Intel® Active Management Technology: ಗೌಪ್ಯತೆ ಸೂಚನೆ

ಕೊನೆಯದಾಗಿ ಪರಿಷ್ಕರಿಸಿದ್ದು: 8/12/2021

ನಿಮ್ಮ ಗೌಪ್ಯತೆಯನ್ನು ರಕ್ಷಿಸಲು Intel Corporation ಬದ್ಧವಾಗಿದೆ. ಈ ಹೇಳಿಕೆಯು Intel® Active Management Technology (Intel® AMT) ಯಾವ ಗೌಪ್ಯತೆ ಸೂಕ್ಷ್ಮ ಕಾರ್ಯವೈಶಿಷ್ಟ್ಯಗಳು ಮತ್ತು ಸಾಮರ್ಥ್ಯಗಳನ್ನು ಸಂಚಾಲಿತಗೊಳಿಸುತ್ತದೆ, IT ಅಡ್ಮಿನಿಸ್ಟ್ರೇಟರ್‌ಗಳು ಮಾಡಲು Intel AMT ಯಾವುದನ್ನು ಅನುಮತಿಸುತ್ತದೆ ಮತ್ತು ಯಾವುದನ್ನು ಅನುಮತಿಸುವುದಿಲ್ಲ ಎನ್ನುವುದನ್ನು ವಿವರಿಸುತ್ತದೆ ಹಾಗೂ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗಳಲ್ಲಿ Intel AMT ಶೇಖರಣೆ ಮಾಡುವ ಡೇಟಾದ ವಿಧಗಳನ್ನು ಸೂಚಿಸುತ್ತದೆ. ಈ ಹೇಳಿಕೆಯು Intel ನ ಆನ್‌ಲೈನ್ ಗೌಪ್ಯತೆ ಸೂಚನೆಗೆ ಪೂರಕವಾಗಿದೆ ಮತ್ತು Intel AMT ಗೆ ಮಾತ್ರ ಅನ್ವಯಿಸುತ್ತದೆ.

Intel AMT ಅಂದರೇನು?

IT ನಿರ್ವಾಹಕರಿಂದ ಅಧಿಕೃತಗೊಳಿಸಿದ ಸಂಸ್ಥೆಯಲ್ಲಿ ಔಟ್-ಆಫ್-ಬ್ಯಾಂಡ್ (OOB) ರಿಮೋಟ್ ಬೆಂಬಲವನ್ನು ಮತ್ತು ನೆಟ್‌ವರ್ಕ್ ಮಾಡಿರುವ ಕಂಪ್ಯೂಟರ್ ಸಿಸ್ಟಂಗಳ ನಿರ್ವಹಣೆಯನ್ನು Intel AMT ಸಾಧ್ಯವಾಗಿಸುತ್ತದೆ.

Intel AMT ಎತ್ತಿದ ಸಂಭಾವ್ಯ ಗೌಪ್ಯತೆ ಸಮಸ್ಯೆಗಳು ಯಾವುವು?

ಸಾಫ್ಟ್‌ವೇರ್ ಮಾರಾಟಗಾರರಿಂದ ರಿಮೋಟ್ ನಿರ್ವಹಣೆ ಸಾಮರ್ಥ್ಯಗಳು ಲಭ್ಯ ಇವೆ ಮತ್ತು ಸಾಕಷ್ಟು ಸಮಯದಿಂದ ಹಲವು ಸಂಸ್ಥೆಗಳ IT ಇಲಾಖೆಗಳಿಂದ ಬಳಕೆಯಲ್ಲಿದೆ.

ಅದಾಗ್ಯೂ, ಬಳಕೆದಾರ ಇಲ್ಲದಿದ್ದರೂ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಆಫ್ ಮಾಡಿದ್ದರೂ ಸಹ, ಬಳಕೆದಾರರ ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ದೂರಸ್ಥವಾಗಿ ಬೆಂಬಲಿಸಲು ಮತ್ತು ನಿರ್ವಹಿಸಲು IT ನಿರ್ವಾಹಕರಿಗೆ Intel AMT ಅವಕಾಶ ಕಲ್ಪಿಸುತ್ತದೆ.

ಸಿಸ್ಟಂನಲ್ಲಿ Intel AMT ಸಕ್ರಿಯಗೊಳಿಸಲಾಗಿದೆಯೇ ಎಂದು ಬಳಕೆದಾರ ಹೇಗೆ ಹೇಳಬಹುದು?

Intel AMT ಯ ಪ್ರಸ್ತುತ ಸ್ಥಿತಿಯ ಕುರಿತು ಅಂತಿಮ ಬಳಕೆದಾರನಿಗೆ ಪಾರದರ್ಶಕತೆ ಮತ್ತು ಅಧಿಸೂಚನೆಯನ್ನು ಒದಗಿಸಲು Intel ಸಿಸ್ಟಂ ಟ್ರೇ ಐಕಾನ್ ಅನ್ನು ಅಭಿವೃದ್ಧಿಪಡಿಸಿದೆ. ಪ್ರಸ್ತುತ ಪ್ರಮಾಣಿತ Intel AMT ಸಾಫ್ಟ್‌ವೇರ್ Intel® Management and Security Status (IMSS) ಅಪ್ಲಿಕೇಶನ್ ಹಾಗೂ ಡ್ರೈವರ್‌ಗಳು ಮತ್ತು ಸೇವೆಗಳೊಂದಿಗೆ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಲಾಗುವ ಸಿಸ್ಟಂ ಟ್ರೇ ಐಕಾನ್ ಅನ್ನು ಒಳಗೊಂಡಿದೆ. IMSS ಸಿಸ್ಟಂ ಟ್ರೇ ಐಕಾನ್ ಸಿಸ್ಟಂನಲ್ಲಿ Intel AMT ಯ ಪ್ರಸ್ತುತ ಸ್ಥಿತಿಯನ್ನು ಪ್ರದರ್ಶಿಸುತ್ತದೆ (ಸಕ್ರಿಯಗೊಳಿಸಲಾಗಿದೆಯೇ ಅಥವಾ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲಾಗಿದೆಯೇ) ಮತ್ತು Intel AMT ಸಾಮರ್ಥ್ಯಗಳನ್ನು

ಸಕ್ರಿಯ/ನಿಷ್ಕ್ರಿಯಗೊಳಿಸುವುದು ಹೇಗೆ ಎನ್ನುವ ಕುರಿತು ಸೂಚನೆಗಳನ್ನು ಕೂಡ ಒದಗಿಸುತ್ತದೆ. ಪ್ರತಿ ಒರಿಜಿನಲ್ ಉಪಕರಣ ತಯಾರಕರು (OEM) IMSS ಅಪ್ಲಿಕೇಶನ್ ಲೋಡ್ ಮಾಡುವಂತೆ Intel ಶಿಫಾರಸು ಮಾಡುತ್ತದೆ. ಅದಾಗ್ಯೂ, Intel ನ ಈ ಶಿಫಾರಸನ್ನು ಅನುಸರಣೆ ಮಾಡದಿರಲು OEM ಗಳು ಆಯ್ಕೆ ಮಾಡಿಕೊಳ್ಳಬಹುದು ಮತ್ತು ಹೆಚ್ಚುವರಿಯಾಗಿ, ಅಂತಿಮ ಬಳಕೆದಾರರಿಗೆ Intel AMT ಸಕ್ರಿಯಗೊಳಿಸಿದ ಸಿಸ್ಟಂಗಳನ್ನು ಒದಗಿಸುವುದಕ್ಕೆ ಮುಂಚೆ ಅಂತಿಮ ಗ್ರಾಹಕ IT ಮ್ಯಾನೇಜರ್‌ಗಳು IMSS ಅಪ್ಲಿಕೇಶನ್ ಅನ್ನು ತೆಗೆದುಹಾಕಬಹುದು. OEM ಅನುಷ್ಠಾನವನ್ನು ಅವಲಂಬಿಸಿ, ತಮ್ಮ ಕಂಪ್ಯೂಟರ್‌ನ ಸಿಸ್ಟಂ BIOS ನಲ್ಲಿ ಬಳಕೆದಾರರು Intel AMT ಯ ಸ್ಥಿತಿಯನ್ನು ಕೂಡ ಪರಿಶೀಲಿಸಬಹುದು. ಅದಾಗ್ಯೂ, Intel AMT ಅನ್ನು ಸಕ್ರಿಯ/ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಲು ಅಥವಾ Intel AMT ಸ್ಥಿತಿಯನ್ನು ಪರಿಶೀಲಿಸಲು ಅವಶ್ಯಕವಾಗಿರುವ ಸಿಸ್ಟಂ BIOS ಗೆ ಅಗತ್ಯವಿರುವ ಪ್ರವೇಶವನ್ನು ಕೆಲವು ಉದ್ಯಮದ IT ವಿಭಾಗಗಳು ಬಳಕೆದಾರರಿಗೆ ನೀಡದೆ ಇರಬಹುದು.

