FEDERAL RESERVE BANK of ATLANTA

IDENTIFYING MISCONFIGURATIONS USING BIGFIX RELEVANCE

IBM InterConnect 2017 Conference

Session: SEM-1182

Presented by:
Ed Redmond
Federal Reserve Bank of Atlanta

DISCLAIMER

FEDERAL RESERVE BANK of ATLANTA

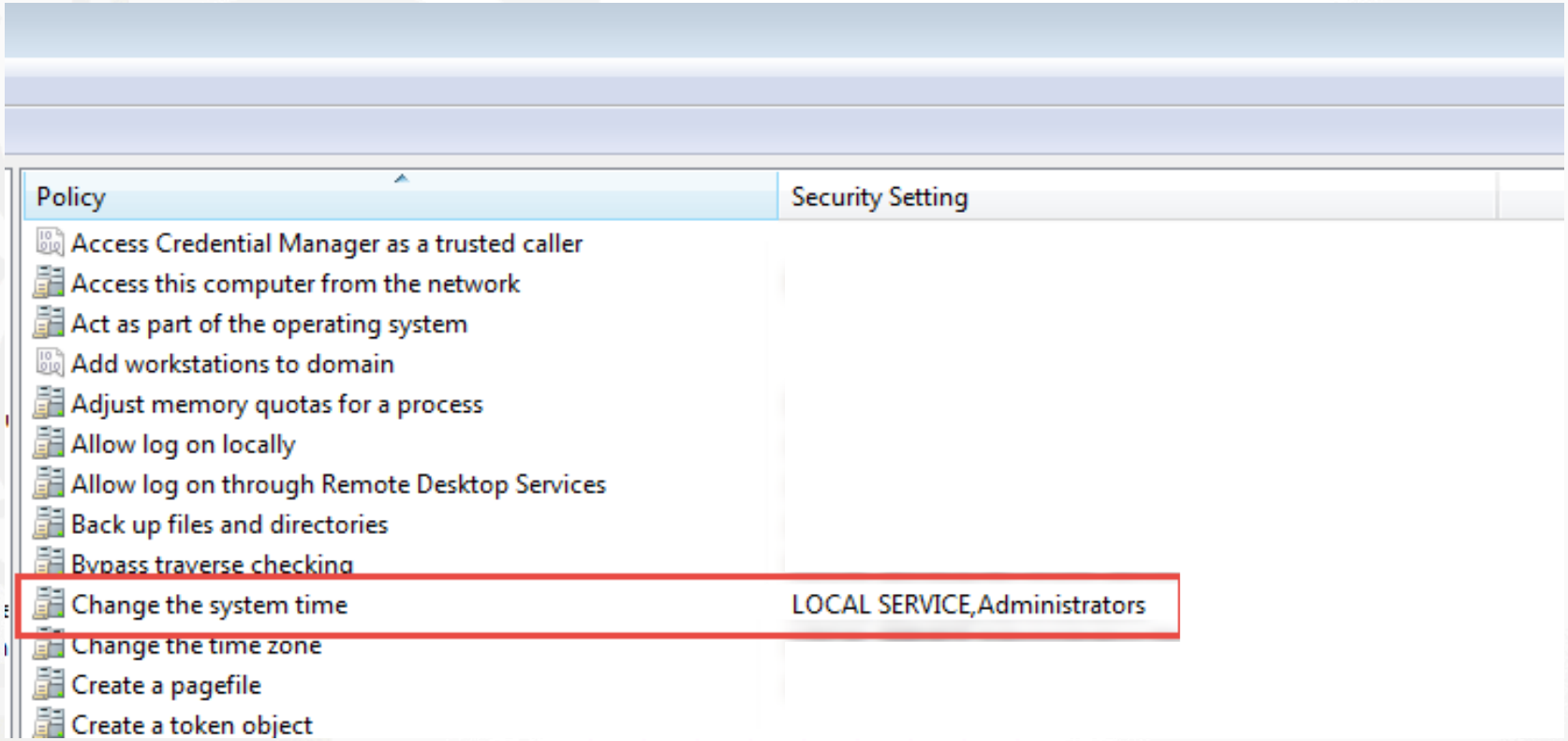
The views presented here are my own personal views and not the views of the Federal Reserve Bank of Atlanta nor the Federal Reserve System.

