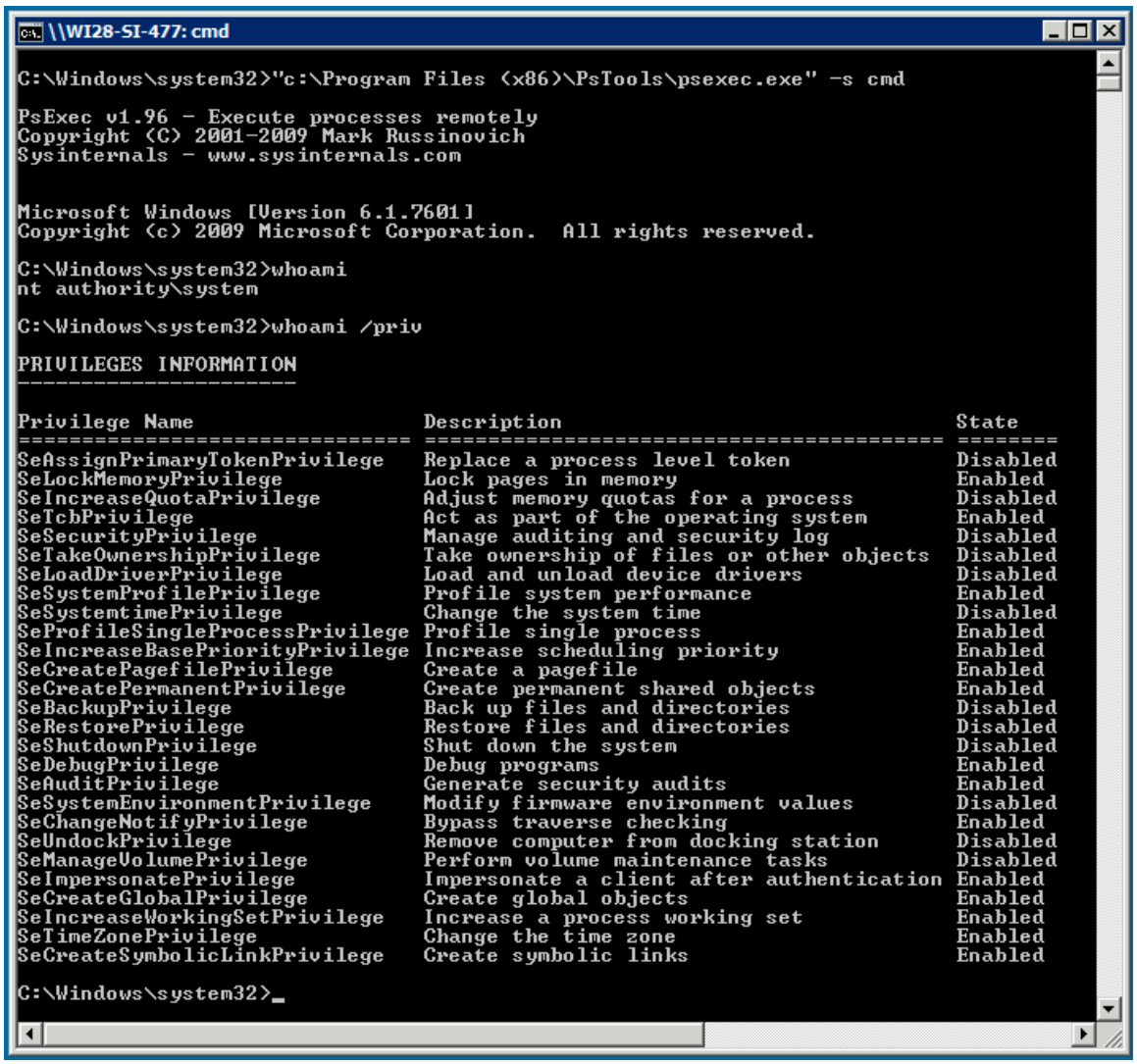
Check Agent Service Account Privileges

This document describes a BMC Database Automation (BDA) Action that will compare the privileges granted to the user a BDA Agent is running as to the privileges that are granted to the `NT AUTHORITY\System` user (the Local System Authority, or LSA).

How it works

The action uses the Windows command `WHOAMI /PRIV` to capture the list of privileges granted to a user.