ಬಳಕೆದಾರರಿಂದ Intel AMT ಯಾವ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಸಂಗ್ರಹಿಸುತ್ತದೆ?

ಬಳಕೆದಾರರಿಂದ Intel AMT ಯಾವುದೇ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು (ಉದಾಹರಣೆಗೆ, ಹೆಸರು, ವಿಳಾಸ, ಫೋನ್ ಸಂಖ್ಯೆ ಇತ್ಯಾದಿ) ಸಂಗ್ರಹಿಸುವುದಿಲ್ಲ.

Intel AMT ಯಿಂದ Intel Corporation ಗೆ ಯಾವ ವಿಧದ ಮಾಹಿತಿಯನ್ನು ಕಳುಹಿಸಲಾಗುತ್ತದೆ ಮತ್ತು ಆ ಮಾಹಿತಿಯನ್ನು ಹೇಗೆ ಬಳಸಲಾಗುತ್ತದೆ?

Intel Corporation ಗೆ Intel AMT ಯಾವುದೇ ಡೇಟಾವನ್ನು ಕಳುಹಿಸುವುದಿಲ್ಲ.

Intel AMT ಯಾವ ವಿಧದ ಮಾಹಿತಿಯನ್ನು ಶೇಖರಣೆ ಮಾಡುತ್ತದೆ?

Intel AMT ಸಿಸ್ಟಂ ಮದರ್‌ಬೋರ್ಡ್‌ನಲ್ಲಿ ಫ್ಲ್ಯಾಶ್ ಮೆಮೊರಿಯಲ್ಲಿ ಮಾಹಿತಿಯನ್ನು ಶೇಖರಿಸುತ್ತದೆ. ಈ ಮಾಹಿತಿಯು ಫರ್ಮ್‌ವೇರ್ ಕೋಡ್, ಹಾರ್ಡ್‌ವೇರ್ ಇನ್ವೆಂಟರಿ ಡೇಟಾ (ಉದಾಹರಣೆಗೆ, ಮೆಮೊರಿ ಗಾತ್ರ, CPU ವಿಧ, ಹಾರ್ಡ್ ಡಿಸ್ಕ್ ವಿಧ), ಪ್ಲಾಟ್‌ಫಾರ್ಮ್ ಈವೆಂಟ್‌ಗಳನ್ನು ದಾಖಲಿಸುವ ಒಂದು ಈವೆಂಟ್ ಲಾಗ್ (ಉದಾಹರಣೆಗೆ, CPU ಬಿಸಿಯಾಗುವುದು, ಫ್ಯಾನ್ ವೈಫಲ್ಯ, BIOS POST ಸಂದೇಶ), Intel AMT ಭದ್ರತಾ ಈವೆಂಟ್‌ಗಳು (ಉದಾಹರಣೆಗೆ, Intel AMT ಪಾಸ್‌ವರ್ಡ್ ದಾಳಿ ಈವೆಂಟ್‌ನ ಎಚ್ಚರಿಕೆ, ಅಥವಾ ಸಿಸ್ಟಂ ಡಿಫೆನ್ಸ್ ಫಿಲ್ಟರ್ ಟ್ರಿಪ್ಪಿಂಗ್), ಹಾಗೂ Intel AMT ಕಾನ್ಫಿಗರೇಷನ್ ಡೇಟಾ (ಉದಾಹರಣೆಗೆ, ಪ್ರೊವಿಷನಿಂಗ್ ಡೇಟಾ, LAN MAC ವಿಳಾಸ, ಕೀಗಳು, ಕೀಬೋರ್ಡ್-ವೀಡಿಯೊ ಮೌಸ್ (KVM) ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಟ್ರಾನ್ಸ್‌ಪೋರ್ಟ್ ಲೇಯರ್ ಭದ್ರತೆ (TLS) ಪ್ರಮಾಣಪತ್ರಗಳು ಮತ್ತು IT ಕಾನ್ಫಿಗರ್ ಮಾಡಿದ ವೈರ್‌ಲೆಸ್ ನೆಟ್‌ವರ್ಕ್ ಪ್ರೊಫೈಲ್‌ಗಳು ಸೇರಿದಂತೆ ನೆಟ್‌ವರ್ಕ್ ಸೆಟ್ಟಿಂಗ್‌ಗಳು, ಆ್ಯಕ್ಸೆಸ್ ಕಂಟ್ರೋಲ್ ಪಟ್ಟಿಗಳು ಮತ್ತು ಸಾರ್ವತ್ರಿಕ ವಿಶಿಷ್ಟ ಐಡೆಂಟಿಫೈಯರ್‌ಗಳು (UUIDs)). ಸೂಕ್ಷ್ಮ ಎಂದು ಪರಿಗಣಿಸಲಾದ ಎಲ್ಲ ಕಾನ್ಫಿಗರೇಷನ್ ಡೇಟಾವನ್ನು ಫ್ಲ್ಯಾಶ್‌ನಲ್ಲಿ ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡಿದ

ಸ್ವರೂಪದಲ್ಲಿ ಶೇಖರಣೆ ಮಾಡಲಾಗುತ್ತದೆ. UUID ಗಳ ಕುರಿತು ಹೆಚ್ಚಿನ ಮಾಹಿತಿಯನ್ನು ಕೆಳಗಿನ ವಿಭಾಗದಲ್ಲಿ ಕಂಡುಕೊಳ್ಳಬಹುದು.

Intel AMT ಆವೃತ್ತಿ 11.0 ಮತ್ತು ಹಿಂದಿನವು ನೋಂದಾಯಿತ ಸ್ವತಂತ್ರ ಸಾಫ್ಟ್‌ವೇರ್ ಮಾರಾಟಗಾರ (ISV) ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಗೆ ತೃತೀಯ ಪಕ್ಷದ ಡೇಟಾ ಶೇಖರಣೆ (3PDS) ಎಂದು ಕರೆಯಲಾಗುವ ಫ್ಲ್ಯಾಶ್ ಮೆಮೊರಿ ಭಂಡಾರದ ಪ್ರದೇಶದಲ್ಲಿ ಡೇಟಾವನ್ನು ಶೇಖರಣೆ ಮಾಡುತ್ತವೆ. Intel AMT ಆವೃತ್ತಿ 11.6 ರಲ್ಲಿ ಆರಂಭಗೊಂಡು, ಈ ವೈಶಿಷ್ಟ್ಯವನ್ನು ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್ ಹೋಸ್ಟಿಂಗ್‌ನಿಂದ ಬದಲಿಸಲಾಗಿದ್ದು ಇದು Intel AMT ಕ್ಲಯಂಟ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ನಲ್ಲಿ ಸ್ಥಳೀಯವಾಗಿ ನಿರ್ವಹಿಸುವ ನಾನ್-ವೊಲಟೈಲ್ ಮೆಮೊರಿಯಲ್ಲಿ (NVM) ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಹೋಸ್ಟ್ ಮಾಡಲು Intel AMT ಗೆ ಅವಕಾಶ ಕಲ್ಪಿಸುತ್ತದೆ.