WHAT IS THE NEED FOR THIS?

So many settings ...

FEDERAL RESERVE BANK of ATLANTA

System Admins need to ensure that the servers they are responsible for are configured properly

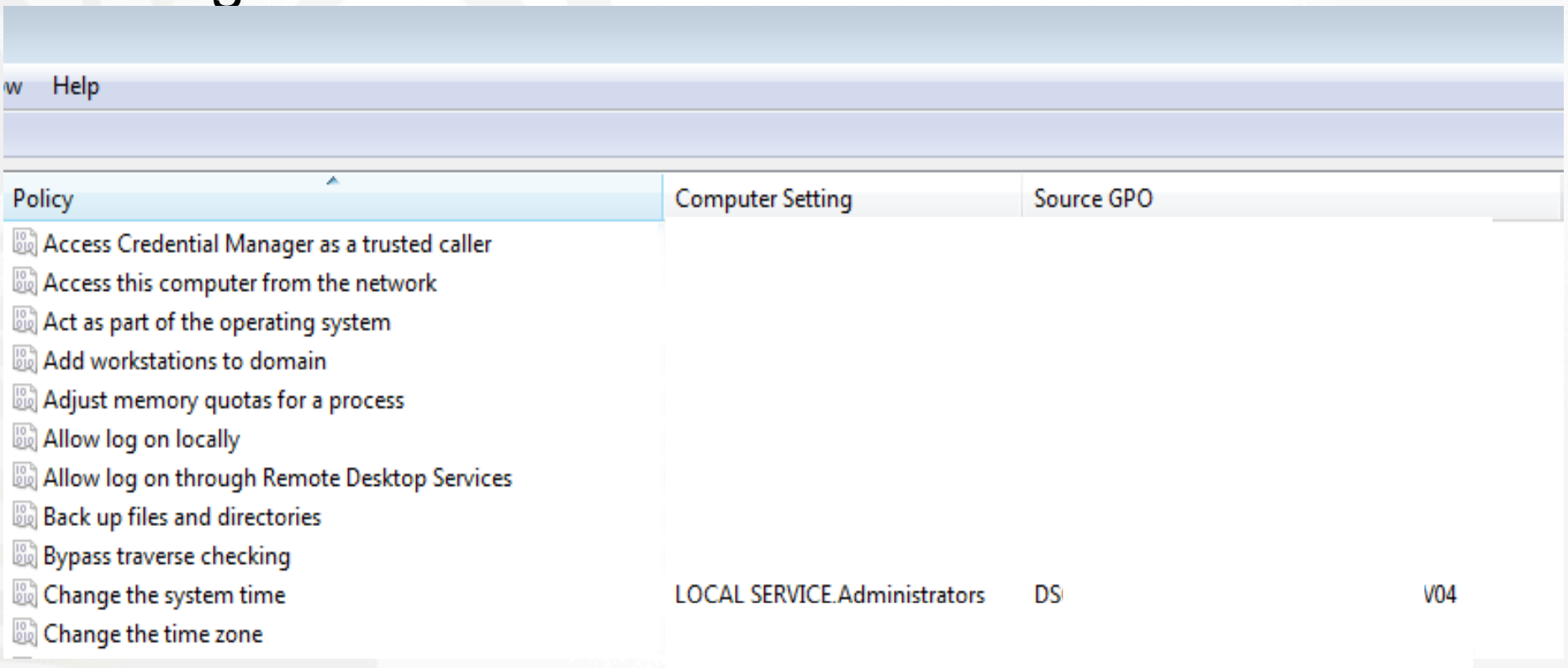


WHERE IS THIS SETTING COMING FROM?

