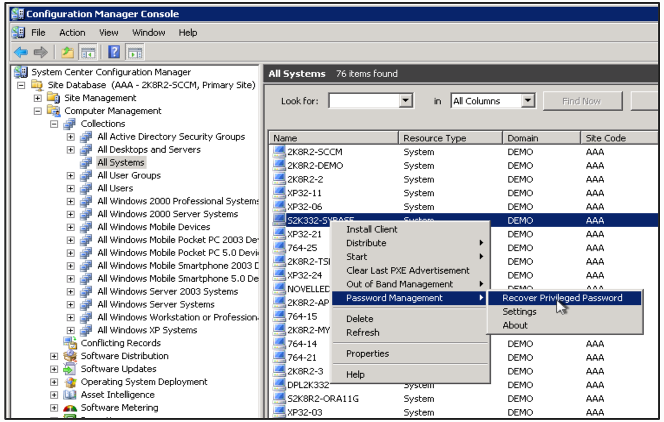
Problem - *SCCM and SCOM Don't Provide Access to Systems*

- SCCM and SCOM **don't grant IT staff admin- and root- level access** to systems being monitored and controlled
- There's no way to assure that authorized employees can access problem systems **in a hurry when needed**
- As a result, too many organizations continue to store privileged logins on **Post-It Notes and spreadsheets**
- Privileged access quickly spreads to the **wrong people**



Solution - *Privileged Identity Management in SCCM and SCOM*

- Deep **ERPM integration** lets you manage and access privileged logins right from **SCCM** and **SCOM**
- Immediately **grants secure, delegated access** to authorized staff
- Secures System Center agents and services that use domain and local passwords
- Provides **detailed reports** to prove compliance



- System Center Configuration Manager
  - Site Database (AAA - 2K8R2-SCCM, Primary Site)
    - Site Management
    - Computer Management
      - Collections
        - All Active Directory Security Groups
        - All Desktops and Servers
        - All Systems
        - All User Groups
        - All Users
        - All Windows 2000 Professional Systems
        - All Windows 2000 Server Systems
        - All Windows Mobile Devices
        - All Windows Mobile Pocket PC 2003 De
        - All Windows Mobile Pocket PC 5.0 Devi
        - All Windows Mobile Smartphone 2003 D
        - All Windows Mobile Smartphone 5.0 De
        - All Windows Server 2003 Systems
        - All Windows Server Systems
        - All Windows Workstation or Profession
        - All Windows XP Systems
      - Conflicting Records
      - Software Distribution
      - Software Updates
      - Operating System Deployment
      - Asset Intelligence
      - Software Metering

All Systems 76 items found

Name	Resource Type	Domain	Site Code
2K8R2-SCCM	System	DEMO	AAA
2K8R2-DEMO	System	DEMO	AAA
2K8R2-2	System	DEMO	AAA
XP32-11	System	DEMO	AAA
XP32-06	System	DEMO	AAA
S2K332-SYBASE	System	DEMO	AAA
XP32-21		DEMO	AAA
764-25		DEMO	AAA
2K8R2-TSI		DEMO	AAA
XP32-24		DEMO	AAA
NOVELLED		DEMO	AAA
2K8R2-AP			
764-15			
2K8R2-MY			
764-14		DEMO	AAA
764-21		DEMO	AAA
2K8R2-3		DEMO	AAA
DPL2K332	System	DEMO	AAA
S2K8R2-ORA11G	System	DEMO	AAA
XP32-03	System	DEMO	AAA

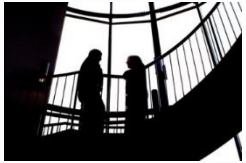
Right-Click to Recover Passwords in SCCM, SCOM

LIEBERMANSOFTWARE

Problem - *SCSM 'Blind Spot'*

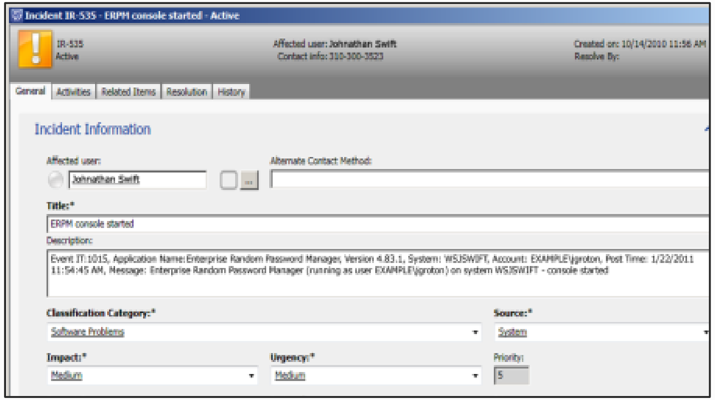
- Unable to **grant privileged access** when incidents or tickets demand it
- Can't **trigger events and update tickets** based on privileged actions
- No way to **control privileged access** based on each incident
- Can't **audit or report** privileged logins that can lead to disruptions

LIEBERMANSOFTWARE™



Solution - *ERPM Integration with SCSM*

- Provides **fast, delegated access** to Help Desk staff from within SCSM
- Grants **relevant IT staff** privileged access –**to relevant systems, applications and devices** – determined by SCSM tickets
- **Opens and updates SCSM** incident-based privileged identity events
- Provides **detailed reports** to prove compliance



Incident IR-535 - ERPM console started - Active

IR-535
Active

Affected user: Johnathan Swift
Contact info: 310-300-3523

Created on: 10/14/2010 11:56 AM
Resolve By:

Incident Information

Affected user: Johnathan Swift

Alternate Contact Method:

Title:* ERPM console started

Description:
Event IT:1015, Application Name:Enterprise Random Password Manager, Version 4.83.1, System: WSJSWIFT, Account: EXAMPLE\jgroton, Post Time: 1/22/2011 11:54:45 AM, Message: Enterprise Random Password Manager (running as user EXAMPLE\jgroton) on system WSJSWIFT - console started

