kaspersky

Kaspersky Security for Storage 製品紹介

2021年10月11日

株式会社カスペルスキー
セールスエンジニアリング部

Kaspersky Security for Storage

各種NASへのリアルタイム保護
多くの受賞歴を誇るカスペルスキーのエンジン。
プロアクティブなセキュリティを可能にする。

RPC と ICAPに準拠したNASのサポート
エンタープライズ市場で多く使用されるNASを保護。
高度な脅威から防御。

冗長性と負荷分散
冗長性を目的として複数の保護サーバーを構築可能。
NAS間の負荷を均衡させる。

ハイパフォーマンスと効率性
NASのパフォーマンスへの影響を抑えた、
最適化されたテクノロジー。

柔軟でパワフルなレポート機能
セキュリティの観点から、データストレージインフラストラクチャー全体を可視化

除外と信頼
セキュリティスキャンから除外する「信頼ゾーン」を作成、細かな設定を施したスキャンパフォーマンス。

アプリケーション起動コントロール
Windows Server上で、信頼されていない
アプリケーション、実行ファイルを起動させない。

ホストのブロック、アンチクリプター
Windows Server上の共有ファイルに対する危険な感染、ランサムウェアから保護。信頼出来ない
ホストからのアクセスをブロック

* Windows Serverのみ, NASに対しては動作しない

kaspersky

サポートされるプラットフォームとプロトコル

EMC²

- Isilon: OneFS
- Celerra/VNX:
- Unity など

ICAP
CAVA
CEE
OAS
ODS

NetApp Alliance Partner

- 7-mode
- Cluster-mode Data ONTAP
- ONTAP

RPC
OAS
ODS

ORACLE Gold Partner

- Oracle ZFS Storage: all appliances

ICAP
OAS

HITACHI Hitachi Data Systems Technology Alliance Partner

- Hitachi HNAS: 3080, 3090, 4040, 4060, 4080, 4100

ICAP
RPC
OAS

DELL

- DELL FS8600: FluidFS 5.x

ICAP
OAS

NUTANIX

Acropolis File Services

ICAP
OAS

Hewlett Packard Enterprise

HP 3PAR-Series

ICAP
OAS
ODS

OAS オンアクセススキャン
ODS オンデマンドスキャン

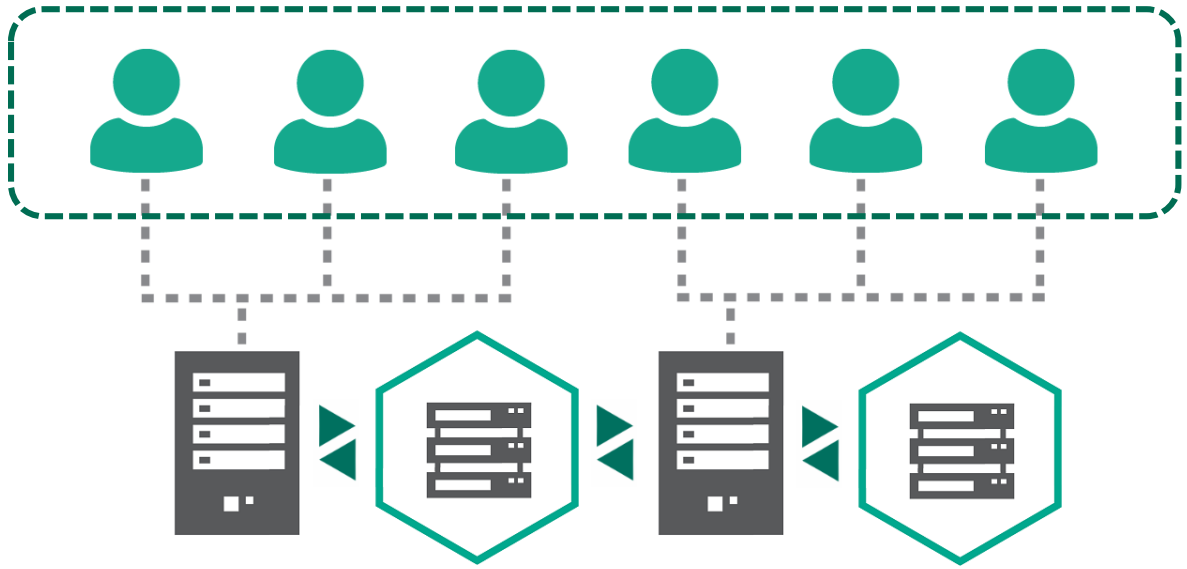
： P9へ

サポートNAS システム要件
https://support.kaspersky.com/KSWS/11.0.1/ja-jp/155511.htm

kaspersky

製品ライセンス体系

NASを使用するユーザー数（端末数）トータル数による課金

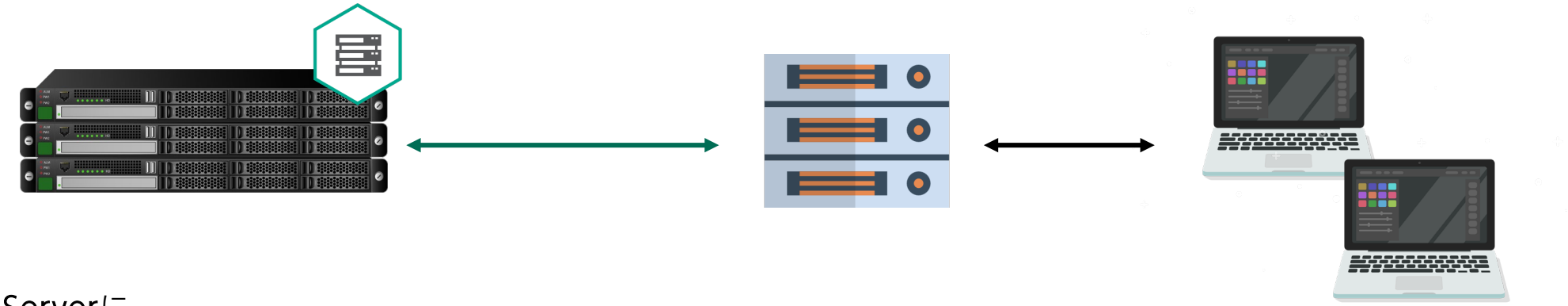


NASが複数台あり、 Kaspersky Security for Storageが複数台あっても、
使用するユーザー数（端末数）トータル数で計算すれば良い。

kaspersky

Kaspersky Security for Storage基本構成

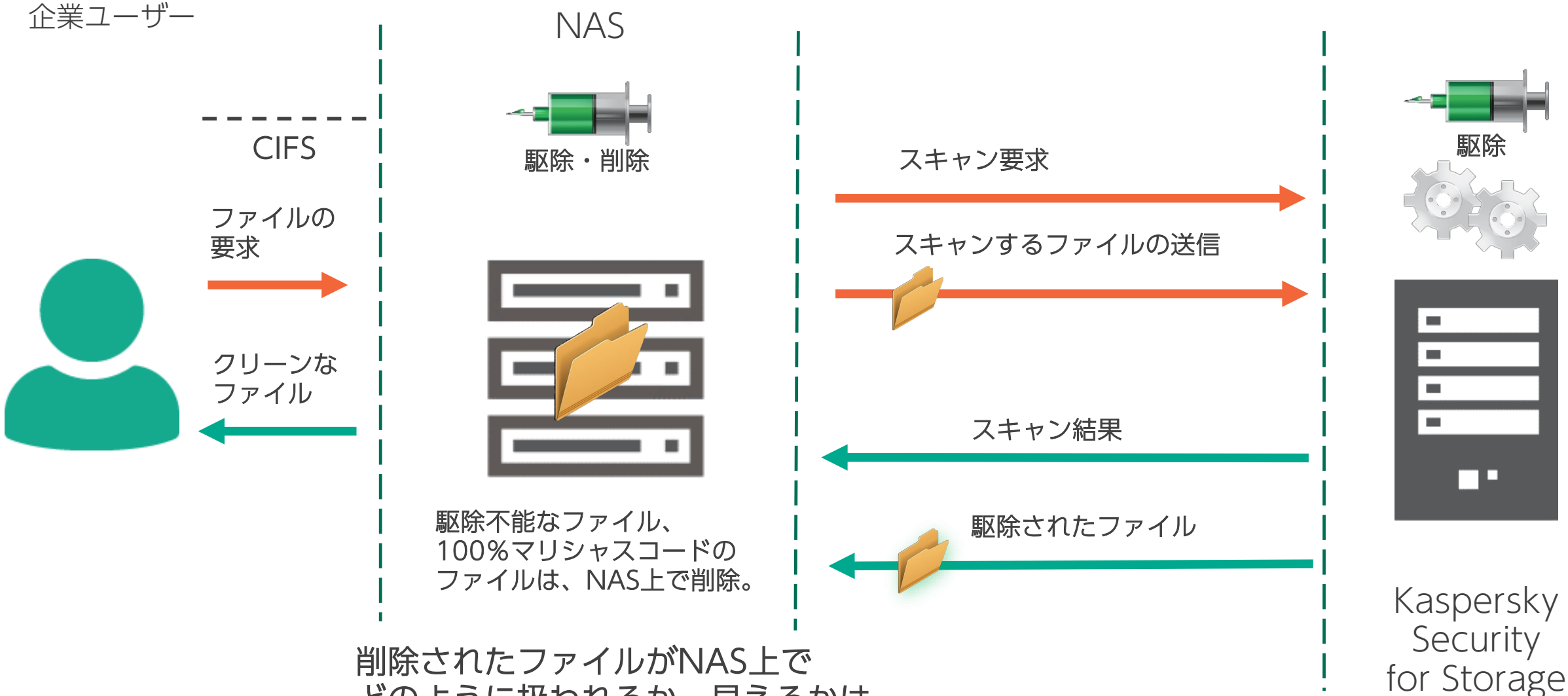
Kaspersky Security for Storage　　NAS　　NASの共有域にアクセス



Windows Serverに、
Kaspersky Security for Windows Serverをインストールし、
Kaspersky Security for Storageライセンスでアクティベート

kaspersky

ICAP (Internet Content Adaptation Protocol)

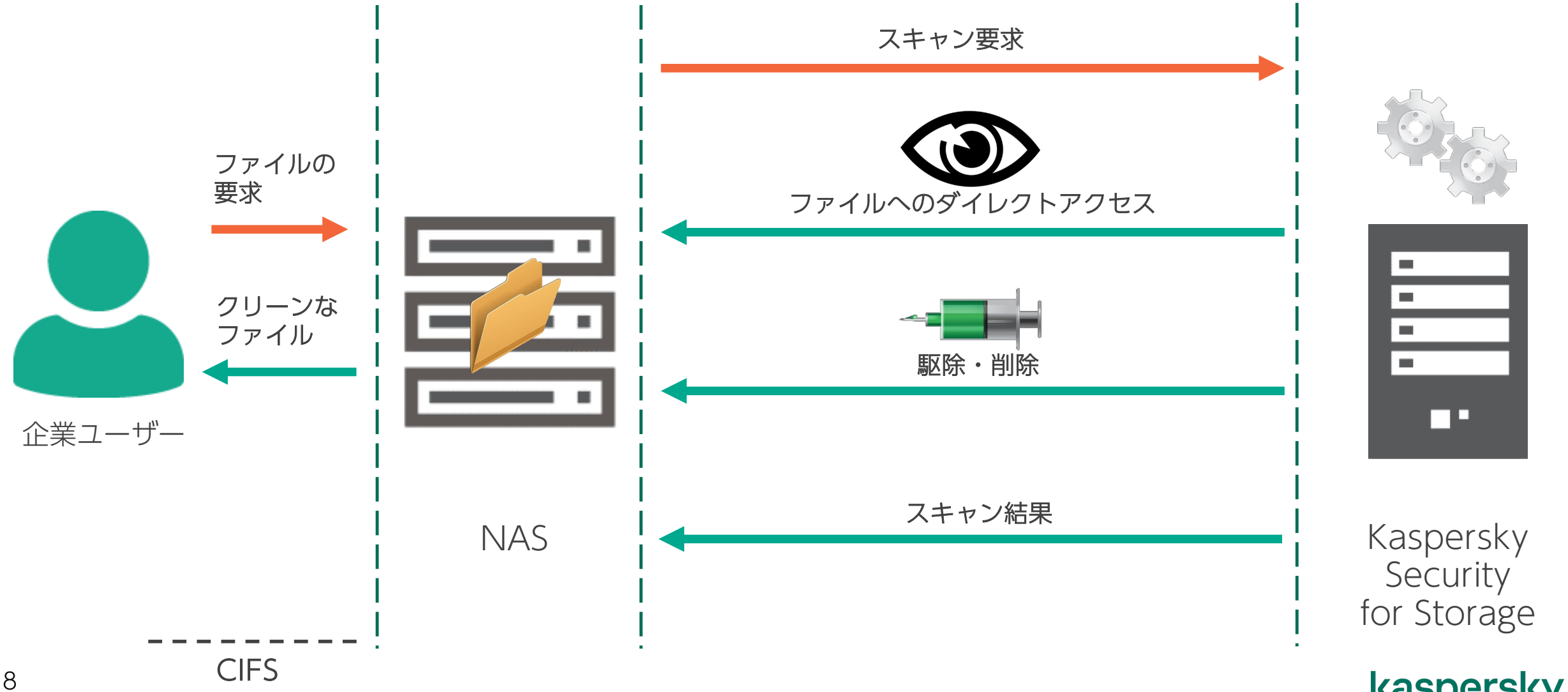


削除されたファイルがNAS上で
どのように扱われるか、見えるかは、
NASに依存する。

Kaspersky
Security
for Storage

kaspersky

RPC (remote procedure call)



kaspersky

Kaspersky Security for Storage　スキャンモード

オンアクセススキャンはユーザーのファイル操作が起点。
オンデマンドスキャンはNASのスケジュール実行が起点。NASに機能がなければ実行できない。

オンアクセススキャン

1. **ユーザー**がファイルをオープンや作成、変更しようとする。
2. NASが Kaspersky Security for Storageにファイルスキャンのために送信。
3. Kaspersky Security for Storage はファイルを処理し、NASに結果を通知。
4. Kaspersky Security for Storage のスキャン結果に従い、
   ユーザーはファイルへのアクセスを許可されるか、拒否される。

オンデマンドスキャン

1. **管理者**が、NAS上のオンデマンドスキャンタスクを追加し、実行する。
2. NASが Kaspersky Security for Storageにスキャンリクエストを送信
3. Kaspersky Security for Storage はファイルを処理し、NASに結果を通知。
4. NASはスキャン結果を記録する。

kaspersky

Kaspersky Security for Storage 管理方法

kaspersky

Kaspersky Security for Storageの管理

Kaspersky Security Center（KSC）による集中管理、
Kaspersky Securityコンソールによるローカル管理、
または、併用が可能。