ತನ್ನ ISV ಗಳಿಗೆ ಜವಾಬ್ದಾರಿಯುತ ಡೇಟಾ ನಿರ್ವಹಣೆಗಾಗಿ ಅತ್ಯುತ್ತಮ ಗೌಪ್ಯತೆ ಅಭ್ಯಾಸಗಳು ಎಂದು ನಂಬಿರುವುದನ್ನು Intel ಸಂವಹನ ಮಾಡುತ್ತದೆಯಾದರೂ, ಅಂತಿಮವಾಗಿ ಫ್ಲ್ಯಾಶ್ ಮೆಮೊರಿಯ ಈ ಪ್ರದೇಶದಲ್ಲಿ ಯಾವ ಡೇಟಾವನ್ನು ಶೇಖರಣೆ ಮಾಡಬಹುದು ಎನ್ನುವುದನ್ನು Intel ನಿರ್ಧರಿಸುವುದಿಲ್ಲ ಮತ್ತು ISV ಡೇಟಾಗಾಗಿ ಎನ್‌ಕ್ರಿಪ್ಶನ್ ವಿಧಾನಗಳನ್ನು ಬೆಂಬಲಿಸುವುದಿಲ್ಲ. ಹಾಗಾಗಿ ISV ಗಳು ತಮ್ಮ ಡೇಟಾವನ್ನು ಸೂಕ್ಷ್ಮ ಎಂದು ಪರಿಗಣಿಸಿದರೆ ಅದನ್ನು ಫ್ಲ್ಯಾಶ್‌ನಲ್ಲಿ ಶೇಖರಣೆ ಮಾಡುವುದಕ್ಕೆ ಮುನ್ನ ಎನ್‌ಕ್ರಿಪ್ಟ್ ಮಾಡುವಂತೆ ಪ್ರೋತ್ಸಾಹಿಸುತ್ತೇವೆ. ಇಲ್ಲಿ ಡೇಟಾ ಶೇಖರಣೆ ಮಾಡಿರುವ ಕಾರಣದಿಂದ ಸಂಭಾವ್ಯ ಗೌಪ್ಯತೆ ಅಪಾಯಗಳ ಕುರಿತು ನೀವು ಕಳವಳ ಹೊಂದಿದ್ದರೆ, ಮಾಹಿತಿಯ ವಿಧ ಮತ್ತು NVM ನಲ್ಲಿ ಶೇಖರಣೆ ಮಾಡುವ ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಹಾಗೂ ಅದನ್ನು ಹೇಗೆ ರಕ್ಷಿಸಲಾಗುತ್ತದೆ ಎನ್ನುವುದಕ್ಕೆ ಸಂಬಂಧಿಸಿ ಹೆಚ್ಚಿನ ವಿವರಗಳಿಗಾಗಿ ದಯವಿಟ್ಟು ಸೂಕ್ತ ತೃತೀಯ ಪಕ್ಷದ ಸಾಫ್ಟ್‌ವೇರ್ ಡೆವಲಪರ್ ಅನ್ನು ಸಂಪರ್ಕಿಸಿ.

UUID ಗಳನ್ನು Intel AMT ಹೇಗೆ ಬಳಸುತ್ತದೆ? Intel AMT-ಸಕ್ರಿಯಗೊಳಿಸಿದ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ UUUID ಗಳು ಯಾವ ಕಾರ್ಯಶೀಲತೆಯನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುತ್ತವೆ ಮತ್ತು ಯಾವುದನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುವುದಿಲ್ಲ?

ಸಾರ್ವತ್ರಿಕ ವಿಶಿಷ್ಟ ಐಡೆಂಟಿಫೈಯರ್‌ಗಳು (UUID ಗಳು) ಪ್ರಕ್ರಿಯೆ, ಸಿಸ್ಟಂನ ಭದ್ರತೆ (ಉದಾಹರಣೆಗೆ, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು, ಕೀಗಳು ಮತ್ತು TLS ಪ್ರಮಾಣಪತ್ರಗಳು) ಒದಗಿಸುವುದು ಹಾಗೂ ಸಂಸ್ಥೆಯೊಳಗೆ ನಿರ್ದಿಷ್ಟ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗೆ ನಿಖರವಾಗಿ ಸಂಪರ್ಕಗೊಳ್ಳಲು ಮತ್ತು ನಿರ್ವಹಿಸಲು IT ನಿರ್ವಾಹಕರಿಗೆ ಸಾಧ್ಯವಾಗುತ್ತದೆ ಎಂದು ಖಚಿತಪಡಿಸಿಕೊಳ್ಳುವುದು ಸೇರಿದಂತೆ, ಹಲವು ಉದ್ದೇಶಗಳಿಗಾಗಿ Intel AMT ಯಿಂದ ಬಳಸಲಾಗುವ ಸಾಧನಗಳಾಗಿವೆ.

ಶೂನ್ಯ-ಸ್ಪರ್ಶ ಒದಗಿಸುವಿಕೆಯಂತಹ ಚಿರಸ್ಥಾಯಿ UUID ಅಗತ್ಯವಿರುವ ಬಳಕೆಯ ಸನ್ನಿವೇಶಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಲು Intel® Unique Platform ID (UPID) ಎಂದು ಕರೆಯಲಾಗುವ ಚಿರಸ್ಥಾಯಿ UUID ಯೊಂದಿಗೆ Intel VPRO ಬರುತ್ತದೆ. UPID ಕಾರ್ಯಶೀಲತೆಯು OEM ಅನುಷ್ಠಾನವನ್ನು ಅವಲಂಬಿಸಿದೆ. UUID ಗಳು ವಸ್ತುಶಃ ಎಲ್ಲ ಆಧುನಿಕ PC ಗಳಲ್ಲಿ ಇವೆ ಮತ್ತು Intel AMT ಗೆ ಸಂಬಂಧವಿಲ್ಲದೆ, ಎಲ್ಲ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳಲ್ಲಿ ಸಾಮಾನ್ಯವಾಗಿ OEM ಗಳಿಂದ ಇನ್‌ಸ್ಟಾಲ್ ಮಾಡಲಾಗಿರುತ್ತದೆ. ವಾಸ್ತವದಲ್ಲಿ, OS ಅಥವಾ ವೈರಸ್ ನಿಯಂತ್ರಣ ಸಿಸ್ಟಂ ಅಪ್‌ಡೇಟ್‌ಗಳ ತಲುಪಿಸುವಿಕೆಯಂತಹ ನಿರೀಕ್ಷಿತ ಕಾರ್ಯವೈಶಿಷ್ಟ್ಯಗಳನ್ನು ಒದಗಿಸುವ

ಸಲುವಾಗಿ ವಿಶಿಷ್ಟ ಸಿಸ್ಟಂ ಮಾಹಿತಿಯನ್ನು ಪ್ರತ್ಯೇಕಿಸಲು ಹಲವು PC ಗಳಲ್ಲಿ ಕಂಡುಬರುವ ಅಪ್ಲಿಕೇಶನ್‌ಗಳಿಂದ ಪ್ರಸ್ತುತ UUID ಗಳು ಬಳಸಲ್ಪಡುತ್ತಿವೆ. Intel AMT ಬಹುತೇಕ ಅದೇ ರೀತಿಯಲ್ಲಿ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್ UUID ಗಳನ್ನು ಬಳಸುತ್ತದೆ – ಮೂಲಭೂತ ವ್ಯತ್ಯಾಸವೆಂದರೆ UUID OOB ಅನ್ನು ಪ್ರವೇಶಿಸಲು Intel AMT ಗೆ ಸಾಧ್ಯವಾಗಿಸುವ ಸಲುವಾಗಿ, UUID ಅನ್ನು ಫ್ಲ್ಯಾಶ್ ಮೆಮೊರಿ ಭಂಡಾರಕ್ಕೆ ನಕಲಿಸಲಾಗುತ್ತದೆ.

