TECHNICAL DESCRIPTION

SECURITY

Product	Snow Inventory
Version	5
Document date	2017-04-21

CONTENTS

1 INTRODUCTION

Snow Inventory discovers all computers in the IT environment, and presents the discovery result in the Snow Inventory Admin Console. Computers that are not yet inventoried can be easily identified using the built-in discovery views in the console. Also, all connected network equipment and mobile devices are discovered and displayed as discovered devices in the console.

Snow Inventory 5 provides the customers with the ability to keep their Snow Inventory Agents up to date with the latest product releases. Updates with new agent version(s) and/or new configuration settings for the different supported operating systems can be centrally managed using the Snow Inventory Admin Console.

2 SERVER-SIDE CERTIFICATES

Server-side certificates enable secure HTTP communication between the server and the agents. The certificate chain must be trusted by the computers on which the agents are run. Best practice is to have the server-side certificate signed by a trusted third-party Certificate Authority (CA).

3 CLIENT-SIDE CERTIFICATES

Client-side certificates enable the server to white-list agents that are trusted. The client-side certificate is a shared secret that needs to be distributed along with each of the Snow Inventory Agents.

4 CUSTOM ENCRYPTION KEYS

The Snow Inventory Agent encrypts the inventory result (called snowpack file) using a default crypto key. However, a customer can choose to use one, or several of their own keys. For that purpose, Snow can provide a tool for customers that want to use their own keys for encryption and decryption of the snowpack files.

5 TRANSPORT LAYER SECURITY (TLS)

5.1 SERVER

The Snow Inventory Server supports TLS versions 1.0, 1.1, and 1.2.

Currently, TLS version 1.3 is only in draft mode and we will make sure to support it once/if it is made official.

5.2 AGENT

The Snow Inventory Agent supports TLS versions 1.0, 1.1, and 1.2.

For customers with a strict TLS 1.2 environment, TLS 1.2 needs to be set as the default secure protocol in WinHTTP on Windows. For details, see the following Microsoft support article:

https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1.1-and-tls-1.2-as-a-default-secure-protocols-in-winhttp-in-windows

5.3 ENCRYPTION

AES 128-bit is used for encryption of the snowpack files. The reasons for using AES 128 are:

- AES 128 is regarded just as secure as the AES 256, since they both will take an infinite time to crack
- Performance, AES 256 is slower to encrypt and decrypt
- AES 128 is FIPS140-2 validated which is the level that many governments are using
- US export regulations prohibits the use of AES 256 in a lot of countries, and there are also many import controls in countries that prohibits the use of AES 256. The full details of the Wassenaar Arrangement, with a complete list of regulations per country is found here:

  http://www.cryptolaw.org/cls2.htm

5.4 “SUDO VS ROOT”

None of the Snow Inventory Agents for Unix, Linux, or macOS require root privileges. Elevated permissions (superuser) can be achieved by using sudo.

For more information, refer to *User guide* for each respective Inventory agent.

5.5 ORACLE SCANNER

The Snow Inventory Oracle Scanner does not require root. Elevated permissions (superuser) can be achieved by using sudo.

For more information, refer to *User guide, Snow Inventory Oracle Scanner*.

6 ANONYMIZATION OF DATA

The Snow Inventory Agent can be configured to send anonymous data from the inventoried computer. The following data can be replaced by SHA-1 hash:

- usernames of logged on users
- usernames within software metering (i.e. users who have used applications on the computer)
- the IP addresses assigned to the network interfaces of the computer

To enable the anonymous data option, add the following system settings to the agent configuration file:

privacy.hide_user=true
privacy.hide_ip=true

For more information, refer to *Configuration guide, Snow Inventory Agents*.

7 POWERSHELL SCRIPTS

The Snow Inventory Agent for Windows has support for running Windows PowerShell scripts as part of the inventory scanning process:

- PowerShell 5.1 – Both signed and unsigned scripts
- PowerShell 5.0 – Signed scripts only
- PowerShell 4.x – Both signed and unsigned scripts
- PowerShell 3.x – Both signed and unsigned scripts

The built-in functionality uses the output of the Windows PowerShell scripts to create software or custom registry keys within the inventory result that is sent from the agent to the Inventory Master Server. This will enable scanning of additional information from software products, but can also be used for custom tasks such as identifying which users are local administrators on each machine.

For more information, refer to *User guide, Snow Inventory Agent for Windows*.

7.1 INTEGRITY MODE

The PowerShell scripts can be run in different integrity modes, depending on their file extensions.

7.1.1 LOW INTEGRITY MODE

PowerShell scripts with file extension ".ps1" are not encrypted by Snow Software, and are executed in low integrity mode. The low integrity mode prevents users from creating scripts that could potentially harm the system. In low integrity mode the scripts, including child processes, cannot modify the underlying system.

7.1.2 MEDIUM INTEGRITY MODE

PowerShell scripts with file extension ".snow-ps1" are encrypted by Snow Software, and are run in medium integrity mode.