併用の場合、KSCにロックをかけた項目を
ローカルコンソールで変更することは出来ない。
ロックしていない項目は、ローカル管理者に委ねられる。

kaspersky

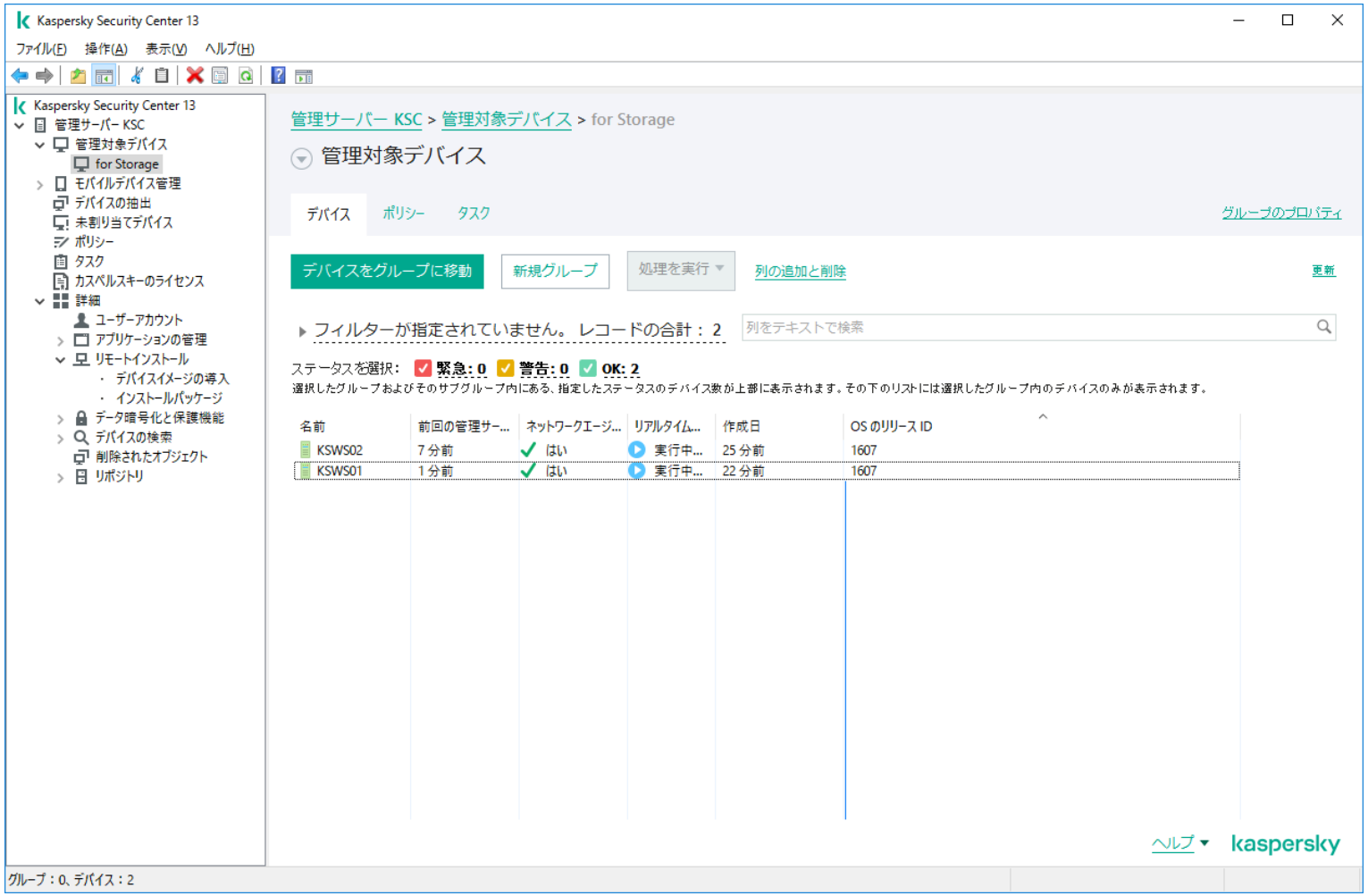
Kaspersky Security Center

シングルコンソールによる集中管理を可能にする、管理サーバー。
様々なアプリケーションを管理。

kaspersky

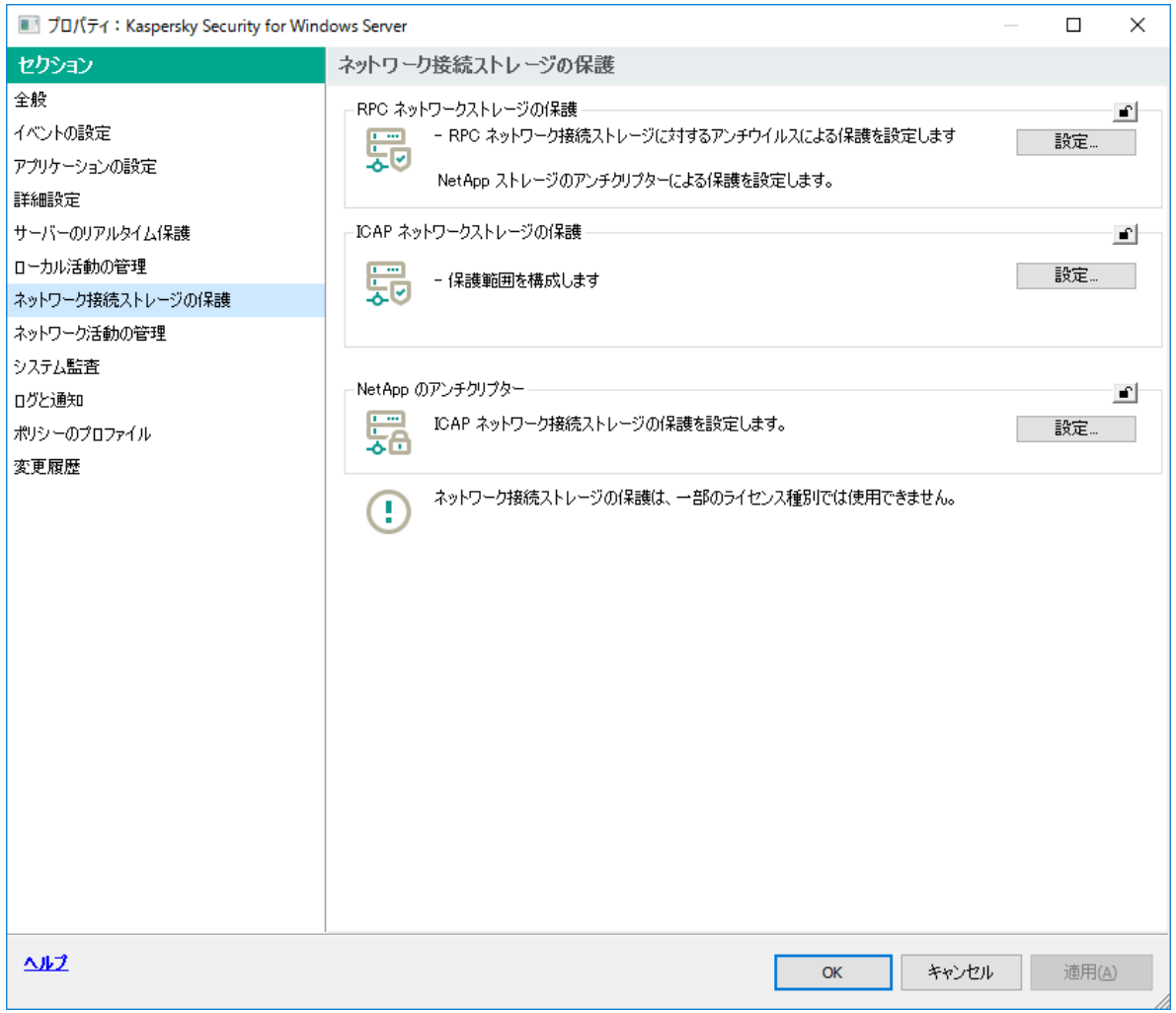
Kaspersky Security Center

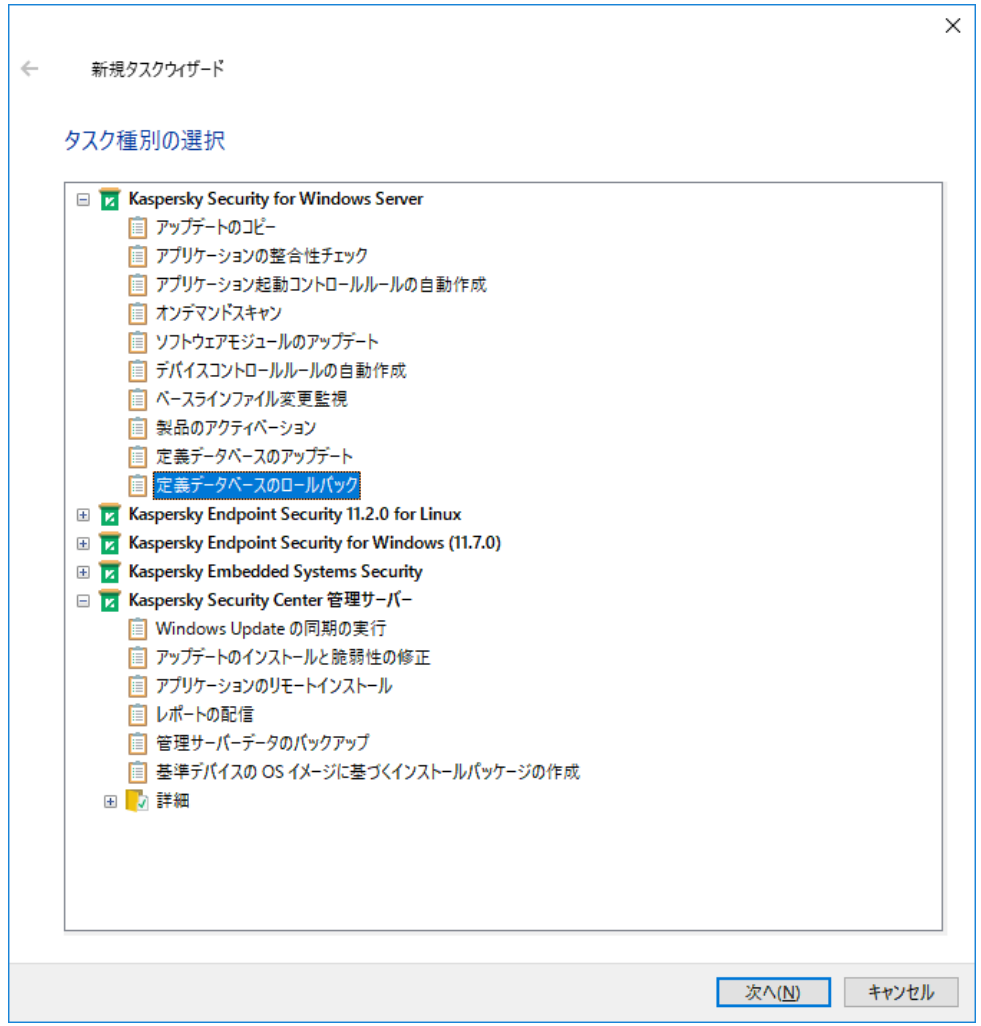
ポリシー・タスクによる一元管理、レポート。



kaspersky

ポリシー・タスク

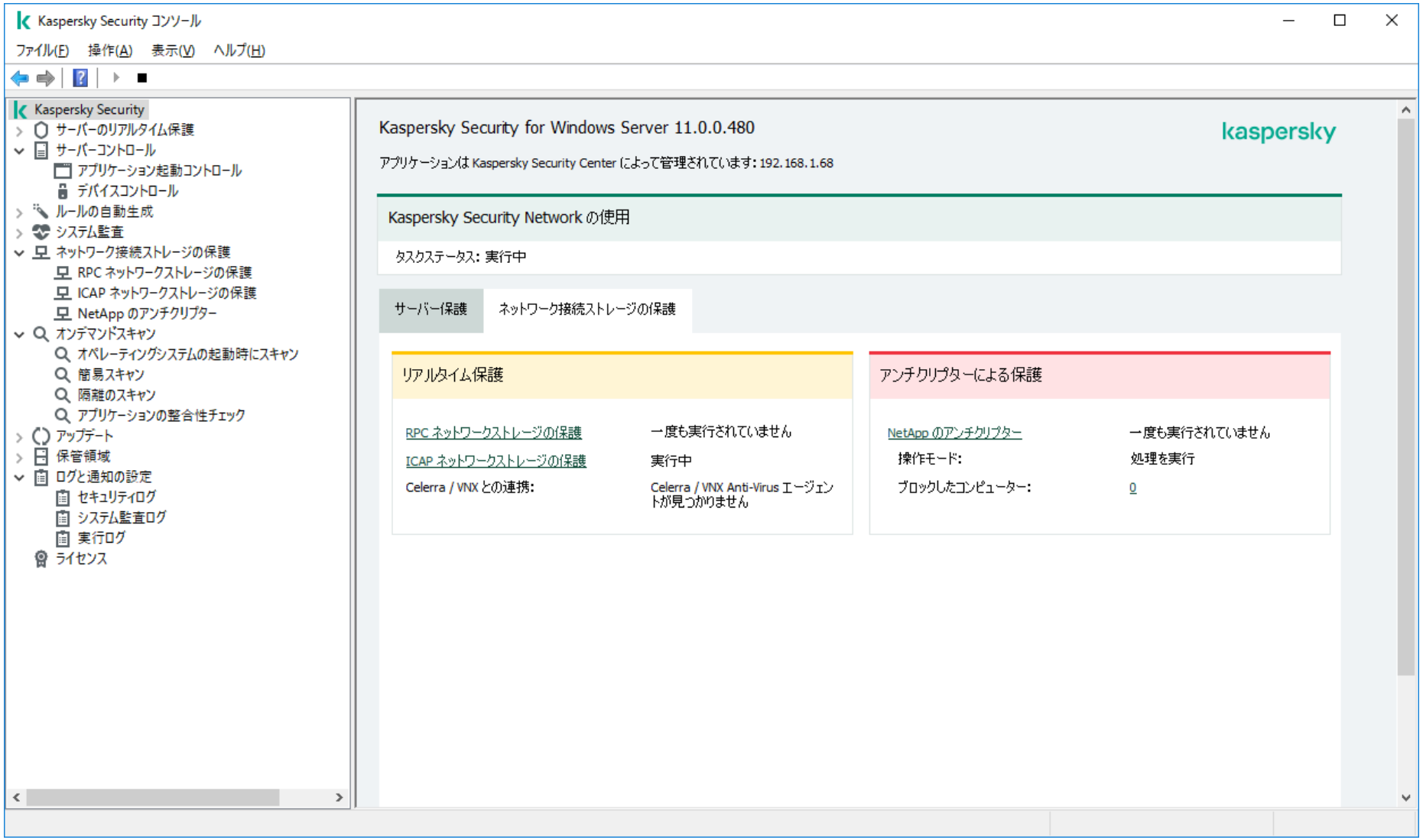




kaspersky

Kaspersky Security コンソール

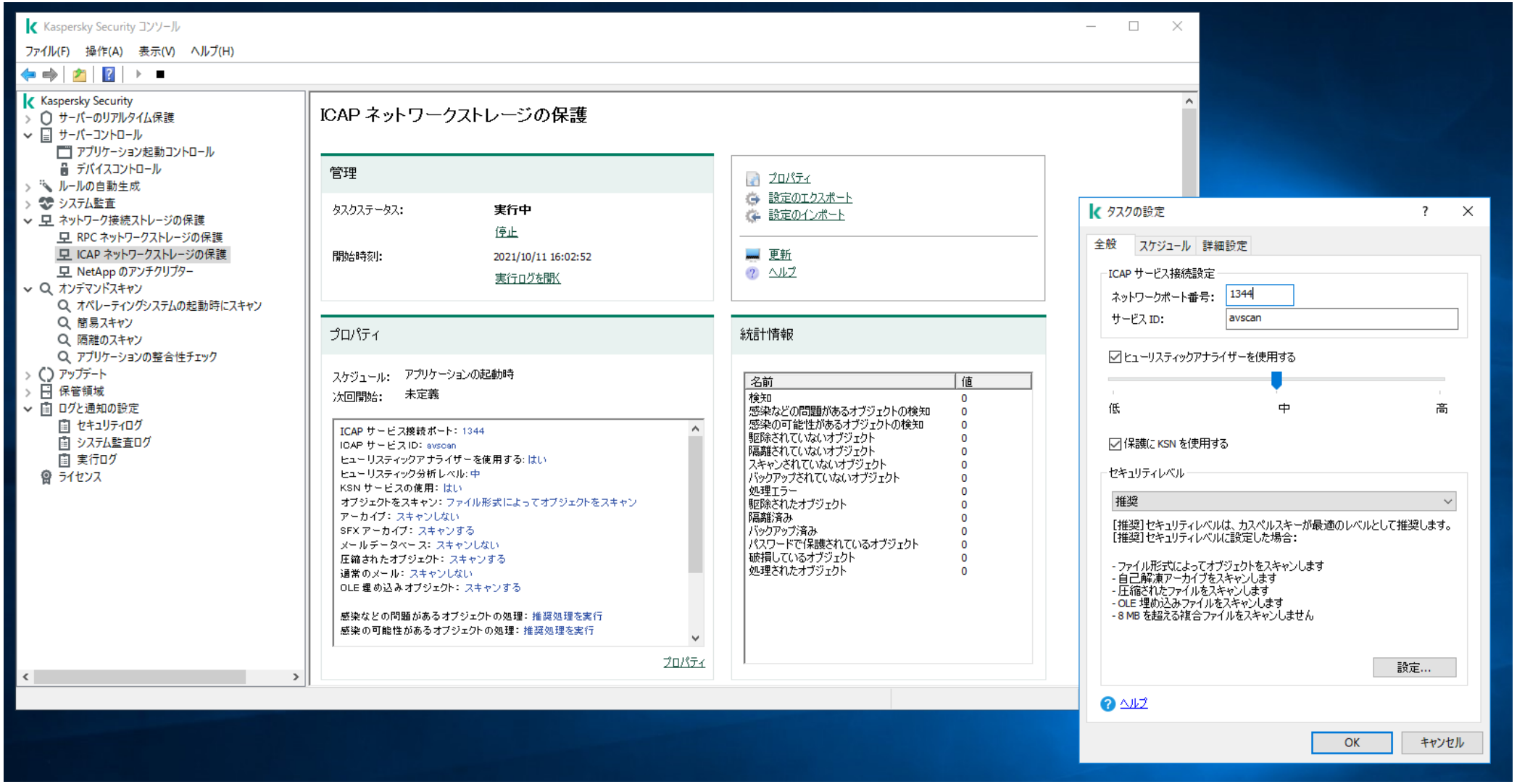
サーバー単位で管理。



kaspersky

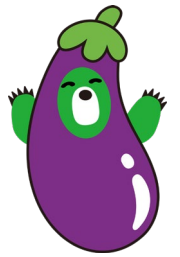
Kaspersky Security コンソール

ポリシー・タスク



kaspersky

高度なセキュリティ機能



kaspersky

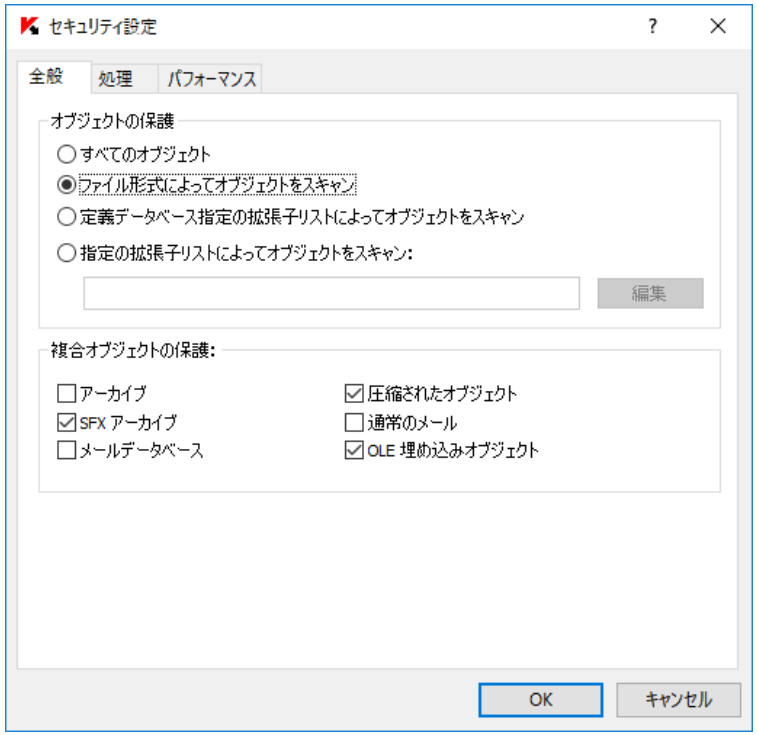
高度なセキュリティ機能

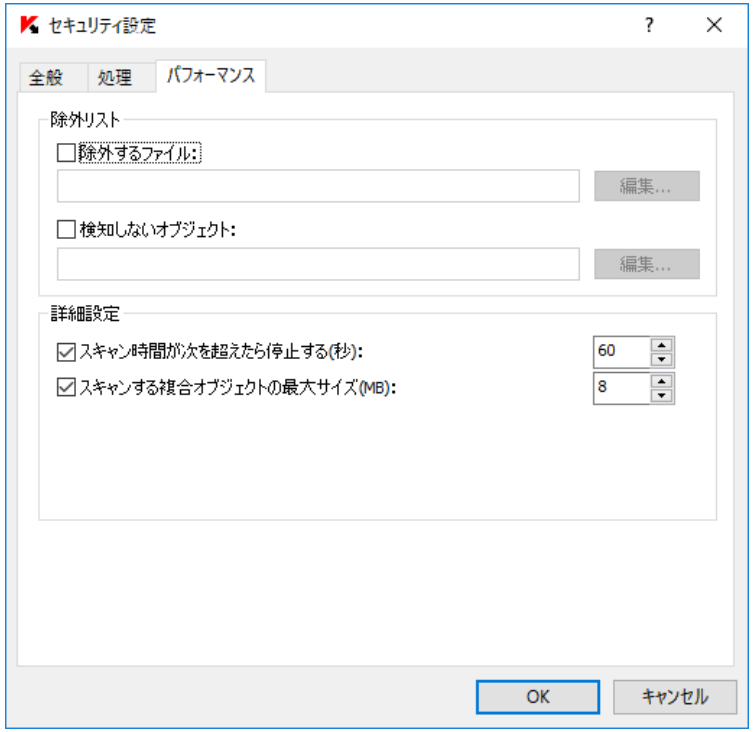
- ヒューリスティックによる検知
- KSNによる検知
- 定義のロールバック

- その他

最適化されたデフォルト設定