Using RSOP

FEDERAL RESERVE BANK of ATLANTA

If a setting is misconfigured, SysAdmins will use RSOP to determine what GPO is configuring that setting



LOOK AT ALL THOSE SERVERS…

So many servers…. So little time…

FEDERAL RESERVE BANK of ATLANTA

IS THERE SOME WAY TO AUTOMATE THIS

Using WMI queries with PowerShell

FEDERAL RESERVE BANK of ATLANTA

What I found when Googling “wmi user right assignment”

WMI query for User Rights Assignment local computer policy

Scripting > The Official Scripting Guys Forum!

Question

What I am trying to do is pull the account values under User Privilege Rights that if explored using gpedit.msc within Windows Server 2012 R2 under:

This is the query I am using as well. I am using the namespace: root\rsop\computer

```
select AccountList from RSOP_UserPrivilegeRight WHERE UserRight='seManageVolumePrivilege' and precedence=1
```

IS THERE A BETTER WAY TO AUTOMATE THIS

Using WMI queries with BigFix Relevance

FEDERAL RESERVE BANK of ATLANTA

What I found when Googling “BigFix WMI query”

Returns the Inspector properties of the specified wmi object.

Summary: This is a <Plain> Property Inspector that takes a <wmi object> type and returns a <wmi select> type.

Type:

<wmi object>

The <wmi object> Inspectors allow you to analyze the properties of WMI objects.

Click for other Inspectors using <wmi object>.

Return type:

<wmi select>

The <wmi select> object represents a value returned as a result of a WMI select query. You can find more information at the MSDN Library (http://msdn.microsoft.com/library/) under WMI Classes. WMI Inspectors can provide you with useful information about your Client computers. For instance, to get the asset tag from a dell, use:

- string value of select "SerialNumber from Win32_systemenclosure" of wmi.

Caution: Because these Inspectors are written on top of the IWbemLocator::ConnectServer APIs you may experience certain problems unique to this interface. On a small number of systems, these APIs may actually hang the client. BES version 7.2 corrects this behavior. If you have an earlier version of BES, you can set _BESClient_Inspector_DisableWMI to 1 to disable these Inspectors. A Fixlet or Task that uses a disabled inspector will report false; retrieved properties that request a disabled inspector value will report an error. For the latest information on issues surrounding the WMI Inspectors, search the BigFix support knowledge base.

Note also:

Here are a few other examples of using the wmi Inspectors. Each of the examples below hands back dozens of wmi objects:

Q: selects "* from Win32_ComputerSystem" of wmi
Q: selects "* from win32_keyboard" of wmi
Q: selects "* from win32_CDROMDrive" of wmi
Q: selects "* from win32_DiskDrive" of wmi
Q: selects "* from win32_BIOS" of wmi
Q: selects "* from win32_CacheMemory" of wmi
Q: selects "* from win32_DMIChannel" of wmi

LET'S TRY THIS OUT

Using WMI queries with BigFix Relevance

FEDERAL RESERVE BANK of ATLANTA

Group Policy Setting	Constant Name
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege
Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight
Allow log on through Remote Desktop Services	SeRemoteInteractiveLogonRight
Back up files and directories	SeBackupPrivilege
Bypass traverse checking	SeChangeNotifyPrivilege
Change the system time	SeSystemtimePrivilege
Change the time zone	SeTimeZonePrivilege

```
q: select object  "AccountList from RSOP_UserPrivilegeRight where
UserRight = 'SeSystemtimePrivilege' AND precedence = 1" of rsop
computer wmi as string
A: %0ainstance of RSOP_UserPrivilegeRight%0a{%0a%09AccountList =
{"LOCAL SERVICE", "Administrators"};%0a};%0a
T: 3.389 ms
I: singular string
```

I THINK WE ARE ON TO SOMETHING

Cleaning up the output of WMI query

FEDERAL RESERVE BANK of ATLANTA

Use string inspectors to clean up the output

```
q: preceding text of first "}" of (select object  "AccountList from
RSOP_UserPrivilegeRight where UserRight = 'SeSystemtimePrivilege'
AND precedence = 1" of rsop computer wmi as string)
A: %0ainstance of RSOP_UserPrivilegeRight%0a{%0a%09AccountList =
{"LOCAL SERVICE", "Administrators"
T: 3.512 ms
I: singular substring
```

