TECHNICAL DESCRIPTION

ZERO FOOTPRINT INVENTORY

Product	Snow Inventory
Version	5
Document date	2017-03-28

CONTENTS

1 INTRODUCTION

The Snow Inventory Agent can be installed locally on each computer, or be used as a zero footprint inventory solution with no locally installed agent on the computer. In the zero footprint inventory scenarios each computer is inventoried using the Snow Inventory Agent as a remotely executed command.

Note that for a zero footprint inventory, no application usage data is gathered.

1.1 SUPPORTED OPERATING SYSTEMS

Zero footprint inventory is available for Windows, Linux, Unix, and macOS platforms.

For information on supported operating systems, see Snow System Requirements document, in the Snow Knowledge Base, which is available for customers and partners.

1.2 PRIVILEGES

For information on required privileges of the account that will run the remote inventory scan, refer to the user guide for each Inventory agent.

1.3 DEFINITIONS

Inventory	To capture Platform Configurations and extract software information
Snow Agent	A set of binaries and a running process on an operating system
Agentless Remote Scan	Central Authority (server) that remotely connects to an operating system with permission to execute queries using native technologies*.
Zero Footprint	Remotely executes the agent (starts a new process) on each operating system, and leaves no trace after execution.
	***** *Native Technology - No additional technology is required in any case to perform all required actions.*

2 PREPARATIONS

In this scenario, a script will initiate a remote inventory scan to run according to a predefined list of target computers.

2.1 SCAN OPTIONS

There are two possible ways to perform a zero footprint scan:

- Copy the agent files directly to the target machine (Remote copy mode)
- Use a network share folder for storing agent files and result files (Net share mode)

2.2 GENERATE LIST

The list must at least contain IP addresses or hostnames of the computers to be inventoried. If different user accounts need to be used for the inventory, user credentials for each computer must be provided in the list.

The list can be put together using information from Snow Inventory Admin Console, from a CMDB, or from any other tool that holds an inventory of the target computers, such as a network monitoring tool, a system operations tool, or a service desk tool.

2.3 PREPARE AGENT AND CONFIGURATION FILES

2.3.1 REMOTE COPY MODE

Prepare necessary Snow Inventory Agent files for each computer that will be inventoried using the script for remote scan. If Snow Inventory Oracle Scanner (SIOS) is to be used, the **sios.jar** file needs to be copied.

Make adjustments to the configuration file as needed. The recommendation is to use the Snow Inventory Admin Console for editing of the configuration file. For details, see the *Snow Inventory Admin Console User Guide.*

For detailed information, see the sections for each specific platform.

2.3.1.1 DECIDE HOW TO HANDLE RESULT FILE

There are two options for handling of the inventory result file:

- As a part of the inventory, let the Snow Inventory Agent send the result file directly to the Snow Inventory Server. The server endpoint must be defined in the configuration file of the Snow Inventory agent.
- As a part of the remote inventory script, copy the result files from the inventoried computers to the computer running the remote inventory script. The inventory files then need to be processed by the Snow Inventory Master Server.

2.3.2 NET SHARE MODE

Prepare a shared folder that is accessible from the same network as where the target machines are located, SMB based sharing is recommended. The folder must be configured to allow guest access with no password required and give users full read/write permissions.

Copy agent files and corresponding configuration files to this folder. Mount the folder on the target and execute scan.

2.3.2.1 DECIDE HOW TO HANDLE RESULT FILE

There are two options for handling of the inventory result file:

- As a part of the inventory, let the Snow Inventory Agent send the result file directly to the Snow Inventory Server. The server endpoint must be defined in the configuration file of the Snow Inventory agent.
- The default configuration setting will put the result files in the **data** folder in your current location. We recommend to switch to the mounted folder before executing the scan so the result files will be placed in the mounted folder. After completion, the files need to be processed by the Snow Inventory Master Server.

2.4 CREATE SCRIPT

The script can be written in any scripting language and must be run on a computer with network access to the target computers.

The script consists of two parts – local runner (1) that iterates over hosts and executes remote commands (2) in order to perform the scan.

Remote scan commands (2) support two different scenarios – **Remote copy mode** when agent files are copied to the target, and **Net share mode** when agent files reside on a network share accessible to all targets.