ファイル形式に基づいて、感染の可能性があるオブジェクトのみがスキャンされます。

除外設定
スキャン上限の設定





kaspersky

高度なセキュリティ機能

ヒューリスティック分析とは何か

既知の脅威を対象とする現在の定義データベースでは検知出来ない未知の脅威を検知する技術。

静的・動的解析

静的解析は、マルウェアに特徴的な疑わしいコードをスキャンし解析する
ヒューリスティックアナライザーは疑わしい痕跡が見つかる度にカウンターを増加させる。
動的解析は、特殊な仮想環境で対象のプログラムを実行し、疑わしい行為を発見したら、
マルウェアと識別しブロックする。

Kaspersky Security Networkによる高度なセキュリティ

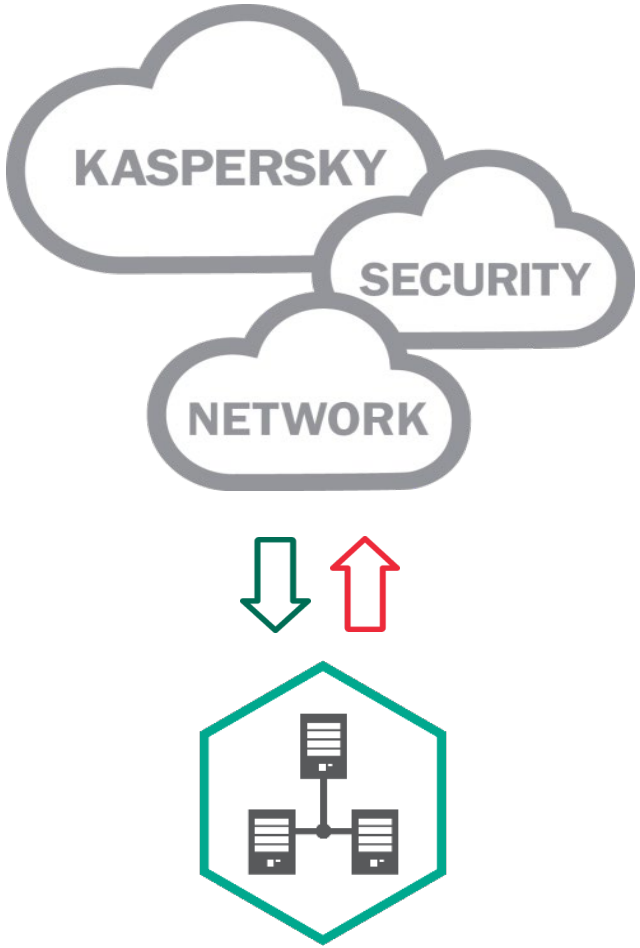
KSNとは何か

最も高度であるグローバルな
クラウドベースセキュリティネットワーク

動的なカテゴライズとレピュテーション

リアルタイム保護を可能にする

カスペルスキーエンタープライズ製品との
完全な統合



kaspersky

参考資料
NASとの連携設定

kaspersky

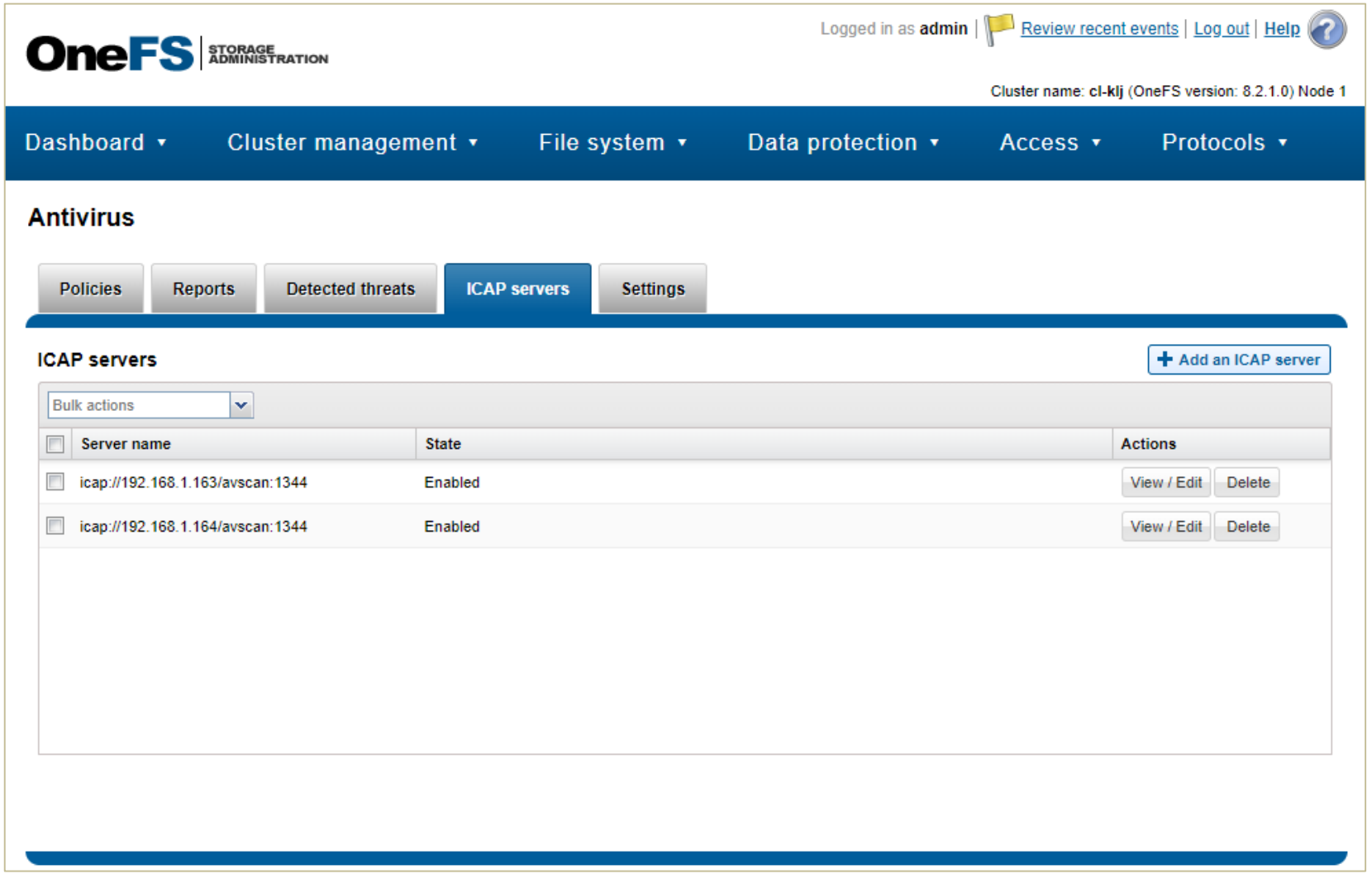
Isilon OneFS
ICAP連携　設定画面

Isilon OneFS ICAP連携のメリット

- リアルタイムスキャンとオンデマンドスキャン
  - スキャン領域ごとのオンデマンドスキャンスケジュール設定
- KSN との統合・ヒューリスティック分析
- ローカルコンソールまたはKSCによる集中管理
  - レポート、アラート、syslog、SIEM連携
- 拡張性と冗長性
- Isilon上へのマルウェア・疑わしいファイルの隔離