UPID ಸೇರಿದಂತೆ, Intel AMT-ಸಕ್ರಿಯಗೊಳಿಸಿದ ಸಿಸ್ಟಂಗಳಲ್ಲಿ UUID ಗಳನ್ನು ಬಳಕೆದಾರರನ್ನು ಅವರ PC ಗಳಲ್ಲಿ ಟ್ರ್ಯಾಕ್ ಮಾಡಲು Intel ನಿಂದ ಬಳಸಲಾಗದು ಅಥವಾ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗೆ ಹಿಂಬಾಗಿಲಿನ ಮೂಲಕ ಬಳಕೆದಾರ ಸಿಸ್ಟಂಗಳಿಗೆ ಅವು Intel ಗೆ ಪ್ರವೇಶ ಕಲ್ಪಿಸುವುದಿಲ್ಲ, ಬಳಕೆದಾರರ ಸಮ್ಮತಿಯಿಲ್ಲದೆ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗೆ ಬಲವಂತದ ಫರ್ಮ್‌ವೇರ್ ಡೌನ್‌ಲೋಡ್ ಮಾಡುವುದಕ್ಕೂ ಸಹ Intel ಗೆ ಅವಕಾಶ ನೀಡುವುದಿಲ್ಲ ಎನ್ನುವುದನ್ನು ಗಮನಿಸುವುದು ಮುಖ್ಯವಾಗಿದೆ. Intel AMT ಯಿಂದ ಫ್ಲ್ಯಾಶ್‌ನಲ್ಲಿ ಶೇಖರಣೆ ಮಾಡಿದ ಯಾವುದೇ UUID ಯನ್ನು ನಿರ್ದಿಷ್ಟ Intel AMT-ಸಕ್ರಿಯಗೊಳಿಸಿದ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಾಗಿ ಅಧಿಕೃತ IT ನಿರ್ವಾಹಕರು ಮಾತ್ರ ಪ್ರವೇಶಿಸಬಹುದು. ವಿಶ್ವಾಸವನ್ನು ಸ್ಥಾಪಿಸಲು Intel AMT ಸಿಸ್ಟಂನಲ್ಲಿ (BIOS ಮೆನು ಅಥವಾ USB ಕೀ ಮೂಲಕ) ಉದ್ಯಮ ಪ್ರಮಾಣಪತ್ರಗಳು ಅಥವಾ ಭೌತಿಕ ಉಪಸ್ಥಿತಿ ಇವೆರಡರಲ್ಲಿ ಒಂದನ್ನು ಬಳಸಿಕೊಂಡು ರಕ್ಷಿಸಿದ ಪ್ರಕ್ರಿಯೆಯ ಸಂದರ್ಭ ಅಂತಿಮ ಗ್ರಾಹಕರ IT ಯಿಂದ ಅಧಿಕೃತ IT ನಿರ್ವಾಹಕರ ಪಟ್ಟಿಯನ್ನು ಕಾನ್ಫಿಗರ್ ಮಾಡಲಾಗುತ್ತದೆ, ಮತ್ತು ಹೀಗೆ ಅಂತಿಮ ಗ್ರಾಹಕರ IT ಯಿಂದ ನಿಯೋಜಿಸಲ್ಪಟ್ಟ ವಿಶ್ವಾಸಾರ್ಹ ಸರ್ವರ್‌ಗಳಲ್ಲಿ ಇರುವ ಕನ್ಸೋಲ್‌ಗಳೊಂದಿಗೆ ಸಂಪೂರ್ಣವಾಗಿ ಸಂಭವಿಸುತ್ತದೆ. ಇನ್ನೊಂದು ರೀತಿಯಲ್ಲಿ ಹೇಳುವುದಾದರೆ, ಅಂತಿಮ ಗ್ರಾಹಕರು ಸ್ಪಷ್ಟವಾಗಿ ಇದನ್ನು ಕಾನ್ಫಿಗರ್ ಮಾಡದ ಹೊರತು Intel AMT ಮೂಲಕ ಅಂತಿಮ ಗ್ರಾಹಕನಿಗೆ ಹೊರಗಿನವರಾದ ಯಾವುದೇ ಪಕ್ಷದಿಂದ ಅಥವಾ ಪಕ್ಷಕ್ಕೆ UUID ಗಳನ್ನಾಗಲೀ ಅಥವಾ ಯಾವುದೇ ಇತರ ಮಾಹಿತಿಯನ್ನಾಗಲೀ ಸಂವಹನ ಮಾಡಲಾಗದು. ನಿರ್ದಿಷ್ಟ ಸಿಸ್ಟಂಗೆ ಅಧಿಕೃತ ನಿರ್ವಾಹಕರನ್ನು ಗುರುತಿಸಲು, https://software.intel.com/en-us/business-client/manageability ಇಲ್ಲಿ ಲಭ್ಯವಿರುವ Intel AMT ಸಾಫ್ಟ್‌ವೇರ್ ಡೆವಲಪರ್ ಕಿಟ್ (SDK) ಡಾಕ್ಯುಮೆಂಟೇಶನ್ ನೋಡಿ, ಇದು ACL ಗಳನ್ನು ಅಥವಾ Kerberos ಅಧಿಕೃತಗೊಳಿಸಿದ ಖಾತೆಗಳನ್ನು ರಿಟ್ರೀವ್ ಮಾಡಲು ಒಂದು API ಅನ್ನು ಒದಗಿಸುತ್ತದೆ.

Intel® Active Management Technology (Intel® AMT) ಯಾವ ವಿಧದ ಮಾಹಿತಿಯನ್ನು ನೆಟ್‌ವರ್ಕ್‌ನಾದ್ಯಂತ ಕಳುಹಿಸುತ್ತದೆ?

Intel AMT ಪೂರ್ವವ್ಯಾಖ್ಯಾನಿತ IANA ನೆಟ್‌ವರ್ಕ್ ಪೋರ್ಟ್‌ಗಳ ಮೂಲಕ ಡೇಟಾವನ್ನು ಕಳುಹಿಸುತ್ತದೆ ಮತ್ತು ಸ್ವೀಕರಿಸುತ್ತದೆ: SOAP/HTTP ಗಾಗಿ ಪೋರ್ಟ್ 16992, SOAP/HTTPS ಗಾಗಿ ಪೋರ್ಟ್ 16993, ಮರುನಿರ್ದೇಶನ/TCP ಗಾಗಿ ಪೋರ್ಟ್ 16994 ಮತ್ತು ಮರುನಿರ್ದೇಶನ/TLS ಗಾಗಿ ಪೋರ್ಟ್ 16995. DASH ಅನುಸರಣೆ ಹೊಂದಿರುವ ಸಿಸ್ಟಂಗಳು HTTP ಗಾಗಿ 623 ಮತ್ತು HTTPS ಗಾಗಿ 664 ಪೋರ್ಟ್‌ಗಳ ಮೂಲಕ ಡೇಟಾವನ್ನು ಕಳುಹಿಸುತ್ತವೆ ಮತ್ತು ಸ್ವೀಕರಿಸುತ್ತವೆ. ಕೀಬೋರ್ಡ್-ವೀಡಿಯೊ-ಮೌಸ್ (KVM) ಸೆಷನ್ ಒಂದೋ ಮೇಲಿನ ಮರುನಿರ್ದೇಶನ ಪೋರ್ಟ್‌ಗಳಲ್ಲಿ (16994 ಅಥವಾ 16995) ಅಥವಾ ಕಸ್ಟಮರಿ RFB (VNC ಸರ್ವರ್) ಪೋರ್ಟ್ - 5900 ನಲ್ಲಿ ಕಾರ್ಯನಿರ್ವಹಿಸುತ್ತದೆ. ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿ ಕಳುಹಿಸಿದ ಮಾಹಿತಿಯ ವಿಧದಲ್ಲಿ

Intel AMT ಕಮಾಂಡ್ ಮತ್ತು ಪ್ರತಿಕ್ರಿಯೆ ಸಂದೇಶಗಳು, ಮರುನಿರ್ದೇಶನ ಟ್ರಾಫಿಕ್ ಮತ್ತು ಸಿಸ್ಟಂ ಅಲರ್ಟ್‌ಗಳು ಸೇರಿವೆ. ಟ್ರಾನ್ಸ್‌ಪೋರ್ಟ್-ಲೇಯರ್ ಭದ್ರತೆ (TLS) ಆಯ್ಕೆಯನ್ನು ಬಳಕೆದಾರನ ಸಿಸ್ಟಂನಲ್ಲಿ ಸಕ್ರಿಯಗೊಳಿಸಿದ್ದರೆ, 16993 ಮತ್ತು 16995 ಪೋರ್ಟ್‌ಗಳ ಮೂಲಕ ಪ್ರಸರಣ ಮಾಡುವ ಡೇಟಾವನ್ನು ಅದರೊಂದಿಗೆ ರಕ್ಷಿಸಲಾಗುತ್ತದೆ.