2.4.1 LOCAL RUNNER (1)

This example of the local runner script assumes that either host name or IP address is provided for each of the target machines. If no host name is given, the script tries to resolve it from given IP address. The target information is stored in the **hosts_win.txt** file as comma-separated values which have the following format of host entries:

<Host Name>,<IP address>

EXAMPLE

```
HOST1,10.100.1.15
,10.100.1.12
HOST3,
```

THE LOCAL RUNNER SCRIPT FOR EXECUTING IN WINDOWS

```
$hosts = Get-Content -Path ".\hosts_win.txt"

$Credentials = Get-Credential
foreach ($target in $hosts) {
    $targetList = $target.split(',')
```

```
    if ($targetList[0]) {
    $hostname = $targetList[0]

    }
    elseif ($targetList[1]){
        $hostname = ([system.net.dns]::GetHostByAddress($targetList[1])).hostname
    }

    $remoteSession = New-PSSession -ComputerName $hostname -Credential $Credentials

        # PUT COMMANDS FOR EXECUTING REMOTE SCAN HERE (2)

    Remove-PSSession -Session $remoteSession

}
```

THE LOCAL RUNNER SCRIPT FOR EXECUTING IN LINUX

```
#!/usr/bin/env bash
hostsfile="hosts_linux.txt"
while read -r line
do
    IFS=',' read -r -a hosts <<< "$line"
    if [ ! -z ${hosts[0]} ]; then
        target=${hosts[0]}
    elif [ ! -z ${hosts[1]} ]; then
        target=${hosts[1]}
    fi

    # PUT COMMANDS FOR EXECUTING REMOTE SCAN HERE (2)

done < "$hostsfile"
```

2.4.2 COMMANDS FOR REMOTE COPY MODE (2)

For each of the target computers in the list, the following actions need to be performed:

1. Connect to the target computer using provided user credentials.
2. Copy the Snow Inventory agent and the configuration file to the target computer.
3. Run the Snow Inventory agent.
4. Monitor the running process of the Snow Inventory agent.
5. After the completed inventory (i.e. when the process is no longer running):
    a. If it has not been sent already by the Snow Inventory agent, copy the inventory result file to the computer running the remote inventory script.
    b. Remove the Snow Inventory agent, the configuration file, the inventory result file, and log files from the target computer.
6. Disconnect from the target computer.

2.4.3 COMMANDS FOR NET SHARE MODE (2)

For each of the target computers in the list, the following actions need to be performed:

1. Connect to the target computer using provided user credentials.

2. If required by the operating system (non-Windows operating systems), mount the shared network folder.
3. Create a new folder where the result files will be placed unless non-default drop location is specified in the configuration file.
4. Switch to the newly created folder.
5. Run the Snow Inventory agent.
6. After the completed inventory (i.e. when the process is no longer running), unmount the folder, if required by the operating system (non-Windows operating systems).
7. Disconnect from the target computer.

3 WINDOWS PLATFORM SPECIFICS

NOTE

- To execute commands, Windows Remoting must be enabled.
  In Windows Server 2012 and higher it is enabled by default. For older machines, use the command Enable-PSRemoting as Administrator. This will also open required firewall ports.
- PowerShell version 3 or higher must be installed.
- The user that executes the scan must be a member of the Local administrator group.

3.1 REMOTE COPY MODE

On the computer that will run the script for remote scan:

1. Copy the files **snowagent.exe** and **snowagent.config** to the current folder (copy from an existing agent installation). If Oracle inventory option is to be used, place **sios.jar** in the same folder.
2. Run the following commands one-by-one or put them into .ps1 script:

```
$remoteSession = New-PSSession -ComputerName <TARGET_NAME> -Credential <Domain
\User>

Invoke-Command -Session $remoteSession {mkdir <TEMP_DIR>\snowagent}

Copy-Item -Path snowagent.exe -Destination <TEMP_DIR>\snowagent -ToSession
$remoteSession

Copy-Item -Path snowagent.config -Destination <TEMP_DIR>\snowagent -ToSession
$remoteSession

Invoke-Command -Session $remoteSession {cd <TEMP_DIR>\snowagent
\snowagent; .\snowagent.exe}

Invoke-Command -Session $remoteSession {cd ..;Remove-Item -Recurse -Path
<TEMP_DIR>\snowagent -Force}

Remove-PSSession -Session $remoteSession
```

Where:

Parameter	Description
<TARGET_NAME>	Domain name of the computer to be scanned
<Domain\User>	User that will execute the scan. It needs to have Local Administrator privileges.
<TEMP_DIR>	Temporary folder where a temporary agent folder will be created, for example **C:\temp**.