Classification Category:* Software Problems

Source:* System

Impact:* Medium

Urgency:* Medium

Priority: 5

Privileged Identity Incident in SCSM

LIEBERMANSOFTWARE

New Orchestration Capabilities

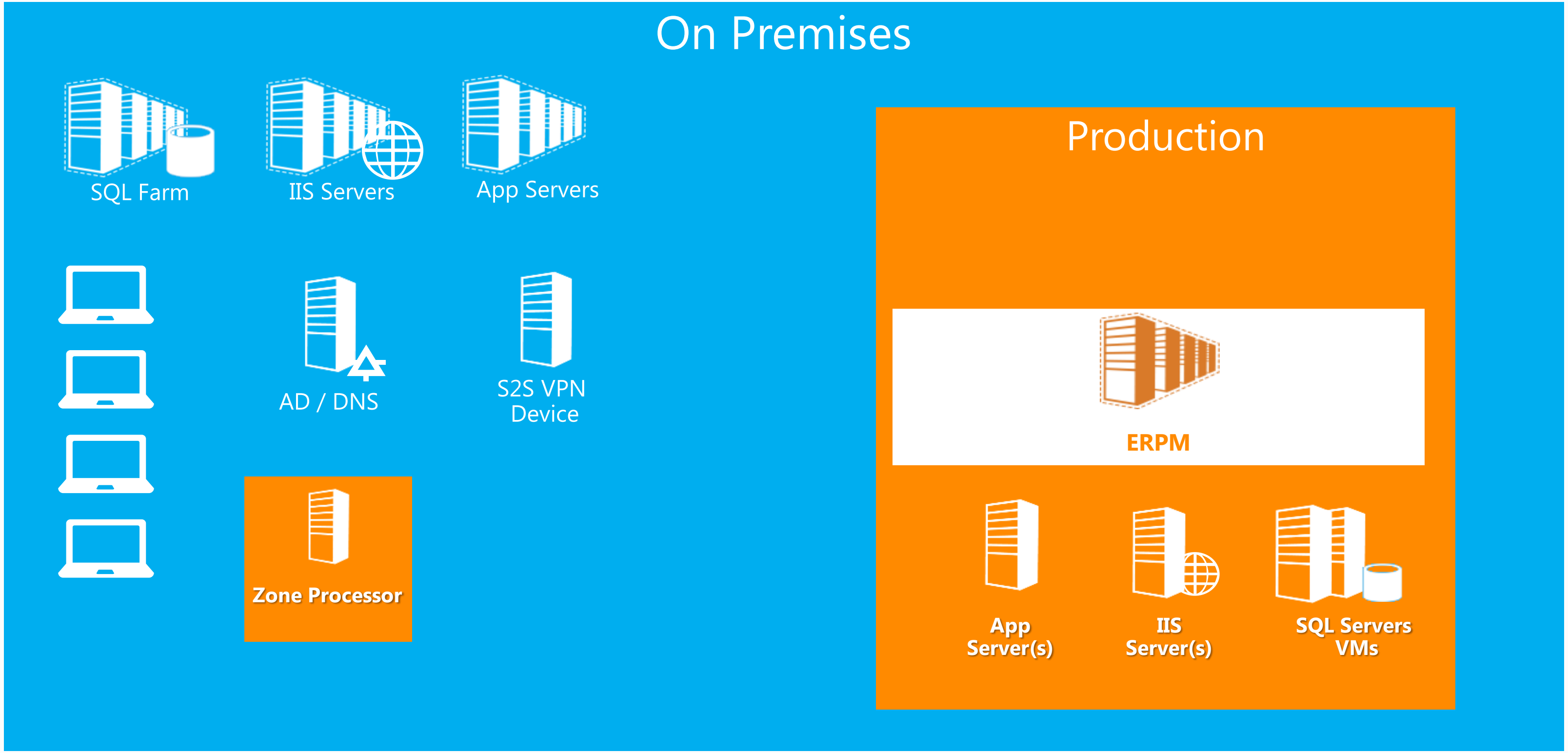
LIEBERMANSOFTWARE

ERPM Architecture

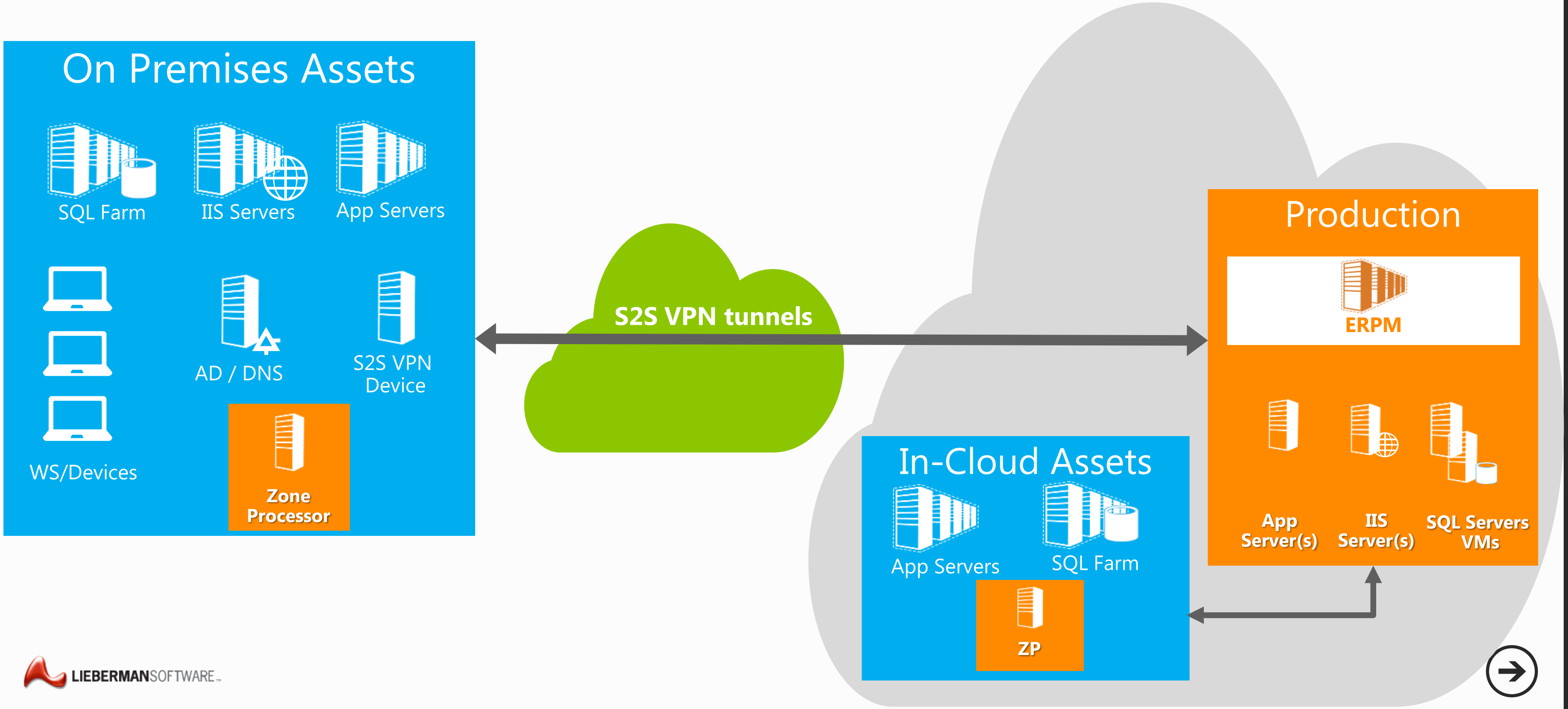
- **Management Console:** Server 2K8/2K12
- **Secure Storage**: SQL Server 2008/12
- **Web Server**: >IIS7

- Physical or Virtualized (Hyper-V and VMW certified)
- Fully-Redundant, N-tier model, cloud-ready
- Zone Processors: for distributed processing, cross DMZ or at Tenant
- Leverages WA IAAS, Virtual Networks site-to-site connectivity