IPV4 ಅಥವಾ IPV6 ನೆಟ್‌ವರ್ಕ್ ಮೂಲಕ Intel AMT ಡೇಟಾವನ್ನು ಕಳುಹಿಸಬಹುದು ಮತ್ತು ಅದು RFC 3041 ಗೌಪ್ಯತೆ ವಿಸ್ತರಣೆಗಳೊಂದಿಗೆ ಅನುಸರಣೆ ಹೊಂದಿದೆ.

Intel® Active Management Technology (Intel® AMT) ಯಾವ ಗುರುತಿಸಬಹುದಾದ ಮಾಹಿತಿಯನ್ನು ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿ ಬಹಿರಂಗಪಡಿಸುತ್ತದೆ?

Intel® AMT ಅನ್ನು ಸಕ್ರಿಯಗೊಳಿಸಿದಾಗ, ಕಂಪ್ಯೂಟರ್ ಅನ್ನು ಗುರುತಿಸಲು ಬಳಸಬಹುದಾದ ಮಾಹಿತಿಯನ್ನು ಓಪನ್ ಪೋರ್ಟ್‌ಗಳು ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿನ ಇತರರಿಗೆ ಪ್ರಸ್ತುತಪಡಿಸುತ್ತವೆ. ಇದು HTTPS ಪ್ರಮಾಣಪತ್ರ, HTTP ಡೈಜೆಸ್ಟ್ ರಿಯಲ್ಮ್, Intel AMT ಆವೃತ್ತಿ ಮತ್ತು ಕಂಪ್ಯೂಟರ್‌ಗೆ ಬೆರಳಚ್ಚು ನೀಡಲು ಬಳಸಬಹುದಾದ ಇತರ ಮಾಹಿತಿಯನ್ನು ಒಳಗೊಂಡಿದೆ. ಈ ಮಾಹಿತಿಯನ್ನು Intel® AMT ಯಿಂದ ಬೆಂಬಲಿತವಾದ ಪ್ರೊಟೋಕಾಲ್‌ಗಳ ಸಾಮಾನ್ಯ ಕಾರ್ಯಾಚರಣೆಗಳ ಭಾಗವಾಗಿ ನೀಡಲಾಗುತ್ತದೆ. Intel® AMT ಪೋರ್ಟ್‌ಗಳಿಗೆ ಆಪರೇಟಿಂಗ್ ಸಿಸ್ಟಂ ಫೈರ್‌ವಾಲ್ ಪ್ರವೇಶವನ್ನು ನಿರ್ಬಂಧಿಸುವುದಿಲ್ಲ, ಅದಾಗ್ಯೂ Intel® AMT ಸ್ಥಳೀಯ ಪೋರ್ಟ್‌ಗಳನ್ನು ಮುಚ್ಚಲು ಮತ್ತು ಈ ಮಾಹಿತಿಗೆ ಪ್ರವೇಶವನ್ನು ಮಿತಿಗೊಳಿಸಲು ನಿರ್ವಾಹಕರು ಪರಿಸರ ಪತ್ತೆಮಾಡುವಿಕೆ ಮತ್ತು ಸಹಾಯಕ್ಕಾಗಿ ಫಾಸ್ಟ್ ಕಾಲ್ (CIRA) ಅನ್ನು ಬಳಸಬಹುದು.

ದೃಢೀಕರಿಸಲ್ಪಟ್ಟ IT ನಿರ್ವಾಹಕರು ಏನನ್ನು ಮಾಡಲು Intel AMT ಅನುಮತಿಸುತ್ತದೆ?

- ಟ್ರಬಲ್‌ಶೂಟಿಂಗ್ ಮತ್ತು ರಿಪೇರಿಗಾಗಿ ದೂರಸ್ಥವಾಗಿ ಸಿಸ್ಟಂ ಅನ್ನು ಪವರ್ ಅಪ್, ಪವರ್ ಡೌನ್ ಮತ್ತು ರೀಬೂಟ್ ಮಾಡುವುದು.
- ಹೋಸ್ಟ್ OS ಆಫ್ ಆಗಿರುವಾಗ ಅಥವಾ ಹಾಳಾಗಿರುವಾಗಲೂ ಸಹ ದೂರಸ್ಥವಾಗಿ ಸಿಸ್ಟಂ ಟ್ರಬಲ್‌ಶೂಟ್ ಮಾಡುವುದು.
- ಸಿಸ್ಟಂನಲ್ಲಿನ BIOS ಕಾನ್ಫಿಗರೇಷನ್‌ಗಳನ್ನು ದೂರಸ್ಥವಾಗಿ ವಿಮರ್ಶಿಸುವುದು ಮತ್ತು ಬದಲಾಯಿಸುವುದು. BIOS ಪಾಸ್‌ವರ್ಡ್ ಅನ್ನು ಹಾದುಹೋಗಲು IT ನಿರ್ವಾಹಕರಿಗೆ ಅವಕಾಶ ಕಲ್ಪಿಸುವ ಆಯ್ಕೆಯನ್ನು Intel AMT ಹೊಂದಿದೆ ಆದರೆ ಎಲ್ಲ OEM ಗಳು ಈ ವೈಶಿಷ್ಟ್ಯವನ್ನು ಜಾರಿಗೊಳಿಸುವುದಿಲ್ಲ.
- ಸಿಸ್ಟಂ ರಕ್ಷಿಸಲು ನೆಟ್‌ವರ್ಕ್ ಟ್ರಾಫಿಕ್ ಫಿಲ್ಟರ್‌ಗಳನ್ನು ಕಾನ್ಫಿಗರ್ ಮಾಡುವುದು.
- ಸಿಸ್ಟಂನಲ್ಲಿ ಜಾರಿಯಲ್ಲಿರುವ ನೋಂದಾಯಿತ ಅಪ್ಲಿಕೇಶನ್‌ಗಳ ಮೇಲೆ ನಿಗಾ ಇರಿಸುವುದು (ಉದಾಹರಣೆಗೆ, ಆ್ಯಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ರನ್ ಆಗುತ್ತಿದೆಯೇ).
- ತಾಂತ್ರಿಕ ಬೆಂಬಲ ಅಗತ್ಯವಿರಬಹುದಾದ ಬಳಕೆದಾರನ ಸಿಸ್ಟಂನಲ್ಲಿನ ಈವೆಂಟ್‌ಗಳನ್ನು ವರದಿ ಮಾಡುವ Intel AMT ಫರ್ಮ್‌ವೇರ್‌ನಿಂದ ಜನರೇಟ್ ಮಾಡಿದ ಅಲರ್ಟ್‌ಗಳನ್ನು ಸ್ವೀಕರಿಸುವುದು, ಉದಾಹರಣೆಗೆ: CPU ಬಿಸಿಯಾಗುವಿಕೆ, ಫ್ಯಾನ್ ವೈಫಲ್ಯ ಅಥವಾ ಸಿಸ್ಟಂ

ಡಿಫೆನ್ಸ್ ಫಿಲ್ಟರ್ ಟ್ರಿಪ್ಪಿಂಗ್. ಇನ್ನಷ್ಟು ಉದಾಹರಣೆಗಳು ಸಾರ್ವಜನಿಕವಾಗಿ ಇಲ್ಲಿ ಲಭ್ಯ ಇವೆ www.intel.com/software/manageability.