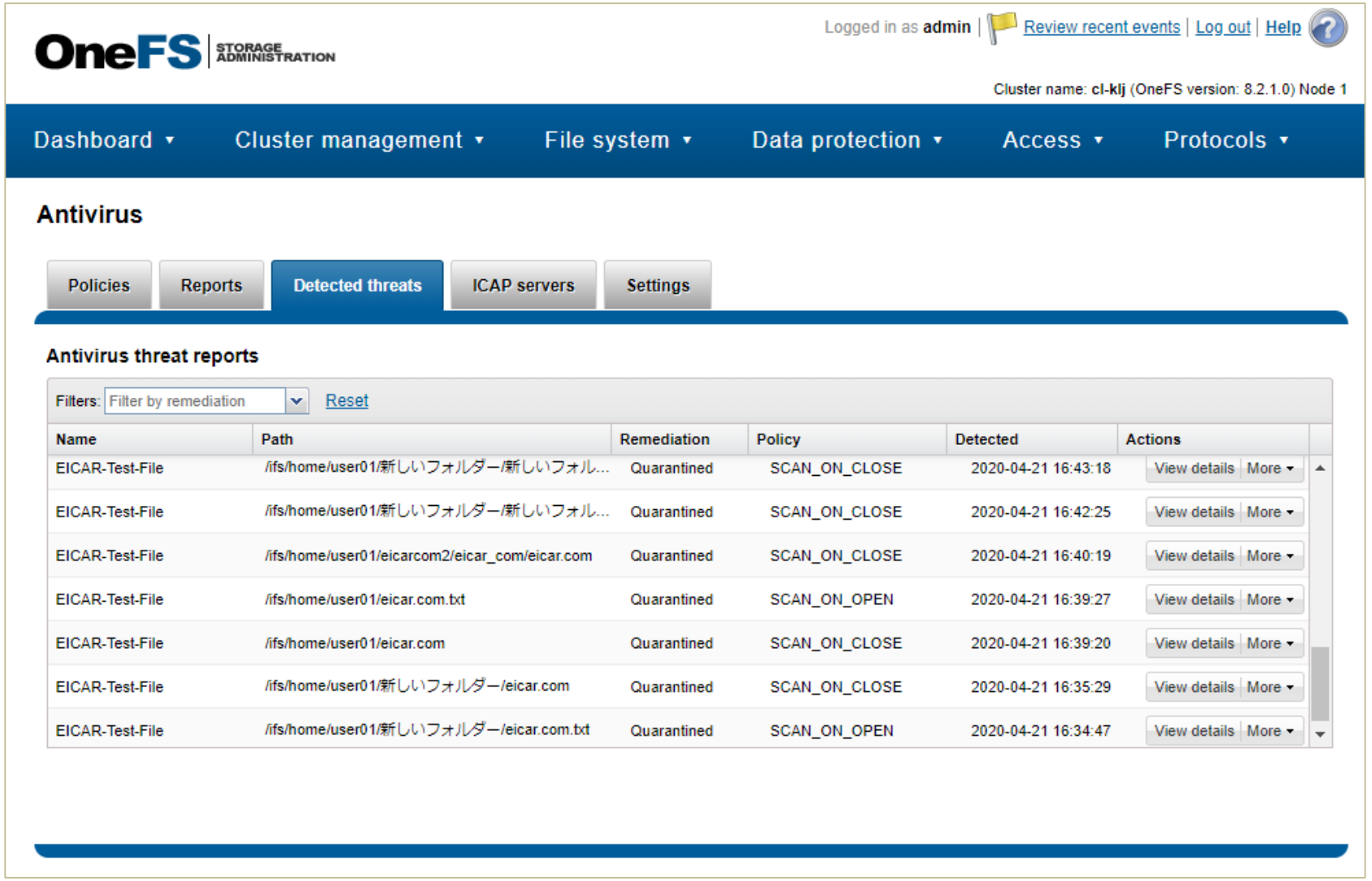
kaspersky

OneFS ICAP設定
2台のKaspersky Security for Storageを設定



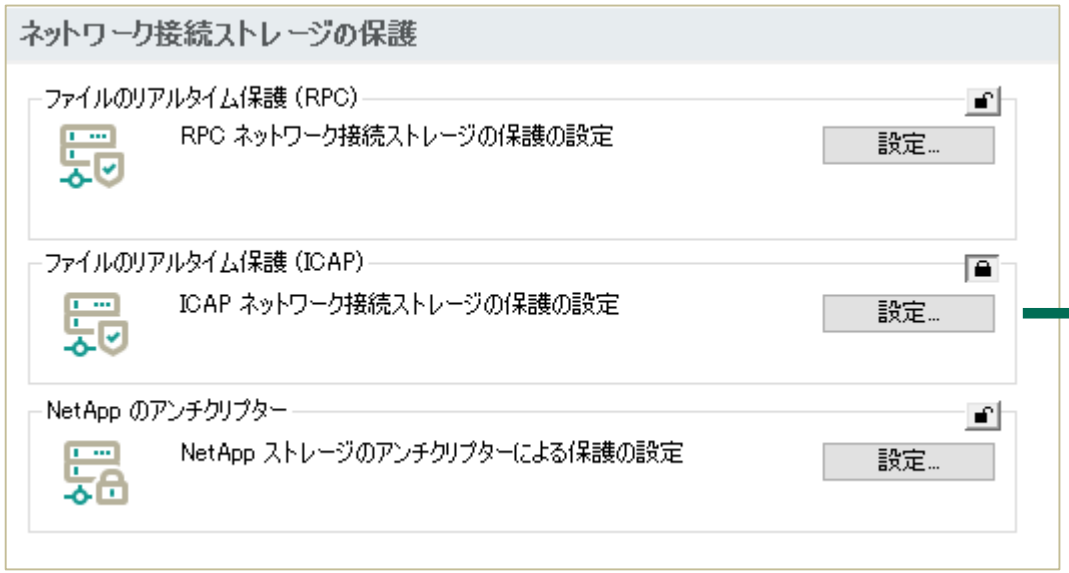
kaspersky

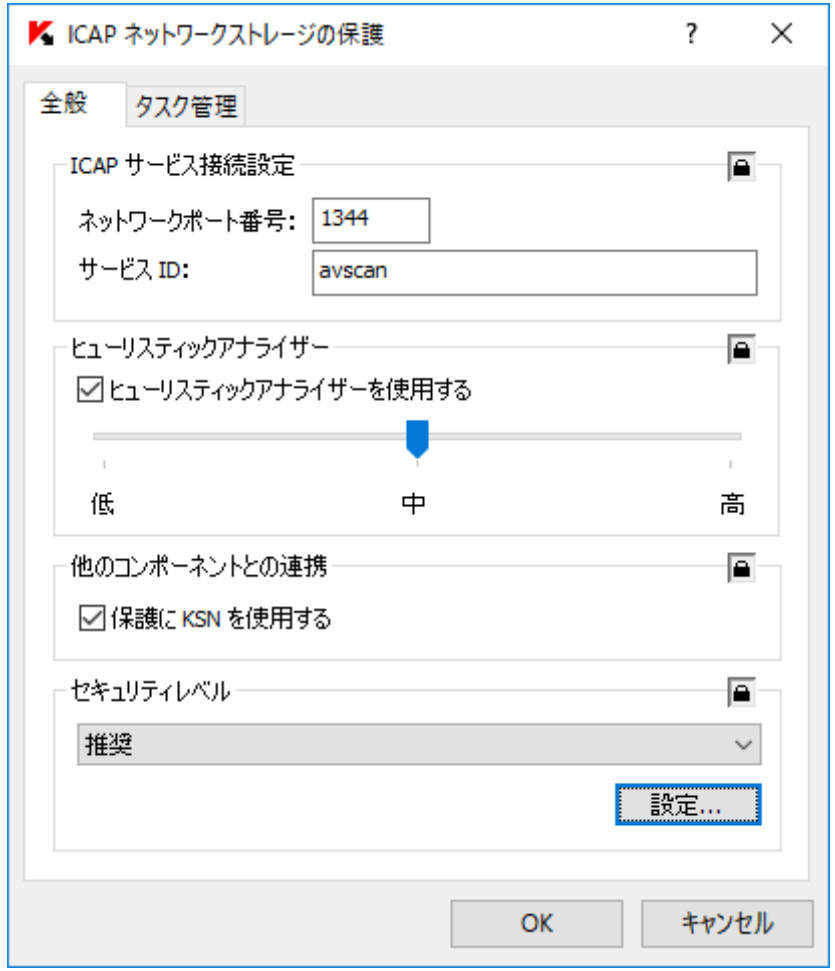
OneFS ICAP設定
オンアクセス時スキャンによる検知



kaspersky

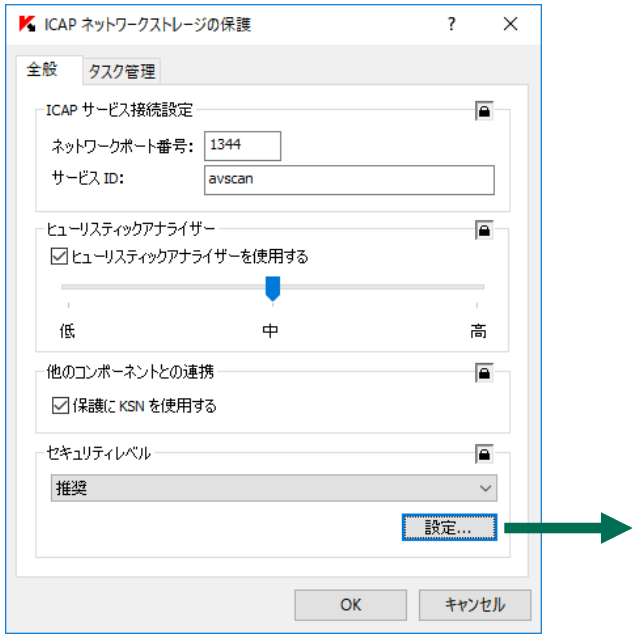
Kaspersky Security for Storage
ICAP設定

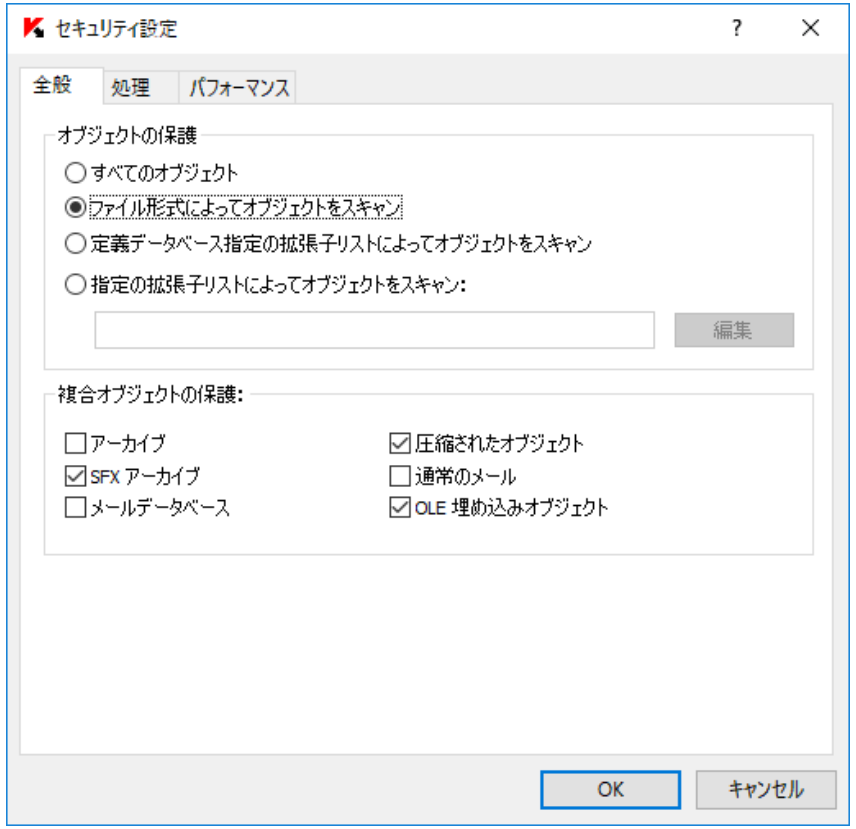