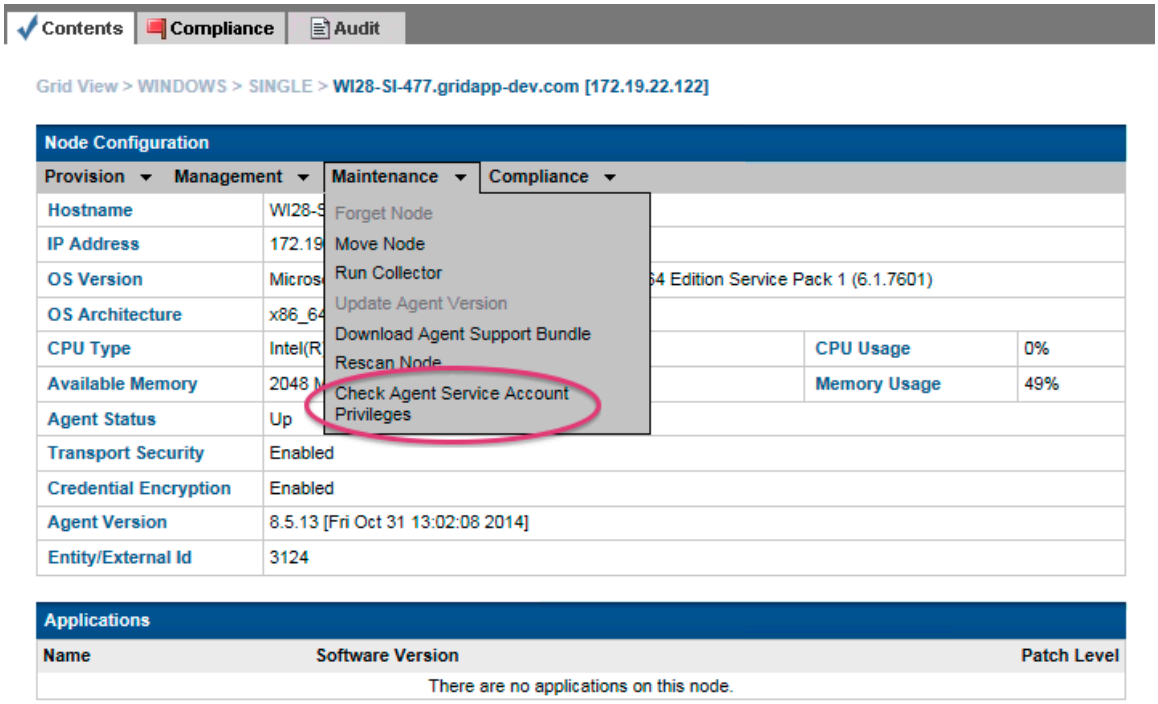
These privileges and their states are then compared to the list of privileges and states returned from a `WHOAMI /PRIV` command run as the `NT AUTHORITY\System` user. For reference, those privileges and states are listed here:

```
Privilege Name                  Description                               State
=============================== ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Disabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeSystemProfilePrivilege        Profile system performance                Enabled
SeSystemtimePrivilege           Change the system time                    Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeDebugPrivilege                Debug programs                            Enabled
SeAuditPrivilege                Generate security audits                  Enabled
SeSystemEnvironmentPrivilege    Modify firmware environment values        Disabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeUndockPrivilege               Remove computer from docking station      Disabled
SeManageVolumePrivilege         Perform volume maintenance tasks          Disabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege   Increase a process working set            Enabled
SeTimeZonePrivilege             Change the time zone                      Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled
```

BMC will only support BDA agents that are running with these privileges in these states.