Parameter	Description
<DRIVE_LETTER>	Drive letter of the disk where <TEMP_DIR> is located, i.e. **C** or **D**.
<TEMP_DIR_WITHOUT_DRIVE>	Temporary folder where a temporary agent folder will be created, with no drive letter present. For example: **temp**
<LOCAL_DROP_LOCATION>	The folder where to drop data to on the local computer.

3. In the case Oracle inventory scan is required, add the following command to the script after copying snowagent.config:

```
Copy-Item -Path sios.jar -Destination <TEMP_DIR>\sios.jar -ToSession
$remoteSession
```

4. In the case a server endpoint is not configured, run snowagent with only "scan" option and then retrieve result files from the machine as following:

```
Invoke-Command -Session $remoteSession {cd <TEMP_DIR>\snowagent
\snowagent; .\snowagent.exe scan}

Copy-Item -Recurse -Path '\\<TARGET_NAME>\<DRIVE_LETTER>$
\<TEMP_DIR_WITHOUT_DRIVE>\snowagent\data' -Destination <LOCAL_DROP_LOCATION>
```

3.2 NET SHARE MODE

On the computer that will run the script for remote scan:

1. Copy the files **snowagent.exe** and **snowagent.config** to the shared network folder \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER> (copy from an existing agent installation).
If Oracle inventory option is to be used, place **sios.jar** in the same folder.
The recommendation is to create a separate folder for each agent variation (32- and 64-bit).
In this example, we assume that 32-bit snowagent.exe is to be put in the following folder:
\\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER>\win32\
2. Run the following commands one-by-one or put them into a .ps1 script:

```
$remoteSession = New-PSSession -ComputerName <TARGET_NAME> -Credential <Domain
\User>

Invoke-Command -Session $remoteSession {cd \\<NET_SHARE_ADDRESS>
\<NET_SHARE_FOLDER>\win32; mkdir <TARGET_NAME>}

Invoke-Command -Session $remoteSession {cd \\<NET_SHARE_ADDRESS>
\<NET_SHARE_FOLDER>\win32\<TARGET_NAME>; ..\snowagent}

Remove-PSSession -Session $remoteSession
```

Where:

Parameter	Description
<TARGET_NAME>	Domain name of the computer to be scanned.
<Domain\User>	User that will execute the scan. It needs to have Local Administrator privileges.

Parameter	Description
<TEMP_DIR>	Temporary folder where a temporary agent folder will be created, for example **C:\temp**.
<NET_SHARE_ADDRESS>	Host name or IP address of the machine that hosts the shared folder.
<NET_SHARE_FOLDER>	Name of the shared folder on the <NET_SHARE_ADDRESS> machine.

3. In the case a server endpoint is not configured, run snowagent with only “scan” option as following:

```
Invoke-Command -Session $remoteSession {cd
\\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER>\win32\<TARGET_NAME>; ..\snowagent
scan}
```

4 MACOS AND LINUX PLATFORM SPECIFICS

Due to security issues SSH doesn't support putting a password on the command line. To avoid entering a password manually at each step of the script, you need to enable key-based SSH authorization for the target user. Simply, add the key of the computer where the script is executed to **~/.ssh/id_rsa.pub to hosts's ~/.ssh/authorized_keys** of the target computer to be scanned.

NOTE

- SSH connections must be enabled both for target and host executing commands.
- Port 22/tcp needs to be open.