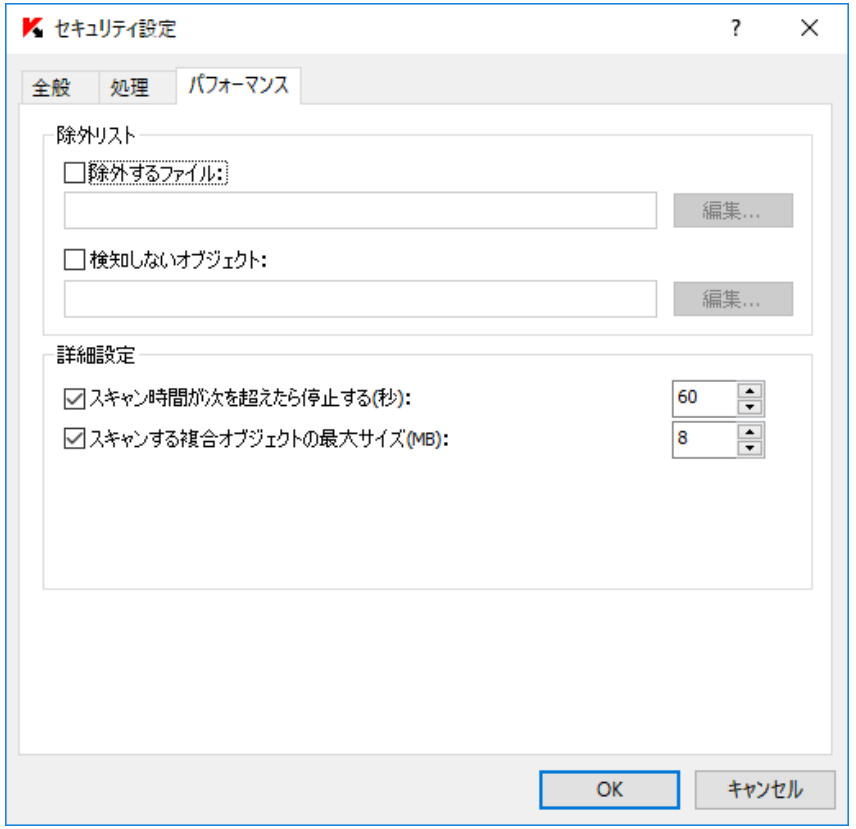


kaspersky

Kaspersky Security for Storage
ICAP設定　詳細

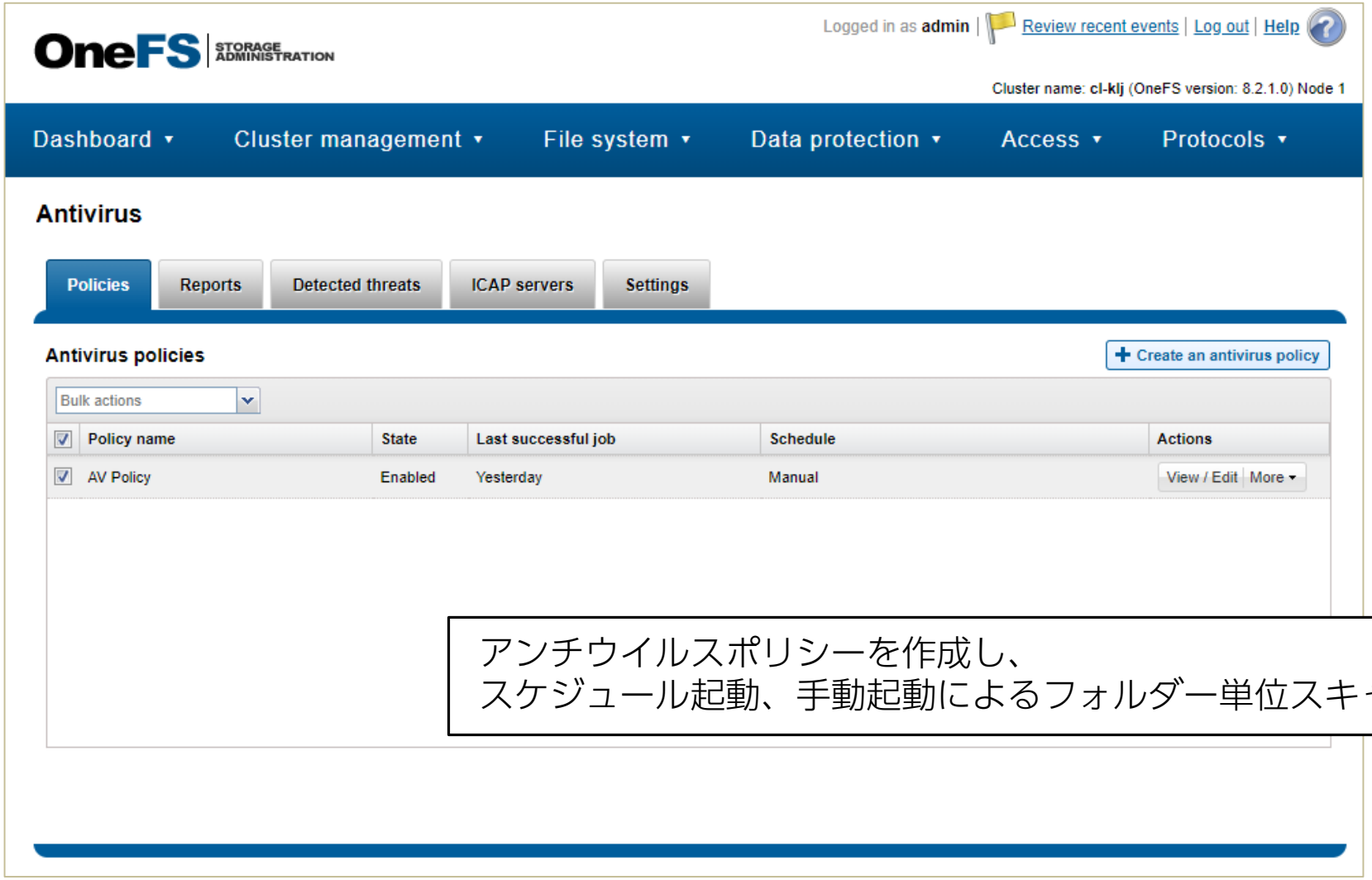






kaspersky

OneFS ICAP設定
スケジュールスキャン設定（オンデマンドスキャン）

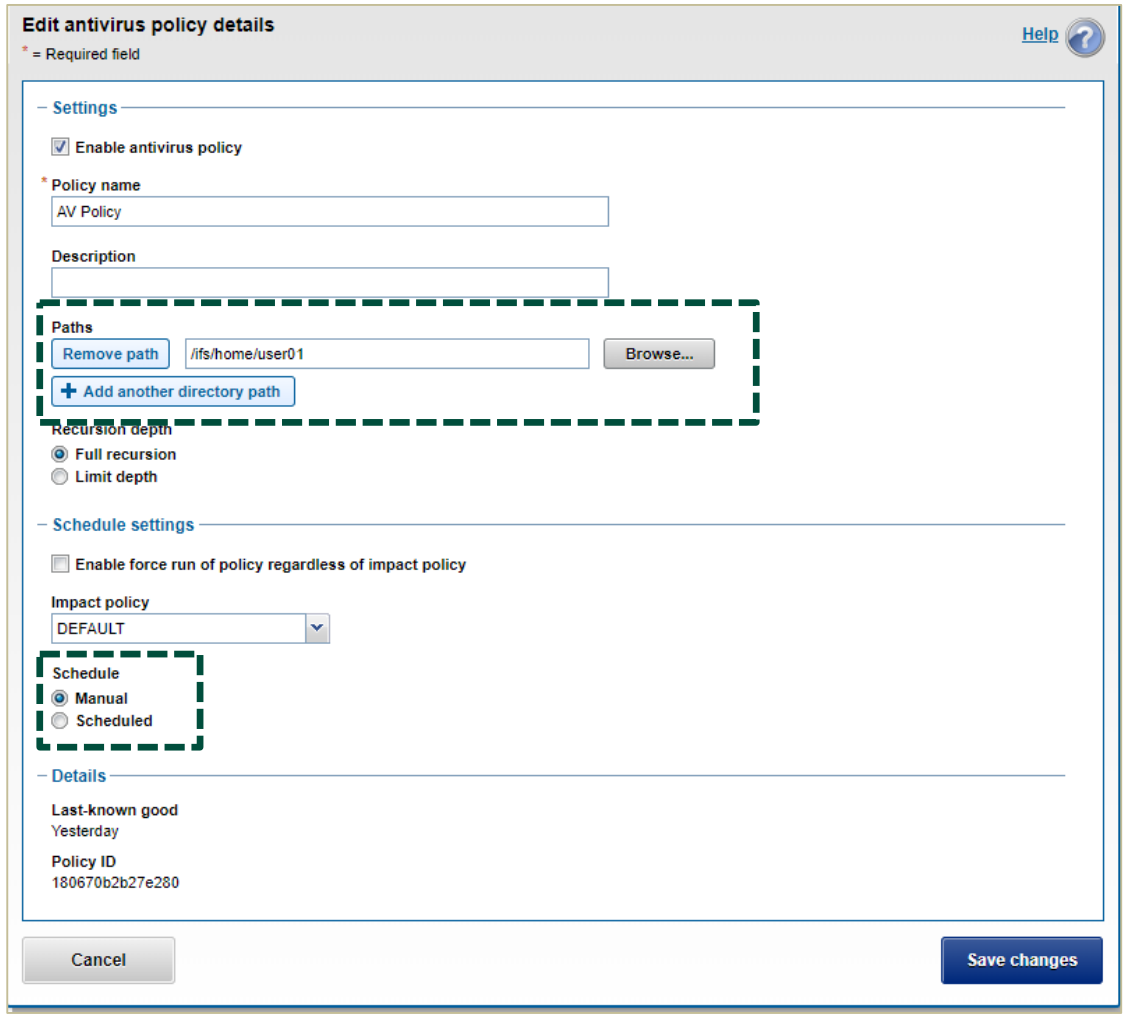


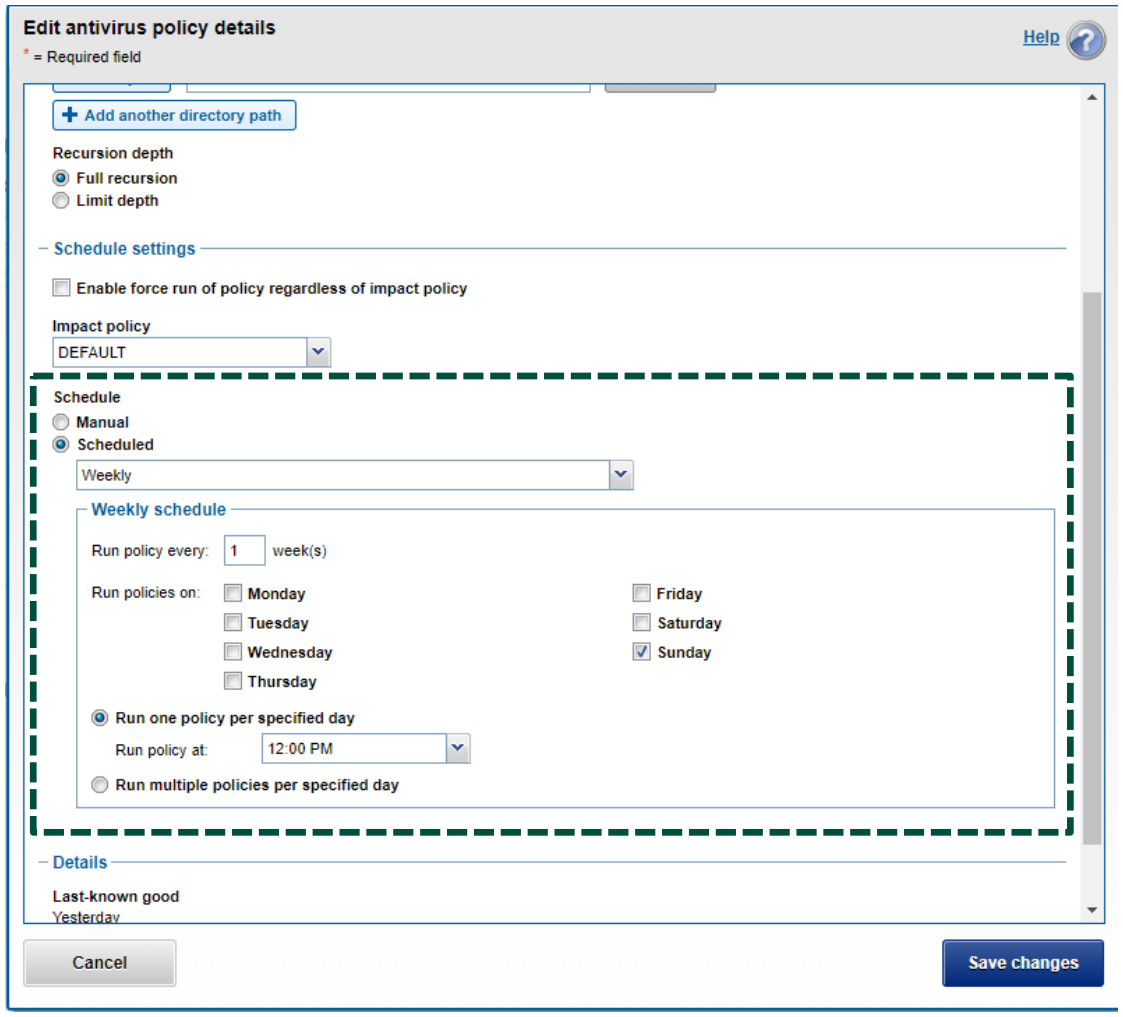
アンチウイルスポリシーを作成し、
スケジュール起動、手動起動によるフォルダー単位スキャンを可能とする