I THINK WE ARE ON TO SOMETHING

Cleaning up the output of WMI query

FEDERAL RESERVE BANK of ATLANTA

Still using string inspectors to clean up the output

```
q: following text of last "{" of preceding text of first "}" of
(select object  "AccountList from RSOP_UserPrivilegeRight where
UserRight = 'SeSystemtimePrivilege' AND precedence = 1" of rsop
computer wmi as string)
A: "LOCAL SERVICE", "Administrators"
T: 3.517 ms
I: singular substring

q:  substrings separated by ", " of following text of last "{" of
preceding text of first "}" of (select object  "AccountList from
RSOP_UserPrivilegeRight where UserRight = 'SeSystemtimePrivilege'
AND precedence = 1" of rsop computer wmi as string)
A: "LOCAL SERVICE"
A: "Administrators"
T: 3.403 ms
I: plural substring
```

WORK SMARTER NOT HARDER

BigFix can determine if configured properly

FEDERAL RESERVE BANK of ATLANTA

BigFix can do analysis for us…

Assume only “LOCAL SERVICE” should be assigned the Change System Time right.

```
q: (if (exists substrings separated by ", " whose (it as lowercase !=
"%22local service%22") of it) then (substrings separated by ", "
whose (it as lowercase != "%22local service%22") of it) else ("You're
good"))of  following text of last "{" of preceding text of first "}"
of (select object  "AccountList from RSOP_UserPrivilegeRight where
UserRight = 'SeSystemtimePrivilege' AND precedence = 1" of rsop
computer wmi as string)
A: "Administrators"
T: 3.893 ms
I: plural string
```

IT LEFT ME WANTING MORE…

Can we report more than just the setting?

FEDERAL RESERVE BANK of ATLANTA

Investigated to see what is actually returned by WMI

```
q: select object "* FROM RSOP_UserPrivilegeRight where UserRight =
'SeSystemtimePrivilege' AND precedence = 1" of rsop computer wmi as string
A: %0ainstance of RSOP_UserPrivilegeRight%0a{%0a%09AccountList = {"LOCAL SERVICE",
"Administrators"};%0a%09ErrorCode = 0;%0a%09GPOID = "cn={0E
A1A1},cn=,cn=,DC=,DC=,DC=,DC=";%0a%09id =
"{5C3131}";%0a%09precedence = 1;%0a%09SOMID = "4";%0
09Status = 1;%0a%09UserRight = "SeSystemtimePrivilege";%0a};%0a
T: 4.082 ms
I: singular string
```

Notice the GPOID returned by the WMI query?

Can I actually find out the name of the GPO?

YOU GOTTA DIG A LITTLE DEEPER

RSOP_GPO Class

FEDERAL RESERVE BANK of ATLANTA

Found this when Googling “RSOP_GPO”

RSOP_GPO class

Represents a Group Policy Object (GPO). Instances of this class are divided into three categories: instances that represent applied GPOs, instances that represent GPOs that have read-access but not **applyGroupPolicy** access, and instances that represent disabled GPOs.

The following syntax is simplified from Managed Object Format (MOF) code and includes all of the inherited properties.

Syntax

```
[AMENDMENT]
class RSOP_GPO
{
  string  id;
  string  name = "";
  string  guidName = "";
  uint32  version = 0;
  boolean enabled = TRUE;
  uint8   securityDescriptor[];
  string  fileSystemPath = "";
  boolean accessDenied = FALSE;
  string  filterId = "";
```

YOU GOTTA DIG A LITTLE DEEPER

Querying RSOP_GPO Class using BigFix

FEDERAL RESERVE BANK of ATLANTA

Performing a general query for RSOP_GPO class

```
q: select objects "* FROM RSOP GPO" of rsop computer wmi as string
A:
                                        guidName = "Local Group Policy"

A:

        guidName = "{57E0C80D-92BB-45B2-8FE4-DF1293E83471}"
```

Assumed that the guidName was the same thing as the GPOID in previous WMI query

YOU GOTTA DIG A LITTLE DEEPER

Querying RSOP_GPO Class using BigFix

FEDERAL RESERVE BANK of ATLANTA

Performed a query of RSOP_GPO using the GPOID we found earlier…

```
q: select objects "* FROM RSOP_GPO Where guidName='{0E
                  A1A1}'" of rsop computer wmi as string
A: %0ainstance of RSOP GPO



   guidName = "{0E                                  A1A1}


   %09name = "D                                      04"
```

It looks like the “name” property is the same as the name of the GPO displayed in the RSOP results.