ERPM: On-Premises



ERPM: Hosted in WA



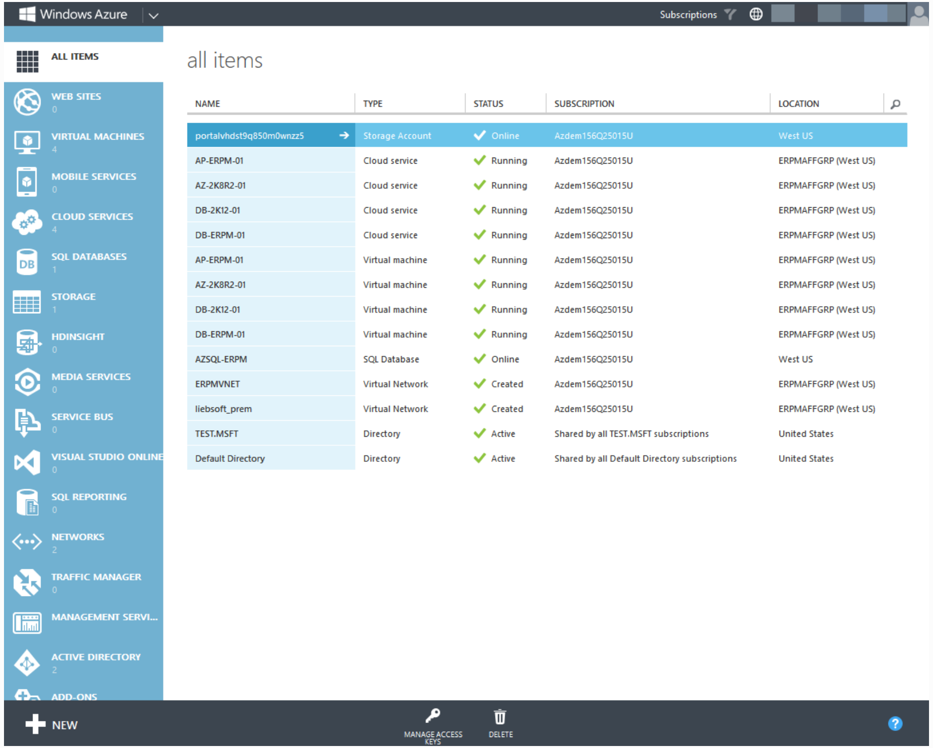
LIEBERMANSOFTWARE

ERPM Hosted Advantages

- Rapid Deployment: ERPM packaged with scripts; deploys each tier
- Easily move from POC to Production
- Mission-Critical Worthy: Highly-Available, Geo-replicated, pick your DC
- Identity/Access: AD on-prem or AAD in cloud

- Licensing: Consume existing Azure EA or new subscription
- Cost Savings: no up-front investment in SQL Enterprise, App Servers

Azure Item List

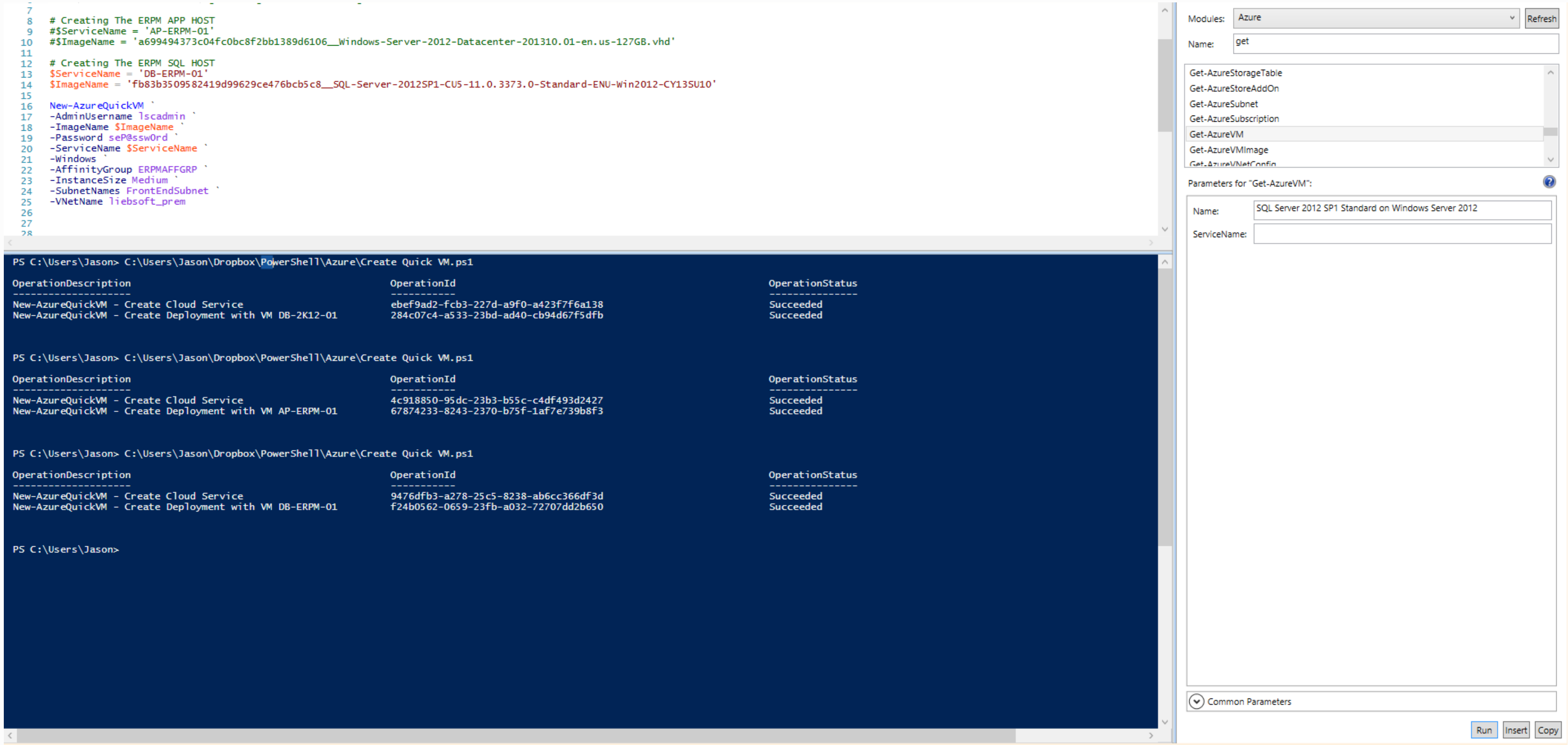


all items

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
portalvhdst9q850m0wnzz5	Storage Account	✓ Online	Azdem156Q25015U	West US
AP-ERPM-01	Cloud service	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
AZ-2K8R2-01	Cloud service	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
DB-2K12-01	Cloud service	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
DB-ERPM-01	Cloud service	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
AP-ERPM-01	Virtual machine	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
AZ-2K8R2-01	Virtual machine	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
DB-2K12-01	Virtual machine	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
DB-ERPM-01	Virtual machine	✓ Running	Azdem156Q25015U	ERPMAFFGRP (West US)
AZSQL-ERPM	SQL Database	✓ Online	Azdem156Q25015U	West US
ERPMVNET	Virtual Network	✓ Created	Azdem156Q25015U	ERPMAFFGRP (West US)
liebsoft_prem	Virtual Network	✓ Created	Azdem156Q25015U	ERPMAFFGRP (West US)
TEST.MSFT	Directory	✓ Active	Shared by all TEST.MSFT subscriptions	United States
Default Directory	Directory	✓ Active	Shared by all Default Directory subscriptions	United States