kaspersky

OneFS ICAP設定
スケジュールスキャン設定

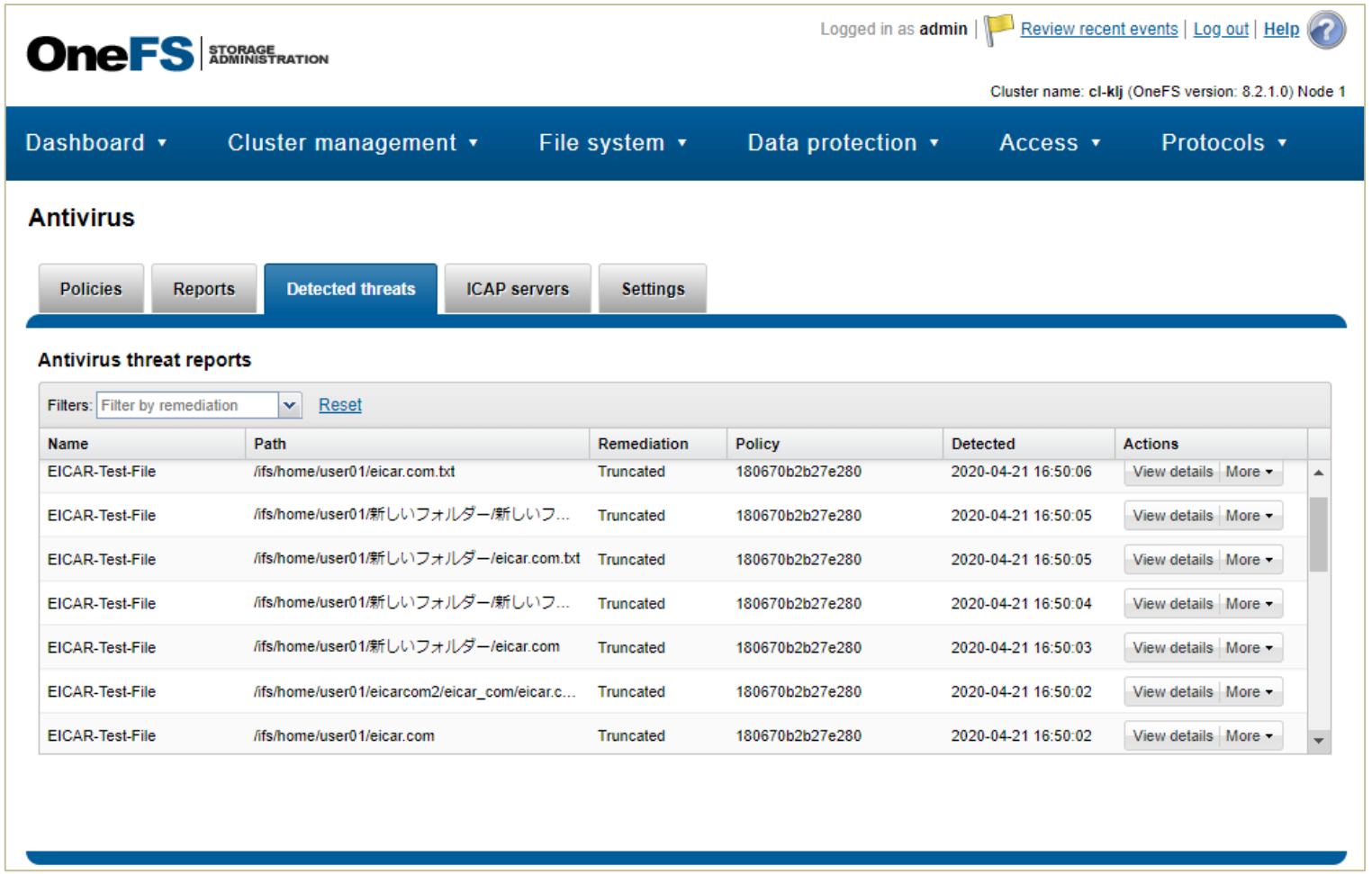
アンチウイルスポリシー設定
パスやスケジュールの指定





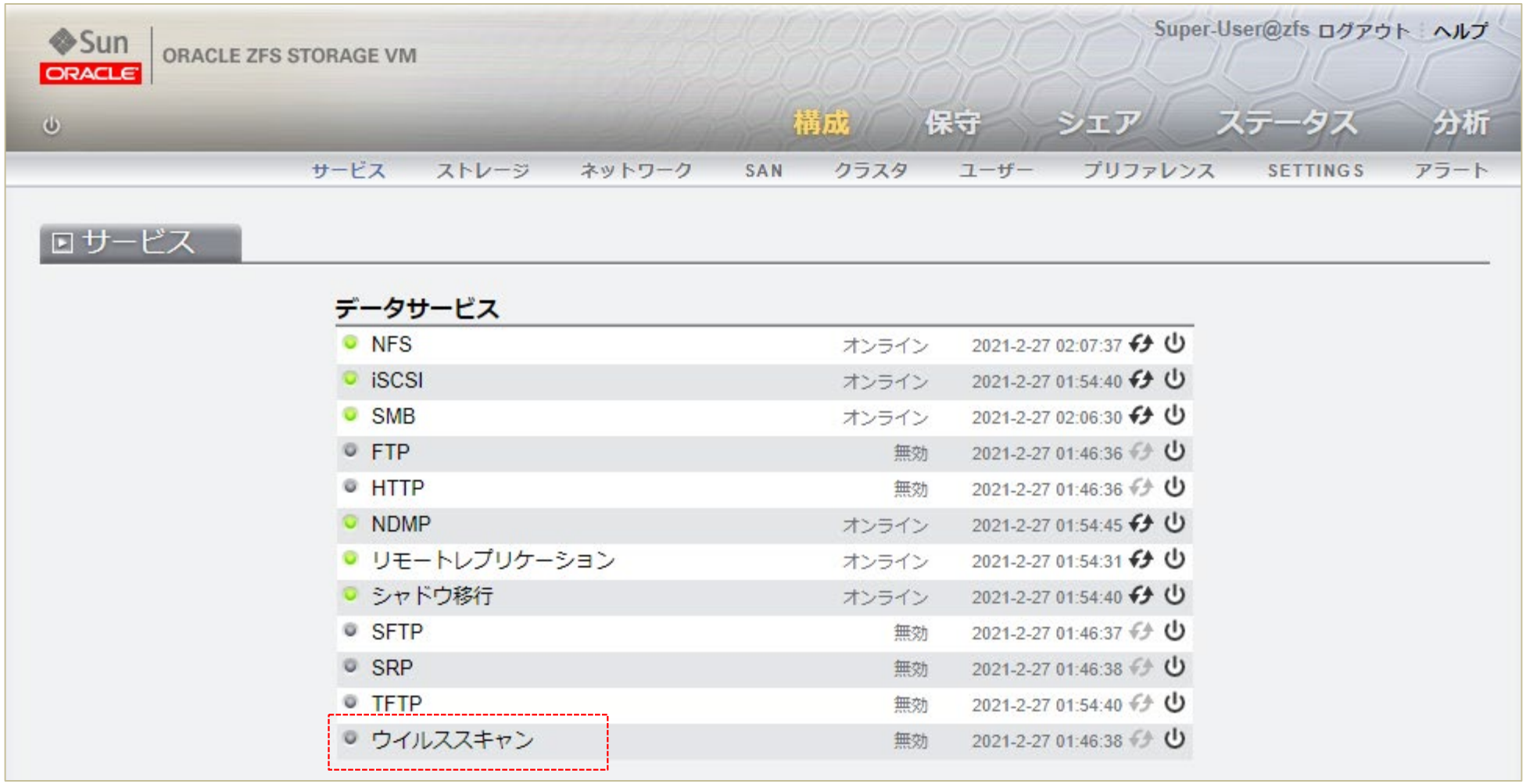
kaspersky

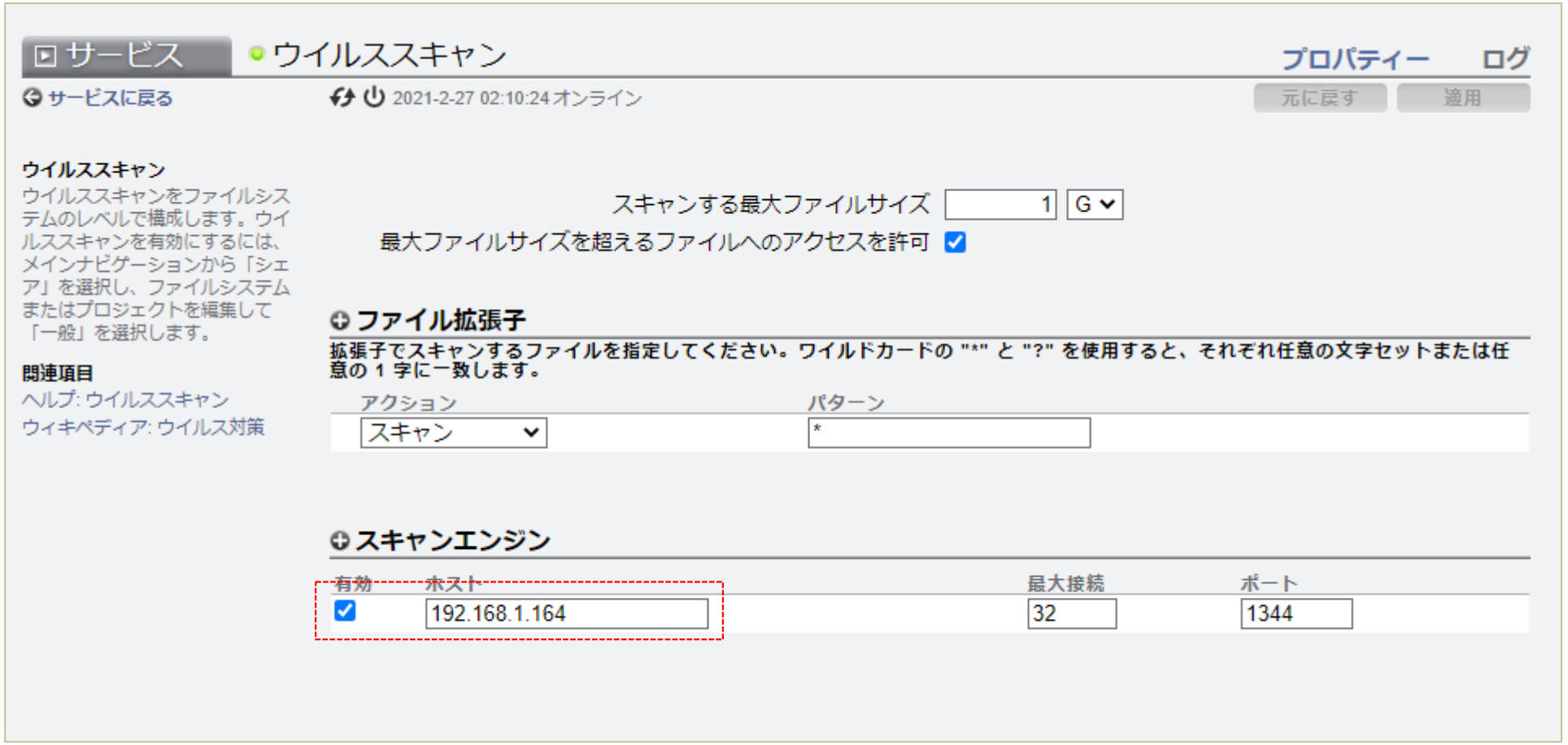
OneFS ICAP設定
スケジュールスキャンポリシー実行（run)でのスキャンによる検知



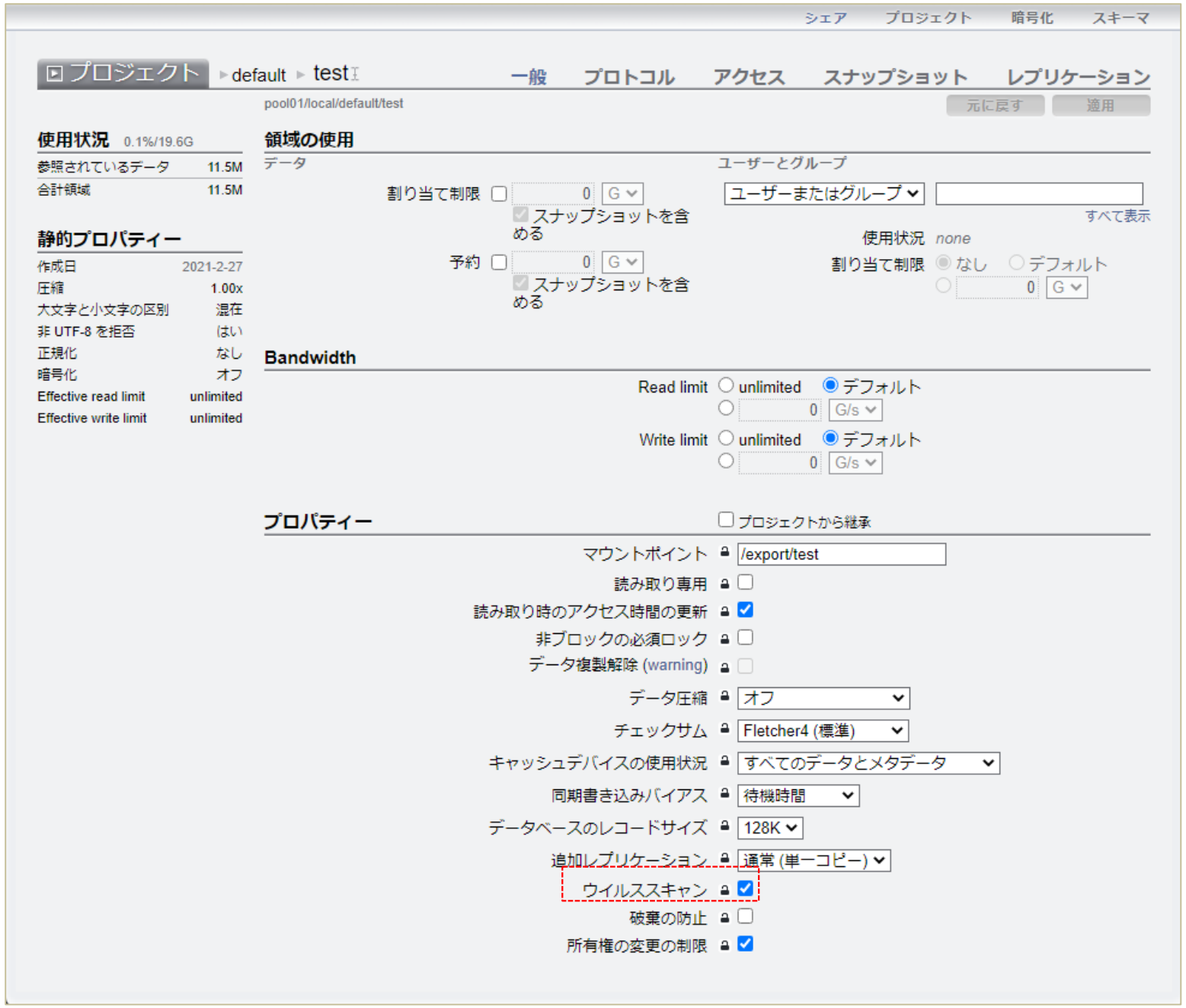
kaspersky

Oracle ZFS
ICAP連携　設定画面

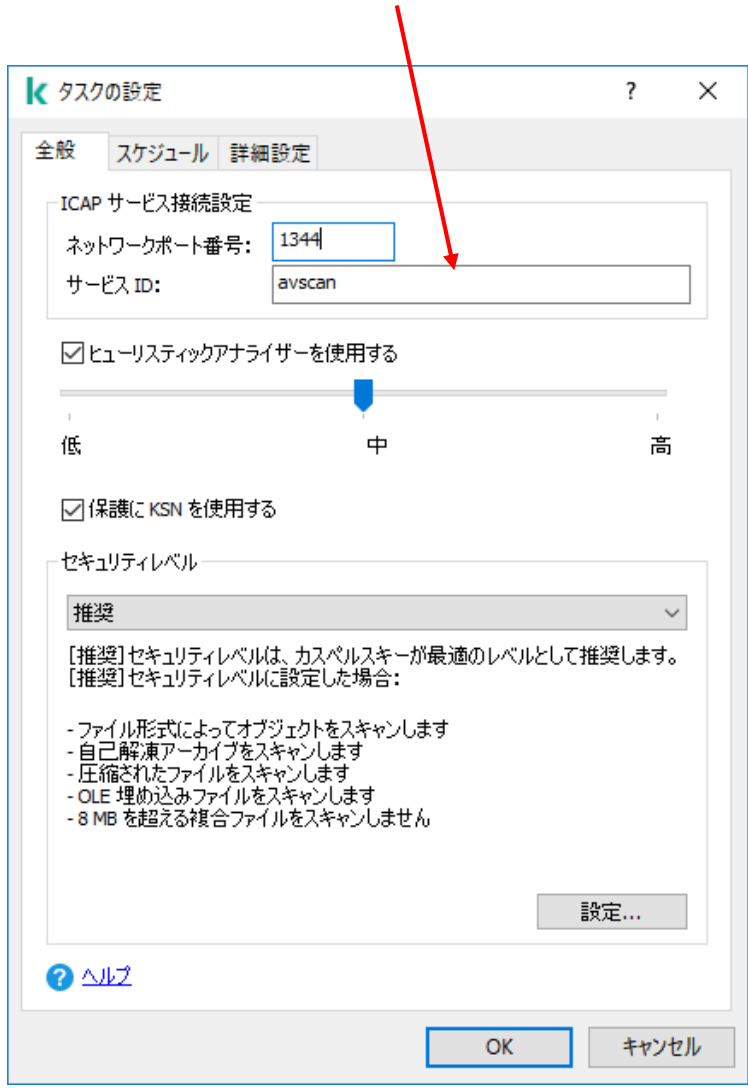

Sun
ORACLE
ORACLE ZFS STORAGE VM
Super-User@zfs ログアウト ヘルプ
構成 保守 シェア ステータス 分析
サービス ストレージ ネットワーク SAN クラスタ ユーザー プリファレンス SETTINGS アラート
サービス
データサービス
NFS オンライン 2021-2-27 02:07:37
iSCSI オンライン 2021-2-27 01:54:40
SMB オンライン 2021-2-27 02:06:30
FTP 無効 2021-2-27 01:46:36
HTTP 無効 2021-2-27 01:46:36
NDMP オンライン 2021-2-27 01:54:45
リモートレプリケーション オンライン 2021-2-27 01:54:31
シャドウ移行 オンライン 2021-2-27 01:54:40
SFTP 無効 2021-2-27 01:46:37
SRP 無効 2021-2-27 01:46:38
TFTP 無効 2021-2-27 01:54:40
ウイルススキャン 無効 2021-2-27 01:46:38