- ಬೂಸ್ಟ್ ಪ್ರಕ್ರಿಯೆಯನ್ನು ಫ್ಲಾಪಿ ಡಿಸ್ಕ್, CD-ROM ಅಥವಾ IT ನಿರ್ವಾಹಕರ ಸಿಸ್ಟಂನಲ್ಲಿ ಇರುವ ಇಮೇಜ್‌ಗೆ ಮರುನಿರ್ದೇಶಿಸುವ ಮೂಲಕ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂ ಅನ್ನು ದೂರಸ್ಥವಾಗಿ ಟ್ರಬಲ್‌ಶೂಟ್ ಮಾಡುವುದು.
- ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗಳಲ್ಲಿ ಕೀಬೋರ್ಡ್ ಇನ್‌ಪುಟ್ ಮತ್ತು ಪಠ್ಯ-ಮೋಡ್ ವೀಡಿಯೊ ಔಟ್‌ಪುಟ್ ಅನ್ನು IT ನಿರ್ವಾಹಕರ ಸಿಸ್ಟಂಗೆ ಮರುನಿರ್ದೇಶಿಸುವ ಮೂಲಕ ಸಿಸ್ಟಂ ಅನ್ನು ದೂರಸ್ಥವಾಗಿ ಟ್ರಬಲ್‌ಶೂಟ್ ಮಾಡುವುದು.
- ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗೆ ಮತ್ತು ಸಿಸ್ಟಂನಿಂದ ಕೀಬೋರ್ಡ್, ವೀಡಿಯೊ ಮತ್ತು ಮೌಸ್ ಅನ್ನು IT ನಿರ್ವಾಹಕರ ಸಿಸ್ಟಂಗೆ (KVM ಮರುನಿರ್ದೇಶನ) ಮರುನಿರ್ದೇಶಿಸುವ ಮೂಲಕ ದೂರಸ್ಥವಾಗಿ ಸಿಸ್ಟಂ ಅನ್ನು ಟ್ರಬಲ್‌ಶೂಟ್ ಮಾಡುವುದು.
- Intel AMT ನಿರ್ವಹಣೆಯ ಕಾರ್ಯವೈಶಿಷ್ಟ್ಯ ಯಾವ ನೆಟ್‌ವರ್ಕ್ ವಾತಾವರಣಗಳಲ್ಲಿ ಪ್ರವೇಶಸಾಧ್ಯವಾಗಿರುತ್ತದೆ ಎನ್ನುವುದನ್ನು ಕಾನ್ಫಿಗರ್ ಮಾಡುವುದು (ಉದಾಹರಣೆಗೆ, ವಿಶ್ವಾಸಾರ್ಹ ಡೊಮೇನ್‌ಗಳನ್ನು ವ್ಯಾಖ್ಯಾನಿಸುವ ಮೂಲಕ).
- ಫ್ಲಾಶ್ ರೆಪೊಸಿಟರಿಯಲ್ಲಿ (ಅಂದರೆ 3PDS ಪ್ರದೇಶದಲ್ಲಿ) ಡೇಟಾ ಬರೆಯಲು/ಅಳಿಸಲು ನೋಂದಾಯಿತ ISV ಅಪ್ಲಿಕೇಶನ್ ಬಳಸುವುದು
- ಕ್ಲಯಂಟ್ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ನಲ್ಲಿ ಸ್ಥಳೀಯವಾಗಿ Intel AMT ನಿರ್ವಹಿಸುವ (Intel AMT 11.6 ಮತ್ತು ಹೊಸತು) ನಾನ್-ವೊಲಟೈಲ್ ಮೆಮೊರಿಯಲ್ಲಿ (NVM) ವೆಬ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ಹೋಸ್ಟ್ ಮಾಡುವುದು.
- UUID ಮೂಲಕ ಉದ್ಯಮ ನೆಟ್‌ವರ್ಕ್‌ನಲ್ಲಿ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂ ಗುರುತಿಸುವುದು.
- Intel AMT ಅನ್ನು ಅನ್‌ಪ್ರೊವಿಷನ್ ಮಾಡುವುದು ಮತ್ತು ಫ್ಲ್ಯಾಶ್ ಕಂಟೆಂಟ್ ಅಳಿಸುವುದು.
- ಮುಂಚಿತವಾಗಿ ಕಾನ್ಫಿಗರ್ ಮಾಡಿದ ಕ್ಲಯಂಟ್-ಆರಂಭಿಸಿದ-ರಿಮೋಟ್-ಆ್ಯಕ್ಸೆಸ್ (CIRA) ಪ್ರೊಫೈಲ್‌ಗಳನ್ನು ಬಳಸಿಕೊಂಡು ಎಂಟರ್‌ಪ್ರೈಸ್ ನೆಟ್‌ವರ್ಕ್‌ನ ಹೊರಗೂ ಸಹ ಸಿಸ್ಟಂಗಳಿಗೆ ದೂರಸ್ಥವಾಗಿ ಕನೆಕ್ಟ್ ಮಾಡುವುದು.

ಬಳಕೆದಾರರ ಸ್ಥಳೀಯ ಹಾರ್ಡ್‌ಡ್ರೈವ್(ಗಳ)ನ್ನು ಪ್ರವೇಶಿಸಲು ದೃಢೀಕರಿಸಿರುವ IT ನಿರ್ವಾಹಕರಿಗೆ Intel AMT ಅವಕಾಶ ನೀಡುತ್ತದೆಯೇ?

ದೂರಸ್ಥ ನಿರ್ವಹಣೆ ಸೆಷನ್ ಸಂದರ್ಭ, IT ನಿರ್ವಾಹಕರು ಬಳಕೆದಾರರ ಸ್ಥಳೀಯ ಹಾರ್ಡ್ ಡ್ರೈವ್‌ಗಳಿಗೆ ಪ್ರವೇಶ ಹೊಂದಿರುತ್ತಾರೆ. ಇದರ ಅರ್ಥ, ಬಳಕೆದಾರರ ಹಾರ್ಡ್ ಡಿಸ್ಕ್‌ನಿಂದ IT ನಿರ್ವಾಹಕರು ಫೈಲ್‌ಗಳನ್ನು ಓದಬಹುದು/ಬರೆಯಬಹುದು, ಉದಾಹರಣೆಗೆ, ದೋಷಪೂರಿತ ಅಪ್ಲಿಕೇಶನ್ ಅಥವಾ OS ಅನ್ನು ರಿಕವರ್ ಅಥವಾ ಮರುಸ್ಥಾಪನೆ ಮಾಡುವ ಮೂಲಕ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂ ರಿಪೇರಿ ಮಾಡಲು. ಈ ರೀತಿಯ ಮಾಹಿತಿಗೆ ಪ್ರವೇಶವನ್ನು IT ನಿರ್ವಾಹಕರಿಗೆ ಒದಗಿಸುವುದರಿಂದ ಉಂಟಾಗುವ ಸಂಭಾವ್ಯ ಗೌಪ್ಯತೆ ಅಪಾಯಗಳನ್ನು ನಿವಾರಿಸಲು ಸಹಾಯ ಮಾಡುವ ಎರಡು ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು Intel AMT ಬೆಂಬಲಿಸುತ್ತದೆ: IMSS ಮತ್ತು ಆಡಿಟ್ ಲಾಗಿಂಗ್. Intel AMT ಮೂಲಕ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗಳಿಗೆ IT ನಿರ್ವಾಹಕರ ಪ್ರವೇಶದ