How to use the action

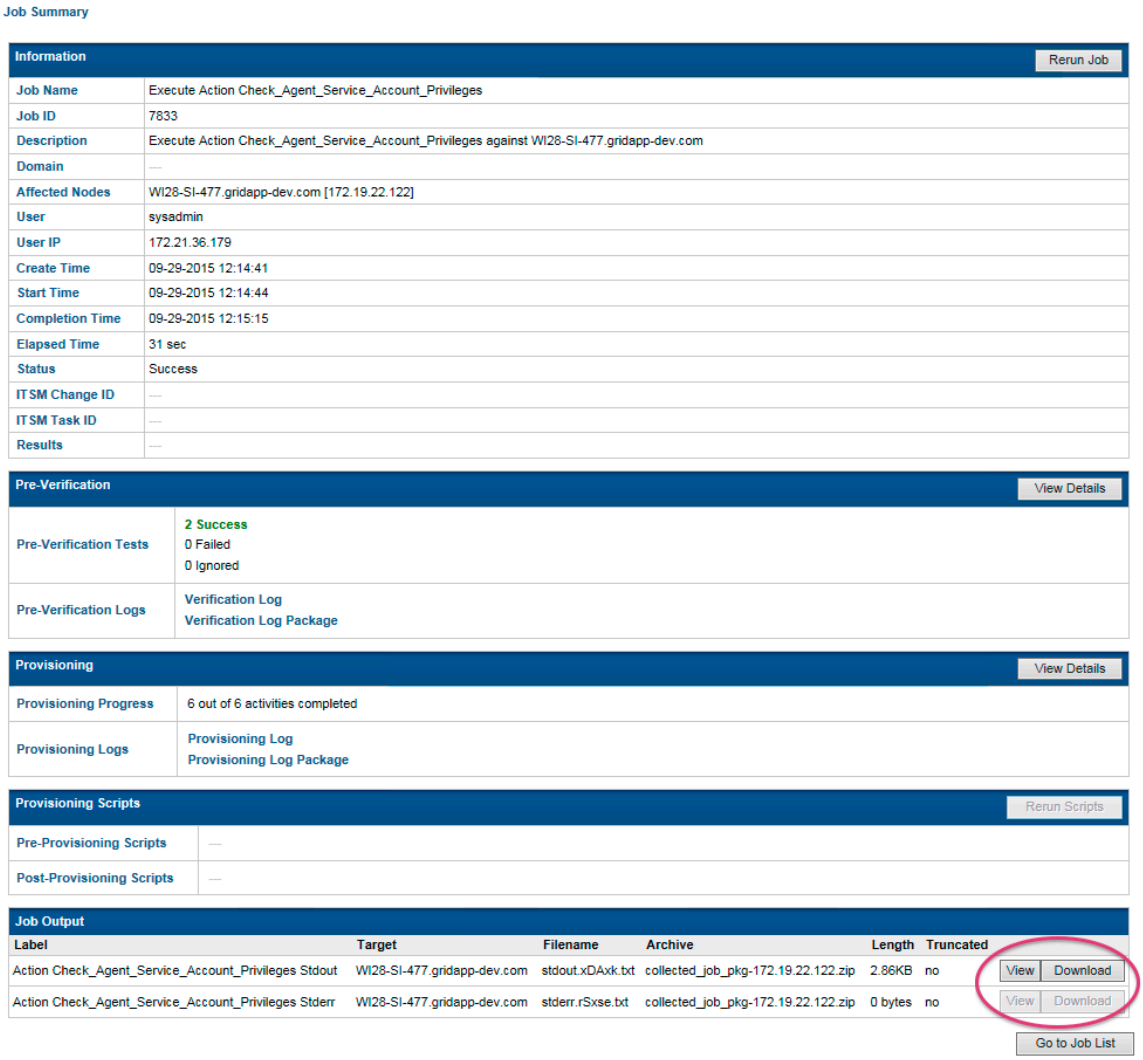
Once the action has been imported into BDA, it can either be run via the Actions Repository, or it may be run via a menu entry in the “Maintenance” menu on the target node’s information page:



If the action runs to completion successfully, the user that the BDA Agent is running as has all the correct privileges and no further action is necessary. If the action fails, the STDOUT from the action will contain a table enumerating what privileges the user has, which privileges it shares with `NT AUTHORITY\System` but are in the incorrect state, and which privileges it is missing but are granted to `NT AUTHORITY\System`. A sample output from a failed run of this action can be found in Appendix B.

Viewing the STDOUT from an action

BDA provides the ability to examine the STDOUT from an Action via the Job Summary page:



Job Summary

Information — Rerun Job

Job Name	Execute Action Check_Agent_Service_Account_Privileges
Job ID	7833
Description	Execute Action Check_Agent_Service_Account_Privileges against WI28-SI-477.gridapp-dev.com
Domain	---
Affected Nodes	WI28-SI-477.gridapp-dev.com [172.19.22.122]
User	sysadmin
User IP	172.21.36.179
Create Time	09-29-2015 12:14:41
Start Time	09-29-2015 12:14:44
Completion Time	09-29-2015 12:15:15
Elapsed Time	31 sec
Status	Success
ITSM Change ID	---
ITSM Task ID	---
Results	---

Pre-Verification — View Details

Pre-Verification Tests	2 Success 0 Failed 0 Ignored
Pre-Verification Logs	Verification Log Verification Log Package

Provisioning — View Details

Provisioning Progress	6 out of 6 activities completed
Provisioning Logs	Provisioning Log Provisioning Log Package