LIEBERMANSOFTWARE™

Azure PowerShell VM Creates



```
# Creating The ERPM APP HOST
#$ServiceName = 'AP-ERPM-01'
#$ImageName = 'a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-Datacenter-201310.01-en.us-127GB.vhd'

# Creating The ERPM SQL HOST
$ServiceName = 'DB-ERPM-01'
$ImageName = 'fb83b3509582419d99629ce476bcb5c8__SQL-Server-2012SP1-CU5-11.0.3373.0-Standard-ENU-Win2012-CY13SU10'

New-AzureQuickVM `
-AdminUsername lscadmin `
-ImageName $ImageName `
-Password seP@ssw0rd `
-ServiceName $ServiceName `
-Windows `
-AffinityGroup ERPMAFFGRP `
-InstanceSize Medium `
-SubnetNames FrontEndSubnet `
-VNetName liebsoft_prem
```

```
PS C:\Users\Jason> C:\Users\Jason\Dropbox\PowerShell\Azure\Create Quick VM.ps1

OperationDescription                                OperationId                                         OperationStatus
--------------------                                -----------                                         ---------------
New-AzureQuickVM - Create Cloud Service             ebef9ad2-fcb3-227d-a9f0-a423f7f6a138                Succeeded
New-AzureQuickVM - Create Deployment with VM DB-2K12-01  284c07c4-a533-23bd-ad40-cb94d67f5dfb           Succeeded


PS C:\Users\Jason> C:\Users\Jason\Dropbox\PowerShell\Azure\Create Quick VM.ps1

OperationDescription                                OperationId                                         OperationStatus
--------------------                                -----------                                         ---------------
New-AzureQuickVM - Create Cloud Service             4c918850-95dc-23b3-b55c-c4df493d2427                Succeeded
New-AzureQuickVM - Create Deployment with VM AP-ERPM-01  67874233-8243-2370-b75f-1af7e739b8f3           Succeeded


PS C:\Users\Jason> C:\Users\Jason\Dropbox\PowerShell\Azure\Create Quick VM.ps1

OperationDescription                                OperationId                                         OperationStatus
--------------------                                -----------                                         ---------------
New-AzureQuickVM - Create Cloud Service             9476dfb3-a278-25c5-8238-ab6cc366df3d                Succeeded
New-AzureQuickVM - Create Deployment with VM DB-ERPM-01  f24b0562-0659-23fb-a032-72707dd2b650           Succeeded


PS C:\Users\Jason>
```

Modules: Azure

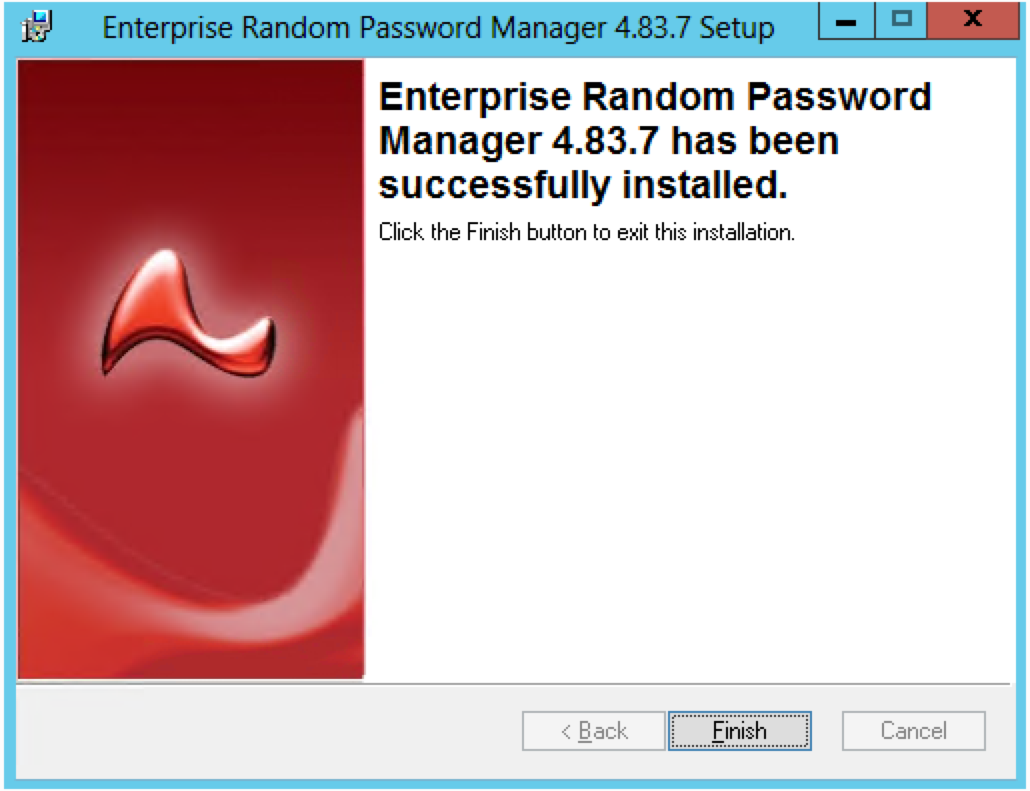
Name: get

Parameters for "Get-AzureVM":

Name: SQL Server 2012 SP1 Standard on Windows Server 2012

ServiceName:

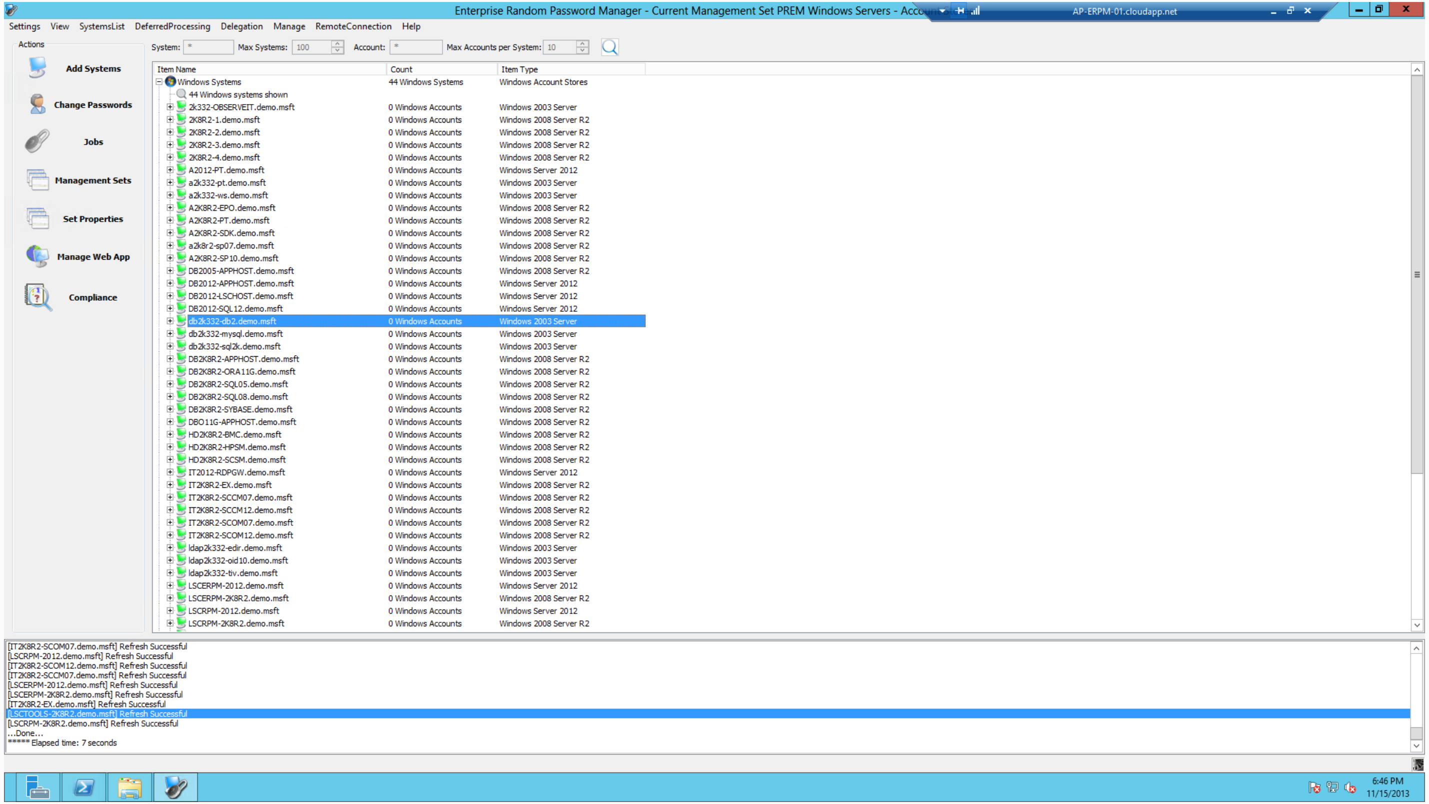
ERPM Install Success



Enterprise Random Password Manager 4.83.7 has been successfully installed.

Click the Finish button to exit this installation.

ERPM Visibility on Prem



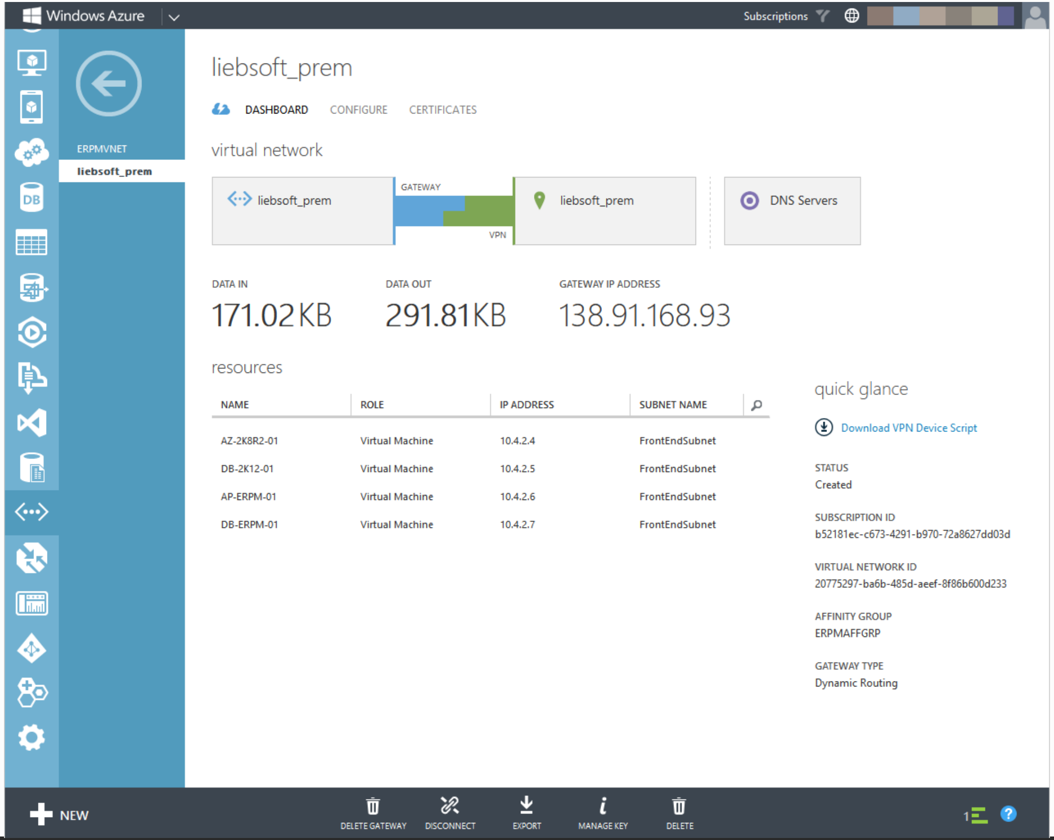
System: * Max Systems: 100 Account: * Max Accounts per System: 10

