OpsMgr Deep Dive into Security and Performance

Christian Heitkamp,
NiCE IT Management Solutions

Christian.Heitkamp@nice.de
@Chris_Heitkamp
Agenda

- Linux/UNIX Security Insights and hints
- Windows Security
- Performance / UNIX
- Performance / Windows
- Special: SCOM 1801 Demo
UNIX/Linux Security for OpsMgr
Demo
Privileged Account Password Retrieval

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
WinRM & OMI Agent Security

- RunAs Profiles
  - UNIX/Linux Accounts
  - Database

- WinRM / WSMan API

Username and password in clear text passed to ProbeAction in task workflow

MMA

Port 1270

omiserver

omiagent

Provider

omiagent

Provider
Risk Mitigation

- By design, the password is passed in clear text
- Review permissions of unix/linux accounts with care
Privileged Account Permissions

To configure sudo elevation for the low-privileged user

1. Log on to the UNIX or Linux computer as root.

2. Use the visudo program to edit the sudo configuration in a vi text editor. Run the following command:
   
   visudo

3. Find the following line:

   root ALL=(ALL) ALL

4. Insert the following line after it:

   opsuser ALL=(ALL) NOPASSWD: ALL

5. TTY allocation is not supported. Ensure the following line is commented out:

   # Defaults requiretty

Demo
Life is not fair, but the root password helps

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
Privileged Account Permissions

To configure sudo elevation for the low-privileged user

1. Log on to the UNIX or Linux computer as root.

2. Use the visudo program to edit the sudo configuration in a vi text editor. Run the following command:
   
   `visudo`

3. Find the following line:
   
   `root ALL=(ALL) ALL`

4. Insert the following line after it:
   
   `opsuser ALL=(ALL) NOPASSWD: ALL`

5. TTY allocation is not supported. Ensure the following line is commented out:
   
   `# Defaults requiretty`


Do not follow this Technet Article! Security risk!!
Sudoers File recommendations

- **Best:** No sudoers entries at all
- **Minimal:**
  - `opsuser ALL=(root) NOPASSWD: /opt/microsoft/scx/bin/tools/scxadmin`
    - Agent stop, start, restart
  - `opsuser ALL=(root) NOPASSWD: /opt/microsoft/scx/bin/scxlogfilereader`
    - Log file monitoring
- **OK for 2016:**
  
OMI Agent & Provider Security

omiserver [root]

omiantagent [HOSTING]

Port 1270

MMA

.cert file

"pam" file

.reg file

.reg file
Demo
OMI Provider permissions

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
Agent Security

- Do not change standard file and directory permissions
- Do not allow Agent installation by the “Discovery Wizard”
- Scripts run by the Agent or agent processes must not be changeable by SCOM User Accounts
Windows Security for OpsMgr
Demo
Create Domain Admin without Domain Account

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
Default Action Account

- Don’t use Local System on Domain Controllers or other Application Servers with similar Security concepts
  - File Servers
  - DHCP / DNS
  - etc.
Default Action Account

- Don’t use a Domain Account as local admin on all Servers
  - One account takes them all
  - Be aware: LSA Cache, Pass the Hash
Default Action Account

- Use low-privileged account whenever it makes sense
- Domain controller: See AD MP Documentation
Low-privileged Account – minimum privileges

- Member of the local Users group
- Member of the local Performance Monitor Users group
- Allow log-on-locally permission (SetInteractiveLogonRight)
What about deployments/upgrades in low privilege scenarios

- Working solution
  - External deployment tools like SCCM for SCOM Agent deployment and upgrades
Security Monitoring MP

- This MP is FREE
- Has tons of features (see slides from Camaron)
Links to more Resources

- http://tinyurl.com/scomsecurity
- http://tinyurl.com/scomagentlowprivilige
Performance for OpsMgr
UNIX/Linux Performance

- All workflows run at the Mgmt Servers
- Mgmt Group Sizing is key
- Cookdown essential, especially for Script Probes and Log Files
Workflow analysis

- WinRM Logging
- WinRM/WSMan Tracing (EnableOpsMgrModuleLogging)
  - Manual execution of winrm
Demo
UNIX/Linux for OpsMgr / Workflow Analysis

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
SCOM performance - basics

- Choose applicable Management Packs to install
  - Don’t install the whole MP catalog
- Configure the installed Management Packs
  - RTFM
- Check for failing or misconfigured Discoveries
  - Configchurn
- Check for failing or misconfigured Monitors / Alert-Rules
  - Statechanges, Alerts
- Choose Performance Data (Rules) wisely
  - Enabling/Disabling via Overrides
- Check Database Retention Settings
  - Database Grooming
Demo
How to check for basic performance considerations

DISCLAIMER: Shown demos and examples are for training and demo purpose only!
How to check Config churn

```sql
-- statistics for discoveries (Config churn)
select
  cast(ecl.lastmodified as date) as [LastModifiedDate],
  datepart(hour, ecl.lastmodified),
  d.DiscoveryName,
  lt.LTValue as [DisplayName],
  min(ecl.lastmodified) as [MINLastModifiedDate],
  max(ecl.lastmodified) as [MAXLastModifiedDate],
  count(distinct etl.EntityTransactionLogId) as [TranCount],
  count(*) as [ChangesCount]
from EntityTransactionLog etl
inner join EntityChangeLog ecl on etl.EntityTransactionLogId = ecl.EntityTransactionLogId
inner join discoverysource ds on etl.DiscoverySourceId = ds.DiscoverySourceId
inner join discovery d on ds.DiscoveryRuleId = d.DiscoveryId
inner join LocalizedText lt on d.DiscoveryId = lt.LTStringId
where lt.LanguageCode = 'ENU' and lt.LTStringType = 1
group by d.DiscoveryName, lt.LTValue, cast(ecl.lastmodified as date), datepart(hour, ecl.lastmodified)
order by count(*) desc, datepart(hour, ecl.lastmodified) desc
```