ಸಂದರ್ಭಗಳನ್ನು ಲಾಗ್ ಮಾಡುವ ಮೂಲಕ ನಿರ್ವಾಹಕರ ಉತ್ತರದಾಯಿತ್ವದ ಒಂದು ಪದರವನ್ನು ಆಡಿಟ್ ಲಾಗಿಂಗ್ ಸಾಮರ್ಥ್ಯಗಳು ಒದಗಿಸುತ್ತವೆ. ಅದಾಗ್ಯೂ, ಯಾವ ಈವೆಂಟ್‌ಗಳನ್ನು ನೈಜವಾಗಿ ಲಾಗ್ ಮಾಡಲಾಗುತ್ತದೆ ಎನ್ನುವುದನ್ನು ಆಡಿಟರ್ ನಿರ್ಣಯಿಸುತ್ತಾರೆ, ಸಾಮಾನ್ಯವಾಗಿ ಸಂಸ್ಥೆಯಲ್ಲಿ ಅವರು ಬಳಕೆದಾರ ಆಗಿರುವುದಿಲ್ಲ. Intel AMT ಸಿಸ್ಟಂಗೆ ದೂರಸ್ಥ ಪ್ರವೇಶವು ಲಾಗ್ ಮಾಡಬೇಕಾದ ಮಾಹಿತಿಯ ವಿಧವಾಗಿದೆ ಎಂದು ತನ್ನ ಬಳಕೆದಾರರಿಗೆ Intel ಶಿಫಾರಸು ಮಾಡುತ್ತದಾದರೂ, ಕೆಲವು ಸಂಸ್ಥೆಗಳ ಪರಿಸರದಲ್ಲಿ ಬಳಕೆದಾರರಿಗೆ ಈ ಮಾಹಿತಿ ಲಭ್ಯವಿಲ್ಲದಿರುವ ಸಾಧ್ಯತೆಯಿದೆ. ಬಳಕೆದಾರರ ಸಿಸ್ಟಂಗಳನ್ನು IT ನಿರ್ವಾಹಕರು ಪ್ರವೇಶಿಸಿರುವ ಸಂದರ್ಭಗಳ ಸೂಚನೆಗಳನ್ನು IMSS ಹೇಗೆ ಬಳಕೆದಾರರಿಗೆ ಒದಗಿಸುತ್ತದೆ ಎನ್ನುವುದಕ್ಕೆ ಸಂಬಂಧಿಸಿದ ಮಾಹಿತಿಯನ್ನು ತಕ್ಷಣವೇ ಕೆಳಗೆ ಒದಗಿಸಲಾಗಿದೆ.

ತಮ್ಮ ಕೀಬೋರ್ಡ್‌ನೆದುರು ಭೌತಿಕವಾಗಿ ಕುಳಿತಿರುವ ರೀತಿಯಲ್ಲಿ ಒಬ್ಬ ಬಳಕೆದಾರನ PC ಯ ದೂರಸ್ಥ ನಿಯಂತ್ರಣವನ್ನು ತೆಗೆದುಕೊಳ್ಳಲು ದೃಢೀಕರಿಸಿದ IT ನಿರ್ವಾಹಕರಿಗೆ Intel AMT KVM ಮರುನಿರ್ದೇಶನ ಅನುಮತಿಸುತ್ತದೆಯೇ?

KVM ಮರುನಿರ್ದೇಶನದೊಂದಿಗೆ ದೂರಸ್ಥ ನಿರ್ವಹಣೆ ಸೆಷನ್ ಸಂದರ್ಭ, ಬಳಕೆದಾರರ PC ಯ ಕೀಬೋರ್ಡ್ ಎದುರು ಕುಳಿತಿರುವ ರೀತಿಯಲ್ಲಿ IT ನಿರ್ವಾಹಕರು ನಿಯಂತ್ರಣ ಹೊಂದಿರುವುದಿಲ್ಲ. KVM ಮರುನಿರ್ದೇಶನ ಸೆಷನ್‌ಗೆ ಸಂಬಂಧಿಸಿದಂತೆ, KVM ಬಳಕೆದಾರ ಸಮ್ಮತಿ ಎಂದು ಕರೆಯಲಾಗುವ, ಬಳಕೆದಾರರಿಂದ ಸ್ಪಷ್ಟ ಸಮ್ಮತಿಯಿಲ್ಲದೆ ಒಂದು KVM ಸೆಷನ್ ಆರಂಭಿಸಲಾಗದ ಅಗತ್ಯವನ್ನು Intel AMT ಸಕ್ರಿಯಗೊಳಿಸುತ್ತದೆ. ಮರುನಿರ್ದೇಶನ ಸೆಷನ್‌ಗೆ ಆಪ್ಟ್-ಇನ್ ಮಾಡುವುದಕ್ಕೆ ಬಳಕೆದಾರರ ಸಮ್ಮತಿಯನ್ನು ಜಾರಿಗೊಳಿಸಲು, ಯಾವುದೇ ಇತರ ವಿಂಡೋದ ಮೇಲೆ, ಬಳಕೆದಾರರ ಸ್ಕ್ರೀನ್‌ನಲ್ಲಿ ಸುರಕ್ಷಿತ ಔಟ್‌ಪುಟ್ ವಿಂಡೋವನ್ನು ("ಸ್ಪ್ಲಾಟ್") ಪ್ರದರ್ಶಿಸಲಾಗುತ್ತದೆ, ಅದರಲ್ಲಿ ಯಾದೃಚ್ಛಿಕವಾಗಿ ಜನರೇಟ್ ಮಾಡಿದ ಸಂಖ್ಯೆಯನ್ನು IT ನಿರ್ವಾಹಕರಿಗೆ ಓದಿ ಹೇಳುವಂತೆ ಬಳಕೆದಾರರಿಗೆ ಸೂಚಿಸಲಾಗುತ್ತದೆ. IT ನಿರ್ವಾಹಕರು ಸರಿಯಾದ ಸೆಷನ್ ಸಂಖ್ಯೆಯನ್ನು ಟೈಪ್ ಮಾಡಿದರೆ ಮಾತ್ರ KVM ಸೆಷನ್ ಆರಂಭವಾಗುತ್ತದೆ. ಒಮ್ಮೆ ಮಾನ್ಯವಾದ KVM ಸೆಷನ್ ಆರಂಭಿಸಿದ ಬಳಿಕ, ಬಳಕೆದಾರರ ಸಂಪೂರ್ಣ ಸ್ಕ್ರೀನ್ ಕೆಂಪು ಮತ್ತು ಹಳದಿ ಅಂಚುಗಳ ಫ್ಲ್ಯಾಶಿಂಗ್‌ನೊಂದಿಗೆ ಆವೃತವಾಗುತ್ತದೆ – ಇದು IT ನಿರ್ವಾಹಕರು KVM ಪರಿಹಾರ ಸೆಷನ್ ಪ್ರಕ್ರಿಯೆಯಲ್ಲಿದ್ದಾರೆ ಎನ್ನುವುದನ್ನು ಸೂಚಿಸುತ್ತದೆ. ಸೆಷನ್ ಸಕ್ರಿಯವಾಗಿರುವ ತನಕ ಈ ಕೆಂಪು ಮತ್ತು ಹಳದಿ ಅಂಚುಗಳ ಫ್ಲ್ಯಾಶಿಂಗ್ ಇರುತ್ತದೆ. Intel AMT ಸಿಸ್ಟಂ ಕ್ಲಯಂಟ್ ಕಂಟ್ರೋಲ್ ಮೋಡ್‌ನಲ್ಲಿರುವಾಗ KVM ಬಳಕೆದಾರ ಸಮ್ಮತಿ ಕಡ್ಡಾಯವಾಗಿರುತ್ತದೆ ಆದರೆ ಅಡ್ಮಿನ್ ಕಂಟ್ರೋಲ್ ಮೋಡ್‌ನಲ್ಲಿರುವಾಗ ಐಚ್ಛಿಕವಾಗಿರುತ್ತದೆ ಎನ್ನುವುದನ್ನು ಗಮನಿಸಿ.

OEM ನ ಸೆಟ್ಟಿಂಗ್‌ಗಳ ಅನುಸಾರ, Intel AMT ಯಲ್ಲಿ SOL/IDER ಅಥವಾ KVM ವೈಶಿಷ್ಟ್ಯಗಳನ್ನು BIOS ಅಥವಾ Intel® Management Engine BIOS Extension (Intel® MEBX) ಸಕ್ರಿಯಗೊಳಿಸಬಹುದು ಅಥವಾ ನಿಷ್ಕ್ರಿಯಗೊಳಿಸಬಹುದು. KVM ಆಪ್ಟ್-ಇನ್ ಅಗತ್ಯವನ್ನು BIOS ಸೆಟ್ಟಿಂಗ್‌ಗಳು ಅಥವಾ Intel AMT ಕಾನ್ಫಿಗರೇಷನ್ ಸೆಟ್ಟಿಂಗ್‌ಗಳ ಮೂಲಕ IT

ನಿರ್ವಾಹಕರು ಬದಲಾಯಿಸಬಹುದು. ಬಳಕೆದಾರರ ಗೌಪ್ಯತೆಯನ್ನು ಕಾಪಾಡುವ ಸಲುವಾಗಿ ಅವರ ಸಮ್ಮತಿಗಾಗಿ ಬಾಧ್ಯತೆಯನ್ನು ಬಳಸುವಂತೆ Intel ಶಿಫಾರಸು ಮಾಡುತ್ತದೆ.