Item Name	Count	Item Type
Windows Systems	44 Windows Systems	Windows Account Stores
44 Windows systems shown		
2k332-OBSERVEIT.demo.msft	0 Windows Accounts	Windows 2003 Server
2K8R2-1.demo.msft	0 Windows Accounts	Windows 2008 Server R2
2K8R2-2.demo.msft	0 Windows Accounts	Windows 2008 Server R2
2K8R2-3.demo.msft	0 Windows Accounts	Windows 2008 Server R2
2K8R2-4.demo.msft	0 Windows Accounts	Windows 2008 Server R2
A2012-PT.demo.msft	0 Windows Accounts	Windows Server 2012
a2k332-pt.demo.msft	0 Windows Accounts	Windows 2003 Server
a2k332-ws.demo.msft	0 Windows Accounts	Windows 2003 Server
A2K8R2-EPO.demo.msft	0 Windows Accounts	Windows 2008 Server R2
A2K8R2-PT.demo.msft	0 Windows Accounts	Windows 2008 Server R2
A2K8R2-SDK.demo.msft	0 Windows Accounts	Windows 2008 Server R2
a2k8r2-sp07.demo.msft	0 Windows Accounts	Windows 2008 Server R2
A2K8R2-SP10.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2005-APPHOST.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2012-APPHOST.demo.msft	0 Windows Accounts	Windows Server 2012
DB2012-LSCHOST.demo.msft	0 Windows Accounts	Windows Server 2012
DB2012-SQL12.demo.msft	0 Windows Accounts	Windows Server 2012
db2k332-db2.demo.msft	0 Windows Accounts	Windows 2003 Server
db2k332-mysql.demo.msft	0 Windows Accounts	Windows 2003 Server
db2k332-sql2k.demo.msft	0 Windows Accounts	Windows 2003 Server
DB2K8R2-APPHOST.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2K8R2-ORA11G.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2K8R2-SQL05.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2K8R2-SQL08.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DB2K8R2-SYBASE.demo.msft	0 Windows Accounts	Windows 2008 Server R2
DBO11G-APPHOST.demo.msft	0 Windows Accounts	Windows 2008 Server R2
HD2K8R2-BMC.demo.msft	0 Windows Accounts	Windows 2008 Server R2
HD2K8R2-HPSM.demo.msft	0 Windows Accounts	Windows 2008 Server R2
HD2K8R2-SCSM.demo.msft	0 Windows Accounts	Windows 2008 Server R2
IT2012-RDPGW.demo.msft	0 Windows Accounts	Windows Server 2012
IT2K8R2-EX.demo.msft	0 Windows Accounts	Windows 2008 Server R2
IT2K8R2-SCCM07.demo.msft	0 Windows Accounts	Windows 2008 Server R2
IT2K8R2-SCCM12.demo.msft	0 Windows Accounts	Windows 2008 Server R2
IT2K8R2-SCOM07.demo.msft	0 Windows Accounts	Windows 2008 Server R2
IT2K8R2-SCOM12.demo.msft	0 Windows Accounts	Windows 2008 Server R2
ldap2k332-edir.demo.msft	0 Windows Accounts	Windows 2003 Server
ldap2k332-oid10.demo.msft	0 Windows Accounts	Windows 2003 Server
ldap2k332-tiv.demo.msft	0 Windows Accounts	Windows 2003 Server
LSCERPM-2012.demo.msft	0 Windows Accounts	Windows Server 2012
LSCERPM-2K8R2.demo.msft	0 Windows Accounts	Windows 2008 Server R2
LSCRPM-2012.demo.msft	0 Windows Accounts	Windows Server 2012
LSCRPM-2K8R2.demo.msft	0 Windows Accounts	Windows 2008 Server R2

```
[IT2K8R2-SCOM07.demo.msft] Refresh Successful
[LSCRPM-2012.demo.msft] Refresh Successful
[IT2K8R2-SCOM12.demo.msft] Refresh Successful
[IT2K8R2-SCCM07.demo.msft] Refresh Successful
[LSCERPM-2012.demo.msft] Refresh Successful
[LSCERPM-2K8R2.demo.msft] Refresh Successful
[IT2K8R2-EX.demo.msft] Refresh Successful
[LSCTOOLS-2K8R2.demo.msft] Refresh Successful
[LSCRPM-2K8R2.demo.msft] Refresh Successful
...Done...
***** Elapsed time: 7 seconds
```

LIEBERMANSOFTWARE

Virtual Network - Azure to Prem



liebsoft_prem

DASHBOARD CONFIGURE CERTIFICATES

virtual network

DATA IN
171.02KB

DATA OUT
291.81KB

GATEWAY IP ADDRESS
138.91.168.93

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
AZ-2K8R2-01	Virtual Machine	10.4.2.4	FrontEndSubnet
DB-2K12-01	Virtual Machine	10.4.2.5	FrontEndSubnet
AP-ERPM-01	Virtual Machine	10.4.2.6	FrontEndSubnet
DB-ERPM-01	Virtual Machine	10.4.2.7	FrontEndSubnet

quick glance

Download VPN Device Script

STATUS
Created

SUBSCRIPTION ID
b52181ec-c673-4291-b970-72a8627dd03d

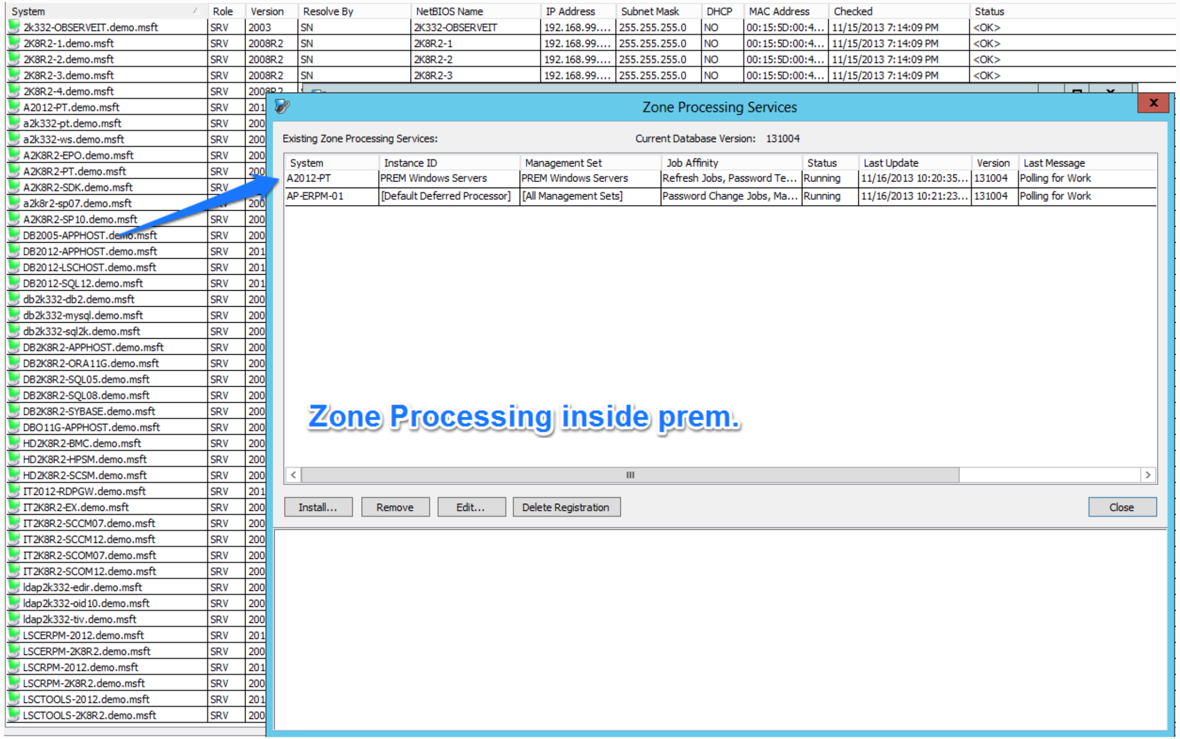
VIRTUAL NETWORK ID
20775297-ba6b-485d-aeef-8f86b600d233