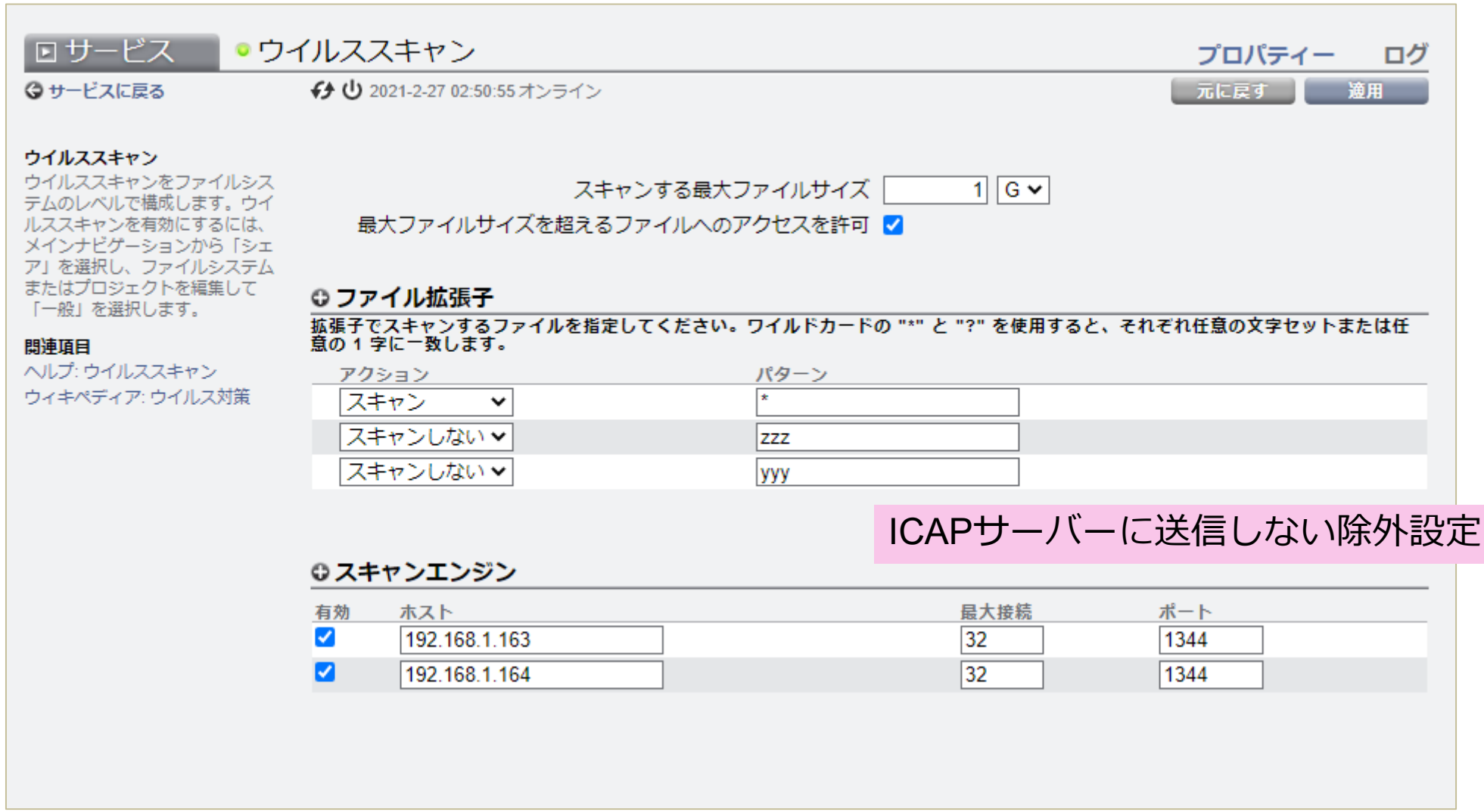


ICAPの指定やサービスIDの指定は無し。

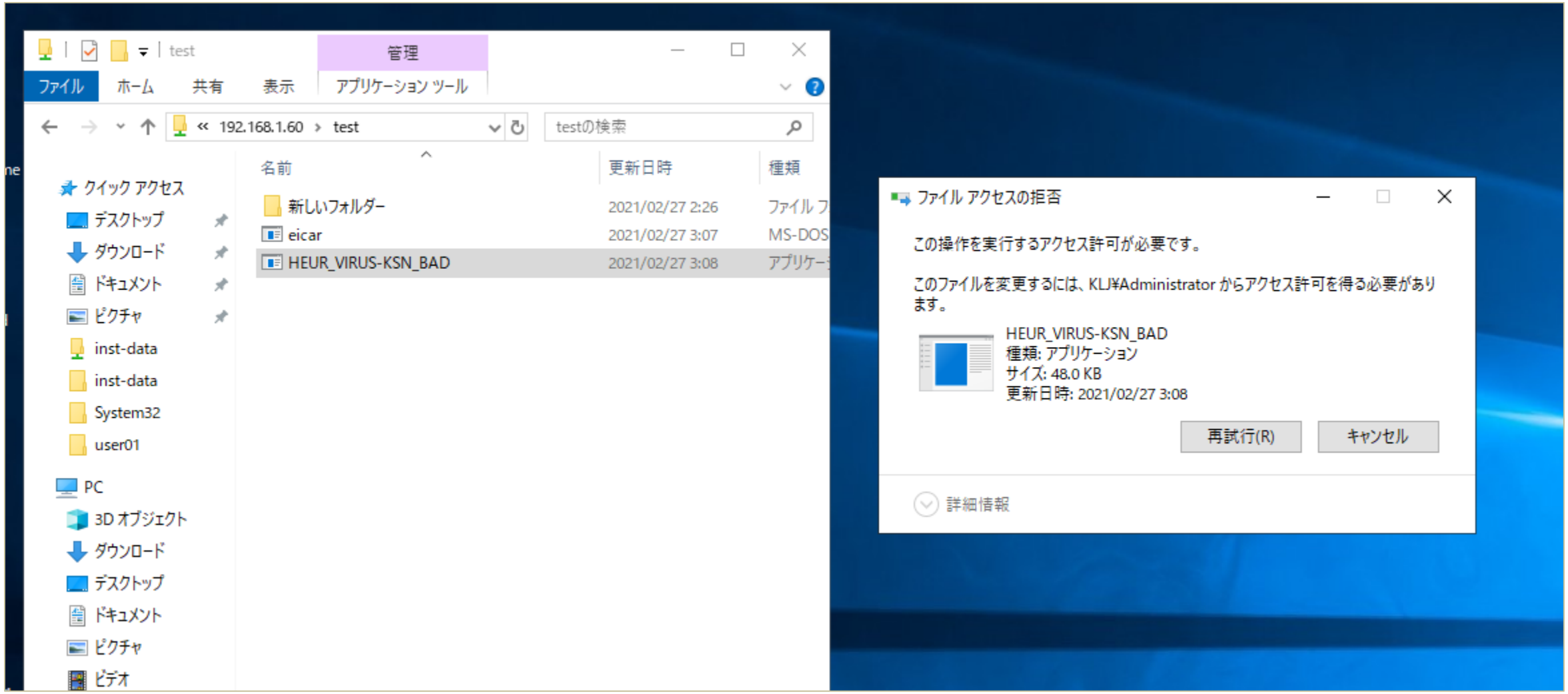

シェア
プロジェクト
暗号化
スキーマ
プロジェクト
default
test
一般
プロトコル
アクセス
スナップショット
レプリケーション
pool01/local/default/test
元に戻す
適用
使用状況 0.1%/19.6G
参照されているデータ 11.5M
合計領域 11.5M
静的プロパティー
作成日 2021-2-27
圧縮 1.00x
大文字と小文字の区別 混在
非 UTF-8 を拒否 はい
正規化 なし
暗号化 オフ
Effective read limit unlimited
Effective write limit unlimited
領域の使用
データ
割り当て制限
スナップショットを含める
予約
スナップショットを含める
ユーザーとグループ
ユーザーまたはグループ
すべて表示
使用状況 none
割り当て制限 なし デフォルト
Bandwidth
Read limit unlimited デフォルト
Write limit unlimited デフォルト
プロパティー
プロジェクトから継承
マウントポイント /export/test
読み取り専用
読み取り時のアクセス時間の更新
非ブロックの必須ロック
データ複製解除 (warning)
データ圧縮 オフ
チェックサム Fletcher4 (標準)
キャッシュデバイスの使用状況 すべてのデータとメタデータ
同期書き込みバイアス 待機時間
データベースのレコードサイズ 128K
追加レプリケーション 通常 (単一コピー)
ウイルススキャン
破棄の防止
所有権の変更の制限

サービスIDは空欄にしなくてもOK。




サービス
ウイルススキャン
プロパティー
ログ
サービスに戻る
2021-2-27 02:50:55 オンライン
元に戻す
適用
ウイルススキャン
ウイルススキャンをファイルシステムのレベルで構成します。ウイルススキャンを有効にするには、メインナビゲーションから「シェア」を選択し、ファイルシステムまたはプロジェクトを編集して「一般」を選択します。
関連項目
ヘルプ: ウイルススキャン
ウィキペディア: ウイルス対策
スキャンする最大ファイルサイズ
1
G
最大ファイルサイズを超えるファイルへのアクセスを許可
ファイル拡張子
拡張子でスキャンするファイルを指定してください。ワイルドカードの "*" と "?" を使用すると、それぞれ任意の文字セットまたは任意の 1 字に一致します。
アクション
パターン
スキャン
*
スキャンしない
zzz
スキャンしない
yyy
ICAPサーバーに送信しない除外設定。
スキャンエンジン
有効
ホスト
最大接続
ポート
192.168.1.163
32
1344
192.168.1.164
32
1344

検知後、ファイルはCIFS上に表示されるが、
ロックされコピーや実行は出来ない。



NetApp

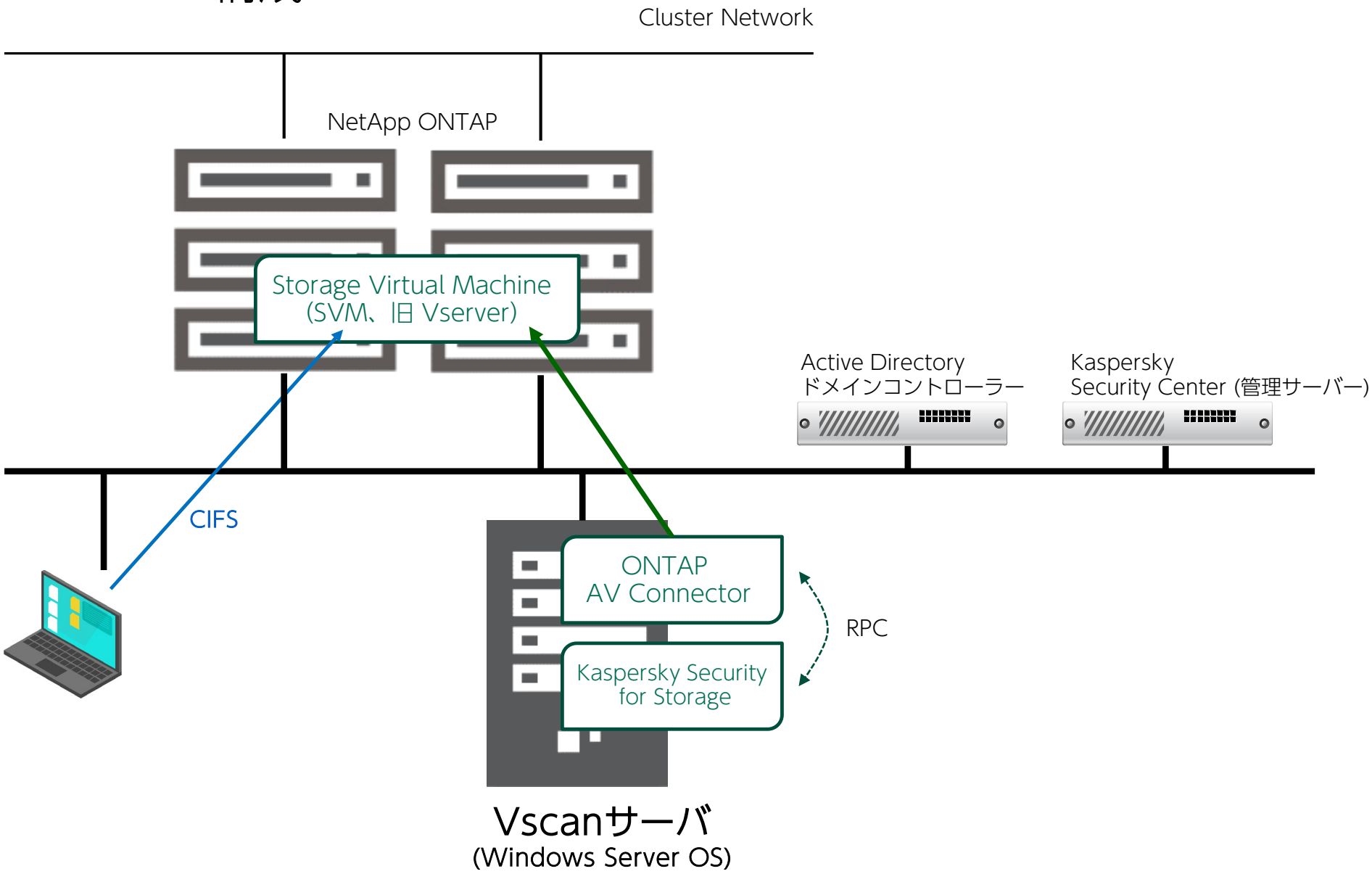
NetAppへ実装可能なセキュリティ

- リアルタイムスキャン（CIFS）
- オンデマンドスキャン（CIFS）
- アンチクリプター（CIFS、 対ランサムウェア）

  NetApp fpolicyとKaspersky Security for Storage アンチクリプタータスクを使用

kaspersky

NetApp Data ONTAP 構成



kaspersky

NetAppにおけるオンデマンドスキャン

ONTAPにて、オンデマンドスキャンタスクを作成

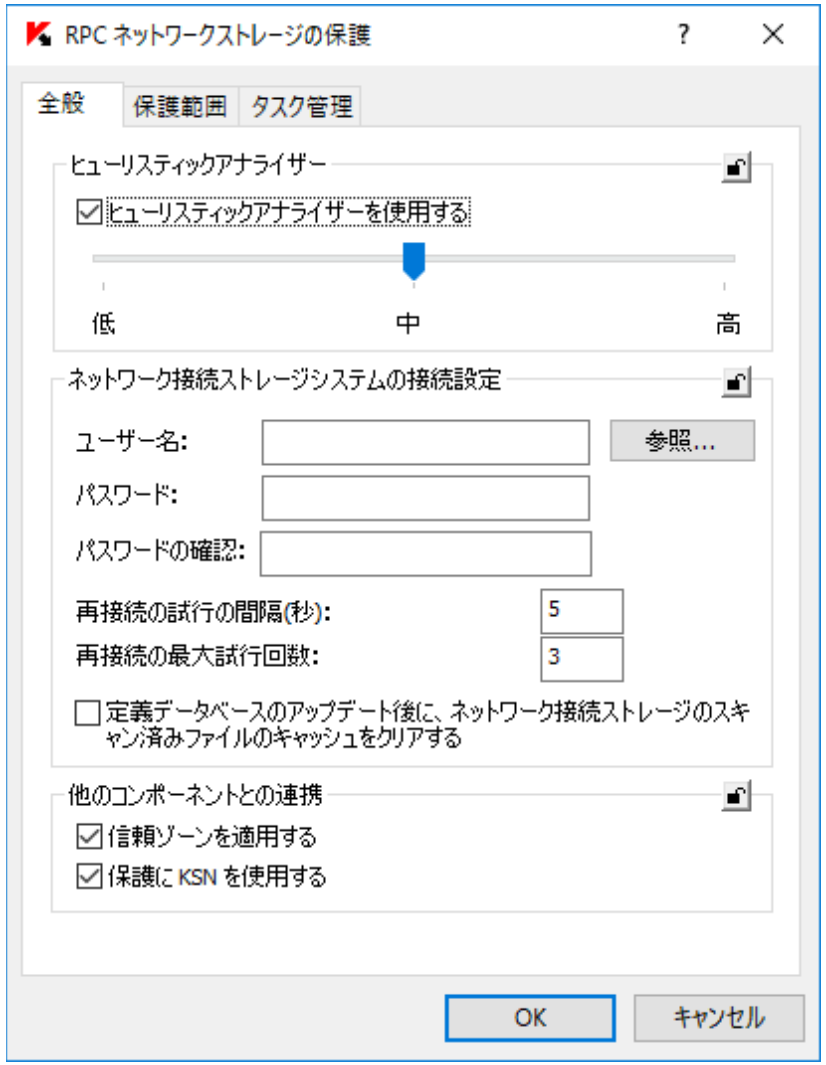
オンデマンド タスクはオンデマンド スキャンの範囲を定義
スキャンするファイルの最大サイズ、
スキャン対象に含めるファイルの拡張子とパス、
スキャン対象から除外するファイルの拡張子とパス