SCOM performance - basics
How to check Statechanges

```
-- statistics monitor (top 50) state changes
select
    distinct top 50 count(sce.StateId) as NumStateChanges,
    m.MonitorName,
    lt.LTValue as [DisplayName],
    mt.typename AS TargetClass
from StateChangeEvent sce with (nolock)
join state s with (nolock) on sce.StateId = s.StateId
join monitor m with (nolock) on s.MonitorId = m.MonitorId
join LocalizedText lt with (nolock) on lt.LTStringId = m.MonitorId
join managedtype mt with (nolock) on m.TargetManagedEntityType = mt.ManagedTypeId
where m.IsUnitMonitor = 1 and lt.LanguageCode = 'ENU' and lt.LTStringType = 1
group by m.MonitorName, lt.LTValue, mt.typename
order by NumStateChanges desc
```
SCOM performance - basics

- How to check Alerts

-- Top 20 Alerts in an Operational Database, by Alert Count

```sql
SELECT TOP 20 SUM(1) AS AlertCount, AlertStringName, AlertStringDescription, MonitoringRuleId, Name
FROM Alertview WITH (NOLOCK)
WHERE TimeRaised is not NULL
GROUP BY AlertStringName, AlertStringDescription, MonitoringRuleId, Name
ORDER BY AlertCount DESC
```

-- Top 20 Alerts in an Operational Database, by Repeat Count

```sql
SELECT TOP 20 SUM(RepeatCount+1) AS RepeatCount, AlertStringName, AlertStringDescription, MonitoringRuleId, Name
FROM Alertview WITH (NOLOCK)
WHERE TimeRaised is not NULL
GROUP BY AlertStringName, AlertStringDescription, MonitoringRuleId, Name
ORDER BY RepeatCount DESC
```
SCOM performance - basics

- How to check Performance Data

```sql
-- Performance insertions per day
SELECT CASE WHEN (GROUPING(CONVERT(VARCHAR(20), TimeSampled, 102)) = 1) THEN 'All Days' ELSE CONVERT(VARCHAR(20), TimeSampled, 102) END AS DaySampled,
       COUNT(*) AS PerfInsertPerDay
FROM PerformanceDataAllView WITH (NOLOCK)
GROUP BY CONVERT(VARCHAR(20), TimeSampled, 102) WITH ROLLUP
ORDER BY DaySampled DESC

-- Top 30 performance insertions by perf object and counter name
SELECT TOP 30
    rv.DisplayName,
    rv.Name,
    rv.Description,
    pcv.ObjectName,
    pcv.CounterName,
    count (pcv.CounterName) AS Total
FROM PerformanceDataAllView AS pdv WITH (nolock) INNER JOIN
    PerformanceCounterView AS pcv WITH (nolock) ON pdv.PerformanceSourceInternalId = pcv.PerformanceSourceInternalId
    INNER JOIN RuleView AS rv WITH (nolock) ON rv.Id = pcv.RuleId
GROUP BY rv.DisplayName, rv.Name, rv.Description, pcv.ObjectName, pcv.CounterName
ORDER BY count (pcv.CounterName) DESC
```
Links to more Resources

- http://tinyurl.com/scomqueries
- http://tinyurl.com/scomtuningmonitors
- http://tinyurl.com/scomhtmlreport
Summary / Wrap Up
UNIX/Linux security check

What is the name of utility to configure elevation on UNIX/Linux?

• sudo

How many UNIX/Linux users should be setup at least?

• One (1)

Should the have sudo elevation assigned?

• No, or only minimal!

Which user should own the Agent binary and configuration files?

• Root only!

What is the good practice to install Linux/UNIX Agents?

• Manually. Discovery Wizard should not be used for deployment
## Related Sessions - Monitoring

<table>
<thead>
<tr>
<th>Time</th>
<th>Speaker</th>
<th>Room</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/8: 10:30</td>
<td>Wren</td>
<td>Waterway 6</td>
<td>Advanced Analytics in Azure</td>
</tr>
<tr>
<td>2/8: 11:45</td>
<td>Fuller</td>
<td>Alden Bridge</td>
<td>Operations Manager (SCOM): Today &amp; Tomorrow</td>
</tr>
<tr>
<td>2/8: 2:15</td>
<td>Fuller</td>
<td>College Park</td>
<td>SCOM – Better together with OMS</td>
</tr>
<tr>
<td>2/9: 9:00</td>
<td>Zehner</td>
<td>Waterway 6</td>
<td>Tesla Management 360</td>
</tr>
<tr>
<td>2/9: 10:30</td>
<td>Heitkamp</td>
<td>Creekside Park</td>
<td>OpsMgr Deep Dive into Security and Performance</td>
</tr>
<tr>
<td>2/9: 10:30</td>
<td>Cornelissen</td>
<td>Alden Bridge</td>
<td>Data visualization techniques with SCOM &amp; OMS</td>
</tr>
<tr>
<td>2/9: 2:00</td>
<td>Zehner</td>
<td>Creekside Park</td>
<td>The OMS Solutions Bakery - how to build a custom solution in 60 minutes</td>
</tr>
<tr>
<td>2/9: 3:30</td>
<td>Wren</td>
<td>Waterway 6</td>
<td>Management in Azure: The Big Picture</td>
</tr>
</tbody>
</table>
Take the Survey!

Your feedback is important! Please rate the session for a chance to win! Survey is below session description at http://elus18.expertslive.us