4.1 REMOTE COPY MODE

4.1.1 MACOS AND LINUX SPECIFIC COMMANDS

On the computer that will run the script for remote scan:

1. Copy the files **snowagent** and **snowagent.config** to the current folder (copy from an existing agent installation). If Oracle inventory option is to be used, place **sios.jar** in the same folder.
2. Example script:

```
ssh <USER>@<REMOTE_MACHINE> mkdir -p <TEMP_DIR>
scp snowagent <USER>@<REMOTE_MACHINE>:<TEMP_DIR>
scp snowagent.config <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/snowagent.config
ssh <USER>@<REMOTE_MACHINE> chmod 700 <TEMP_DIR>/snowagent
ssh -t <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>; sudo ../snowagent'
ssh -t <USER>@<REMOTE_MACHINE> 'sudo rm -rf <TEMP_DIR>'
```

   Where:

Parameter	Description
<REMOTE_MACHINE>	IP address or DNS name of the remote machine.
<USER>	User that will execute the commands.
<TEMP_DIR>	Temporary folder where the agent files will be copied to, for example **/tmp/snowagent**.

3. In the case Oracle inventory scan is required, add the following command to the script after copying snowagent.config:

```
scp sios.jar <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/sios.jar
```

4. In the case a server endpoint is not configured, run snowagent with only "scan" option and then retrieve result files from the machine as following:

```
ssh -t <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>; sudo ../snowagent scan'
scp -rp <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/data ..
```

4.2 NET SHARE MODE

4.2.1 LINUX (DEBIAN AND RHEL BASED) SPECIFIC COMMANDS

NOTE
In addition to previously mentioned requirements, package **cifs-utils** and its prerequisites must be installed.

On the computer that will run the script for remote scan:

1. Copy the files **snowagent** and **snowagent.config** to the shared network folder \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER> (copy from an existing agent installation). If Oracle inventory option is to be used, place **sios.jar** in the same folder.
   The recommendation is to create a separate folder for each agent variation (32- and 64-bit). In this example, we assume that 32-bit **snowagent** is to be put in the following folder: \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER>\linux32\
2. Example script:

   ```
   ssh <USER>@<REMOTE_MACHINE> mount.cifs //<NET_SHARE_ADDRESS>/
   <NET_SHARE_FOLDER> <TEMP_DIR> -o user=guest,password= rw

   ssh <USER>@<REMOTE_MACHINE> mkdir <TEMP_DIR>/linux32/<TARGET_NAME>

   ssh <USER>@<REMOTE_MACHINE> cd <TEMP_DIR>/linux32/<TARGET_NAME>; sudo ../
   snowagent

   ssh <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>/../; umount <MOUNT_LOCATION>'
   ```

   Where:

Parameter	Description
<REMOTE_MACHINE>	IP address or DNS name of the remote machine.
<USER>	User that will execute the commands.
<NET_SHARE_ADDRESS>	Host name or IP address of the machine that hosts the shared folder.
<NET_SHARE_FOLDER>	Name of the shared folder on the <NET_SHARE_ADDRESS> machine.
<TEMP_DIR>	Temporary folder which the shared network folder will be mounted to, for example **/tmp/snowagent**.

3. In the case a server endpoint is not configured, run snowagent with only “scan” option as following:

   ```
   ssh <USER>@<REMOTE_MACHINE> cd '<TEMP_DIR>/linux32/<TARGET_NAME>; sudo ../
   snowagent scan'
   ```

4.2.2 MACOS SPECIFIC COMMANDS

On the computer that will run the script for remote scan:

1. Copy the files **snowagent** and **snowagent.config** to the shared network folder \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER> (copy from an existing agent installation).

If Oracle inventory option is to be used, place **sios.jar** in the same folder.
In this example, we assume that 32-bit **snowagent** is to be put in the following folder: \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER>\osx\

2. Example script:

```
ssh <USER>@<REMOTE_MACHINE> mount -o rw -t smbfs //guest:@<NET_SHARE_ADDRESS>/
<NET_SHARE_FOLDER> <TEMP_DIR>

ssh <USER>@<REMOTE_MACHINE> mkdir <TEMP_DIR>/osx/<TARGET_NAME>

ssh <USER>@<REMOTE_MACHINE> cd '<TEMP_DIR>/osx/<TARGET_NAME>; sudo ../
snowagent'

ssh <USER>@<REMOTE_MACHINE> 'cd < TEMP_DIR >/../; umount <MOUNT_LOCATION>'
```

Where:

Parameter	Description
<REMOTE_MACHINE>	IP address or DNS name of the remote machine.
<USER>	User that will execute the commands.
<NET_SHARE_ADDRESS>	Host name or IP address of the machine that hosts the shared folder.
<NET_SHARE_FOLDER>	Name of the shared folder on the <NET_SHARE_ADDRESS> machine.
<TEMP_DIR>	Temporary folder which the shared network folder will be mounted to, for example **/tmp/snowagent**.