Intel AMT ಮೂಲಕ IT ನಿರ್ವಾಹಕರು ಸಿಸ್ಟಂ ಪ್ರವೇಶಿಸಿದ್ದಾರೆಯೇ ಎಂದು ಬಳಕೆದಾರ ಹೇಗೆ ಹೇಳಬಹುದು?

ಒಂದು ದೂರಸ್ಥ ಮರುನಿರ್ದೇಶನ ಸೆಷನ್‌ನ (ಅಂದರೆ, SOL/IDER) ಓಪನಿಂಗ್/ಕ್ಲೋಸಿಂಗ್ ಮೂಲಕ ಅವರ ಸಿಸ್ಟಂ ಅನ್ನು IT ನಿರ್ವಾಹಕರು ಪ್ರವೇಶಿಸುತ್ತಿದ್ದಾರೆಯೇ ಅಥವಾ ಪ್ರವೇಶಿಸಿದ್ದಾರೆಯೇ ಎನ್ನುವ ಕುರಿತು ಹಾಗೂ ಒಬ್ಬ IT ನಿರ್ವಾಹಕರಿಂದ ಬಳಕೆದಾರರ ಸಿಸ್ಟಂ ಡಿಫೆನ್ಸ್ ಸಕ್ರಿಯಗೊಳಿಸುವಿಕೆ ಮತ್ತು ರಿಮೋಟ್ ಬೂಟ್ ಸೇರಿದಂತೆ, ಹಲವಾರು ಈವೆಂಟ್‌ಗಳಿಗಾಗಿ ಬಳಕೆದಾರ ಸೂಚನೆಗಳನ್ನು IMSS ಸಿಸ್ಟಂ ಟ್ರೇ ಐಕಾನ್ ಸಕ್ರಿಯಗೊಳಿಸುತ್ತದೆ ಮತ್ತು ಬೆಂಬಲಿಸುತ್ತದೆ. ಹೆಚ್ಚುವರಿಯಾಗಿ, ಸಕ್ರಿಯ ದೂರಸ್ಥ ಮರುನಿರ್ದೇಶನ ಸೆಷನ್ ಸಂದರ್ಭ ಸ್ಕ್ರೀನ್‌ನ ಮೇಲ್ಭಾಗದ ಬಲಬದಿಯಲ್ಲಿ ಫ್ಲ್ಯಾಶಿಂಗ್ ಐಕಾನ್ ಕಾಣಿಸುತ್ತದೆ. ಅದಾಗ್ಯೂ, ಒಂದು ಸಂಸ್ಥೆಯ ಸೆಟ್ಟಿಂಗ್‌ನಲ್ಲಿ IMSS ನಿಂದ ನೈಜವಾಗಿ ಸಕ್ರಿಯಗೊಳಿಸಿದ ಈವೆಂಟ್‌ಗಳು IT ನಿರ್ವಾಹಕರಿಂದ ನಿರ್ಣಯಿಸಲ್ಪಡುತ್ತವೆ, ಬಳಕೆದಾರನಿಂದಲ್ಲ. Intel AMT ಸಿಸ್ಟಂಗಳನ್ನು ನಿಯೋಜಿಸುವ ಸಂಸ್ಥೆಗಳು ಈ ಪ್ಯಾರಾದಲ್ಲಿ ಉಲ್ಲೇಖಿಸಿರುವ IMSS ಸೂಚನೆಗಳನ್ನು ಸಕ್ರಿಯಗೊಳಿಸುವಂತೆ Intel ಶಿಫಾರಸು ಮಾಡುತ್ತದೆಯಾದರೂ, Intel AMT ಸಿಸ್ಟಂಗೆ ದೂರಸ್ಥ ಸಂಪರ್ಕಗಳಿಗೆ ಸಂಬಂಧಿಸಿದ ಮಾಹಿತಿಯು ಎಲ್ಲ ಬಳಕೆದಾರರಿಗೆ ಲಭ್ಯವಿಲ್ಲದಿರುವ ಸಾಧ್ಯತೆಯಿದೆ.

ಎಲ್ಲ Intel AMT ಕಾನ್ಫಿಗರೇಷನ್ ಮತ್ತು ಖಾಸಗಿ ಡೇಟಾವನ್ನು ಬಳಕೆದಾರ ಹೇಗೆ ತೆರವುಗೊಳಿಸಬಹುದು?

Intel AMT ಸಿಸ್ಟಂ ಅನ್ನು ಭಾಗಶಃ/ಪೂರ್ಣವಾಗಿ ಅನ್‌ಪ್ರೊವಿಷನ್ ಮಾಡಲು Intel AMT, BIOS ಆಯ್ಕೆಗಳನ್ನು ಒದಗಿಸುತ್ತದೆ. ಮರುಮಾರಾಟ/ಮರುಸಂಸ್ಕರಣೆ ಮಾಡುವುದಕ್ಕೂ ಮುನ್ನ ಸಿಸ್ಟಂ ಅನ್ನು ಪೂರ್ಣವಾಗಿ ಅನ್‌ಪ್ರೊವಿಷನ್ ಮಾಡುವಂತೆ ಹಾಗೂ ಒಂದು ವೇಳೆ ನೀವು Intel AMT ಸಾಮರ್ಥ್ಯವಿರುವ ಬಳಕೆ ಮಾಡಿದ ಸಿಸ್ಟಂ ಅನ್ನು ಖರೀದಿಸುವುದಾದರೆ Intel AMT ಅನ್ನು ಪೂರ್ಣವಾಗಿ ಅನ್‌ಪ್ರೊವಿಷನ್ ಮಾಡಲಾಗಿದೆಯೇ ಎಂದು ಪರಿಶೀಲಿಸುವಂತೆ ಅಂತಿಮ ಬಳಕೆದಾರರಿಗೆ Intel ಶಿಫಾರಸು ಮಾಡುತ್ತದೆ.

ಗೌಪ್ಯತೆ ಹೇಳಿಕೆ ಅಪ್‌ಡೇಟ್‌ಗಳು

ಈ ಗೌಪ್ಯತೆ ಹೇಳಿಕೆಯನ್ನು ನಾವು ಸಾಂದರ್ಭಿಕವಾಗಿ ಅಪ್‌ಡೇಟ್ ಮಾಡಬಹುದು. ನಾವು ಮಾಡಿದಾಗ, ಗೌಪ್ಯತೆ ಹೇಳಿಕೆಯ ಮೇಲ್ಭಾಗದಲ್ಲಿ ಕೊನೆಯದಾಗಿ ಅಪ್‌ಡೇಟ್ ಮಾಡಿದ ದಿನಾಂಕವನ್ನು ನಾವು ಪರಿಷ್ಕರಿಸುತ್ತೇವೆ.

ಹೆಚ್ಚಿನ ಮಾಹಿತಿಗಾಗಿ

ಈ ಗೌಪ್ಯತೆ ಪೂರಕ ಹೇಳಿಕೆಯ ಕುರಿತು ನಿಮ್ಮಲ್ಲಿ ಯಾವುದೇ ಪ್ರಶ್ನೆಗಳಿದ್ದರೆ ಅಥವಾ ಹೆಚ್ಚಿನ ಮಾಹಿತಿಯನ್ನು ಬಯಸಿದರೆ, ನಮ್ಮನ್ನು ಸಂಪರ್ಕಿಸಲು ದಯವಿಟ್ಟು

ಈ ನಮೂನೆಯನ್ನು ಬಳಸಿ.

ಗೌಪ್ಯತೆ ಸೂಚನೆ ಲಿಂಕ್‌ಗಳು

- Intel ಗೌಪ್ಯತೆ ಸೂಚನೆ
- ಅಭ್ಯರ್ಥಿ ಸೂಚನೆ