デフォルトでは、サブディレクトリ内のファイルもスキャンされる

vserver vscan on-demand-task runコマンドで、即時実行も可能

Kaspersky Security for Storage

RPC用設定詳細



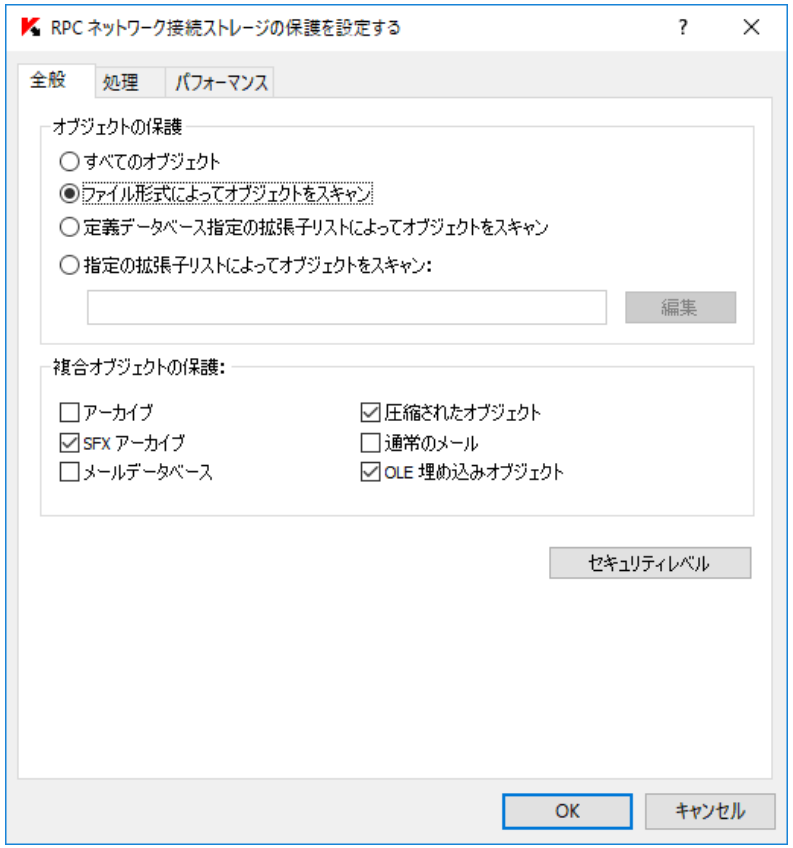
AV Connectorの場合、127.0.0.1

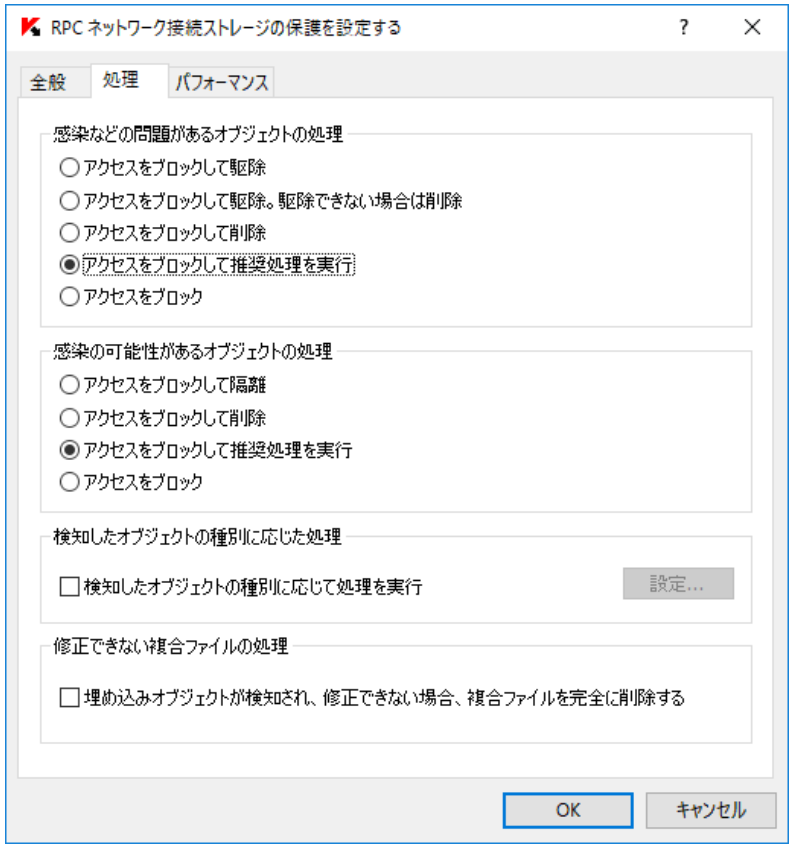
次ページ

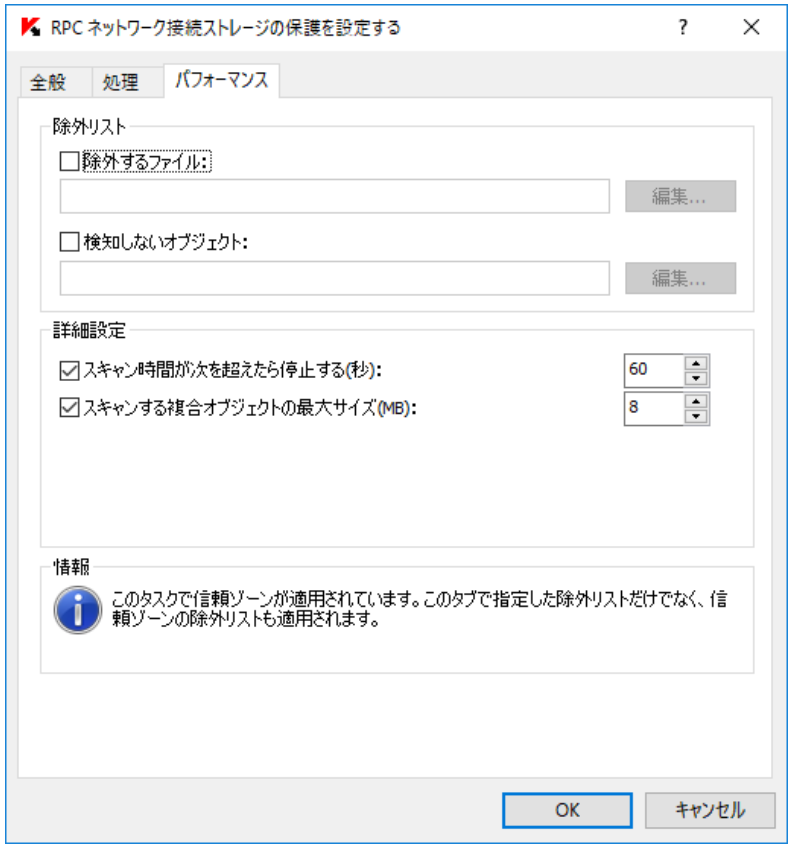
kaspersky

Kaspersky Security for Storage

RPC用設定詳細



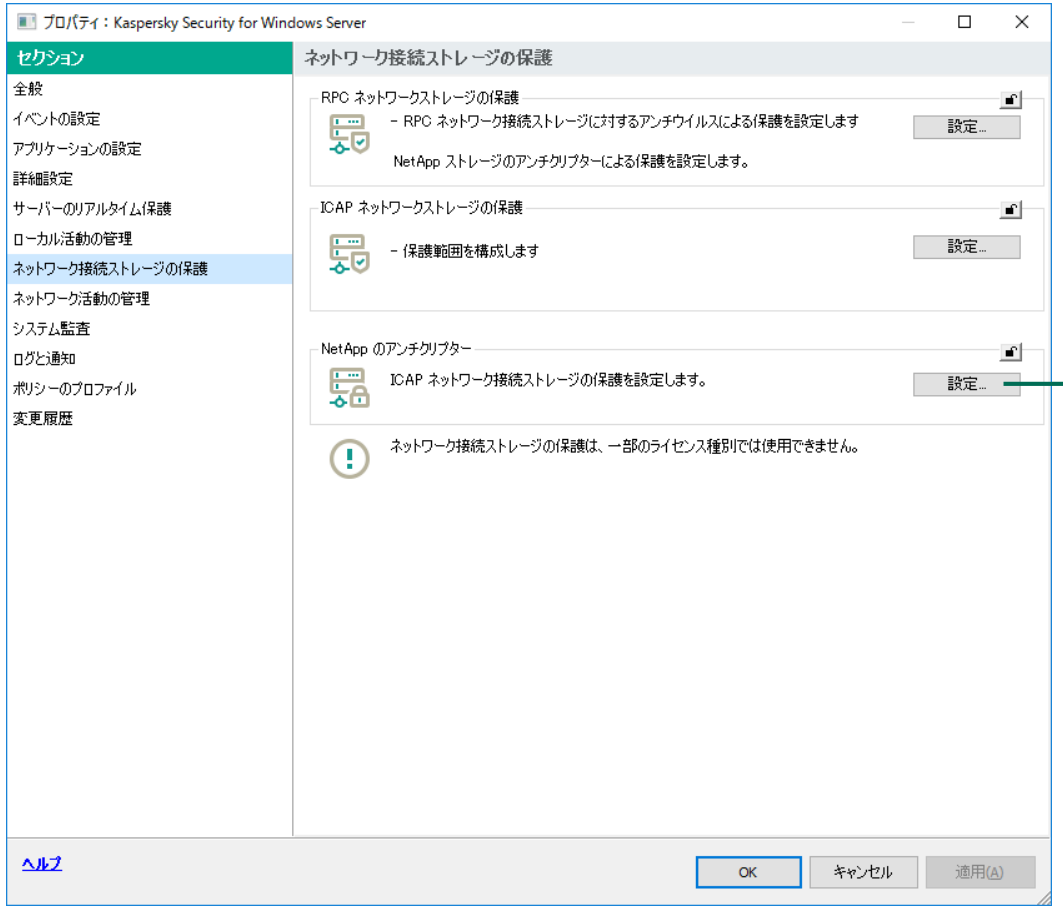


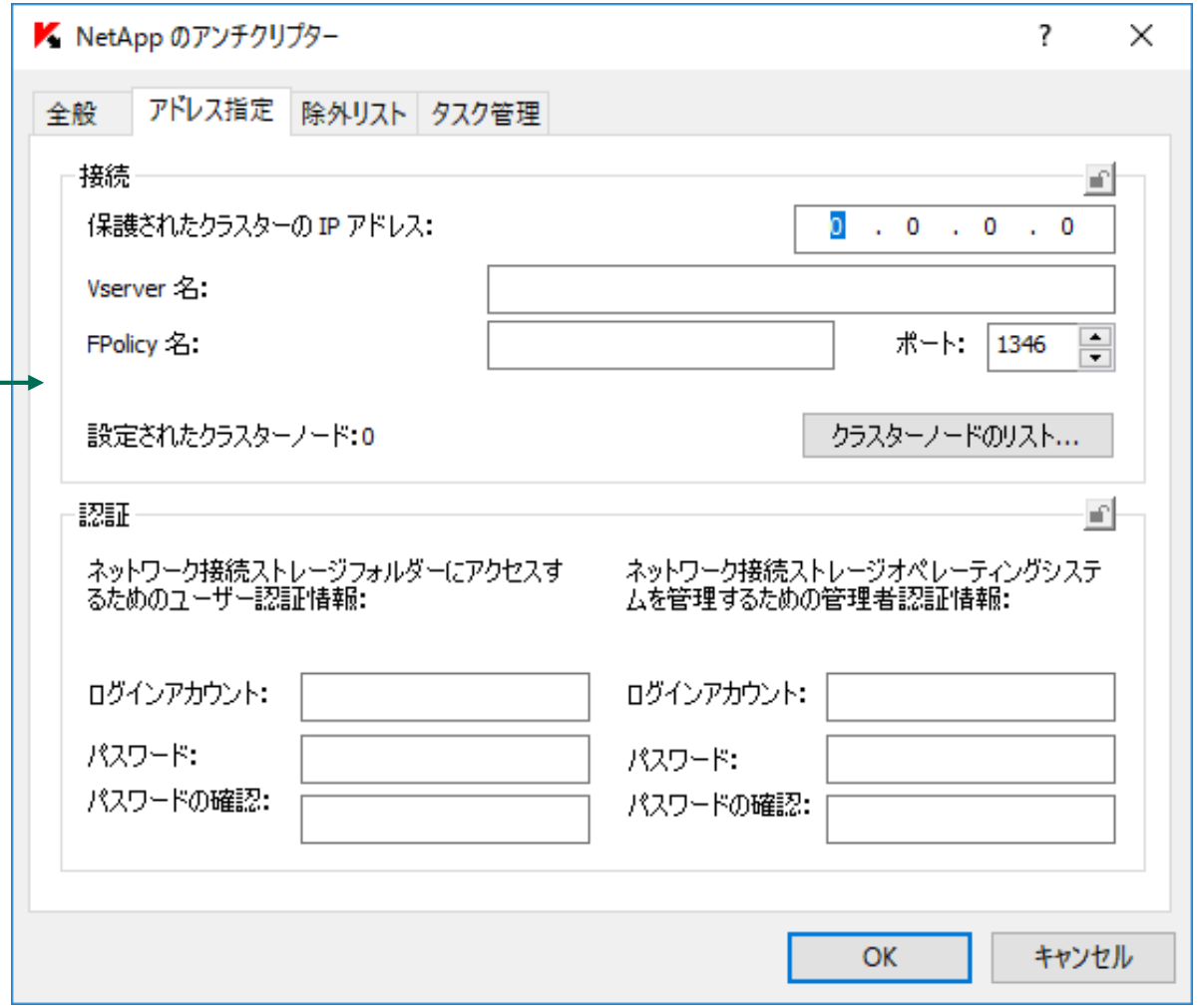


kaspersky

Kaspersky Security for Storage

NetApp アンチクリプター 設定詳細

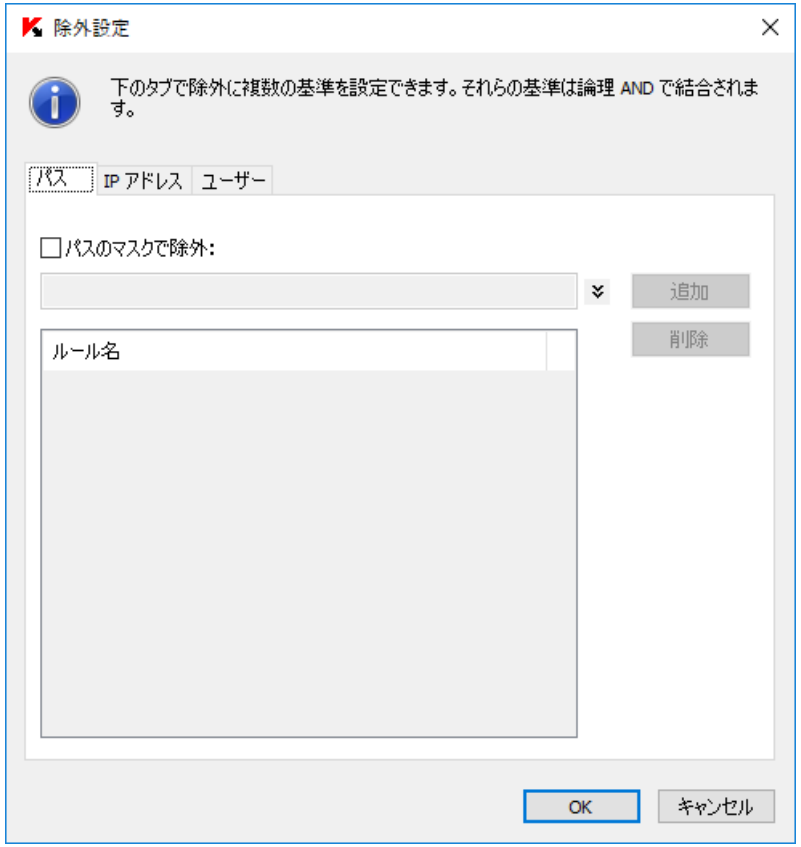


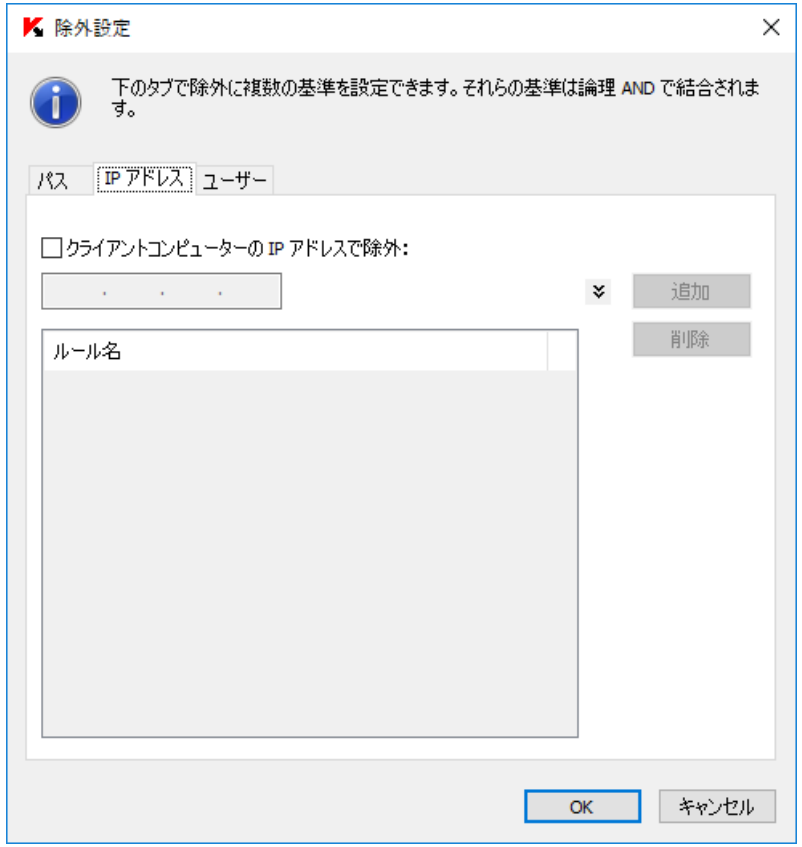


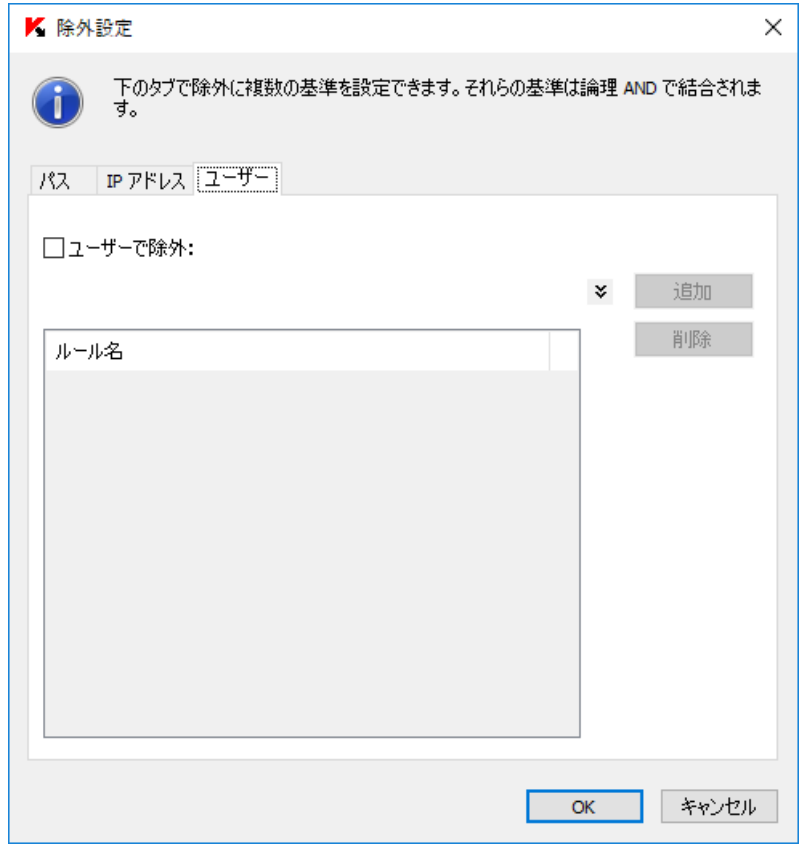
kaspersky

Kaspersky Security for Storage

NetApp アンチクリプター 設定詳細







kaspersky