Provisioning Scripts — Rerun Scripts

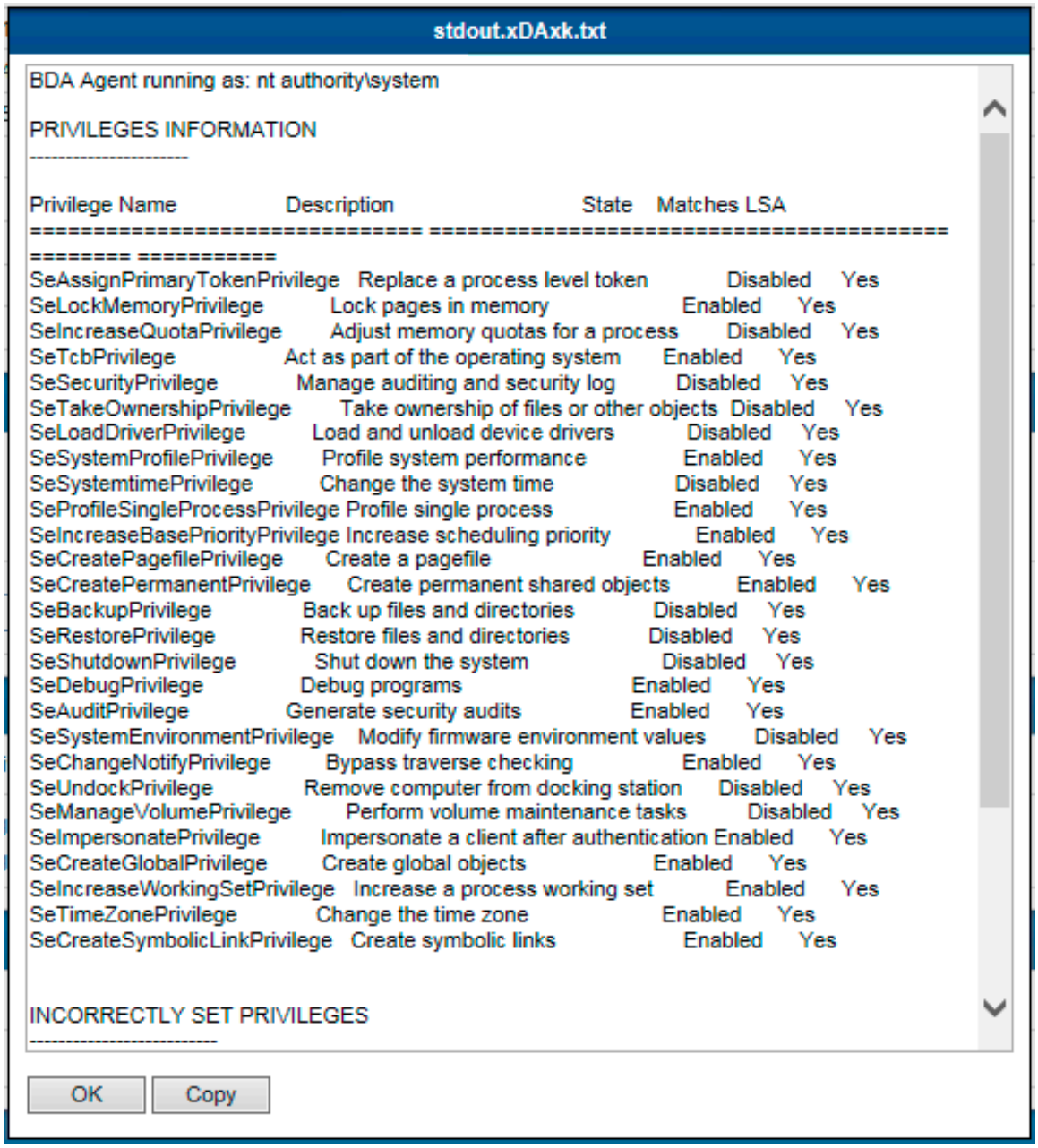
Pre-Provisioning Scripts	---
Post-Provisioning Scripts	---

Job Output

Label	Target	Filename	Archive	Length	Truncated	
Action Check_Agent_Service_Account_Privileges Stdout	WI28-SI-477.gridapp-dev.com	stdout.xDAxk.txt	collected_job_pkg-172.19.22.122.zip	2.86KB	no	View Download
Action Check_Agent_Service_Account_Privileges Stderr	WI28-SI-477.gridapp-dev.com	stderr.rSxse.txt	collected_job_pkg-172.19.22.122.zip	0 bytes	no	View Download

Go to Job List

If you choose to view the output by using the “View” button, the table will be displayed in a variable-width font, so it may be difficult to read:



We recommend downloading the file and viewing it in a text editor.