AFFINITY GROUP
ERPMAFFGRP

GATEWAY TYPE
Dynamic Routing

LIEBERMANSOFTWARE

Zone Processor inside Prem



System	Role	Version	Resolve By	NetBIOS Name	IP Address	Subnet Mask	DHCP	MAC Address	Checked	Status
2k332-OBSERVEIT.demo.msft	SRV	2003	SN	2K332-OBSERVEIT	192.168.99....	255.255.255.0	NO	00:15:5D:00:4...	11/15/2013 7:14:09 PM	<OK>
2K8R2-1.demo.msft	SRV	2008R2	SN	2K8R2-1	192.168.99....	255.255.255.0	NO	00:15:5D:00:4...	11/15/2013 7:14:09 PM	<OK>
2K8R2-2.demo.msft	SRV	2008R2	SN	2K8R2-2	192.168.99....	255.255.255.0	NO	00:15:5D:00:4...	11/15/2013 7:14:09 PM	<OK>
2K8R2-3.demo.msft	SRV	2008R2	SN	2K8R2-3	192.168.99....	255.255.255.0	NO	00:15:5D:00:4...	11/15/2013 7:14:09 PM	<OK>
2K8R2-4.demo.msft	SRV	2008R2								
A2012-PT.demo.msft	SRV	201								
a2k332-pt.demo.msft	SRV	200								
a2k332-ws.demo.msft	SRV	200								
A2K8R2-EPO.demo.msft	SRV	200								
A2K8R2-PT.demo.msft	SRV	200								
A2K8R2-SDK.demo.msft	SRV									
a2k8r2-sp07.demo.msft		200								
A2K8R2-SP10.demo.msft	SRV	200								
DB2005-APPHOST.demo.msft	SRV	200								
DB2012-APPHOST.demo.msft	SRV	201								
DB2012-LSCHOST.demo.msft	SRV	201								
DB2012-SQL12.demo.msft	SRV	201								
db2k332-db2.demo.msft	SRV	200								
db2k332-mysql.demo.msft	SRV	200								
db2k332-sql2k.demo.msft	SRV	200								
DB2K8R2-APPHOST.demo.msft	SRV	200								
DB2K8R2-ORA11G.demo.msft	SRV	200								
DB2K8R2-SQL05.demo.msft	SRV	200								
DB2K8R2-SQL08.demo.msft	SRV	200								
DB2K8R2-SYBASE.demo.msft	SRV	200								
DBO11G-APPHOST.demo.msft	SRV	200								
HD2K8R2-BMC.demo.msft	SRV	200								
HD2K8R2-HPSM.demo.msft	SRV	200								
HD2K8R2-SCSM.demo.msft	SRV	200								
IT2012-RDPGW.demo.msft	SRV	201								
IT2K8R2-EX.demo.msft	SRV	200								
IT2K8R2-SCCM07.demo.msft	SRV	200								
IT2K8R2-SCCM12.demo.msft	SRV	200								
IT2K8R2-SCOM07.demo.msft	SRV	200								
IT2K8R2-SCOM12.demo.msft	SRV	200								
ldap2k332-edir.demo.msft	SRV	200								
ldap2k332-oid10.demo.msft	SRV	200								
ldap2k332-tiv.demo.msft	SRV	200								
LSCERPM-2012.demo.msft	SRV	201								
LSCERPM-2K8R2.demo.msft	SRV	200								
LSCRPM-2012.demo.msft	SRV	201								
LSCRPM-2K8R2.demo.msft	SRV	200								
LSCTOOLS-2012.demo.msft	SRV	201								
LSCTOOLS-2K8R2.demo.msft	SRV	200								

Zone Processing Services

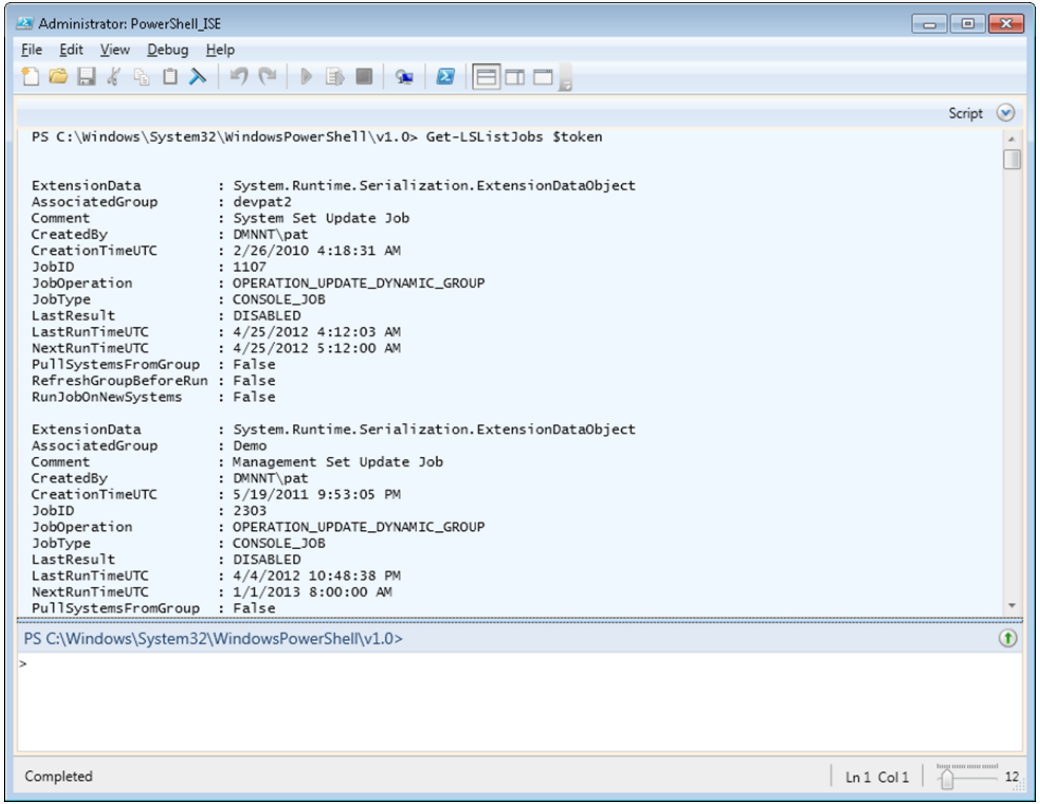
Existing Zone Processing Services:

Current Database Version: 131004

System	Instance ID	Management Set	Job Affinity	Status	Last Update	Version	Last Message
A2012-PT	PREM Windows Servers	PREM Windows Servers	Refresh Jobs, Password Te...	Running	11/16/2013 10:20:35...	131004	Polling for Work
AP-ERPM-01	[Default Deferred Processor]	[All Management Sets]	Password Change Jobs, Ma...	Running	11/16/2013 10:21:23...	131004	Polling for Work

Zone Processing inside prem.