3. In the case a server endpoint is not configured, run snowagent with only “scan” option as following:

```
ssh <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>/osx/<TARGET_NAME>; sudo ../
snowagent scan'
```

5 UNIX PLATFORM SPECIFICS - AIX

NOTE

- The Java version on the target machine must correspond to the Java version required by the agent.
- The user of the AIX system that executes the scan must be a member of the administrator's group.

5.1 REMOTE COPY MODE

On the computer that will run the script for the remote scan:

1. Copy the files **snowagent.jar** and **snowagent.config** to the current folder (copy from an existing agent installation). If Oracle inventory option is to be used, place **sios.jar** in the same folder.
2. Example script:

```
ssh <USER>@<REMOTE_MACHINE> mkdir -p <TEMP_DIR>

scp snowagent.jar <USER>@<REMOTE_MACHINE>:<TEMP_DIR>

scp snowagent.config <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/snowagent.config

ssh <USER>@<REMOTE_MACHINE> chmod 700 <TEMP_DIR>/snowagent.jar

ssh -t <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>;sudo <JAVA_LOCATION> -jar
<TEMP_DIR>/snowagent.jar'

ssh -t <USER>@<REMOTE_MACHINE> 'rm -rf <TEMP_DIR>'
```

   Where:

Parameter	Description
<JAVA_LOCATION>	Path to the Java executable, for example **/usr/java8_64/jre/bin/java**.

3. In the case Oracle inventory scan is required, add the following command to the script after copying snowagent.config:

```
scp sios.jar <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/sios.jar
```

4. In the case a server endpoint is not configured, run snowagent with only “scan” option and then retrieve result files from the machine as following:

```
ssh -t <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>;sudo <JAVA_LOCATION> -jar
<TEMP_DIR>/snowagent.jar scan'

scp -rp <USER>@<REMOTE_MACHINE>:<TEMP_DIR>/data ..
```

5.2 NET SHARE MODE

NOTE

- The system package **bos.cifs_fs.rte** and its dependencies must be installed. You may check if the package is present by running

  ```
  lslpp -L |grep cifs
  ```

- To install the package, use the official AIX installation media.

On the computer that will run the script for remote scan:

1. Copy the files **snowagent.jar** and **snowagent.config** to the shared network folder \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER> (copy from an existing agent installation). If Oracle inventory option is to be used, place **sios.jar** in the same folder.
   In this example, we will assume that **snowagent.jar** is to be put in the following folder: \\<NET_SHARE_ADDRESS>\<NET_SHARE_FOLDER>\aix\
2. Example script:

   ```
   ssh <USER>@<REMOTE_MACHINE> mount -v cifs -n <NET_SHARE_ADDRESS> -o fmode=777 /
   <NET_SHARE_FOLDER> <TEMP_DIR>

   ssh <USER>@<REMOTE_MACHINE> mkdir <TEMP_DIR>/aix/<TARGET_NAME>

   ssh <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>/aix/<TARGET_NAME>; sudo java -
   jar ../snowagent.jar'

   ssh <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>/../; umount <TEMP_DIR>'
   ```

   Where:

Parameter	Description
<JAVA_LOCATION>	Path to the Java executable, for example **/usr/java8_64/jre/bin/java**.
<TEMP_DIR>	Temporary folder which the shared network folder will be mounted to, for example **/tmp/snowagent**.
<NET_SHARE_ADDRESS>	Host name or IP address of the machine that hosts the shared folder.
<NET_SHARE_FOLDER>	Name of the shared folder on the <NET_SHARE_ADDRESS> machine.

3. In the case a server endpoint is not configured, run snowagent with only “scan” option as following:

   ```
   ssh <USER>@<REMOTE_MACHINE> 'cd <TEMP_DIR>/aix/<TARGET_NAME>; sudo java -
   jar ../snowagent.jar scan'
   ```