Appendix A: Output of a successful run of this action

```
BDA Agent running as: nt authority\system

PRIVILEGES INFORMATION
----------------------

Privilege Name                  Description                               State    Matches LSA
=============================== ========================================= ======== ===========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled     Yes
SeLockMemoryPrivilege           Lock pages in memory                      Enabled      Yes
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled     Yes
SeTcbPrivilege                  Act as part of the operating system       Enabled      Yes
SeSecurityPrivilege             Manage auditing and security log          Disabled     Yes
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled     Yes
SeLoadDriverPrivilege           Load and unload device drivers            Disabled     Yes
SeSystemProfilePrivilege        Profile system performance                Enabled      Yes
SeSystemtimePrivilege           Change the system time                    Disabled     Yes
SeProfileSingleProcessPrivilege Profile single process                    Enabled      Yes
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled      Yes
SeCreatePagefilePrivilege       Create a pagefile                         Enabled      Yes
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled      Yes
SeBackupPrivilege               Back up files and directories             Disabled     Yes
SeRestorePrivilege              Restore files and directories             Disabled     Yes
SeShutdownPrivilege             Shut down the system                      Disabled     Yes
SeDebugPrivilege                Debug programs                            Enabled      Yes
SeAuditPrivilege                Generate security audits                  Enabled      Yes
SeSystemEnvironmentPrivilege    Modify firmware environment values        Disabled     Yes
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled      Yes
SeUndockPrivilege               Remove computer from docking station      Disabled     Yes
SeManageVolumePrivilege         Perform volume maintenance tasks          Disabled     Yes
SeImpersonatePrivilege          Impersonate a client after authentication Enabled      Yes
SeCreateGlobalPrivilege         Create global objects                     Enabled      Yes
SeIncreaseWorkingSetPrivilege   Increase a process working set            Enabled      Yes
SeTimeZonePrivilege             Change the time zone                      Enabled      Yes
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled      Yes


INCORRECTLY SET PRIVILEGES
--------------------------

None


MISSING PRIVILEGES
------------------

None
```

Appendix B: Sample output of an unsuccessful run of this action

```
BDA Agent running as: gridapp-dev\sqlserver

PRIVILEGES INFORMATION
----------------------

Privilege Name                  Description                               State    Matches LSA
============================== ========================================= ======== ===========
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled     Yes
SeSecurityPrivilege             Manage auditing and security log          Disabled     Yes
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled     Yes
SeLoadDriverPrivilege           Load and unload device drivers            Disabled     Yes
SeSystemProfilePrivilege        Profile system performance                Disabled     No
SeSystemtimePrivilege           Change the system time                    Disabled     Yes
SeProfileSingleProcessPrivilege Profile single process                    Disabled     No
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Disabled     No
SeCreatePagefilePrivilege       Create a pagefile                         Disabled     No
SeBackupPrivilege               Back up files and directories             Disabled     Yes
SeRestorePrivilege              Restore files and directories             Disabled     Yes
SeShutdownPrivilege             Shut down the system                      Disabled     Yes
SeDebugPrivilege                Debug programs                            Disabled     No
SeSystemEnvironmentPrivilege    Modify firmware environment values        Disabled     Yes
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled      Yes
SeRemoteShutdownPrivilege       Force shutdown from a remote system       Disabled     No
SeUndockPrivilege               Remove computer from docking station      Disabled     Yes
SeManageVolumePrivilege         Perform volume maintenance tasks          Disabled     Yes
SeImpersonatePrivilege          Impersonate a client after authentication Enabled      Yes
SeCreateGlobalPrivilege         Create global objects                     Enabled      Yes
SeIncreaseWorkingSetPrivilege   Increase a process working set            Disabled     No
SeTimeZonePrivilege             Change the time zone                      Disabled     No
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Disabled     No


INCORRECTLY SET PRIVILEGES
--------------------------

Privilege Name                  Description                               State    Matches LSA
============================== ========================================= ======== ===========
SeSystemProfilePrivilege        Profile system performance                Disabled     No
SeProfileSingleProcessPrivilege Profile single process                    Disabled     No
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Disabled     No
SeCreatePagefilePrivilege       Create a pagefile                         Disabled     No
SeDebugPrivilege                Debug programs                            Disabled     No
SeIncreaseWorkingSetPrivilege   Increase a process working set            Disabled     No
SeTimeZonePrivilege             Change the time zone                      Disabled     No
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Disabled     No


MISSING PRIVILEGES
------------------

Privilege Name                  Description                               State    Matches LSA
============================== ========================================= ======== ===========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled     No
SeLockMemoryPrivilege           Lock pages in memory                      Enabled      No
SeTcbPrivilege                  Act as part of the operating system       Enabled      No
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled      No
SeAuditPrivilege                Generate seccurity audits                 Enabled      No
```