PowerShell Functionality (cont)



```
PS C:\Windows\System32\WindowsPowerShell\v1.0> Get-LSListJobs $token


ExtensionData         : System.Runtime.Serialization.ExtensionDataObject
AssociatedGroup       : devpat2
Comment               : System Set Update Job
CreatedBy             : DMNNT\pat
CreationTimeUTC       : 2/26/2010 4:18:31 AM
JobID                 : 1107
JobOperation          : OPERATION_UPDATE_DYNAMIC_GROUP
JobType               : CONSOLE_JOB
LastResult            : DISABLED
LastRunTimeUTC        : 4/25/2012 4:12:03 AM
NextRunTimeUTC        : 4/25/2012 5:12:00 AM
PullSystemsFromGroup  : False
RefreshGroupBeforeRun : False
RunJobOnNewSystems    : False

ExtensionData         : System.Runtime.Serialization.ExtensionDataObject
AssociatedGroup       : Demo
Comment               : Management Set Update Job
CreatedBy             : DMNNT\pat
CreationTimeUTC       : 5/19/2011 9:53:05 PM
JobID                 : 2303
JobOperation          : OPERATION_UPDATE_DYNAMIC_GROUP
JobType               : CONSOLE_JOB
LastResult            : DISABLED
LastRunTimeUTC        : 4/4/2012 10:48:38 PM
NextRunTimeUTC        : 1/1/2013 8:00:00 AM
PullSystemsFromGroup  : False
```

```
PS C:\Windows\System32\WindowsPowerShell\v1.0>
>
```

Who Needs SAAS PIM?

- **Cloud and large enterprises** already have and generate large quantities of mismanaged:
  - Certificates
  - User Identities/passwords
  - Privileged Identities/passwords
  - Application Identities/passwords

- All have lifecycles of creation, required regular changes, periodic disclosure and disposal

- Human management of sensitive assets on an ongoing basis is impractical

Who Needs SAAS PIM? (cont.)

- **Cloud providers, critical national infrastructure companies**, and others must show proper management of privileged accounts
- Most **fail regulatory compliance audits** with PIM finding
- **Government contracts withheld** due to poor security audit findings
- **Nation state attacks** knock down those with weak PIM security regularly

Who Needs SAAS PIM? (cont.)

- Because of **scale, complexity, cost, history, culture** - PIM problem is not fixed, only hidden from auditors, but not criminals and nation states

- REALLY large environments **can't find off-the-shelf solutions** that work at scale

Who Needs SAAS PIM? (cont.)

Due to scale of secrets management in large enterprises, point is reached where only way to keep up is to create:

Comprehensive programmatic interface for lifecycle management of privileged identities, files (i.e. certificates) and secrets

Think of it as an open platform for orchestration of privileged assets and their usage

What is Orchestrated?

- **Cross-Platform Machine Lists** for Discovery
- **Privileged Account List** Management
- **Discovery and Change** Job Management
- **Secure File** Upload/Download/Update/Delete
- **ACL Delegation Management** of Authorization Scope
- **Identity Management** of Recognized Accounts/Groups for Delegation
- **Audit Log**

How is Orchestration Applied? Example

- **PowerShell script** to add new machines to domain using temporary domain admin account

```
$password =
   Get-LSPasswordWithReason $token devpat3 DomainName TestUser
  “Adding machine to domain”

$DomainCredential =
   New-Object System.Management.Automation.PSCredential TestUser
   $password

Add-Computer –DomainName DomainName  –Credential  $DomainCredential

Set-LSPasswordCheckIn $token devpat3 DomainName TestUser
   “Added machine to domain”
```

How is Orchestration Applied? Example

- **PowerShell script** to rotate all local passwords in a given environment without service impact

```
$LocalAccounts = Get-LSListWindowsAccountsForSystem $token devpat3
# create a new empty array to store our local admin accounts
$LocalAdmins = @()
foreach ($account in $LocalAccounts)
{
# this will add only the accounts that have admin permissions to the list for job creation
   if ($account.Privilege -eq 2)
   {
      $LocalAdmins = $LocalAdmins + $account;
   }
}
Foreach ($LocalAdmin in $LocalAdmins)
{
# this creates a new job for each local admin account on the system, will not create the account if it is not
    found, sets the password to a random 14 character string, and schedules the job to run immediately.
New-LSJobWindowsChangePassword $token devpat3 $LocalAmdin.AccountName $false 14 -RunNow
}
```

How is Orchestration Applied?

- **Request time limited credentials** for specific machine and identity on machine via API

- **Escalate a known user** to be member of Administrators group on specific machine for limited time via API

How is Orchestration Applied? (cont.)

- Using API, **upload and secure certificate** and matching certificate password
- **Retrieve certificate in a secure and auditable manner** programmatically or via web interface

How is Orchestration Applied? (cont.)

- Previous scenarios **can be carried out in PowerShell, C# or platform independent languages** such as Java (i.e. Apache AXIS) from any platform

- **Calls can be made from any System Center product** using PowerShell and may be used within System Center Orchestrator

Why Is This So Important?

- Large scale 7/24 security management of privileged identities and certificates must be baked into organization’s systems so that **management is entirely automated**
- To achieve coverage, PIM must move from separate application to a **platform for programmers and users**
- At this point **PIM becomes a core service of the enterprise**

About Lieberman Software

- Founded in 1978, first ISV solutions in 1994
- Pioneers of Privileged Identity Management
- Line of Windows security management tools
- 1200+ enterprise customers in all verticals
- US-based, management-owned and profitable
- Headquarters in Los Angeles, office in Austin, TX and channel partners worldwide

Partnership

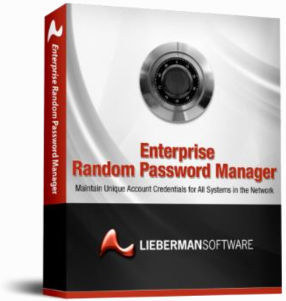
Microsoft and Lieberman Software

- **Managed Microsoft Gold Certified Partner** in ISV category
- Broadest **privileged account discovery and management** capabilities on all **Windows platforms**
- More **Windows Server 2008, Server 2008 R2, Vista, Hyper-V and Windows 7 product certifications** than any other management vendor
- Centralized management for **SharePoint** and its privileged accounts
- Uses **Microsoft SQL** as back-end data store and manages its accounts
- Discovery, propagation and management of **ASP.NET** credentials
- Deep integrations with **SCOM**, **SCSM**, **SCCM**

Next Steps

- Evaluate ERPM as a **Hyper-V or VMware image**
- Access our **online demo environment**
- Request a free privileged account **Risk Assessment**

emeasales@liebsoft.com


Enterprise Random Password Manager
Enterprise
Random Password Manager
Maintain Unique Account Credentials for All Systems in the Network
LIEBERMANSOFTWARE