YOU GOTTA DIG A LITTLE DEEPER

Cleaning up output

FEDERAL RESERVE BANK of ATLANTA

We can clean up the output like we did earlier

```
q:  select objects "name FROM RSOP_GPO Where guidName='{0E
                                A1A1}'" of rsop computer wmi as string
A: %0ainstance of RSOP_GPO%0a{%0a%09name = "DS
                          V04";%0a};%0a
T: 3.745 ms
I: plural string
```

YOU GOTTA DIG A LITTLE DEEPER

Cleaning up output

FEDERAL RESERVE BANK of ATLANTA

Still cleaning up the output…

```
q: preceding text of first "%22" of following text of first "name =
%22" of (select objects "name FROM RSOP GPO Where
guidName='{0E                                    A1A1}'" of rsop computer
wmi as string)
A: DS                                           V04
T: 5.824 ms
I: singular substring
```

YOU GOTTA DIG A LITTLE DEEPER

Making the query more dynamic

FEDERAL RESERVE BANK of ATLANTA

Since we do not know the guid of the GPO that is configuring a particular setting we need to make our query more dynamic

```
q: preceding text of first "%22" of following text of first "name = %
22" of ((select objects ("name from RSOP_GPO where guidName = '" &
preceding text of first "," of following text of first "cn=" of
(select objects "GPOID FROM RSOP_UserPrivilegeRight where UserRight =
'SeSystemtimePrivilege' AND precedence = 1" of rsop computer wmi as
string as lowercase)& "'") of rsop computer wmi) as string)
A: DS                                    V04
T: 7.316 ms
I: singular substring
```

WONDER TWIN POWERS ACTIVATE!!!

Joining both queries

FEDERAL RESERVE BANK of ATLANTA

For more robust information, we can join both of our previous queries..

```
q: following text of last "{" of preceding text of first "}" of
(select object  "AccountList from RSOP_UserPrivilegeRight where
UserRight = 'SeSystemtimePrivilege' AND precedence = 1" of rsop
computer wmi as string) & " Set by GPO: " &  preceding text of first
"%22" of following text of first "name = %22" of ((select objects
("name from RSOP_GPO where guidName = '" & preceding text of first
"," of following text of first "cn=" of (select objects "GPOID FROM
RSOP_UserPrivilegeRight where UserRight = 'SeSystemtimePrivilege' AND
precedence = 1" of rsop computer wmi as string as lowercase)& "'") of
rsop computer wmi) as string)
A: "LOCAL SERVICE", "Administrators" Set by GPO: DS
                                  V04
T: 10.317 ms
I: singular string
```

SO WHAT'S THE BIG DEAL?

Efficiencies Gained

FEDERAL RESERVE BANK of ATLANTA

- Deployed this for 42 settings across ~4500 servers (189,000 settings)
- Reduced misconfigurations from 20,000+ to around 800
- Saves about 30 man hours per week

HELPFUL WEBSITES

FEDERAL RESERVE BANK of ATLANTA

BigFix Forum
https://forum.bigfix.com

BigFix.me
https://bigfix.me

IBM Inspector Documentation
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/Inspector%20Documentation

BigFix Support
https://support.bigfix.com/

BigFix Developer
https://developer.bigfix.com/

QUESTIONS

FEDERAL RESERVE BANK of ATLANTA

CONTACT INFO

FEDERAL RESERVE BANK of ATLANTA

Ed Redmond

Email: ebredmond@gmail.com

BigFix Forum: eredmond